How Did They get Aboard my Ship? Analysing Vessel Cyber Incidents Using the Cyber Kill Chain

Jeroen Pijpker and Stephen McCombie
NHL Stenden University of Applied Sciences, Leeuwarden, The Netherlands

jeroen.pijpker@nhlstenden.com
stephen.mccombie@nhlstenden.com

Abstract: The Global Maritime Transportation System (GMTS) is increasingly reliant on digitized and interconnected systems. This trend also applies to one of the most essential elements of the GMTS, vessels themselves. The Maritime Cyber Attack Database (MCAD) contains listings of maritime cyber incidents from public sources, including those involving vessels. Utilizing MCAD in this paper, we categorize and analyse these specific listings related to vessels. Vessels have complex networks of Information Technology (IT) and Operational Technology (OT). In this paper, we further categorize and systematically analyse selected cyber-attacks against vessels with the Lockheed Martin Cyber Kill Chain. This work also shows a significant rise in attacks against vessels since 2016. These case studies help industry more clearly understand the specific tactics and techniques used in cyber-attacks on vessels.

Keywords: Maritime cybersecurity, Cyber kill chain, MCAD, GMTS

1. Introduction

The Maritime Sector is increasingly dependent on digital systems, this is also the case for perhaps the key element, vessels themselves. Vessels are becoming more reliant on digitized and interconnected systems to support the different onboard systems. Vessels are also increasingly using systems that rely on an Internet connection to operate. Thus, extending the attack surface of vessels and exposing new vulnerabilities in these cloud-based connections.

Modern vessels integrate IT and OT systems into a single ecosystem. The OT systems on a ship control essential functions, such as engine management, radar, and dynamic positioning. Many of these systems were designed with safety and reliability in mind, but not cybersecurity. The increasing digitalization of maritime operations has introduced vulnerabilities that adversaries can exploit in the vessel's complex network of IT and OT.

This work illustrates how cyber-attacks against vessels are crafted according to the steps of the Cyber Kill Chain. The Lockheed Martin Cyber Kill Chain framework is applied to model the sequence of events for selected attacks from the Maritime Cyber Attack Database (MCAD) relating to vessels (Maritime IT Security Research Group, 2025).

1.1 Related Work

The research area of maritime cybersecurity is relatively new and niche. That said, there is some focus in the literature about cyber-attacks on the maritime sector and vessels in particular.

The paper by Simola et al. 2023 (Simola, Pöyhönen and Lehto, 2023) discusses different cyber-attacks against the GMTS utilizing the MITRE ATT&CK framework to map threat actors' objectives. The paper provides an overview of 13 attacks on ports from 2013 to 2023 in most cases targeted by ransomware. Iqbal and Khan (Iqbal and Khan, 2021) discuss different cyber-attacks against GMTS and provide an overview of 13 attacks. Of these 13 attacks, two of them involved vessels. In one case, a cyber-attack was impacting the shipboard network, and the case was investigated by the US Coast Guard.

Other research focuses on the specific methods and possible defense measures. The paper written by Mraković and Vojinović (Mraković and Vojinović, 2019) discusses cybersecurity threats and attacks to the GMTS, highlighting 9 incidents including "NotPetya" malware incident which impacted maritime companies COSCO, Maersk, and others.

Farah et al. (Ben Farah *et al.*, 2022) gives a summary of 16 cyberattacks on the GMTS. One case of a spoofing attack carried out by a research team was just a proof of concept rather than a real incident. Five of the attacks involved vessels. Those vessel incidents included navigation systems attacks, a ransomware attack and a phishing attack. The paper written by Schwarz et al. (Schwarz, Marx and Federrath, 2021) provides a comprehensive analysis of information security incidents in the GMTS over the previous 20 years. It covers 90 publicly reported attacks and 15 proof of concepts, categorizing them into different threat categories. Many of the attacks involved vessels.

Meland et al. (Meland *et al.*, 2021) identified and analysed 46 cyber incidents in the GMTS, making a top-ten list of maritime cyber threats, ranging from threats in IT and OT systems, to economic fraud and manipulation of GNSS signals. Number one in the top-ten list is the exposed shipping company/carrier IT-systems. Oruc (Oruc, 2020) emphasizes the impact of cyber-attacks on the maritime industry due to its widespread use of information technology (IT) and operational technology (OT). Twenty-two maritime cybersecurity incidents were analysed that occurred between 2011 and 2019. Five of these were attacks on vessels. The vessels were targeted with malware, GPS jamming/spoofing and other undefined navigation attacks. Cichocki (Cichocki, 2023) discusses state-sponsored and organized crime threats to maritime transportation systems of the Ukraine. The focus is more on cyber warfare not directly related to maritime threats. In a study conducted by Jones et al. (Tam, Jones and Papadaki, 2016) they presented several scenarios to demonstrate possible cyber-attacks on vessels.

2. Background

2.1 Why is the GMTS so Critical and Vulnerable

The role of GMTS in the global economy is significant with over 80 percent of the world's cargo transported by ship (Bronk and deWitte, 2020) and representing 70 percent of global trade by value (Loomis *et al.*, 2021). At the same fleets are aging and their technology is aging with them and thus more vulnerable to cyber-attacks. 38 percent of oil tankers and 59 percent of general cargo ships are older than 20 years (Tam and Jones, 2018). Supply chains are increasingly impacted by cyber-attacks. This is particularly stark in recent years with a four fold increase in supply chain cyber-attacks in 2021 compared to 2020 (Kessler and Shepard, 2020). The GMTS is a key part of global supply chains.

Many vessels have vulnerable legacy systems and using Operating Systems (OS) that themselves are no longer under support. These legacy systems have many published vulnerabilities with exploits available. Even newer systems are delivered on outdated OS due to the costs of re-engineering to suit more modern OS versions. Physical access to vessels is limited for remediation. As a result, vessels are often only available for updating and patching due to small windows they spend in their home port. There is also limited IT expertise on board and functions related to IT often are only part-time responsibility for those involved. Naturally, cybersecurity expertise is usually not present on board. VSAT systems used for vessels are also poorly maintained and have been targeted by various threat actors given their critical role in vessels. Network segmentation is primitive if it exists at all. While there is some monitoring of security events taking place it is the exception far from the rule.

2.2 Methodology

The methodology for this work was to firstly to identify and collect vessel cyber incidents where enough detail exists to categorize and summarize each incident according to the Cyber Kill Chain. MCAD is the primary data source utilized for this analysis.

2.2.1 MCAD

The authors and other researchers at NHL Stenden University of Applied Sciences in the Netherlands have compiled MCAD since 2021. MCAD catalogues cyber-attacks targeting the GMTS. Currently, MCAD has catalogued over 440 cyber incidents against GMTS dating back to 2001. The MCAD database is online and publicly available. MCAD contains listings of actual maritime cyber incidents from public sources, including those involving vessels. MCAD defines a cyber incident as a discrete malicious attack with a cyber element, perpetrated by a particular threat actor against one or more victims and causing significant impact on one or more victims, possibly over an extended period. A cyber incident is eligible for inclusion in MCAD if it involves at least one component of the GMTS, which is defined as a ''system of systems'' that encompasses several key components essential to global trade and mobility. At its core are port operations, where the loading, unloading, and transshipment of goods take place, and shipping lines, which facilitate the movement of cargo and passengers on designated routes. This system also integrates vessel traffic control systems, which monitor and direct maritime traffic to ensure safe and efficient operations, and vessels themselves—ranging from container ships to tankers and passenger liners—that transport goods and people across oceans. MCAD has 67 cyber incidents relating to vessels. The conversion to cyber kill chain included all the relevant information from the various sources and listed in MCAD.

3. Cyber Attack on Vessels

Per Figure 1, we have extracted all maritime cyber incidents relating to vessels from MCAD and there are 67 cyber incidents falling into 7 category types. The top three are related to navigation AIS/GPS Spoofing (25), Going

Dark (15) and GPS Jamming (12). Then two categories related to malware, Ransomware (4) and Other Malware (3). Lastly Hacking (6) and Other (2). The number of cyber-attacks has been significantly increasing over time. Between 2001-2015 (14 years) there were only 7 incidents while between 2016-2025 (9 years) there were 60.

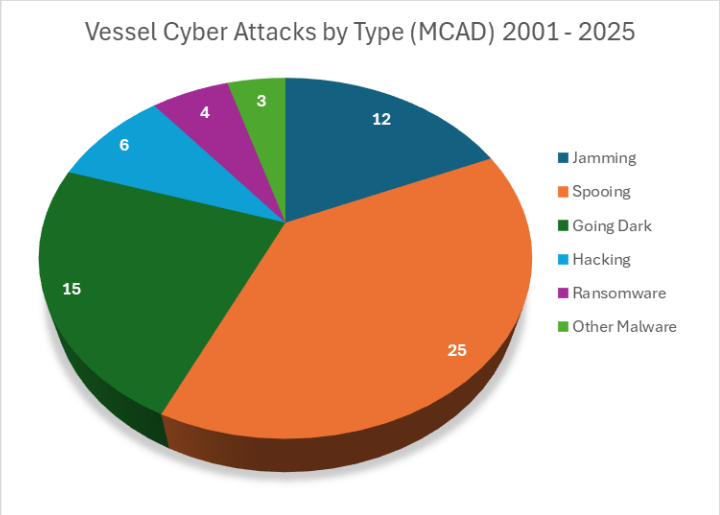

Figure 1 The figure represents MCAD cyber incidents from 2001-2025 relating to vessels.

4. Cyber Kill Chain

Cyber Kill Chain was developed by Lockheed Martin in 2011 (Hutchins, Cloppert and Amin, 2011). The Cyber Kill Chain is part of the Intelligence Driven Defense model for identifying and preventing cyber intrusion activity, identifying what a threat actor must complete in order to achieve their goals. The cyber kill chain helps in analyzing how an attacker must successfully and consecutively progress through all seven stages to successfully complete a cyber-attack. The seven stages of the cyber kill chain are defined as Reconnaissance, Weaponization, Delivery, Exploitation, Installation, Command and Control (C2) and Actions on Objectives. In a study conducted by Bahrami et al. (Bahrami *et al.*, 2019), a Cyber Kill Chain taxonomy is presented based on a large-scale analysis of attacks from 40 APT campaigns. The taxonomy captures the TTPS utilized by attackers. This taxonomy can help by choosing the right terminology in the kill chain analysis.

5. Case Studies

5.1 Selection of Case Studies

The cyber incidents are described based on the information in the MCAD (Maritime IT Security Research Group, 2025). The selected incidents are shown in Table 1. For each selected incident, there is a table mapping the event to the Cyber Kill Chain Table 2 - Table7. The selection of these six specific case studies was made based on the availability of information required for the Cyber Kill Chain framework. The selected cases (Table 1) range from physical breaches through USB and remote phishing to signal spoofing.

Table 1: Selected vessel cyber incidents from MCAD for analysing

Year	Incident	Impact area	Incident location	Method	References
2018	New-build dry bulk ship in port hit by ransomware attack	Vessel	not available	MalwareRansomware	(Safety4Sea, 2018; SecureWorld, 2018; ZDNet, 2018; Akpan, 2022)
2019	Two ships hit by ransomware attack	Vessel	not available	Malware Ransomware	(Abrams, 2018; Meland *et al.*, 2021; Akpan *et al.*, 2022)
2019	Chinese Hackers Targeting Ships Across Europe with Malware on USB Sticks	Vessel	Norway, Greece, Netherlands	Malware	(News, 2024; SupplyChainBrain, 2024; The Maritime Executive, 2024)
2025	Hacktivists Disrupt Communications of Iranian Oil Tankers	Vessels	Persian Gulf	VSAT hacking	(Cydome, 2025)

Year	Incident	Impact area	Incident location	Method	References
2012	USS Harry S Truman Insider Attack	Nuclear Aircraft Carrier	Atlantic Ocean	SQL Injection	(Naked Security, 2014; U.S. Attorney's Office, Northern District of Oklahoma, 2014; Zetter, 2014)
2018	Stena Impero GPS Spoofing	Vessel	Strait of Hormuz	GPS Spoofing	(Androjna and Perkovič, 2021)

5.2 Case Study 1: New-build dry Bulk Ship in Port hit by Ransomware Attack

In 2018, a bunker surveyor on a new build ship inserted a USB thumb drive into an onboard computer and unwittingly introduced malware onto the ship's administrative network which executed a ransomware attack. (Safety4Sea, 2018, 2018; SecureWorld, 2018; ZDNet, 2018; Akpan, 2022). The malware went undetected until a cyber assessment was conducted on the ship later after the crew reported a computer issue affecting the business network. The ship owner paid the ransom. The mapping of the Cyber Kill Chain to Case Study 1 is displayed in Table 2.

Table 2: Case Study 1 Mapped to Cyber Kill Chain

Stage	Mapping to the incident
Reconnaissance	The attacker carried out none due to limited surveillance. This can be seen as opportunistic infection via third-party USB device.
Weaponization	The malware was preloaded on the USB drive, likely due to an earlier infection on the surveyor's computer.
Delivery	Delivery of the malware took place through the use of the USB device into the computer in the engine room.
Exploitation	The malware had the opportunity to spread because the system allowed the use of untrusted removable media devices, and there is a likelihood of auto-executing upon insertion due to outdated OS or autorun settings.
Installation	The malware was able to install itself on the administrative network, spreading to the connected business network.
Command and Control (C2)	The cyber incident does not mention anything related to communication. But there is always the possibility that the malware has connected to a command and control, for example, for further instructions.
Actions on Objectives	The business network was disrupted, leading to delays and the ransom was paid. The recovery costs were totalled at around $100,000.

5.3 Case Study 2: Two ships hit by Ransomware Attack

In 2019, two ships were hit by simultaneous ransomware attacks. The infection came as a macro-enabled Word document attached to an email, and multiple workstations on the administrative networks were affected (Abrams, 2018; Meland *et al.*, 2021; Akpan *et al.*, 2022). When these emails were opened, they installed the AZORult information-stealing Trojan and the Hermes 2.1 ransomware onto the recipient's computer. All versions of Hermes (2.0 \& 2.1) Ransomware avoid infecting Russian, Ukrainian and Belarusian netizens. The result of mapping the Cyber Kill Chain to Case Study 2 is displayed in Table 3.

Table 3: Case Study 2 Mapped to Cyber Kill Chain

Stage	Mapping to the incident
Reconnaissance	Probably minimal reconnaissance from the attacker in this situation. The attackers probably performed broad targeting using an email address list of (maritime) companies or staff
Weaponization	Word document (named: Invoice.doc) was weaponized with the AZORult Trojan and the Hermes 2.1 ransomware
Delivery	Delivered via phishing spam campaign with email subject "Invoice Due". The email contained a password protected malicious attachment.
Exploitation	The exploitation took place through user interaction. 1. Entering the password ('1234') 2. Clicking "Enable Content" allowed macros to be executed.
Installation	The AZORult Trojan (azo.exe) downloaded and started executing. Next step was the downloading of the Hermes 2.1 ransomware (hrms.exe).

Stage	Mapping to the incident
Command and Control (C2)	AZORult established an outbound communication channel for callback traffic. Possible exfiltration of credentials, session info, or host data.
Actions on Objectives	The Hermes 2.1 encrypted data on the target system. It showed a ransom note (DECRYPT_INFORMATION.html). The Hermes 2.1 ransomware avoided infecting Russian, Ukrainian, and Belarusian netizens.

5.4 Case Study 3: Chinese Hackers Targeting Ships Across Europe with Malware on USB Sticks

In early 2024, Mustang Panda, a Chinese threat actor, targeted cargo shipping companies in Europe using Korplug loaders (ESET Research, 2024; News, 2024; SupplyChainBrain, 2024; The Maritime Executive, 2024). These loaders, dropped from USB drives with suspicious filenames, compromised systems in Norway, Greece, and the Netherlands. Some malware samples were blocked, but others had altered signatures and utilized DLL hijacking. The result of mapping the Cyber Kill Chain to Case Study 3 is displayed in Table 4.

Table 4: Case Study 3 Mapped to Cyber Kill Chain

Stage	Mapping to the incident
Reconnaissance	Targeted European cargo shipping companies. Specific victims in Norway, Greece, and the Netherlands.
Weaponization	Korplug (PlugX) malware was packaged with custom loaders and suspicious filenames. DLL hijacking was used to bypass defences.
Delivery	The malware was delivered through an infected USB thumb drive.
Exploitation	The execution of the payload started when files on the USB were opened. The attack relied on user interaction or autorun setting. Through DLL hijacking exploited further system weaknesses.
Installation	Persistence was achieved through backdoors (e.g. PlugX), this enabled remote access to the infected machines.
Command and Control (C2)	Some of the acquired malware samples maintained communication with external servers controlled by the attacker. This enabled remote command and data exfiltration.
Actions on Objectives	Espionage, surveillance, with the exfiltration of sensitive data and operational data.

5.5 Case Study 4: Hacktivists Disrupt Communications of Iranian Oil Tankers

In March 2025 cybersecurity company Cydome reported that the anti-Iranian government hacktivist group "Lab Dookhtegan" ("sealed lips" in Farsi) claimed to have disrupted communications on over 100 oil tankers associated with Iranian government-linked company (Cydome, 2025). While Lab Dookhtegan did not disclose the specific methods used, it is believed they exploited vulnerabilities in the ships' satellite communication systems, such as VSAT terminals. These systems are known to be susceptible to cyber-attacks, especially when default passwords remain unchanged. From those systems, they can take complete control over all communications of the vessel and even spread out to the IT and OT systems. The result of mapping the Cyber Kill Chain to Case Study 4 is displayed in Table 5.

Table 5: Case Study 4 Mapped to Cyber Kill Chain

Stage	Mapping to the incident
Reconnaissance	Lab Dookhtegan identified Iranian government linked tankers probably through AIS data, IP ranges of SATCOM terminals (Shodan), or vendor documentation.
Weaponization	The attackers exploited the insecure SATCOM systems (e.g. default credentials, exposed web interfaces).
Delivery	Gained access through remote accessible SATCOM devices. Probably using known IP addresses and (default) login credentials.
Exploitation	Exploitation of default/weak passwords, remote shell access to SATCOM.
Installation	Possible creation of backdoors to maintain access. For example, installation of scripts, altering of startup job, or SATCOM config files.
Command and Control (C2)	Remote control through custom C2 channel.
Actions on Objectives	Disrupted vessel communication on 100+ ships. Ships are isolated at sea. Possibility of lateral movement to onboard IT/OT systems.

5.6 Case Study 5: USS Harry S Truman Insider Attack

In June 2012, a land based IT system of the United States Navy was impacted by a SQL hacking attack (Naked Security, 2014; Zetter, 2014; United States Department of Justice, 2015). The impact of hacking on the Navy-SWM system was theft of confidential information of approximately 220,000 Navy service people who were being transferred. As a result, Navy-SWM system was shut down and never resumed operation. The incident caused a loss to the Navy of approximately USD$514,000. The US Naval Criminal Investigation Service (NCIS) worked out the attack was executed from onboard a US Navy nuclear aircraft carrier, the USS Harry S. Truman, which was at sea at the time. The threat actor they determined was a serving US Navy sailor; Nicholas Paul Knight whose job onboard was to run the IT Network for the nuclear reactor. The surprising thing is not the attack on the US Navy system but the fact it was executed from aboard a US Navy ship. Thus, the compromise most significantly was of the USS Harry S. Truman by an insider. The result of mapping the Cyber Kill Chain to Case Study 5 is displayed in Table 6.

Table 6: Case Study 5 Mapped to the Cyber Kill Chain

Stage	Mapping to the incident
Reconnaissance	Knight was a Navy systems administrator aboard the USS Harry S. Truman. As an administrator, Knight had privileged internal access and knowledge about the onboard and Navy systems.
Weaponization	SQL injection was used to hack the US Navy's SWM database.
Delivery	SQL code injection took place within the Navy-SWM system.
Exploitation	SQL Injection enabled unauthorized queries which were able to extract personnel records form Navy-SWM database.
Installation	No known installation of malware.
Command and Control (C2)	Threat actor had admin access to his own systems and compromised access to the victim system. So, command and control was direct not via a botnet or other intermediary system.
Actions on Objectives	Personal data from over 220,000 service members was stolen and posted online. The Navy-SWM platform was prematurely shutdown, over 700 deployed overseas Service Members could not access logistical support for transfers for more than 10 weeks. Team Digi7al's Navy-SWM hack caused a loss to the US Navy of approximately USD$514,000.

5.7 Case Study 6: Stena Impero GPS Spoofing

In July 2019, the British-flagged tanker Stena Impero fell victim to a GPS spoofing incident in the Strait of Hormuz, Iran, resulting in the vessel violating Iranian territorial waters (Androjna and Perkovič, 2021). Subsequently, the vessel was seized by Iran's Revolutionary Guards and it has been reported that Iran and/or Russia were involved in purposefully spoofing the ship, so it strayed into Iranian waters. The result of mapping the Cyber Kill Chain to Case Study 6 is displayed in Table 7.

Table 7: Case Study 6 Mapped to the Cyber Kill Chain

Stage	Mapping to the incident
Reconnaissance	Target vessel, identifying its routes and possible geopolitical opportunities.
Weaponization	Spoofed GPS signal and possible AIS data spoofing/tampering
Delivery	Broadcasting of fake navigation signals
Exploitation	The shipboard equipment receives fake signals.
Installation	Deception becomes persistent. Spoofed location
Command and Control (C2)	Continues signal GPS spoofing
Actions on Objectives	Vessels enters Iranian waters and is taken over.

6. Discussion

The six case studies illustrate the varying nature of cyber-attacks on vessels. Applying the Cyber Kill Chain to the selected case studies indicates that vessels can be compromised via conventional IT attack vectors rather than via zero-day exploits. Reconnaissance is minimal for most attacks, except in geopolitically motivated incidents with the Stena Impero. Most attacks are opportunistic; attackers instead rely on broad targeting or accidental infection. Analysis of the Reconnaissance and weaponization phases shows that, for the selected case studies, threat actors do not need to develop specialized, maritime-specific code to breach a vessel. They can weaponize

standard available malware, such as the AZORult Trojan or generic ransomware, to carry out their attack. Looking at the delivery methods used in the attacks, we see both opportunistic infections and targeted state-sponsored campaigns that utilize USB drives to bridge air-gapped systems. Phishing remains an effective method. Phishing is also in the GMTS an effective method, primarily because it exploits the human element in the exploitation phase. The success of the techniques used in the exploitation phase depends on the still existing legacy systems on board some older vessels. Outdated features, such as autorun for USB devices, still exist. Examining the installation phase showed in the different case studies that attackers rarely require sophisticated persistence mechanisms. In some case studies, the malware successfully executed because onboard systems permit untrusted code to run, lack application whitelisting, and operate on legacy configurations. Command and Control (C2) phase showed two different patterns. Malware was able to establish an outbound connection due to the limited logging and monitoring on the vessels. The other, more advanced incidents include VSAT compromises, which enabled remote access through misconfigured satellite communications systems. So the lack of visibility means that C2 is mostly undetected. When examining the Actions on Objectives, incidents range from financial crime to geopolitical disruption. In the case of the Stena Impero, GPS spoofing caused the vessel to enter Iranian waters. Lack of network segmentation enabled malware to move from the engine room to the administrative network. The case studies examined highlight recurring technical weaknesses: reliance on removable media, minimal network segmentation, legacy systems, and insufficient access control. Summarizing the weak points, the GMTS must, for example, enforce removable media policies, network segmentation and harden systems against unauthorized access.

7. Conclusion

This work explored the mapping of maritime cybersecurity incidents from MCAD to the cyber kill chain. These maritime cybersecurity incidents are publicly documented and have multiple sources. The analysis of vessel specific cyber incidents with the Cyber Kill Chain reveals several behavioural patterns. The case studies used in this work range from opportunistic infections to highly sophisticated, targeted campaigns. This work illustrates that attackers are able to exploit a combination of technical weaknesses and human factors to gain access to shipboard systems. The Cyber Kill Chain proves to be a valuable tool for analyzing maritime cybersecurity incidents. The discussion also highlighted the persistence of legacy systems onboard and unpatched vulnerabilities, allowing conventional IT threats to get to the OT segment of the network. A key conclusion from the research is the fact that it is difficult within the GMTS to be able to detect and respond to threats in real time. This comes because of the nature of the vessels. Poor network segmentation, outdated systems, and a lack of cyber hygiene aboard a vessel can play a crucial role in cyber incidents. Further work will explore the use of a ship honeynet (McCombie and Pijpker, 2022; Pijpker and McCombie, 2023) to better understand the tactics, techniques and procedures (TTPs) used in cyber-attacks on vessels. This can help better understand the attacker's behaviours and can in the future also be mapped to frameworks like MITRE ATT&CK. The efforts will contribute to a more resilient maritime cybersecurity posture.

AI Declaration: Artificial intelligence tools (e.g., Grammarly) were used to assist in editing and improving the language of this paper. The authors are fully responsible for the content, analysis, and conclusions.

Ethics Declaration: This research did not require ethical clearance as it did not involve human participants, personal data, or animal experiments.

References

Abrams, L. (2018) "Beware of Spam with Fake Invoices Pushing Hermes 2.1 Ransomware and AZORult," *BleepingComputer* [Preprint]. Available at: https://www.bleepingcomputer.com/news/security/beware-of-spam-with-fake-invoices-pushing-hermes-21-ransomware-and-azorult/.

Akpan, E. (2022) "Cyberattacks on Maritime Transportation Systems: A Threat to Global Supply Chains," *Journal of Marine Science and Engineering*, 2(1). Available at: https://www.mdpi.com/2673-8732/2/1/9/pdf.

Akpan, F. *et al.* (2022) "Cybersecurity Challenges in the Maritime Sector," *Network*, 2(1), pp. 123–138. Available at: https://doi.org/10.3390/network2010009.

Androjna, A. and Perkovič, M. (2021) "Impact of Spoofing of Navigation Systems on Maritime Situational Awareness," *Transactions on Maritime Science*, 10(2), pp. 361–373. Available at: https://doi.org/10.7225/toms.v10.n02.w08.

Bahrami, P.N. *et al.* (2019) "Cyber kill chain-based taxonomy of advanced persistent threat actors: Analogy of tactics, techniques, and procedures," *Journal of information processing systems*, 15(4), pp. 865–889.

Ben Farah, M.A. *et al.* (2022) "Cyber Security in the Maritime Industry: A Systematic Survey of Recent Advances and Future Trends," *Information*, 13(1), p. 22. Available at: https://doi.org/10.3390/info13010022.

Bronk, R. and deWitte, P. (2020) "Maritime Cybersecurity: Meeting Threats to Globalization's Great Conveyor," in. Available at: https://doi.org/10.24251/HICSS.2020.240.

Cichocki, R. (2023) "State-Sponsored and Organized Crime Threats to Maritime Transportation Systems in the Context of the Attack on Ukraine," *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 17(3), pp. 717–721. Available at: https://doi.org/10.12716/1001.17.03.24.

Cydome (2025) *Lab Dookhtegan cyber attack on Iranian oil tankers disrupts operations*. Available at: https://cydome.io/lab-dookhtegan-cyber-attack-on-iranian-oil-tankers-disrupts-operations/.

ESET Research (2024) *APT Activity Report Q4 2023–Q1 2024: Iran-aligned Cyberattacks – Rise in Disruptive Operations*. ESET. Available at: https://web-assets.esetstatic.com/wls/en/papers/threat-reports/eset-apt-activity-report-q4-2023-q1-2024.pdf.

Hutchins, E.M., Cloppert, M.J. and Amin, R.M. (2011) "Intelligence-driven computer network defense informed by analysis of adversary campaigns and intrusion kill chains," *Leading Issues in Information Warfare & Security Research*, 1(1), p. 80.

Iqbal, Z. and Khan, M.K. (2021) "Maritime cybersecurity: Vulnerabilities and counter measures," *Journal of Contemporary Studies*, 9(II), pp. 42–58.

Kessler, G.C. and Shepard, S.D. (2020) *Maritime cybersecurity: a guide for leaders and managers*. Gary C. Kessler and Steven D. Shepard.

Loomis, W. *et al.* (2021) "Raising the Colors: Signaling for Cooperation on Maritime Cybersecurity."

Maritime IT Security Research Group (2025) "Maritime Cyber Attack Database (MCAD)," *NHL Stenden University of Applied Sciences* [Preprint]. Available at: https://maritimecybersecurity.nl/.

McCombie, S.J. and Pijpker, J. (2022) "A Ship Honeynet Project to Collect Data on Cyber Threats to the Maritime Sector."

Meland, P.Há. *et al.* (2021) "A Retrospective Analysis of Maritime Cyber Security Incidents," *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 15(3), pp. 519–530. Available at: https://doi.org/10.12716/1001.15.03.04.

Mraković, I. and Vojinović, R. (2019) "Maritime Cyber Security Analysis – How to Reduce Threats?," *Transactions on Maritime Science*, 8(1), pp. 132–139. Available at: https://doi.org/10.7225/toms.v08.n01.013.

Naked Security (2014) *Team Digi7al: US Navy hacker sentenced to 2 years in jail*. Available at: https://web.archive.org/web/20211018083537/https://nakedsecurity.sophos .com/2014/10/29/teamdigi7al-us-navy-hacker-sentenced-to-2-years-in-jail/.

News, N.B.C. (2024) "China-linked group uses malware to try to spy on commercial shipping, new report says," *NBC News* [Preprint]. Available at: https://www.nbcnews.com/news/world/china-linked-group-malware-spy-commercial-shipping-cargo-report-eset-rcna152129.

Oruc, A. (2020) "Claims of State-Sponsored Cyberattack in the Maritime Industry."

Pijpker, J. and McCombie, S.J. (2023) "A Ship Honeynet to Gather Cyber Threat Intelligence for the Maritime Sector," in *2023 IEEE 48th Conference on Local Computer Networks (LCN)*. *2023 IEEE 48th Conference on Local Computer Networks (LCN)*, pp. 1–6. Available at: https://doi.org/10.1109/LCN58197.2023.10223347.

Safety4Sea (2018) "BIMCO Guidelines on Cyber Security Onboard Ships." Available at: https://safety4sea.com/wp-content/uploads/2018/12/BIMCO-Guidelines-on-cyber-security-onboard-ships-2018_12.pdf.

Schwarz, M., Marx, M. and Federrath, H. (2021) "A Structured Analysis of Information Security Incidents in the Maritime Sector." arXiv. Available at: http://arxiv.org/abs/2112.06545 (Accessed: January 31, 2024).

SecureWorld (2018) "Ships at Sea: More Ways to Hack Them." Available at: https://www.secureworld.io/industry-news/ships-at-sea-more-ways-to-hack-them.

Simola, J., Pöyhönen, J. and Lehto, M. (2023) "Smart Terminal System of Systems' Cyber Threat Impact Evaluation," *European Conference on Cyber Warfare and Security*, 22(1), pp. 439–449. Available at: https://doi.org/10.34190/eccws.22.1.1070.

SupplyChainBrain (2024) "Chinese Hackers Targeting Ships Across Europe With Malware on USB Sticks," *SupplyChainBrain* [Preprint]. Available at: https://www.supplychainbrain.com/articles/40018-chinese-hackers-targeting-ships-across-europe-with-malware-on-usb-sticks.

Tam, K., Jones, K. and Papadaki, M. (2016) "Threats and Impacts in Maritime Cyber Security," *Engineering & Technology Reference*, 1. Available at: https://doi.org/10.1049/etr.2015.0123.

Tam, K. and Jones, K.D. (2018) "Maritime cybersecurity policy: the scope and impact of evolving technology on international shipping," *Journal of Cyber Policy*, 3(2), pp. 147–164. Available at: https://doi.org/10.1080/23738871.2018.1513053.

The Maritime Executive (2024) "Chinese Spy Malware Found in European Shipping Companies' Systems." Available at: https://maritime-executive.com/article/chinese-spy-malware-found-in-european-shipping-companies-systems.

United States Department of Justice (2015) *Northern District of Oklahoma | Former U.S. Navy Nuclear Systems Administrator Sentenced To 2 Years For Hacking The U.S. Navy And National Geospatial-Intelligence Agency Computer Systems | United States Department of Justice*. Available at: https://www.justice.gov/usao-ndok/pr/former-us-navy-nuclear-systems-administrator-sentenced-2-years-hacking-us-navy-and (Accessed: October 1, 2025).

U.S. Attorney's Office, Northern District of Oklahoma (2014) *United States of America v. Nicholas Paul Knight: Indictment*. Indictment Case No. 4:14-cr-00074-JHP. Tulsa, OK: U.S. District Court for the Northern District of Oklahoma. Available at: https://cdn.theatlantic.com/assets/media/img/posts/050514_Knight.pdf.

ZDNet (2018) "Ships infected with ransomware, USB malware, worms." Available at: https://www.zdnet.com/article/ships-infected-with-ransomware-usb-malware-worms/.

Zetter, K. (2014) “Network Admin Allegedly Hacked Navy—While on an Aircraft Carrier,” *WIRED* [Preprint]. Available at: https://www.wired.com/2014/05/navy-sysadmin-hacking/.