# Real Life Scenarios of Cyberthreats at Sea Report Confidential

| | |
|---|---|
| ***Project Acronym:*** | CyberSEA |
| ***Full Title:*** | CyberSEA - Increasing Cyber Security at SEA through digital training |
| ***Project no.:*** | 2023-1-ES01-KA220-VET-000159793 |
| ***File Ref:*** | WP2-Real Life Scenarios |
| ***Version:*** | 1.0 |
| ***Status:*** | Final |
| ***Start date of the project:*** | 01.09.2023 ***Duration:*** 36 months |
| ***Dissemination level:*** | RE Restricted to a group specified by the consortium (including the national agency services) |
| ***Funding body:*** | Co-funded by the European Union |
| ***Partners' logo:*** | |

The CyberSEA - Increasing Cyber Security at SEA through digital training project is co-funded by the European Union. The opinions and points of view expressed (in this press release/publication/etc.) commit only the author(s) and not necessarily those of the European Union or of the Spanish Service for the Internationalisation of Education (SEPIE). Neither the European Union or the SEPIE National Agency can be considered responsible for them.
**Project Number:** 2023-1-ES01-KA220-VET-000159793

## List of CyberSEA Beneficiaries

| No. | Participant Organisation Name | Participant Short Name | Country |
|---|---|---|---|
| 1 | UNIVERSITAT POLITECNICA DE CATALUNYA | UPC | ES |
| 2 | AINTEK SYMVOULOI EPICHEIRISEON EFARMOGES YPSILIS TECHNOLOGIAS EKPAIDEFSI ANONYMI ETAIREIA | IDEC | GR |
| 3 | SPINAKER, navticno izobrazevanje in trgovina, d.o.o. | SPINAKER | SI |
| 4 | Academia Navala "Mircea cel Batran" | RNA | RO |
| 5 | Berlin School of Business and Innovation GmbH | BSBI | DE |
| 6 | Centre for Factories of the Future | C4FF | SE |
| 7 | POLITECHNIKA MORSKA W SZCZECINIE PM | MUS | PL |
| 8 | ELLINIKO MESOGEIAKO PANEPISTIMIO | HMU | GR |
| 9 | SATAKUNNAN AMMATTIKORKEAKOULU OY | SAMK | FI |

## List of Output Contributors

| No. | Participant Organisation Name | Participant Short Name | Country |
|---|---|---|---|
| 1 | UNIVERSITAT POLITECNICA DE CATALUNYA | UPC | ES |
| 2 | AINTEK SYMVOULOI EPICHEIRISEON EFARMOGES YPSILIS TECHNOLOGIAS EKPAIDEFSI ANONYMI ETAIREIA | IDEC | GR |
| 3 | SPINAKER, navticno izobrazevanje in trgovina, d.o.o. | SPINAKER | SI |
| 4 | Academia Navala "Mircea cel Batran" | RNA | RO |
| 5 | Berlin School of Business and Innovation GmbH | BSBI | DE |
| 6 | Centre for Factories of the Future | C4FF | SE |
| 7 | POLITECHNIKA MORSKA W SZCZECINIE PM | MUS | PL |
| 8 | ELLINIKO MESOGEIAKO PANEPISTIMIO | HMU | GR |
| 9 | SATAKUNNAN AMMATTIKORKEAKOULU OY | SAMK | FI |

# Contents

# 1 Introduction

## 1.1 Document Purpose

This document presents the findings and achievements of Work Package 2 (Task 4) within the CyberSEA project. WP2 focuses on developing practical training resources for cadets and seafarers, enhancing their awareness of cyber threats, and improving their ability to respond effectively. The report outlines key cybersecurity challenges within the maritime industry, supported by real-life cyber incidents affecting critical onboard and shore-based systems.

The purpose of this document is to provide stakeholders with a structured overview of major cyber threats in maritime operations. It highlights the consequences of cyber incidents, methods for identifying threats, best practices for mitigation, and possible solutions. Additionally, the document incorporates cross-industry cybersecurity knowledge to enhance the resilience of maritime systems against cyberattacks.

## 1.2 Approach Applied

To achieve the objectives of Work Package 2 (WP2) within the CyberSEA project, a comprehensive and multi-faceted approach was applied, focusing on the analysis of maritime cyber threats, identifying best practices, and developing practical training resources for seafarers and cadets. This approach included several key elements.

The first element was the analysis of real-life cyber incidents. Documented cyber incidents in ten areas of marine systems were examined to assess the impact of cyber threats, identify vulnerabilities, and propose practical mitigation strategies. These incidents covered areas such as navigation systems, cargo management, propulsion control, and communication networks. Based on the analysis of real incidents, scenario-based training resources were created to help seafarers recognize cyber threats, implement preventive measures, and respond effectively to attacks. Each cyber incident was categorized according to the type of threat, its consequences, and potential security measures to counteract it.

# 2 Real life Scenarios of Cyberthreats on Sea

## 2.1 Introduction

The maritime industry is increasingly dependent on digital technology and network-based communication systems, making it more vulnerable to cyber threats. Cyberattacks can disrupt essential vessel operations, lead to data breaches, and pose safety risks to crew and cargo. In response to these challenges, the CyberSEA project has focused on analysing real-life incidents and developing practical training materials to enhance cybersecurity awareness and preparedness among seafarers.

As part of WP2, ten real-life cyber incidents in the maritime sector were analysed. Each scenario includes a description of the incident, providing detailed information about the cyberattack and its impact. It also identifies the key cybersecurity risk arising from the incident. The result of a threat outlines the consequences of the attack, including operational disruptions, financial losses, and safety risks. Additionally, each scenario explains how to identify threats and what to pay attention to, highlighting warning signs and techniques for detecting cyber threats. Solutions are provided, recommending cybersecurity measures to mitigate risks and enhance system resilience. Lastly, a source section includes references to relevant research and case studies supporting the analysis.

Each of these scenarios provides valuable insights for seafarers and vessel operators, helping them understand cyber threats and implement effective countermeasures. The following sections of this document provide a detailed analysis of each incident, including methods for detecting cyber threats and recommended solutions to enhance the maritime sector's resilience against cyberattacks.

## 2.2 Scenarios by areas of risk

### 2.2.1 Cargo Management Systems

Cargo Management Systems are an important part of the global supply chain, but their increasing digitization brings cybersecurity threats. In recent years, attacks have caused operational disruptions, data breaches, and financial losses. The incidents described below illustrate various threats, such as system shutdowns, confidential data breaches, unauthorized control over customs systems, and cargo data manipulation in ports. Additionally, the section presents the consequences of these threats (Result of a threat), ways to identify them (How to identify/What to pay attention), possible solutions (Solution), and sources of information (Source).

| **Example 1** | |
|---|---|
| **Description of incident** | In 2017, the global shipping company was hit by the ransomware attack, which caused significant disruption to their operations, including their cargo management systems. |

| | |
|---|---|
| | Possible situation based on the incident:<br>The attack affected computer servers in Europe and India. The encrypted malware has been targeted at all services of the shipping company. As a result, 17 shipping container terminals had been affected and more than USD 200 million was lost. The attack severely destroyed the operating system of the computers by infecting its master boot record (MBR). |
| **Identified threat** | Off use operational systems with possibility of disclosure of confidential data. |
| **Result of a threat** | Data Breaches: Unauthorised access to sensitive information such as cargo contents, shipping schedules, and routes.<br>Ransomware: Malicious software that encrypts data, demanding a ransom for its release.<br>These threats can lead to cargo theft, operational disruptions, and financial losses. It's crucial to implement robust cybersecurity measures to protect against these risks. |
| **How to identify/ What to pay attention to** | Monitor Network Traffic: Regularly check for unusual activity or unauthorised access attempts. Look for spikes in data traffic, especially during off-hours.<br>Use Intrusion Detection Systems (IDS): Implement IDS to detect and alert you to potential threats in real-time.<br>Regular System Audits: Conduct frequent audits of your systems to identify any vulnerabilities or signs of compromise.<br>Analyse Logs: Review system and application logs for any suspicious activities or errors that could indicate an attack.<br>Employee Vigilance: Train employees to recognize signs of phishing attempts, such as unexpected emails or requests for sensitive information.<br>Implement Security Information and Event Management (SIEM): Use SIEM tools to aggregate and analyse data from various sources to detect potential threats.<br>Conduct Penetration Testing: Regularly perform penetration tests to identify and fix security weaknesses before attackers can exploit them. |
| **Solution** | Regular Risk Assessments: Identify vulnerabilities in your system and address them proactively.<br>Data Backups: Maintain regular backups of critical data to ensure you can recover quickly in case of an attack.<br>Strong Authentication: Use multi-factor authentication (MFA) to add an extra layer of security.<br>Firewalls and Antivirus Software: Install and regularly update firewalls and antivirus software to protect against malware and unauthorised access.<br>SSL Certificates: Use SSL certificates to encrypt data transmitted between your systems and users.<br>Employee Training: Educate employees about phishing attacks and other social engineering tactics to prevent them from falling victim to such schemes.<br>Incident Response Plan: Develop and regularly update an incident response plan to quickly address any security breaches.<br>Collaboration with Partners: Work with suppliers, vendors, and partners to ensure they also follow strong cybersecurity practices. |
| **Source** | https://www.mdpi.com/2078-2489/13/1/22 |
| **Example 2** | |

| | |
|---|---|
| **Description of incident** | In 2012, the cargo handling system used by a national customs authority was compromised by cybercriminals. The attackers gained access to the system to monitor whether their shipments were flagged as suspicious. If any smuggled goods were marked for inspection, the attackers would abandon those shipments, thus avoiding interception by authorities.<br>Possible situation based on the incident:<br>Cybercriminals infiltrated the customs' cargo management system, giving them visibility into which shipments were identified as high-risk or flagged for inspection. Upon learning that certain shipments contained contraband and were flagged for further scrutiny, the criminals intentionally abandoned these containers, preventing law enforcement from apprehending the smuggled goods. |
| **Identified threat** | Compromised customs cargo handling system. |
| **Result of a threat** | Criminals were able to avoid law enforcement by tracking the status of their illegal shipments.<br>Enabled a significant amount of contraband to pass through customs without detection.<br>Undermined the trust in the integrity of the customs and border protection system, posing a serious national security risk.<br>Led to operational inefficiencies, as flagged containers were left abandoned without yielding results from investigations. |
| **How to identify/ What to pay attention to** | Unusual patterns of abandoned containers, particularly those flagged as suspicious.<br>Regularly audit the cargo handling system for unauthorized access or abnormal activity.<br>Monitor system logs for attempts to access high-risk shipment data or areas where security checks are performed.<br>Be aware of any sudden decrease in container pickups following high-risk flags or system alerts. |
| **Solution** | Enhanced access control and monitoring: Implement multi-level security access protocols to restrict sensitive shipment data only to authorized personnel. Use real-time monitoring and alerts for unauthorized access attempts.<br>Encryption and compartmentalization: Ensure that flagged shipment information is encrypted and compartmentalized to prevent access by unauthorized users.<br>Cybersecurity training for customs personnel: Regularly train customs officers and system administrators to recognize potential cyber threats and respond quickly to unusual system behavior.<br>Strengthened auditing systems: Increase the frequency and depth of system audits to detect any unauthorized access or data manipulation attempts, especially concerning high-risk shipments.<br>Collaboration with law enforcement: Develop a secure communication channel between customs and law enforcement agencies to ensure that flagged shipments are closely monitored without tipping off cybercriminals. |
| **Source** | Industry report on maritime cyber risks:<br>https://maritimecyprus.files.wordpress.com/2015/06/maritime-cyber-risks.pdf |

| **Example 3** | |
|---|---|
| **Description of incident** | In 2018, a major European port experienced a cyberattack in which its internal IT systems were infected with ransomware. The attack primarily affected administrative and internal operational systems, but fortunately, it did not disrupt ship traffic or critical port operations. The incident raised concerns about the vulnerability of port infrastructure to ransomware attacks and their potential impact on logistics and cargo handling.<br>Possible situtation based on the incident:<br>Ransomware infiltrated the port's IT network, encrypting critical files and rendering several internal systems inoperable.<br>Although the port's ship traffic management was unaffected, administrative tasks, cargo tracking, and communication systems were disrupted. This resulted in delays in processing cargo and disrupted internal coordination. |
| **Identified threat** | Unavailability of internal IT systems due to a ransomware attack. |
| **Result of a threat** | Significant disruptions to internal administrative and operational functions.<br>Potential delays in cargo handling, customs clearances, and scheduling.<br>Possible financial losses due to downtime and the cost of restoring affected systems.<br>Increased vulnerability to future attacks if system weaknesses are not addressed. |
| **How to identify/ What to pay attention to** | Sudden inability to access internal systems or encrypted files.<br>Unusual pop-up warnings or ransom notes demanding payment in cryptocurrency.<br>Sluggish performance or network slowdowns, which may be early signs of infection.<br>Discrepancies in cargo management records or difficulty accessing tracking systems. |
| **Solution** | Regular backups and disaster recovery: Implement frequent system backups and ensure that they are stored offline or in secure, isolated environments. This allows for quick restoration in case of ransomware infection.<br>Network segmentation: Separate critical operational systems (e.g., ship traffic management) from administrative IT systems to minimize the impact of ransomware on key functions.<br>Anti-ransomware measures: Use advanced endpoint detection and response (EDR) systems to identify and neutralize ransomware threats before they can spread.<br>Cybersecurity awareness and training: Conduct regular training for port employees on phishing, malware, and ransomware prevention, as these attacks often begin with social engineering tactics.<br>Incident response plan: Develop a robust incident response plan to handle ransomware attacks swiftly, including steps to isolate affected systems, communicate with stakeholders, and restore operations. |
| **Source** | Source Cimpanu, C.: US Coast Guard discloses Ryuk ransomware infection at maritime facility, 529 https://www.zdnet.com/article/us-coast-guard-disclosesryuk- |

| | |
|---|---|
| | ransomware-infection-at-maritime-facility/<br><br>Safety4Sea: 2018 Highlights: Major cyber attacks reported in maritime industry, https://safety4sea.com/cm-2018-highlights-major-cyberattacks-reported-in-maritime-industry/ |
| **Example 4** | |
| **Description of incident** | In 2018, shortly after a similar ransomware incident at another European port, a major North American port experienced a severe disruption of its internal IT systems. The attack primarily affected local administrative and operational functions, while ship traffic and critical port operations remained unaffected. The incident raised concerns about the ability of ports to withstand multiple ransomware attacks occurring within a short time frame.<br>Possible situtation based on the incident:<br>Ransomware infected the port's internal IT systems, encrypting essential files and disabling various administrative functions. This led to delays in processing documentation, handling local logistics, and communicating within port departments, while key operational systems continued running unaffected. The disruption strained the port's day-to-day management and raised concerns about the readiness of ports to face similar cyberattacks in quick succession. |
| **Identified threat** | Off use internal IT systems of Port Authority |
| **Result of a threat** | Severe disruption of internal IT functions and communication systems.<br>Delays in local logistics, cargo processing, and administrative tasks.<br>Financial and reputational damage due to operational inefficiencies and extended recovery times.<br>Increased fear of ports becoming repeated targets for ransomware attacks. |
| **How to identify/ What to pay attention to** | Inability to access internal systems or files, with accompanying ransom messages demanding payment in cryptocurrency.<br>Widespread system slowdowns or complete lockout of administrative functions.<br>Sudden and unexplained halting of essential port operations (especially paperwork and coordination).<br>System warnings or alerts of unauthorized access or encryption attempts. |
| **Solution** | System backups and restoration procedures: Regularly back up IT systems, ensuring backups are secure and isolated from the main network to avoid being compromised during an attack.<br>Segmentation of administrative and operational networks: Divide the administrative IT network from mission-critical systems like ship traffic management and cargo handling to prevent cross-system infections.<br>Advanced ransomware detection: Implement enhanced monitoring systems, such as intrusion detection/prevention systems (IDS/IPS), and conduct regular vulnerability assessments to detect and prevent ransomware attacks. |

| | |
|---|---|
| | Employee training on cybersecurity best practices: Conduct awareness programs for staff, focusing on recognizing phishing attempts, safe internet use, and responding to ransomware threats.<br>Incident response planning: Develop and maintain an up-to-date incident response plan for handling ransomware attacks, which includes isolating affected systems, notifying stakeholders, and quickly restoring services. |
| **Source** | Cimpanu, C.: US Coast Guard discloses Ryuk ransomware infection at maritime facility, 529 https://www.zdnet.com/article/us-coast-guard-disclosesryuk-ransomware-infection-at-maritime-facility/<br>Safety4Sea: 2018 Highlights: Major cyber attacks reported in maritime industry, https://safety4sea.com/cm-2018-highlights-major-cyberattacks-reported-in-maritime-industry/ |
| **Example 5** | |
| **Description of incident** | Between 2011 and 2013, the cargo tracking system was compromised by cybercriminals to enable the smuggling of drugs and weapons. By gaining unauthorized access to the port's system, the attackers altered shipping data, concealing illegal goods (disguised as legitimate cargo, such as bananas from South America). The attack continued undetected for two years. A similar cyberattack targeted the port again in 2018.<br>Possible situtation based on the incident:<br>Cybercriminals gained access to the port's cargo management system, modifying the manifest data of incoming shipments. Through this, the criminals hid the presence of illegal cargo, rerouting it to designated areas where it could be retrieved without detection by law enforcement or customs authorities. As a result, illicit goods such as drugs and weapons entered Europe without being discovered. |
| **Identified threat** | Compromised cargo tracking system. |
| **Result of a threat** | Misrepresentation of cargo details allowed illegal goods to enter the port undetected, leading to security breaches.<br>Facilitated the smuggling of contraband over an extended period.<br>Created significant legal, operational, and reputational risks for the port and shipping operators. |
| **How to identify/ What to pay attention to** | Monitor cargo manifests and tracking data for discrepancies, especially for containers originating from high-risk regions.<br>Conduct regular audits of cargo documentation, looking for unusual or repeated routing changes.<br>Use real-time monitoring systems that alert on deviations in container movement or handling.<br>Be alert to unusual activity around containers, such as unauthorized access or tampering with cargo seals. |

| | |
|---|---|
| **Solution** | Enhanced cybersecurity protocols: Implement robust access controls, multi-factor authentication, and encryption for all cargo-related data to prevent unauthorized system access.<br>Regular audits and system monitoring: Schedule frequent checks and cybersecurity audits on cargo tracking systems to detect anomalies early.<br>Cross-industry collaboration: Share threat intelligence between ports, customs, and law enforcement agencies to stay ahead of emerging cyber threats.<br>Training and awareness: Regularly train port personnel and supply chain operators on the latest cyber threats and how to spot potential signs of system compromise.<br>Backup and contingency plans: Ensure that redundant systems or manual checks can verify cargo manifests in the event of a cyberattack. |
| **Source** | Kristoffersen, P.B., Hartvigsen, T., Myrvang, P., Torjusen, A.: Digitale Sårbarheter Maritim Sektor. DNVGL, Lysneutvalget (2015).<br>Nguyen, L.: Collaboration in the Shipping Industry: Innovation and Technology, https://informaconnect.com/epaper-collaboration-in-theshipping-industry-innovation-and-technology/<br>Polychronis, K.: Cybersecurity at Sea. In: Otto, L. (ed.) Global Challenges in Maritime Security. p. 243 Springer International Publishing (2020)<br>Walker, J., Spencer, J.: Cyber Marine: Risks & Loss Scenarios, http://www.marineclaimsconference.com/imccdocs/docs/Cyber%20workshop.pdf. |

### 2.2.2 Communication Networks

Communication networks on ships are crucial for ensuring safety and efficient information exchange, but their vulnerability to cyberattacks poses a significant threat to maritime operations. In recent years, numerous incidents have been reported, leading to the degradation of onboard system functionality, data loss, and ransom demands.

The cases described below illustrate various threats, such as disruptions to control systems, loss of data on ship servers, and malware infections. Additionally, the section presents the consequences of these threats (Result of a threat), ways to identify them (How to identify/What to pay attention), possible solutions (Solution), and sources of information (Source).

| **Example 1** | |
|---|---|
| **Description of incident** | In February 2019, a large ship bound for a major port radioed a national coast guard authority warning that the vessel was "experiencing a significant cyber incident impacting their shipboard network."<br>The Coast Guard led an incident-response team to investigate the issue and found that malware had infected the ships systems and significantly degraded functionality. Fortunately, essential systems for the control of the vessel were unimpeded. |
| **Identified threat** | Significantly degraded functionality of onboard control system. |

| | |
|---|---|
| **Result of a threat** | The onboard control system network was infected with malware, resulting in significantly degraded functionality. |
| **How to identify/ What to pay attention to** | Use malware detection software that uses various tools and techniques to identify the presence of malicious software on a system. In that case the malware can be detected and removed even before it can cause any damage. Check regularly the functionality of the malware detection software. Pay attention to all working systems if they are working properly, in case of any alerts or blockages the malware can be the cause. |
| **Solution** | Physical secure ship and devices and limit the access.<br>Segment shipboard network so that in case of malware attack the vital system may not be accessed and infected.<br>Enforce per-user passwords and roles.<br>Restrict the use of memory sticks, reading of personal e-mails and downloads.<br>Installing basic security protections and malware detection software and patch it regularly.<br>Educate all the employees about the best practice and the evolving nature of cyber threats.<br>Try to avoid temporary crew and independent contractors that are unfamiliar with a specific company's information security policy. |
| **Source** | https://www.darkreading.com/vulnerabilities-threats/coast-guard-warns-shipping-firms-of-maritime-cyberattacks<br>https://www.transnav.eu/files/A_Retrospective_Analysis_of_Maritime_Cyber_Security_Incidents,1144.pdf<br>https://www.dco.uscg.mil/Portals/9/DCO%20Documents/5p/CG-5PC/INV/Alerts/0619.pdf<br>https://www.forbes.com/sites/daveywinder/2019/07/09/u-s-coast-guard-issues-alert-after-ship-heading-into-port-of-new-york-hit-by-cyberattack/?sh=6597dc5c41aa |
| **Example 2** | |
| **Description of incident** | In 2019, a tanker operating near a Northern European port was hit by a ransomware attack. As a result, its administration server was infected and the back up disk was wiped. Reportedly, the method of intrusion remains unclear but a Remote Desktop Protocol (RDP), a USB device or an email attachment are identified as probable attack vectors. The same vessel was infected again 4 months later near the same port. The threat actor and motives behind the attack remain a mystery. |
| **Identified threat** | Loss of data on backup disk, impeded use of administrative server, ransom demand. |
| **Result of a threat** | Administration server was infected and the back up disk was wiped. |
| **How to identify/ What to pay** | Use malware detection software that uses various tools and techniques to identify the presence of malicious software on a system. In that case the ransomware/malware can be detected and removed even before it can cause any damage.<br>Check regularly the functionality of the malware detection software. |

| | |
|---|---|
| **attention to** | Pay attention to all working systems if they are working properly, in case of any alerts or blockages the malware can be the cause.<br>Use efficient backup system. |
| **Solution** | Physical secure ship and devices and limit the access.<br>Segment shipboard network so that in case of ransomware attack the vital system may not be accessed and infected.<br>Enforce per-user passwords and roles.<br>Restrict the use of memory sticks, reading of personal e-mails and downloads.<br>Installing basic security protections and malware detection software and patch it regularly.<br>Educate all the employees about the best practice and the evolving nature of cyber threats.<br>Try to avoid temporary crew and independent contractors that are unfamiliar with a specific company's information security policy. |
| **Source** | https://www.maritimecybersecurity.nl/incident/j7NoOqjm5a<br>https://www.transnav.eu/files/A_Retrospective_Analysis_of_Maritime_Cyber_Security_Incidents,1144.pdf |
| **Example 3** | |
| **Description of incident** | In 2020, a vessel anchored near a port in Northern Europe had its ship server and multiple PC clients infected with ransomware. Two specialists from the IT service provider were sent onboard and found that all data were encrypted and lost. A full reinstall was necessary to restore the systems, |
| **Identified threat** | Loss of data on server and PC clients, impeded use of ships server, ransom demand. |
| **Result of a threat** | Ships server and multiple PC clients were infected and the data were encrypted. A full reinstall of the system was necessary. |
| **How to identify/ What to pay attention to** | Use malware detection software that uses various tools and techniques to identify the presence of malicious software on a system. In that case the ransomware/malware can be detected and removed even before it can cause any damage.<br>Check regularly the functionality of the malware detection software.<br>Pay attention to all working systems if they are working properly, in case of any alerts or blockages the malware can be the cause. |
| **Solution** | Physical secure ship and devices and limit the access.<br>Segment shipboard network so that in case of ransomware attack the vital system may not be accessed and infected.<br>Regularly back up files and data and use efficient restore system.<br>Enforce per-user passwords and roles.<br>Restrict the use of memory sticks, reading of personal e-mails and downloads.<br>Install basic security protections and malware detection software and patch it regularly. |

| | |
|---|---|
| | Educate all the employees about the best practice and the evolving nature of cyber threats. Train users to avoid opening unexpected emails and email attachments. Try to avoid temporary crew and independent contractors that are unfamiliar with a specific company's information security policy. |
| **Source** | https://www.transnav.eu/files/A_Retrospective_Analysis_of_Maritime_Cyber_Security_Incidents,1144.pdf |

### 2.2.3 Integrated bridge systems

Integrated Bridge Systems are an essential component in ensuring safe navigation by combining various control and navigation systems into a single unit. However, their vulnerability to cyberattacks and technical failures can pose significant risks to vessel safety.

The cases described below illustrate different threats, such as false vessel positioning, loss of weather data, malware infections, and the interception of confidential voyage information. Additionally, the section presents the consequences of these threats (Result of a threat), ways to identify them (How to identify/What to pay attention), possible solutions (Solution), and sources of information (Source).

| **Example 1** | |
|---|---|
| **Description of incident** | A failure within an integrated navigational system resulted in the loss of system independence, where a malfunction in one part affected other sub-systems. This situation occurred after an unsafe memory stick was connected to the ECDIS system. |
| **Identified threat** | False vessel position and navigational information. Loss of electronic chart display and information system redundancy. |
| **Result of a threat** | Collision, grounding. Loss of operation. |
| **How to identify/ What to pay attention to** | General functionality of ECDIS system. A defect book is widely used onboard to list anomalies in systems assisting in revealing patterns and repetition of errors. |
| **Solution** | Data fed to the ECDIS comes from a trusted source. Use only reputable ENC service providers. Ensure transfer of data to the vessel is in an encrypted form (bit locker or equivalent). Memory sticks connected to ships safety critical systems must be dedicated and not personal. |
| **Source** | https://www.imo.org/en/OurWork/Safety/Pages/IntegratedBridgeSystems.aspx https://iho.int/uploads/user/Services%20and%20Standards/ENCWG/ENCWG7/ENCWG7-4.5_2022_EN_ECDIS%20cyber%20security%20guideline%20draft.pdf |

| **Example 2** | |
|---|---|
| **Description of incident** | A device installation results to a spread of malicious software. |
| **Identified threat** | Faulty bridge integrated system. |
| **Result of a threat** | Collision, grounding. |
| **How to identify/ What to pay attention to** | Multiple navigation errors. Alarms of faulty messages between devices. |
| **Solution** | Only rely on recognized providers when making changes to the bridge systems. Thorough risk analyses and management of change process must. |
| **Source** | https://www.mdpi.com/2077-1312/7/10/350 |
| **Example 3** | |
| **Description of incident** | Loss of weather data. |
| **Identified threat** | No data available for navigation and voyage planning. |
| **Result of a threat** | Inability to safely operate ships and conduct weather routing. |
| **How to identify/ What to pay attention to** | Test different weather areas and monitor the messages the NAVTEX is sending. |
| **Solution** | Apply multiple sources for the weather routing. An online option is nowadays available opening a possibility to order an external weather routing service providing navigation instructions via email daily. |
| **Source** | https://www.mdpi.com/2077-1312/7/10/350 |
| **Example 4** | |
| **Description of incident** | Hacking of vessel emails. |

| | |
|---|---|
| **Identified threat** | Loss of confidential routing data in high-risk areas. |
| **Result of a threat** | Hi-jacking of vessel. |
| **How to identify/ What to pay attention to** | Slowing of internet connection. |
| **Solution** | Email and internet fire wall protection. No visiting to suspicious pages nor opening suspicious emails and in particular, suspicious attachments. |
| **Source** | https://www.mdpi.com/2077-1312/7/10/350 |

### 2.2.4 Navigation systems

Navigation systems are essential for accurately determining a vessel's position and ensuring safe maritime operations. However, cybersecurity threats such as jamming and spoofing of signals can lead to serious consequences, including false vessel positioning and misinformation being transmitted to other ships and navigators.

The cases described below highlight various threats, such as incorrect vessel positioning, misleading data being shared with other vessels, and manipulation of navigational information. Additionally, the section presents the consequences of these threats (Result of a threat), ways to identify them (How to identify/What to pay attention), possible solutions (Solution), and sources of information (Source).

| **Example 1** | |
|---|---|
| **Description of incident** | Jamming and spoofing of GPS signal in the Gulf of Finland. |
| **Identified threat** | False vessel position. |
| **Result of a threat** | Collision, grounding.<br>In time, when the latitude information is gone, the gyro compasses are lost and the heading information goes with it leaving the vessel with magnetic compass. |
| **How to identify/ What to pay attention to** | Offset in the own vessel position.<br>Radar based positioning using parallel index in congested waters.<br>Comparison of positioning data from multiple GPS receivers.<br>Comparison of data from the differential correction receivers. |

| | |
|---|---|
| **Solution** | There is no solution to an external hazard. This is the point in security related items. We cannot remove the root cause, but we can prepare for the threat trying to minimise the consequences. |
| **Source** | Link to news report from the Finnish authorities from last September. https://yle.fi/a/74-20111823 |
| **Example 2** | |
| **Description of incident** | Jamming and spoofing of AIS signal. |
| **Identified threat** | False vessel position passed on to other vessels. |
| **Result of a threat** | Collision, grounding.<br>Other vessels are provided with false position of you |
| **How to identify/ What to pay attention to** | Offset in the other vessel position.<br>Radar based positioning using parallel index in congested waters.<br>Comparison of positioning data from multiple GPS receivers.<br>Comparison of data from the differential correction receivers. |
| **Solution** | There is no solution to an external hazard. This is the point in security related items. We cannot remove the root cause, but we can prepare for the threat trying to minimise the consequences.<br>One must not rely on AIS information as bases for navigation decision making. The AIS information is created and originated to the other vessel, and therefore you cannot verify its accuracy. Use radar for determining the position of the other vessel. |
| **Source** | Link to news report from the Lloyds: https://www.lloydslistintelligence.com/knowledge-hub/risk-and-compliance/the-case-of-the-shanaye-queen |
| **Example 3** | |
| **Description of incident** | Jamming and spoofing of GPS signal. |
| **Identified threat** | False marine aids-to-navigation (AtoN) data provided for the navigators. |
| **Result of a threat** | Navigation errors made based on false navigations aids data. Collision, grounding. |
| **How to identify/ What to pay attention to** | Offset in radar position and ECDIS position of navigation marks. |
| **Solution** | There is no solution to an external hazard. This is the point in security related items. We cannot remove the root cause, but we can prepare for the threat trying to minimise the consequences.<br>Radar based positioning using parallel index in congested waters. Radar based definition of position of navigation marks and fairway infrastructure. |

| | |
|---|---|
| | One must not rely solely on ECDIS information as bases for navigation decision making.<br>Use radar for determining the position of the other vessel and navigation marks. |
| **Source** | Link to news report from The General Lighthouse Authorities of the United Kingdom and Ireland, Harwich, UK<br>https://www.porttechnology.org/wp-content/uploads/2019/05/PT46-09.pdf |
| **Example 4** | |
| **Description of incident** | Jamming and spoofing of GPS signal. |
| **Identified threat** | False vessel position provided by the GMDSS system DSC equipment. |
| **Result of a threat** | In the distress situation help is guided to false position. |
| **How to identify/ What to pay attention to** | If the error exists in navigation systems it will also exist in other system fed by the GPS receivers. DSC (digital selective calling) is one such system. |
| **Solution** | There is no solution to an external hazard. This is the point in security related items. We cannot remove the root cause, but we can prepare for the threat trying to minimise the consequences.<br>Radar based positioning using parallel index in congested waters. Radar based definition of position of navigation marks and fairway infrastructure. |
| **Source** | Link to news report from The General Lighthouse Authorities of the United Kingdom and Ireland, Harwich, UK<br>https://www.porttechnology.org/wp-content/uploads/2019/05/PT46-09.pdf |

### 2.2.5 Onboard Entertainment Systems

Onboard entertainment systems provide passengers with access to multimedia content, but their integration with other ship systems makes them vulnerable to cyberattacks. In recent years, cases of malware infections and unauthorized access have been reported, leading to service disruptions and potential security risks for onboard data.

The incidents described below highlight various threats, such as disruption of entertainment services, unauthorized access to data, and an increased risk of compromising other onboard systems. Additionally, the section presents the consequences of these threats (Result of a threat), ways to identify them (How to identify/What to pay attention), possible solutions (Solution), and sources of information (Source).

| **Example 1** |
|---|

| | |
|---|---|
| **Description of incident** | In 2020, a major cruise line experienced a cyber attack that compromised its onboard entertainment systems. The attackers used malware to infiltrate the ship's Wi-Fi network, which was interconnected with the entertainment systems. As a result, services such as movie streaming and gaming were disrupted for passengers, leading to significant dissatisfaction. Although the personal data of guests was reportedly not compromised, concerns arose about the security of other systems on the ship. The incident highlighted vulnerabilities that could potentially expose critical systems to further attacks. |
| **Identified threat** | Disruption of onboard entertainment services, unauthorised access to interconnected systems, and increased risk of data breaches. |
| **Result of a threat** | Entertainment systems became inoperable, leading to guest complaints and financial loss for the cruise line due to compensation demands and negative publicity. |
| **How to identify/ What to pay attention to** | Use efficient backup system.<br>Use network monitoring tools to detect unusual traffic patterns indicative of malware activity.<br>Regularly audit the entertainment systems for vulnerabilities and ensure they are not directly accessible from the broader shipboard network.<br>Train staff to report any anomalies or disruptions in the entertainment systems promptly. |
| **Solution** | Implement network segmentation to isolate entertainment systems from critical operations and communication networks.<br>Regularly update software and systems to patch vulnerabilities and strengthen security protocols.<br>Install antivirus and anti-malware solutions specifically designed for onboard systems and ensure they are regularly updated.<br>Educate all crew members about cybersecurity best practices, emphasizing the importance of reporting suspicious activity and adhering to security protocols.<br>Limit access to entertainment systems to essential personnel only and monitor user activity closely to detect any unauthorized access attempts. |
| **Source** | Cybersecurity and Infrastructure Security Agency (CISA): Best Practices for Securing Onboard Entertainment Systems<br>Maritime Cyber Risk Management: Lessons Learned from Industry Incidents |
| **Example 2** | |
| **Description of incident** | In early 2022, a luxury yacht was hit by a malware infection that impacted its onboard entertainment system. The malware spread through a compromised USB drive used by crew members for system updates. This incident disrupted video and audio services onboard, frustrating guests and affecting the yacht's reputation. |
| **Identified threat** | Malware infection leading to system downtime, unauthorised access to data, and breach of guest information. |
| **Result of a threat** | The entertainment system was rendered inoperable for several days while the malware was removed and systems were restored. |

| | |
|---|---|
| **How to identify/ What to pay attention to** | Implement endpoint protection to detect and quarantine malware before it spreads.<br>Regularly scan USB drives and other external devices for malware before connecting them to onboard systems.<br>Monitor the functionality of entertainment systems for any irregularities or performance issues. |
| **Solution** | Establish strict policies on the use of external devices, such as USB drives, to prevent malware introduction.<br>Train crew members on safe handling of USB devices and the risks associated with their use.<br>Install and maintain robust antivirus software to detect and remove malware promptly.<br>Create a robust backup system for entertainment systems to ensure quick recovery in the event of an infection. |
| **Source** | https://www.transnav.eu/files/A_Retrospective_Analysis_of_Maritime_Cyber_Security_Incidents,1144.pdf |
| **Example 3** | |
| **Description of incident** | In late 2021, a cruise ship faced a cyber incident when hackers exploited vulnerabilities in its onboard entertainment system. The attack was traced back to a third-party application used for streaming services that had not been properly secured. Attackers gained access to the application and subsequently infected the entertainment system with malware, causing the system to crash and disrupting services for passengers. |
| **Identified threat** | Infiltration of the entertainment system, leading to malware deployment and service disruption. |
| **Result of a threat** | The onboard entertainment system went offline for several days while cybersecurity teams worked to remove the malware, causing dissatisfaction among passengers and impacting the ship's overall experience. |
| **How to identify/ What to pay attention to** | Regularly audit third-party applications and their security measures to identify potential vulnerabilities.<br>Monitor entertainment system performance for unusual behavior, such as slow response times or unexpected reboots.<br>Implement logging and monitoring to track access and changes to the entertainment system. |
| **Solution** | Conduct regular security assessments of all third-party applications used onboard to ensure they meet cybersecurity standards.<br>Isolate the entertainment system network from critical operational systems to minimize risks associated with malware infections.<br>Implement robust access controls and authentication measures for all applications used within the entertainment system. |

| | |
|---|---|
| | Educate crew members about the potential risks of third-party applications and the importance of following cybersecurity protocols.<br>Maintain up-to-date software on all entertainment systems and applications to address known vulnerabilities promptly. |
| **Source** | https://www.cisa.gov/publication/guidelines-securing-onboard-systems<br>https://www.imo.org/en/OurWork/Security/Pages/Cybersecurity.aspx |

### 2.2.6 Passenger and Crew Management Systems

Passenger and crew management systems are essential for the efficient operation of maritime transport, handling reservations, passenger identification, and crew organization. However, their vulnerability to cyberattacks, such as phishing, SQL injection, and DDoS attacks, can lead to severe operational disruptions and the leakage of confidential data.

The incidents described below highlight various threats, including unauthorized access to databases, interception of financial communications, theft of personal data, and the shutdown of reservation systems. Additionally, the section presents the consequences of these threats (Result of a threat), ways to identify them (How to identify/What to pay attention), possible solutions (Solution), and sources of information (Source).

| **Example 1** | |
|---|---|
| **Description of incident** | In 2014, a publicly available security report detailed multiple vulnerabilities in widely used SATCOM systems, including a Blind SQL Injection vulnerability in a login form. Possible situation based on the incident: Attackers were able to obtain corporate data. |
| **Identified threat** | The attacker uses SQL injection to manipulate the system's database query, gaining access to restricted areas of the database that store login information and credentials. |
| **Result of a threat** | Data Breach: The attacker retrieves confidential information about passengers, including credentials and contact information.<br>Security Threat: The unauthorized access could allow the attacker to modify or delete data, potentially posing a safety risk if critical information is changed or removed.<br>Financial Loss and Reputational Damage: Leaked passenger information could lead to legal consequences, loss of customer trust, and financial penalties. |
| **How to identify/ What to pay attention to** | Unusual Database Activity: Monitor for anomalous queries, especially those containing unexpected SQL commands.<br>Unusual Login Patterns: Track repeated failed login attempts or successful logins from suspicious IP addresses.<br>System Performance Issues: A sudden slowdown in the system might indicate a database under stress from malicious queries. |
| **Solution** | **Prevention Measures:** |

| | |
|---|---|
| | Input Validation: Implement input validation by validating and sanitizing user inputs before they reach the database. Using parameterized queries or prepared statements to ensure inputs cannot inject SQL queries.<br>Least Privilege Principle: Ensure that the database user accounts interacting with web applications have the least possible privileges required for their functionality.<br>Regular Security Patching: Keep the database management systems and applications updated with the latest security patches to fix known vulnerabilities.<br>Web Application Firewall (WAF): Deploy a WAF to filter and monitor incoming traffic, detecting and blocking SQL injection attempts.<br>**Mitigation (After a Successful Attack):**<br>Immediate Disconnection: Disconnect compromised databases or systems from the network to prevent further exploitation.<br>Log Analysis: Perform a detailed analysis of the logs to identify the attack vector and entry points.<br>Data Integrity Checks: Conduct integrity checks to assess if data has been modified, and restore from backups if necessary.<br>Implement Additional Monitoring: Increase real-time monitoring on the affected systems to detect any subsequent attack attempts. |
| **Source** | https://ioactive.com/amosconnect-maritime-communications-security-has-its-flaws/<br>https://ioactive.com/pdfs/IOActive_SATCOM_Security_WhitePaper.pdf |

| **Example 2** | |
|---|---|
| **Description of incident** | In 2023, the UK ferry company was impacted by a significant cyberattack. The attack involved phishing tactics that led to unauthorized access to the passenger and crew management systems. This compromised sensitive data, disrupted ferry schedules, and caused operational delays.<br>Possible situation based on the incident: Attackers could access the personal data of passengers and crew members, potentially leading to identity theft, unauthorized access to ferry services, and the manipulation of operational schedules. |
| **Identified threat** | The attack involved malware that granted the attackers access to sensitive systems. |
| **Result of a threat** | Data Breach: Sensitive data, including personal information of crew and passengers, was exposed.<br>Service Disruption: Schedules were delayed, causing inconvenience and operational loss.<br>Financial and Reputational Impact: Potential fines, loss of customer trust, and financial penalties could ensue. |
| **How to identify/ What to pay attention to** | Suspicious Emails: Look for unexpected emails with attachments or links asking for login information.<br>Unusual Login Attempts: Monitor for logins from unknown IP addresses or failed login attempts.<br>System Irregularities: Pay attention to any unexpected system outages or slowdowns, which may indicate unauthorized access. |
| **Solution** | **Prevention Measures:**<br>User Awareness Training: Conduct regular training sessions for crew and shore-based staff on how to recognize phishing emails and social engineering tactics. |

| | |
|---|---|
| | Multi-Factor Authentication (MFA): Enforce MFA across all accounts, especially for access to critical systems, ensuring that phishing attempts requiring credentials are prevented.<br>**Mitigation (After a Successful Attack):**<br>Immediate Account Lockdown: If credentials are compromised, immediately change affected accounts.<br>System Scan: Scan all systems for malware that may have been affected through phishing emails or malicious attachments.<br>Awareness Recap: Brief the entire crew about the attack vector to ensure no further similar phishing attacks are successful.<br>Audit Logs: Review the logs to determine the extent of the compromise and trace the attacker's actions. |
| **Source** | https://maritime-executive.com/article/ferry-operator-red-funnel-hit-by-cyberattack |
| **Example 3** | |
| **Description of incident** | In 2019, a technology startup was defrauded of $1 million during a wire transfer to an investment firm through a man-in-the-middle attack. The attackers created lookalike email domains to intercept and manipulate communication between the two parties. |
| **Identified threat** | Attackers employed sophisticated email spoofing techniques to impersonate both the startup and the VC firm, altering communication to redirect the transfer of funds to a fraudulent account. |
| **Result of a threat** | Data Breach: Confidential transaction details were intercepted.<br>Financial Loss: $1 million intended for the startup was fraudulently redirected.<br>Reputational Damage: Both entities suffered damage to their trustworthiness and financial integrity. |
| **How to identify/ What to pay attention to** | Anomalies in Email Communication: Slight variations in domain names that mimic legitimate business contacts.<br>Unusual Transaction Requests: Requests for changes in payment details or unexpected transaction methods.<br>Lack of Direct Verification: Absence of secondary confirmation through other communication channels. |
| **Solution** | **Prevention Measures:**<br>Encryption: Use strong encryption protocols (e.g., TLS/SSL) to secure all communications between onboard systems and shore-based systems, ensuring data cannot be intercepted.<br>Network Segmentation: Segment sensitive networks, such as passenger systems and crew systems, to limit the exposure of critical systems to MITM attacks.<br>VPNs for Remote Access: Require VPN access for all remote connections, encrypting data and preventing interception on open networks.<br>**Mitigation (After a Successful Attack):**<br>Network Reconfiguration: Reconfigure network devices to eliminate the source of the MITM attack, such as insecure access points or routers.<br>User Notification: Inform all affected users of the MITM attack and recommend that they change passwords and secure their accounts. |

| | |
|---|---|
| | Session Termination: Immediately terminate all active sessions that may have been intercepted. |
| **Source** | https://threatpost.com/ultimate-mitm-attack-steals-1m-from-israeli-startup/150840/ |
| **Example 4** | |
| **Description of incident** | In May 2018, a railway operator experienced a Distributed Denial of Service (DDoS) attack that severely affected its ability to provide passenger services. The attack targeted the railway's digital infrastructure, particularly the ticketing and passenger management systems, rendering them non-functional for a significant period. This disruption prevented passengers from purchasing tickets online and at physical ticket machines, leading to chaos at stations and delaying numerous services. |
| **Identified threat** | The DDoS attack flooded the railway's systems with excessive traffic, overwhelming the network infrastructure. As a result, legitimate users, including passengers and staff, were unable to access essential services like ticket purchases and scheduling updates. |
| **Result of a threat** | Service Disruption: Thousands of passengers were unable to purchase tickets or access essential travel information.<br>Operational Chaos: The attack caused delays and cancellations, disrupting the railway's entire scheduling system.<br>Reputational Damage: The inability to serve customers led to public dissatisfaction, damaging the railway's reputation.<br>Potential Financial Loss: Loss of ticket sales during the disruption, along with the cost of mitigating the cyberattack, had financial implications for the company. |
| **How to identify/ What to pay attention to** | Network Slowdowns: Monitor for sudden performance degradation in ticketing systems and other online services.<br>Increased Traffic: Pay attention to unusually high volumes of traffic in the network, particularly from suspicious IP addresses.<br>Service Downtime: Track any unexpected outages or long periods of system unavailability. |
| **Solution** | **Prevention Measures:**<br>Traffic Monitoring: Use network traffic monitoring tools to detect unusual traffic spikes and block malicious IPs before they disrupt operations.<br>Cloud-Based DDoS Protection: Utilize cloud-based DDoS protection services that can block large-scale traffic.<br>**Mitigation (After a Successful Attack):**<br>Block Malicious IPs: Identify and block the IP addresses involved in the attack at the firewall level.<br>Service Restoration: Prioritize restoring critical services for crew and passenger systems to ensure minimal system break.<br>Attack Analysis: Analyze the attack to understand its scope, target, and vectors, and strengthen the defenses based on the findings. |
| **Source** | https://www.itgovernance.eu/blog/en/danish-rail-network-dsb-hit-by-cyber-attack#:~:text=DSB%2C%20the%20Danish%20state%20rail,a%20network%20or%20machines%20unavailable. |

### 2.2.7 Power Management Systems

Power management systems on ships are responsible for automatic power distribution, generator synchronization, and fuel consumption control, impacting both operational safety and the environment. Their integration with IT and OT systems makes them vulnerable to cyber threats, such as malware infections, which can disrupt onboard operations.

The incidents described below highlight various threats, such as the infection of power management systems through unsecured USB devices and network-connected printers. Additionally, the section presents the consequences of these threats (Result of a threat), ways to identify them (How to identify/What to pay attention), possible solutions (Solution), and sources of information (Source).

| **Example 1** | |
|---|---|
| **Description of incident** | **Scenario:**<br>The vessel is equipped with a complex power management system. It consists of switchboards and generators that control the automatic load distribution, power control, and automatic synchronization systems. Power management is important for the safety of the crew, the ship, and the cargo. It also has a clear environmental impact since power is generated by using fuel, either by the ship's main engine (shaft generator) or the auxiliary engines.<br>The first engineer officer of the vessel used, for his own convenience, a printer from the engine room control chamber, which was connected to the ship's automatic control system. This system was connected, through IT, to shore-based systems. As a result of this action, a malware virus was introduced that affected the power management or electrical supply system. |
| **Identified threat** | The threat of infection of the Power Management System or Power Supply, through a malware virus, can be detected because the computer takes a long time to start, applications do not load and stop responding, the System does not stop giving error messages and unknown icons appear.<br>All the above symptoms are indicating that the System is infected with malware. |
| **Result of a threat** | The malware can be controlled remotely and may cause a blackout at times when the ship is operating near the coast, entering port, or sailing in congested maritime areas. |
| **How to identify/ What to pay attention to** | The malware virus can introduce errors into the power control and electricity generation system, potentially causing a blackout on the ship and paralysing all electrically dependent equipment, that is, it would stop the propulsion and auxiliary motors, leaving the ship without propulsion and without electrical power in all its services. |
| **Solution** | Disconnect the automatic control system for the power and electricity generation control system and operate them in manual mode.<br>Resilient infrastructure: Use redundant systems, if available. |

| | |
|---|---|
| | Cyber awareness and training: Education on best practices and the changing nature of cyber threats. |
| **Source** | Own source |
| **Example 2** | |
| **Description of incident** | **Scenario:**<br>The bulk carrier had just completed bunkering operations in the bay. The bunker surveyor boarded the ship and requested permission to the first engineer officer to access a computer on board and this carried to him in the engine control room to print documents for signature. The surveyor inserted a USB drive into the computer and unwittingly introduced malware onto the ship's operations technologies network. The malware went undetected until a cyber assessment was conducted on the ship later, and after the crew had reported a "computer issue" affecting the operations technologies networks of the power management systems. |
| **Identified threat** | The threat of infection of the Power Management System or Power Supply, through a malware virus, can be detected because the computer takes a long time to start, applications do not load and stop responding, the System does not stop giving error messages and unknown icons appear.<br>All the above symptoms are indicating that the System is infected with malware. |
| **Result of a threat** | The malware can be controlled from shore and cause a blackout at times when the ship is operating near the coast, entering port, or sailing in congested maritime areas. |
| **How to identify/ What to pay attention to** | The malware virus can introduce errors into the power control and electricity generation system, potentially causing a blackout on the ship and paralysing all electrically dependent equipment, that is, it would stop the propulsion and auxiliary motors, leaving the ship without propulsion and without electrical power in all its services. |
| **Solution** | Disconnect the automatic control system for the power and electricity generation control system and operate them in manual mode.<br>Resilient infrastructure: Use redundant systems, if available.<br>Cyber awareness and training: Education on best practices and the changing nature of cyber threats.<br>It is necessary to do a procedure to avoid that members outside of the crew can use any computer scientist equipment on board. |
| **Source** | Own source |

### 2.2.8 Propulsion and Engine Control Systems

Propulsion and engine control systems are essential for the safe and efficient operation of vessels. Their digitization and integration with IT and OT networks increase the risk of cyberattacks, which can result in a loss of propulsion control and serious navigational hazards.

The incidents described below highlight various threats, such as ransomware infections during system updates and human-machine interface malware contamination through external devices. Additionally, the section presents the consequences of these threats (Result of a threat), ways to identify them (How to identify/What to pay attention), possible solutions (Solution), and sources of information (Source).

| **Example 1** | |
|---|---|
| **Description of incident** | **Scenario:**<br>During the process of updating the computer program of the propulsion engines of the ship, a ransomware virus was introduced that encrypted the automatic control system of the propulsion engines, and that began to act once the ship was sailing near the coast, with the aim of leaving the ship without propulsion. |
| **Identified threat** | Once the threat has been identified, the following must be done: Since the propulsion engines cannot be started, the automatic control of the same must be disconnected and they must be operated manually. To do this, it is necessary to disconnect them from the Automatic Control System, in addition to removing all the protections and interlocks of the automatic control on which the operation of the propulsion engines depended. Act on the control of the propulsion engines to cause the loss of propulsion of the vessel and the possibility of an accident if it is close to the coast or in an area of high navigation density, etc. |
| **Result of a threat** | Once the ransomware virus has acted by encrypting the automatic control of the propulsion engines, these have been stopped and the safety of the ship is compromised by losing propulsion. This can cause the ship to drift towards the coast, since it is under the action of the sea and the wind, and collide or run aground with it and the possibility of an accident when it is in an area of high navigation density, etc. |
| **How to identify/ What to pay attention to** | In the case of the ransomware virus, it is identified immediately, since, when the virus acts, it immobilizes your entire computer without being able to enter it and only a screen appears in which it tells you that the System is encrypted and that you must pay to decrypt it. |
| **Solution** | Disconnect the automatic control system for the propulsion engines and operate them in manual mode.<br>Resilient infrastructure: Use redundant systems, if available.<br>Cyber awareness and training: Education on best practices and the changing nature of cyber threats. |
| **Source** | Own source |
| **Example 2** | |
| **Description of incident** | **Scenario:**<br>The control of propulsion engine the ship called as consequence of a human-machine interface malware contamination due to the fact of a connection to an external device. Such a device could be a technician's or engineer's |

| | |
|---|---|
| | laptop, or an external storage drive used to update control system software during maintenance operations. |
| **Identified threat** | Loss of control of the main propulsion and ship´s rudder. |
| **Result of a threat** | The automatic control of the propulsion due the malware virus engines has stopped the propulsion engines and the safety of the ship is compromised by losing propulsion. This can cause the ship to drift towards the coast, since it is under the action of the sea and the wind, and collide or run aground with it and the possibility of an accident when it is in an area of high navigation density, etc. |
| **How to identify/ What to pay attention to** | The data of propulsion control system has been erased and the control doesn´t answer to any order. |
| **Solution** | One of the preventive barriers in this case would be the monitoring, control, or blockage of the use of or access to the communication interface ports. In this way, unintentional or intentional transfer of malware to systems is eliminated.<br>Another preventive barrier would be operator training, which would raise cyber-awareness and cyber hygiene practices and improve the monitoring of critical operational parameters and intervention in the case of excessive deviations being noticed.<br>The use of an antivirus software is also a useful tool and a preventive barrier for both cases, eliminating the installation of malware.<br>Disconnect the automatic control system for the propulsion engines and operate them in manual mode.<br>Resilient infrastructure: Use redundant systems, if available.<br>Cyber awareness and training: Education on best practices and the changing nature of cyber threats. |
| **Source** | Own source |

### 2.2.9 Satellite communication systems

Satellite communication systems are a vital part of navigation and maritime communication, enabling vessels to maintain independent connectivity and access accurate positioning data. However, threats such as intentional jamming and GPS spoofing can lead to severe operational disruptions and navigational misinformation.

The incidents described below highlight various threats, including GPS and Inmarsat signal interference, the inability to establish satellite communication, and the manipulation of a vessel's positioning data. Additionally, the section presents the consequences of these threats (Result of a threat), ways to identify them (How to identify/What to pay attention), possible solutions (Solution), and sources of information (Source).

| **Example 1** | |
|---|---|
| **Description of incident** | Intentional jamming can be carried out non-state actors, individuals, or small groups with portable jammers or state-sponsored. In some |

| | |
|---|---|
| | situations, GPS signal can be jammed unintentionally by aircrafts altimeters, TV harmonics, certain radars, satellite communication equipment and malfunctioning electronic devices.<br>Possible situtation based on the incident:<br>GPS devices do not receive the position signal unit. The ship's Master decided to use the position given by an alternative positioning system. |
| **Identified threat** | Jamming of GPS signal |
| **Result of a threat** | A distorted position signal can result in poor navigational decisions, potentially leading to navigational safety risks especially in restricted areas and increased navigation risks. |
| **How to identify/ What to pay attention to** | This kind of attack is difficult to detect unless navigator can obtain position by independent sources and analyses reason of positions discrepancy.<br>Observe previous recorded positions and the trend of their changes.<br>Compare the actual position with another positioning systems. |
| **Solution** | Use of the Navigation Message Authentication (NMA) in GPS signal.<br>Take the actual position from alternative positioning systems.<br>Use older methods of determining position.<br>The following steps are recommended before a GPS problem is reported:<br>● Reset the device by cycling power to the unit.<br>● Confirm the settings for the GPS unit or GPS application.<br>● Refer to the equipment manual.<br>● Update the equipment software or firmware and GPS mapping software.<br>Contact the equipment manufacturer for additional assistance. |
| **Source** | Own source |
| **Example 2** | |
| **Description of incident** | Jamming of Satellite signal. Two-way communication via satellite system cannot be established.<br>Possible situtation based on the incident:<br>Satellite transceiver can't establish the connection with satellite. The ship's Master decided to use second satellite transceiver. If that doesn't work use the MF/HF radiocommunication systems for achieve the communication. |
| **Identified threat** | Jamming of Inmarsat communication. |
| **Result of a threat** | Lack of connectivity can increase navigation safety risks, especially in areas with limited access and increased navigation risks. It can also put lives at risk, for example, if medical advice and assistance are not available. |
| **How to identify/ What to pay attention to** | The inability of connection between satellite transceiver and satellite. |
| **Solution** | Try to establish the connection using a second satellite system transceiver. If previous doesn't work, use the MF/HF radiocommunication systems. |
| **Source** | Own source |
| **Example 3** | |

| | |
|---|---|
| **Description of incident** | The attack begins with transmission of signals with slightly higher power and synchronised with GPS signal. When receivers lock onto bogus signal it gradually phases out genuine GPS signal and gives false position. GPS devices do not receive the position signal unit. The ship's Master decided to use the position given by an alternative positioning system. |
| **Identified threat** | Spoofing of GPS signal |
| **Result of a threat** | A wrong position can result in poor navigational decisions, potentially leading to navigational safety risks especially in restricted areas and increased navigation risks. |
| **How to identify/ What to pay attention to** | This kind of attack is difficult to detect unless navigator can obtain position by independent sources and analyses reason of positions discrepancy.<br>Observe previous recorded positions and the trend of their changes.<br>Compare the actual position with another positioning systems. |
| **Solution** | Use of the Navigation Message Authentication (NMA) in GPS signal.<br>Take the actual position from alternative positioning systems.<br>Use older methods of determining position.<br>Before reporting a GPS-related problem, the following steps should be taken:<br>● Reset the device by cycling power to the unit.<br>● Confirm the settings for the GPS unit or GPS application.<br>● Refer to the equipment manual.<br>● Update the equipment software or firmware and GPS mapping software.<br>● Contact the equipment manufacturer for additional assistance. |
| **Source** | Own source |
| **Example 4** | |
| **Description of incident** | Jamming of Satellite EGC signal. EGC information can't be received.<br>Possible situtation based on the incident:<br>Inmarsat device don't receive the Maritime Safety Informations – a especially SafetyNet - EGC. The ship's Master decided to use second satellite Inmarsat receiver. If that doesn't work use the MF/HF radiocommunication systems for achieve the maritime safety information. |
| **Identified threat** | Jamming of Inmarsat-C EGC signal. |
| **Result of a threat** | Lack of navigation safety information (navigational and meteorological warnings) increases navigation safety risks, especially in areas with limited access and increased navigation risks. |
| **How to identify/ What to pay attention to** | The inability of a satellite receiver to receive EGC information. |
| **Solution** | Try to receive EGC information using a second satellite system receiver.<br>If previous doesn't work, use the MF/HF radiocommunication systems. |
| **Source** | Own source |

### 2.2.10 Weather Monitoring Systems

Weather monitoring systems are an essential part of ensuring maritime safety by providing up-to-date meteorological data used for route planning and navigation. However, their vulnerability to cyberattacks, such as data manipulation, signal spoofing, and transmission interference, can pose significant operational risks.

The incidents described below highlight various threats, including disruption or manipulation of weather maps, the insertion of false meteorological data into autopilot systems, and interference with WEFAX transmissions. Additionally, the section presents the consequences of these threats (Result of a threat), ways to identify them (How to identify/What to pay attention), possible solutions (Solution), and sources of information (Source).

| **Example 1** | |
|---|---|
| **Description of incident** | In 2021, unauthorized access to meteorological information systems was reported, raising concerns about the integrity of weather information. No impact on critical infrastructure or economic losses was reported.<br>Possible situation based on the incident:<br>Distributed map of 3 days weather prediction consisting: temperature, rain falls, air pressure, winds and wave heights was disrupted by unauthorized access to weather prediction systems leading to the disseminated of fabricated, outdated or postponed weather indications. On the basis of Such map, the Captain decides to change the vessel route. |
| **Identified threat** | Disrupted weather map |
| **Result of a threat** | Disrupted weather prediction could affect decision-making processes, potentially leading to safety hazard and economic losses. |
| **How to identify/ What to pay attention to** | Observe the actual weather and compare with disseminated weather map.<br>Compare the prognosed weather indications with the onboard systems: thermometer, barometer, wind indicator, etc.<br>Compare with online marine weather services.<br>Compare with radio weather services if the vessel is within the range of onshore radio connection. |
| **Solution** | Enhanced data security: authentication protocols to protect meteorological data integrity from unauthorized access and manipulation – for weather prediction agencies.<br>Resilient infrastructure: use redundancy systems (like online services) to ensure continuous check and operation even during cyber incidents, like shiptraffic.net, marine.meteoconsult.co.uk, oceanweather.com, accuweather.com.<br>Meteorological education: continue training in observing weather changing to be able to compare it with the distributed faxymile weather map.<br>Cyber awareness and training: educated about best practice and the evolving nature of cyber threats. |
| **Source** | Own source |

| **Example 2** | |
|---|---|
| **Description of incident** | Although no significant incidents of cyberattacks specifically targeting weather on-board systems were reported, there is a possibility to use manipulated measurement readings from ships equipment that could impact route planning or autopilot performance.<br>Possible situation:<br>The attacker, having gained access to the ship's systems (e.g., via social engineering, malware introduced by a crew member, or another attack vector), installs malicious software aboard the vessel. The software begins manipulating the weather data collected by the onboard sensors and feeds it into the autopilot and navigation system. The anemometer reports light winds from a safe direction, while in reality, a storm with strong crosswinds is approaching or the barometer shows stable pressure, while in reality, pressure is dropping rapidly. Autopilot adjusts course based on false data. |
| **Identified threat** | The identified threat in this scenario is the insertion of false weather data into the ship's navigation and autopilot systems, making it appear as though the data is coming from onboard weather sensors. The goal of the attack is to manipulate the ship's course and make it vulnerable to hazardous conditions like storms, dangerous currents, or collisions by providing incorrect weather information. |
| **Result of a threat** | The result might be unsafe navigation decisions, loss of control due to incorrect manoeuvres or delay in crew response. The ship's safety is compromised, leading to potential damage to the vessel and cargo, which may lead to environmental consequences and/or legal liabilities and insurance claims due to the incident. |
| **How to identify/ What to pay attention to** | Discrepancies between real-world observations and system data; compare visual clues, radar or external satellite data showing incoming storms or dangerous conditions that conflict with onboard sensor data.<br>Inconsistent autopilot behaviour like unexpected course changes. If the autopilot makes navigation decisions that are illogical or hazardous.<br>Network and system activity anomalies or unusual communication.<br>Examination of system logs might show unexpected modifications to weather data or irregularities in how sensors are reporting data, such as static or non-changing values that don't align with the dynamic nature of real-world weather.<br>Compare data from external sources, such as satellite weather forecasts or reports from nearby ships, with onboard sensor data. Any significant differences between these sources and the onboard system suggest a potential manipulation of data. |
| **Solution** | The crew should disable the autopilot and switch to manual navigation, relying on their own observations, external data (e.g., radar, satellite), and standard navigational tools.<br>Attempt a system reboot or reset to restore normal sensor functioning and check if the issue is a result of a temporary glitch or a persistent attack.<br>Investigate system logs and network traffic: IT personnel should immediately review log data to identify any unusual activity, such as |

| | |
|---|---|
| | unauthorized access, and monitor for signs of tampering with the weather data.<br>Inspect the physical weather sensors on the ship to ensure they are functioning correctly and have not been tampered with or altered. |
| **Source** | https://www.bimco.org/-/media/bimco/about-us-and-our-members/publications/ebooks/guidelines-on-cyber-security-onboard-ships-v4.ashx?rev=e86ee4330cce44d7b90ad718e8af3c2e |
| **Example 3** | |
| **Description of incident** | Although no significant incidents of cyberattacks specifically targeting weather facsimile (WEFAX) transmissions have been widely documented, similar disruption techniques, such as jamming and spoofing, have been employed against other maritime communication systems (GPS, AIS). These methods could feasibly be applied to weather facsimile systems, given their dependence on radio frequencies for transmission. Jamming involves overwhelming the radio frequency used by WEFAX systems with noise, rendering the signal unreadable by the ship's receiver.<br>Possible situation:<br>A cargo ship navigating through a busy commercial shipping route is relying on WEFAX to receive crucial weather updates, including storm forecasts and sea conditions. A malicious actor, equipped with a radio frequency jammer, targets the ship's WEFAX reception. As a result, the ship is unable to download the latest weather maps. |
| **Identified threat** | Missed storm warning; the crew, aware of the transmission failure but unaware of its cause, attempts to troubleshoot the equipment, delaying any potential shift to backup systems (Iridium, Inmarsat). As weather conditions worsen, the ship encounters heavy seas and strong winds, which were not anticipated due to the lack of weather updates. |
| **Result of a threat** | The ship's safety is compromised, leading to potential damage to the vessel and cargo, which may lead to environmental consequences and/or legal liabilities and insurance claims due to the incident. |
| **How to identify/ What to pay attention to** | Signs of jamming is an abrupt loss of the WEFAX signal without any apparent environmental cause, if the signal was stable and strong but suddenly degrades or cuts off entirely, this could indicate intentional jamming.<br>When a jammer is in operation, the weather fax receiver may still pick up some signal, but the resulting maps will likely appear distorted or contain heavy noise, making them unusable.<br>Unusual fluctuations in signal strength can be a sign of jamming. If the signal alternates between strong and weak levels in rapid succession without obvious environmental factors.<br>Reports of similar issues from nearby vessels can indicate a region-wide jamming attack rather than an isolated technical failure on one ship.<br>If other HF-based systems, like NAVTEX or long-range communication systems, are also experiencing difficulties at the same time as the WEFAX, this can suggest a broader jamming operation affecting multiple systems. |

| | |
|---|---|
| **Solution** | Cross-checking data sources: compare weather fax data with alternative sources (Inmarsat, Iridium, or NAVTEX) to identify discrepancies.<br>WEFAX operates on multiple frequencies. The crew can attempt to tune to an alternative frequency within the WEFAX spectrum to see if other channels remain unaffected by the jamming.<br>In extreme cases, where all communication systems are compromised, relying on manual observations (e.g., barometric pressure, cloud patterns, wind direction). |
| **Source** | https://www.cisa.gov/sites/default/files/publications/safecom-ncswic_rf_interference_best_practices_guidebook_2.7.20_-_final_508c.pdf |
| **Example 4** | |
| **Description of incident** | A media report described a 2014 incident in which state-sponsored attackers allegedly breached the systems of a national meteorological authority, including weather satellites.<br>Possible situation based on the incident:<br>The transmission of outdated weather information, delayed by two hours, leading to inaccurate forecasts for temperature, precipitation, air pressure, winds, and wave heights. This could result in dangerous decisions at sea, such as changing a ship's route under unfavourable weather conditions, increasing the risk of accidents and threats to crew and cargo. |
| **Identified threat** | Outdated weather map - delayed information. |
| **Result of a threat** | Outdated weather forecasts can impact decision-making processes, potentially leading to safety hazards and economic losses. |
| **How to identify/ What to pay attention to** | Observe the actual weather and compare with disseminated weather map.<br>Compare the prognosed weather indications with the onboard systems: termometer, barometer, wind indicatior, etc.<br>Compare with online marine weather services.<br>Compare with radio weather services if the vessel is within the range of onshore radio connection. |
| **Solution** | Enhanced data security: authentication protocols to protect meteorological data integrity from unauthorized access and manipulation – for weather prediction agencies.<br>Resilient infrastructure: use redudancy systems (like online services) to ensure continous check and operation even during cyber incidents, like shiptraffic.net, marine.meteoconsult.co.uk, oceanweather.com, accuweather.com.<br>Meteorological education: continiue training in observing weather changing to be able to compare it with the distributed faxymile weather map.<br>Cyber awarness and training: educated about best practice and the evolving nature of cyber threats. |
| **Source** | https://eu.usatoday.com/story/weather/2014/11/12/china-weather-satellite-attack/18915137/ |

## 2.3 Conclusion

The growing digitization of maritime systems has improved efficiency and navigation but has also introduced cybersecurity risks, including malware infections, GPS spoofing, ransomware, and unauthorized access. These threats impact critical systems such as cargo management, communication networks, navigation, propulsion, and power management, leading to operational disruptions, financial losses, and safety hazards.

Cyberattacks have resulted in data breaches, false navigational data, loss of control over vessel systems, and manipulation of weather and satellite communication. To counter these risks, the maritime industry must implement strong cybersecurity measures, including regular updates, access controls, network segmentation, crew training, and backup systems.

Enhancing cybersecurity awareness and adopting best practices will help the sector strengthen its defenses, ensuring safer and more secure maritime operations.

# 3 Summary

The CyberSEA project seeks to strengthen cybersecurity awareness among seafarers also by analysing real-life cyber incidents affecting maritime operations. The WP2.T4 report presents an in-depth examination of cyber threats targeting onboard and shore-based systems, outlining vulnerabilities, consequences, and mitigation strategies. The document highlights key cybersecurity risks in maritime operations and aims to provide practical training resources to enhance cyber resilience. The approach involves analyzing documented cyber incidents across ten maritime domains, assessing their impact, identifying vulnerabilities, and proposing countermeasures. The goal is to equip seafarers with the necessary knowledge to detect and respond effectively to cyber threats, minimizing the risk of disruptions to maritime operations.

The report covers ten critical areas of cybersecurity risk in the maritime sector. Cargo management systems, crucial for global supply chains, have been targeted by ransomware attacks reported in a major global shipping incident in 2017, which severely disrupted the operations of a large shipping company and resulted in significant financial losses. Effective mitigation strategies include continuous network monitoring, intrusion detection systems, regular system audits, and the implementation of multi-factor authentication to enhance security. Communication networks, which ensure the seamless exchange of information at sea, have also been affected. A 2019 malware attack on a ship bound for a major international port degraded onboard control system functionality, highlighting the need for network segmentation, strict access controls, and restrictions on the use of USB devices to prevent unauthorized access.

Integrated bridge systems, which integrate navigational tools and vessel control systems, are also vulnerable to cyber threats. An example includes malware infiltration through an unsafe USB device connected to an Electronic Chart Display and Information System (ECDIS), leading to navigational

errors that could result in vessel collisions or groundings. To prevent such incidents, it is essential to use encrypted navigation data sources, perform thorough risk assessments before system updates, and implement strict protocols for data transfer. Similarly, cyber threats to navigation systems have led to GPS jamming and spoofing attacks, particularly in congested Northern European waters, where false vessel positioning has posed significant navigational risks. To counteract such threats, vessels must cross-check data from multiple navigation sources, use radar-based positioning techniques, and avoid over-reliance on a single system.

Beyond navigational tools, cyberattacks have also affected onboard entertainment systems, which are increasingly interconnected with critical ship networks. A notable case involved a malware attack on a cruise vessel's Wi-Fi network, leading to widespread service disruptions for passengers. Implementing network segmentation, deploying antivirus software, and enforcing strict policies on external device use can help minimize these risks. Passenger and crew management systems, which handle sensitive personal data and facilitate operations such as reservations and identification, have also been targeted. A 2023 phishing attack on a European ferry operator resulted in unauthorized access to passenger and crew data, leading to operational delays and reputational damage. To strengthen security, maritime operators must prioritize cyber awareness training, enforce multi-factor authentication, and monitor system access for anomalies.

Power management systems, responsible for regulating energy distribution on ships, have also been compromised through cyber incidents. In one case, malware was introduced via a printer in an engine room, leading to power disruptions that could have severely impacted vessel operations. Disconnecting automated control systems when necessary and conducting regular cybersecurity assessments can help mitigate such risks. Similarly, propulsion and engine control systems, which ensure a vessel's mobility, have been affected by cyberattacks. A ransomware attack targeting propulsion software updates caused a vessel to lose propulsion control while navigating near the coast, highlighting the importance of manual operation capabilities and strict access control policies.

Satellite communication systems, essential for global maritime connectivity, have also faced targeted cyber incidents. A 2017 GPS spoofing incident in a strategically sensitive maritime region resulted in false vessel positioning, raising concerns about the reliability of satellite navigation. To counter such threats, vessels must maintain alternative communication methods, cross-check navigation data, and utilize authentication mechanisms for GPS signals. Additionally, weather monitoring systems, which support route planning and safe navigation, have been targeted through data manipulation and signal interference. A 2021 cyber incident involving unauthorized access to a national meteorological authority's data disrupted weather forecasting, emphasizing the need for secure data authentication, redundant communication channels, and crew training on meteorological observations.

The increasing reliance on digital systems within the maritime industry has led to heightened cybersecurity risks, including malware infections, GPS spoofing, ransomware, and unauthorized access to critical infrastructure. These threats have resulted in data breaches, false navigational data, loss of control over vessel systems, and operational disruptions, which can cause financial losses and safety

hazards. To address these challenges, the report underscores the importance of implementing cybersecurity best practices. Regular audits, crew training on cyber hygiene, enhanced network segmentation, and robust incident response plans are crucial to strengthening maritime cybersecurity. Collaboration among industry stakeholders is also essential to sharing threat intelligence and developing a proactive approach to mitigating cyber risks. By adopting these measures, the maritime sector can improve its resilience against evolving cyber threats and ensure the safety and efficiency of global maritime operations.