

37. Országos Tudományos Diákköri Konferencia
Had- és Rendészettudományi Szekció
Budapest, 2025. április 22–24.
Nemzeti Közzolgálati Egyetem
Hadtudományi és Honvédtisztképző Kar

**HAJÓZÁSI KIBERBIZTONSÁG ÉS A HAJÓZÁSI INCIDENSEK
NEMZETKÖZI KEZELÉSÉNEK STRATÉGIAI MEGKÖZELÍTÉSE**

HAJÓZÁSI KIBERBIZTONSÁG BEMUTATÁSA ÉS EGY NEMZETKÖZI
KIBER INCIDENS MEGOLDÁSA, AVAGY A CYBER 9/12 VERSENY
TANULSÁGAI

**MARITIME CYBER SECURITY AND A STRATEGIC APPROACH TO
THE INTERNATIONAL MANAGEMENT OF SHIPPING INCIDENTS**

Jelige: Ship

Kézirat lezárásának dátuma: 2024. 04. 18.

Table of Content

Table of Content

Abstract	4
1. ACM Classification.....	4
2. Introduction	5
2.1. Introduction to maritime.....	5
2.2. Introduction to maritime security	7
2.3. Cybersecurity in the maritime shipping	7
2.4. My motivation	8
2.5. Cyber 9/12 Description in Brief	9
3. Actuality of the Topic	10
3.1. Scientific Representation in MTMT 2024 April	10
3.2. Scientific Representation in IEEEExplore 2024 April	10
3.3. Scientific Representation in JSTORE 2024 April.....	11
3.4. Scientific Representation in Scopus 2024 April	12
4. Structure of Ships	12
4.1. Structure of maritime mechanics.....	12
4.2. Structure of maritime Information Technology Systems	12
4.3. Structure of maritime Cyber Security Standards.....	13
4.4. Structure of maritime Cyber Security Incidents and maritime weak point identification	13
5. Cyber 9/12 - Case Study.....	14
5.1. The scenario	14
5.2. Forensics.....	15
5.2.1. Introduction to cyber forensic	15
5.2.2. Forensic in the case study	16
5.3. Diplomacy in the cyber incident	16
5.3.1. Defence, Security and Geopolitics behind the sensitive case.....	16
5.3.2. Diplomatic interest in the decision making	16
6. Conclusion.....	17

7. Sources	18
Hivatkozások.....	18

Abstract

Cybersecurity in shipping is becoming increasingly critical in the modern shipping industry. Ships are increasingly digitalised with networked systems, increasing the vulnerability to cyber-attacks. Cyber attacks can have serious consequences, including compromised shipping safety, human casualties, environmental damage and economic losses.

Key factors affecting cyber security in shipping:

Digitalisation: ships are increasingly using networked systems such as navigation, engine control and load management systems.

Cyber threats: cybercriminals are launching increasingly sophisticated attacks to hack and compromise ships' IT systems.

State actors in cyberspace.

Human factor: the awareness and training of ship crews on cyber security is key to preventing attacks.

While shipping has been at the forefront of the Russia-Ukraine conflict in our neighbourhood, the detection and hijacking of ships has been reported in 14 active armed conflicts around the world. We have also seen that a ship stranded in the Suez Canal can cripple world trade!

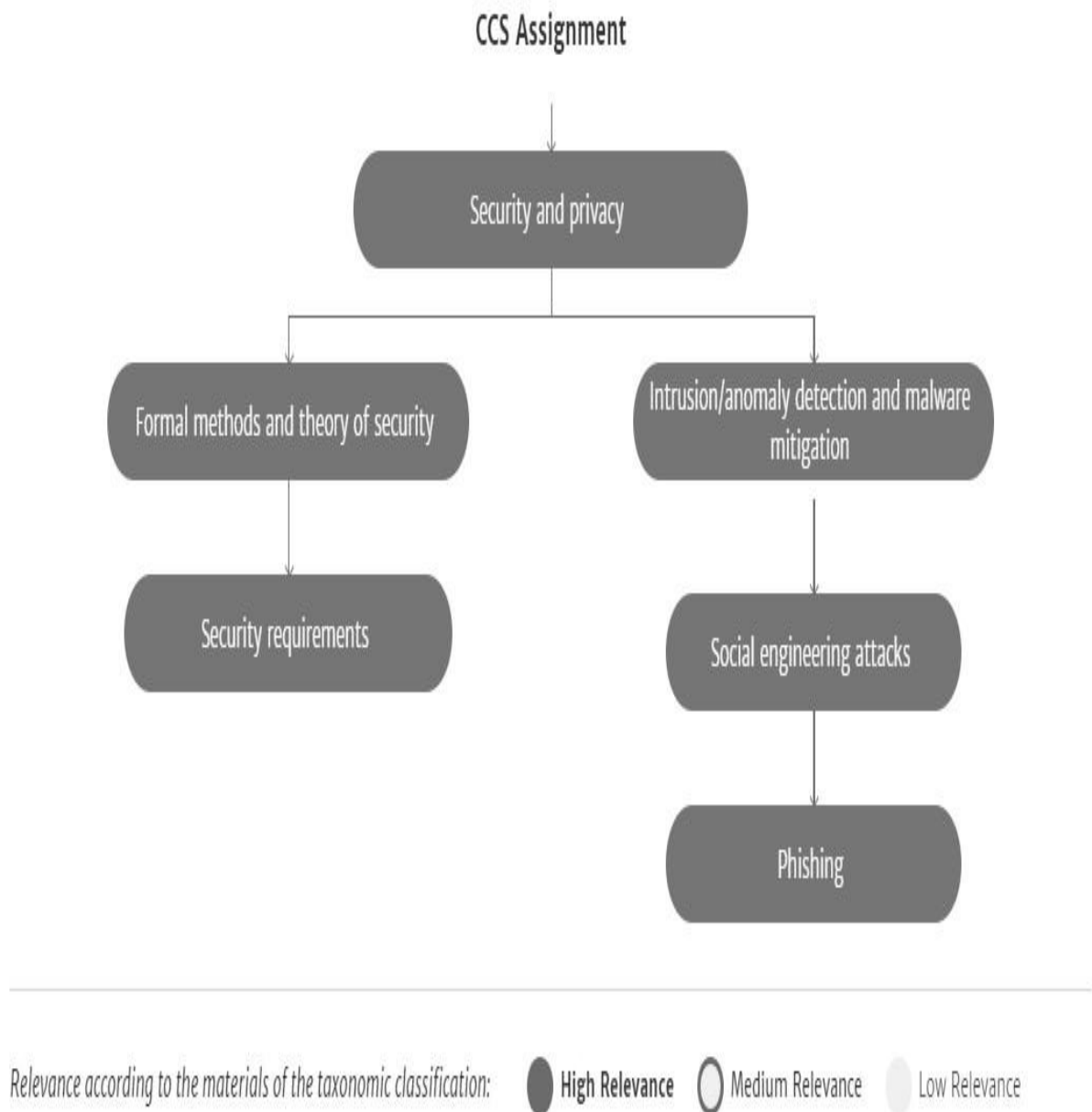
Ships are becoming more and more digital and any IT device can bypass their defences. The first aim of my thesis is to present the vulnerabilities on ships and the current defence systems.

The secondary purpose of my thesis is to share the experiences, simulations and case studies from the 2024 Cyber 9/12 International Cyber Security Strategy and Cyber Policy Competition, in which I participated with a team of professional students.

In the competition, we had to implement an incident management of an attack on a geopolitically sensitive ship in an international arena under the auspices of ENISA.

1. ACM Classification

Based on the recommendation of the National Council of Scientific Students (OTDT), I prepared a polyhierarchical ontology of my research in the ACM (Association for Computing Machinery) Computing Classification System (CCS).



2. Introduction

2.1. Introduction to maritime

Global trade, the cornerstone of the modern economic landscape, hinges on the efficient movement of goods across vast distances. At the heart of this intricate system lies maritime shipping, the lifeblood of international commerce responsible for transporting over 90% of the world's tradable goods [1, p. 12]. However, the successful navigation of this complex web extends beyond mere transportation. Maritime logistics, the intricate coordination of activities that ensures the seamless flow of cargo through maritime channels, plays a critical role in optimizing efficiency, minimizing costs, and mitigating risks [2].

This introductory section delves into the interconnected worlds of maritime shipping and maritime logistics. We begin by exploring the fundamental principles of maritime shipping, outlining the various vessel types, trade routes, and operational considerations that underpin this global industry. Subsequently, we will dissect the multifaceted domain of maritime logistics, encompassing activities such as port management, cargo handling, customs clearance, and supply chain integration. By elucidating the symbiotic relationship between these two disciplines, we aim to shed light on their combined significance in facilitating international trade and fostering global economic prosperity.

Maritime shipping is the most efficient and economical way to transport goods, thanks to the lower fuel consumption and emissions of waterborne transport compared to land-based alternatives [3]. The shipping industry is vast and complex, with tens of thousands of ships operating around the world, transporting billions of tonnes of goods every year [4]. The most common types of ships include container ships, which transport goods in standardised containers; tankers, which transport liquids such as oil and gas; bulk carriers, which transport dry goods such as grain and minerals; and passenger ships, which transport passengers.

Maritime shipping involves a global network of ports, shipping lanes and logistics centres. Ports are vital nodes in maritime transport where goods are unloaded, transhipped and distributed. Shipping lanes are defined to manage maritime traffic and prevent accidents. And logistics centres coordinate the different parts of the supply chain to ensure the smooth flow of goods from producer to consumer.

Maritime logistics is a key element in the efficient operation of maritime shipping. Maritime logistics activities include cargo handling, customs clearance, warehousing, transport and freight forwarding. A wide range of maritime logistics service providers are available to meet the specific needs of shippers. As technology advances, maritime logistics is becoming more sophisticated. Real-time tracking, electronic documentation and data-driven decision-making are just a few examples of the innovations that are revolutionising the field of maritime logistics.

Shipping and maritime logistics are inextricably linked and together they drive global trade. Shipping provides an efficient and economical mode of transport, while maritime logistics ensures the seamless flow of goods from the point of production to the point of consumption. Technological advances and the growth of global trade will continue to shape the future of maritime shipping and maritime logistics, ensuring that these sectors play a key role in the global economy.

2.2. Introduction to maritime security

Global commerce thrives on the uninterrupted flow of goods across vast oceanic distances. Maritime transportation, the lifeblood of this system, carries over 90% of the world's tradable goods [1]. However, this vital artery faces a multitude of threats, jeopardizing not only cargo but also crew safety, environmental well-being, and national security. Maritime security, therefore, emerges as a critical domain safeguarding the integrity and smooth operation of maritime activities.

Maritime security encompasses a broad spectrum of threats and corresponding countermeasures. Piracy, the age-old menace of armed robbery at sea, continues to pose a significant threat in certain regions. Modern pirates often operate in sophisticated vessels, targeting cargo ships and crews for ransom or stolen goods . [4]

Beyond traditional piracy, other security concerns loom large. Armed robbery at sea, distinct from piracy in terms of location and intent, involves opportunistic attacks on smaller vessels closer to shore [5]. Illegal, unreported, and unregulated (IUU) fishing poses a significant threat to marine ecosystems and undermines legitimate fishing practices. The International Maritime Organization (IMO) estimates that IUU fishing accounts for up to 26 million tons of fish annually, jeopardizing sustainable resource management [6].

Maritime terrorism, though less frequent, presents a devastating potential. Attacks on port facilities, cruise ships, or critical infrastructure can have catastrophic consequences. The 2000 bombing of the USS Cole in Yemen serves as a stark reminder of the vulnerabilities to terrorist actions. [7]

Countering these threats necessitates a multi-layered approach. International cooperation is paramount, with coastal states collaborating to patrol their territorial waters and share intelligence. The International Maritime Organization (IMO) plays a vital role in developing regulations and fostering cooperation among member states. [8]

Technological advancements also play a crucial role in maritime security. Automated identification systems (AIS) enable the tracking of vessels, while satellite imagery provides broader surveillance capabilities. Additionally, private security companies offer armed guards and other protective measures for vessels traversing high-risk areas. [9]

In conclusion, maritime security is an intricate and evolving field safeguarding the global maritime domain. By acknowledging the diverse threats and implementing a comprehensive strategy encompassing international cooperation, technological advancements, and robust regulations, we can ensure the continued safe and efficient operation of maritime transportation, the lifeblood of global trade.

2.3. Cybersecurity in the maritime shipping

The global economy hinges on the smooth operation of maritime shipping, which transports over 90% of the world's tradable goods [1]. However, this vital sector faces

a growing threat – cyberattacks targeting critical infrastructure and operational systems. Cybersecurity in maritime shipping has become an urgent concern, demanding immediate attention to ensure the safety, efficiency, and security of global trade.

The maritime industry presents a unique and vulnerable landscape for cyberattacks. Ships often operate in remote locations, with limited access to secure internet connections and IT expertise onboard. Additionally, legacy technology systems, some dating back decades, may lack the necessary security features to withstand modern cyber threats. [3]

The potential consequences of successful cyberattacks in maritime shipping are severe. Disruptions to shipboard systems, such as navigation and propulsion controls, can lead to collisions, groundings, and environmental disasters. Cybercriminals could also target cargo management systems, disrupting supply chains and causing economic losses.

Furthermore, attacks on port infrastructure, such as container terminals and vessel traffic management systems, could cause significant delays and disruptions to global trade. The potential for data breaches compromising sensitive commercial information or exposing personal data of crew members adds another layer of concern [10]

Several key areas require attention to enhance cybersecurity in maritime shipping. Modernizing onboard technology systems with robust security features and regular software updates is crucial. Investing in crew training on cyber hygiene practices and building awareness of potential cyber threats are equally important.

Additionally, the industry needs to adopt secure communication protocols and implement network segmentation to isolate critical systems from non-essential ones, minimizing the potential damage caused by an attack. Collaboration and information sharing among stakeholders, including shipping companies, port authorities, classification societies, and cybersecurity experts, is essential to develop effective strategies and share best practices [11].

Regulatory bodies also have a role to play. The International Maritime Organization (IMO) has developed guidelines and recommendations for cyber risk management in the maritime industry. Furthermore, national and regional regulations need to evolve to mandate minimum cybersecurity standards for ships and port infrastructure [8]

Cybersecurity in maritime shipping necessitates a proactive approach. By investing in secure technology, fostering cyber awareness among personnel, promoting collaboration across stakeholders, and establishing robust regulations, we can navigate the troubled waters of cyber threats, ensuring the continued safe, efficient, and secure operation of maritime transportation, the lifeblood of global trade. [12]

ezekhez a források:

2.4. My motivation

My motivation about maritime security come from the Cyber 9/12 competition organised by the Atlantic Council. In this year I had received the opportunity to participate in this competition and in this year the theme was based on a maritime cyber security incident scenario. Our team,

(which consisted of 4 members 1 international security and defence policy expert, 1 geopolitics and diplomacy expert, 1 military officer and me as a cyber security engineer) was tasked to handle an international cyber security incident where a Russian ship has been hacked and there were casualties. We tasked to collect evidence, find out what happened, with great respect to the diplomacies and international politics boggy ground, which made so much harder the technical work.

I really enjoyed this topic, and I decided I want to research the maritime security!

2.5. Cyber 9/12 Description in Brief

For years, policymakers have grappled with the potential consequences of a catastrophic cyberattack. Terms like "Cyber Pearl Harbor" or "Cyber 9/11" were frequently used in the United States to illustrate the potential severity of such an event. Recognizing this growing concern, the Cyber Statecraft Initiative launched the Cyber 9/12 Challenge in 2012. This initiative took the existing debate a step further, shifting the focus from simply imagining a "Cyber 9/11" to preparing future leaders for the aftermath – the "Cyber 9/12."

The Cyber 9/12 Challenge emerged from a critical question: how can we equip future cyber policy leaders to handle not just the initial cyber crisis, but also the complex issues that would arise in its wake? The competition program has blossomed into a globally recognized brand and experience for students interested in cyber policy, fostering their development over the past twelve years.

The Cyber 9/12 Challenge serves as a unique platform for students to test their critical thinking and policy development skills within a simulated large-scale cyber crisis scenario. By participating, students gain invaluable experience in strategic thinking, crisis management, and collaboration – all crucial components of effective cyber policy leadership. [13]

3. Actuality of the Topic

As the hackers get better and better and we also try to digitalise our ships this could only mean one thing. The attack rates will start to increase! Mission Secure stated that since 2020 February the increase in cyberattacks and attempts is 400% [1]. Through out this period the maritime industry loses \$1 trillion. To prevent this, we need to defend complex systems, with very limited human resources on board, which is pretty challenging.

Before my secunder research I conducted a scientific representation to get an overview about the research area and get quantitative results from it.

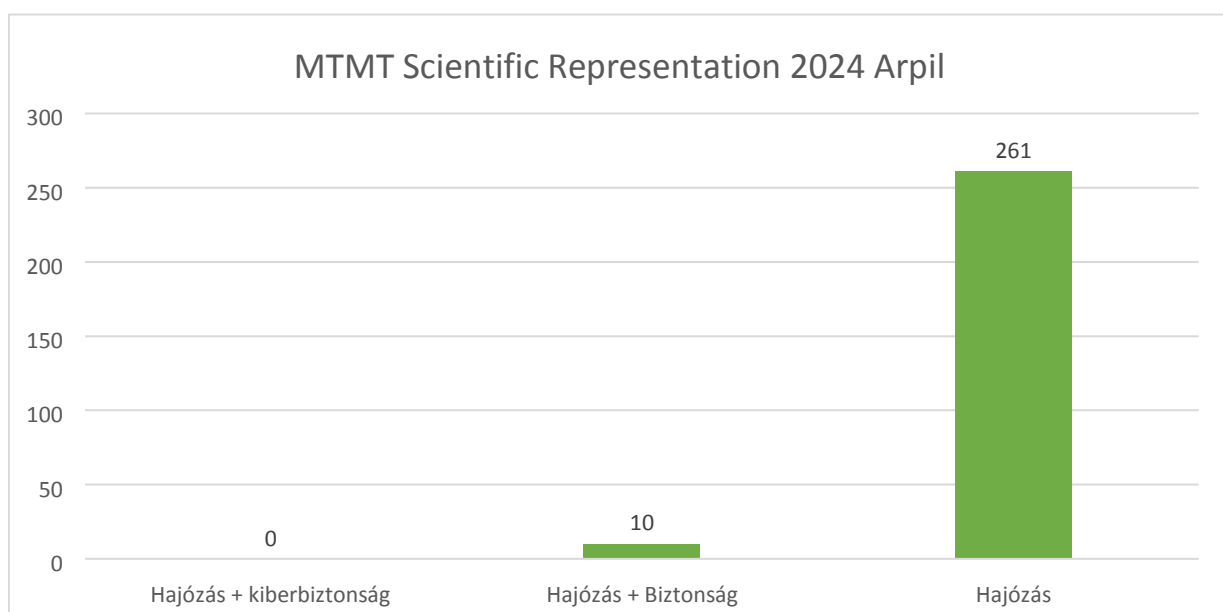
I conducted the scientific representation in 4 platforms. Frist in MTMT, because I was curious about the Hungarian perspective. I also used the IEEEExplore database, because as far as my prior knowledge this is the best indexing page at electrical engineering based topics. I also checked at Scopus and JSTORE databases.

3.1. Scientific Representation in MTMT 2024 April

In April 2024, I conducted a keyword search in the database of the Hungarian Library of Science. I searched for the following keywords together: “shipping + cyber security”.

Unfortunately, I could not find any results. The query for the “shipping + security” resulted in 10 articles and conference presentations. The query for “shipping” was the last keyword search that I had conducted which resulted in 261 indexes.

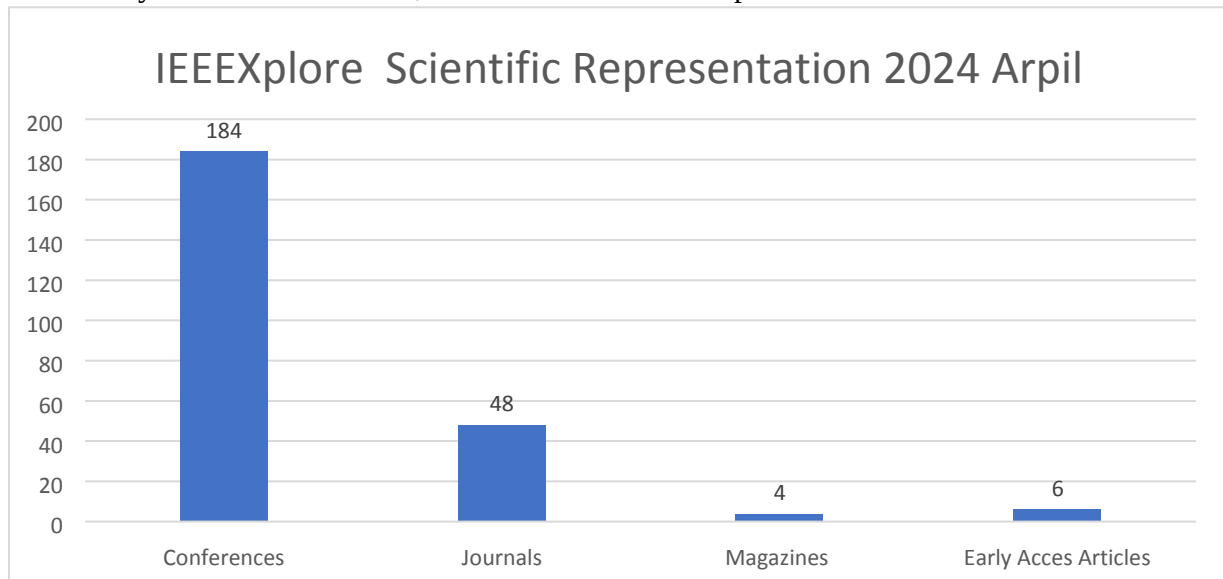
From these queries I get the conclusion that in 2024 April in Hungary this is not a wellresearched topic, which is not surprising, because Hungary is a landlocked country.



3.2. Scientific Representation in IEEEExplore 2024 April

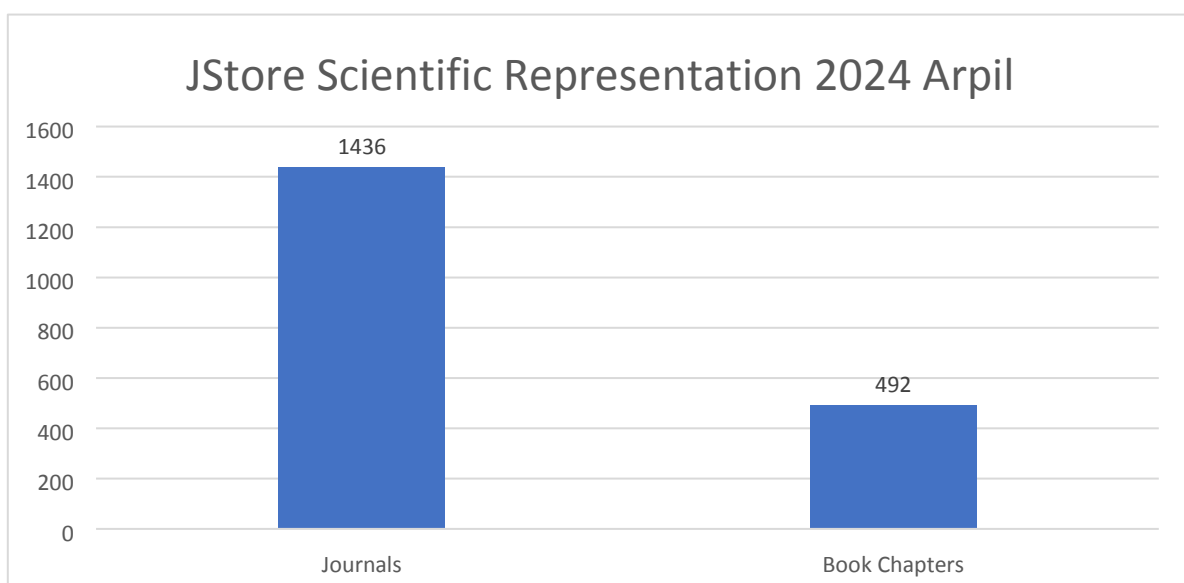
I conducted a search in IEEEExplore in 2024 April in advanced search mode with the following syntax: “(“All Metadata”:Maritime) AND (“All Metadata”:Cyber Security)”.

The results were 184 conference article, 48 journal article, 4 magazine article and 6 early access article. From this I could draw the conclusion that within the international electrical engineering community is a well-researched, but not a mainstream topic.



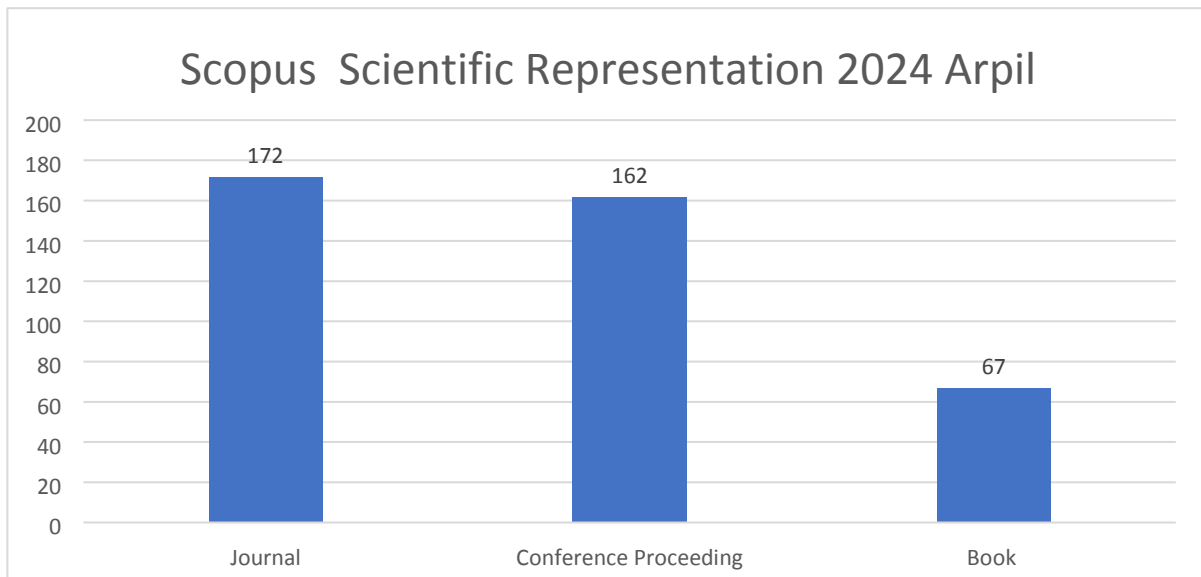
3.3. Scientific Representation in JSTORE 2024 April

I conducted the same type of search in JSTORE as well. With the search syntax: “Maritime Cyber Security”. I limited my search to the following science areas: Computer Science, Engineering, Military Studies, Science and Technology Studies and Security Studies. With this query I got 1436 matching within journals and 492 book chapters as it could be seen in the graph below.



3.4. Scientific Representation in Scopus 2024 April

I conducted the same type of search in Scopus as well. With the search syntax: “Maritime Cyber Security”. With this query I got 172 matching within journals and 67 books as well as 162 conference proceedings as it could be seen in the graph below.



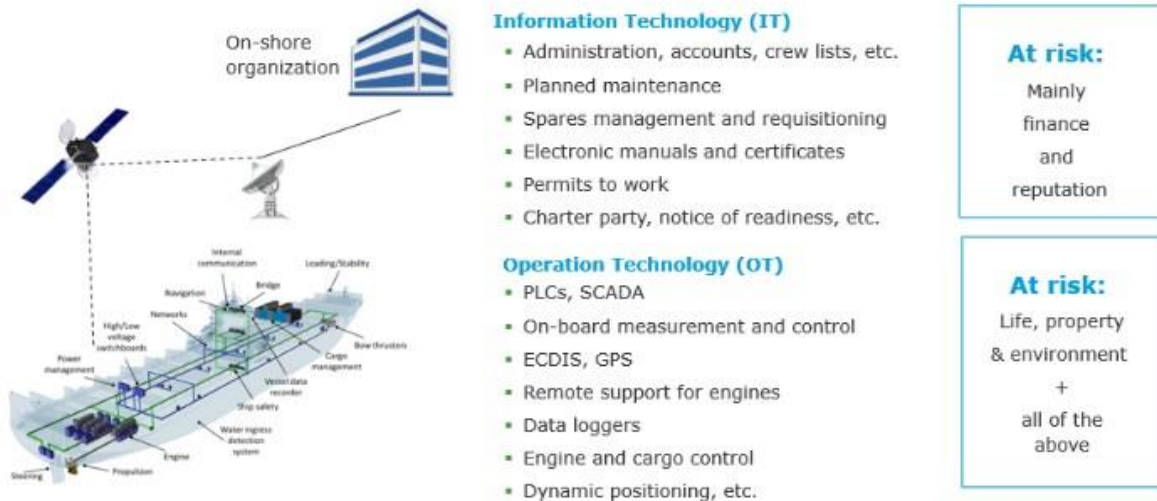
From this scientific representation we could draw a conclusion that this is a well-researched topic in the international field, but due to the increasing threats it is beneficial to conduct research at this field.

4. Structure of Ships

4.1. Structure of maritime mechanics

4.2. Structure of maritime Information Technology Systems

There are Information Technology (IT) Systems and Operational Technology (OT) Systems on a ship, which are different. OT systems need to work 24/7 to get the ship moving, while the IT systems are mainly for administration and other higher-level tasks. The IT systems have the widely known CIA triad guide policy (Confidentiality, Integrity, Availability) where the OT systems use the CAIC model (Control, Availability, Integrity, Confidentiality).



[2]

4.3. Structure of maritime Cyber Security Standards

The International Maritime Organization (IMO) provided a document in 2021 called “Guidelines on cyber risk management in the maritime industry” which sets the guidelines for managing cyber risks, and incident response.

4.4. Structure of maritime Cyber Security Incidents and maritime weak point identification

The following systems use some kind of network on a ship, and they are potentially vulnerable:

1. Bridge Control

1.1. Bridge systems, automatic identification system (AIS), voyage data recorder (VDR), automatic radar plotting aid (ARPA)

2. Propulsion & Power

2.1.1. Engine control, steering, fuel management, onboard machinery monitoring and control, generators

3. Navigation

3.1.1. GPS/GNSS, electronic chart display and information system (ECDIS), radar, weather systems

4. Loading & Stability

4.1. Ballast systems, hull stress, stability control, stability decision support systems, cargo management systems

5. Safety Systems

5.1. Fire and flood control, tracking, shipboard security, CCTV, emergency shutdown

6. Communications

6.1. Satellite internet communications, ship-to-shore, ship-to-ship, handheld radios, voiceover-IP (VoIP)

7. Operations Security

- 7.1. Human-machine interfaces (HMIs), logic controllers (PLCs), digital and analog sensors, electronics

8. Network Security

- 8.1. Firewalls, segmentation devices, antivirus software, software updates, vendor patches

9. Physical Security

- 9.1. Server rooms, access control, bridge, machinery spaces, network infrastructure

10. Ship Networks

- 10.1. Email, customs and immigration, personnel administration, maintenance and spares management

11. Crew Network

- 11.1. Email, Wi-Fi, wired, bring your own device (BYOD)

12. Supply Chain

- 12.1. Remote or onshore vendor updates, maintenance, and administration

[2] [14]

5. Cyber 9/12 - Case Study

5.1. The scenario

This scenario description is based on the Atlantic Councils Cyber 9/12 Intelligence Report 2024: A Russian scientific vessel stuck in ice near the north pole in a series of daring helicopter operations Norway managed to evacuate 22 crew members. The crew members were aboard the vessel Severny Polyus, a Russian scientific research platform.

After performing geological mapping in the Barents Sea, the ship was intentionally frozen into the ice above Norway's Svalbard archipelago, some 250 nautical miles from the North Pole, to conduct its over-winter Arctic research.

Sometime late Friday night, an unknown incident rendered the ship's HVAC systems nonoperational. At the request of Russian authorities, Norway dispatched a set of Super Puma helicopters from Longyearbyen, the main town on Svalbard some 500 nautical miles away, to evacuate the crew. The operation was carried out in accordance with Norwegian-Russian bilateral accords on Arctic search and rescues, and despite a cooling of relations between the two countries since the start of Russia's war in Ukraine.

The evacuated Russian crew members arrived in Longyearbyen and were transferred to medical plane headed for the Norwegian mainland. Details of their condition, and of the causes of the failure of systems aboard the vessel, were not known.

Press Release from The Ministry of Foreign Affairs of the Russian Federation:

“Press release on attack on Arctic research vessel Severny Polyus An unwarranted and malicious cyber-attack against the Arctic research vessel Severny Polyus violated principles of Arctic cooperation and led to an unacceptable loss of Russian life. The attack, which compromised the vessel's operational controls, including its autonomous navigation system and temperature control systems, left the vessel's crew and researchers stranded in treacherous Arctic conditions, and destroyed significant portions of vital scientific data, undermining years of dedicated research and cooperation in the Arctic region. The Russian Federation condemns this attack in the strongest possible terms. Such reckless actions not only endanger lives but also the invaluable scientific research critical to understanding our changing world. We are initiating a thorough investigation to identify and bring to justice those responsible for this act of sabotage. It is imperative to note the unfortunate history of attacks on Russian scientific endeavors by hackers affiliated with the Ukrainian armed forces. Whether or not such a link is substantiated, the Russian Federation calls upon the international community, in particular those members of the Arctic Council, to join us in condemning this attack, its perpetrators, and any other collaborators who may have supported and participated in this act. Without strong international unity, it will be impossible to cooperate in ensuring the safety and security of scientific research missions in the Arctic and worldwide.” [4, pp. 8-20]

5.2. Forensics

5.2.1. Introduction to cyber forensic

Cyber forensics is the scientific process of collecting, analyzing, and preserving digital evidence from electronic devices and computer networks [5]. It aims to reconstruct past events related to a cybercrime and provide compelling evidence that can be presented in court [6]. Imagine it as digital detective work, meticulously following the electronic footprints left behind by cybercriminals.

The process typically involves multiple stages [6]:

Identification: Recognizing and securing potentially relevant digital evidence.

Collection: Carefully extracting the evidence while maintaining a chain of custody to ensure its integrity.

Analysis: Examining the evidence using specialized tools and techniques to uncover incriminating information.

Reporting: Documenting the findings and presenting them in a clear and concise manner suitable for legal proceedings.

Cyber forensics professionals, often referred to as cyber forensic investigators, possess a unique blend of skills. They need a strong understanding of computer science and digital technology, coupled with investigative prowess and a keen eye for detail [7]. They are also well-versed in legal procedures and digital evidence handling protocols [7]

5.2.2. Forensic in the case study

The proposal option in the brief:

The forensic investigation would be conducted by deploying the EU ENISA Joint Cyber Unit (JCU) to the scene of the incident, interviewing researchers, involved stakeholders, and obtaining information from civilian companies and EU member states through the EU CyCLONe platform. Leveraging the Cyber Solidarity Act, ENISA can broaden its investigation by engaging civilian cyber threat intelligence (CTI) companies and non-member states, while also utilizing EU CyCLONe, as authorized by NIS2, to gather additional intelligence on potential cyber incidents in the Arctic region that could validate or contradict Russian claims. Ultimately, by comprehensively analyzing all accumulated technical data, investigators can determine with greater certainty whether the ship was indeed the target of a deliberate cyberattack.

The JCU must board on the vessel and need to collect all available log files and metadata that is available and also look for signs of deleted files in the file system. JCU must inspect the OT systems that has controlled the HVAC systems, but also need to identify the way where the attack could come from! Because from the intelligence report we can see that the Russians blaming the Ukrainian IT army, which is heavily specialized in Social Engineering within that phishing campaigns, the email server should be investigated also.

From the forensic perspective it is important to get seconder sources as well. The email security gateway has CTI capabilities and the ENISA need to have information from the vendor that this kind of attack could happened in their device or not.

5.3. Diplomacy in the cyber incident

5.3.1. Defence, Security and Geopolitics behind the sensitive case

This incident was very sensitive, because the scenarios description mentioned that the Russian – Ukrainian conflict has not been resolved and the fact that a Russian researcher died because of the cyber attack against the ship makes it difficult to find the right path. The situation could be easily escalated into a bigger conflict, and we also don't want Russian aggression in the northern part of the EU.

5.3.2. Diplomatic interest in the decision making.

From the technical and engineering perspective this is a challenging forensic task, but what also made this more challenging is the fact that the Russians DO NOT want nobody on their vessel, especially the ENISAs Joint Cyber Unit where they are basically breaking into the vessels system. This could easily lead to an escalation and the decision makers might not want to interfere with Russians by diplomatic and security reasons and maybe the only case is when we ask Russia about the information that they gathered. Which might not be the most reliable information source.

Our team proposed two options:

“Proposed Alternatives:

- (a) Deploying the EU Joint Cyber Unit to Norway to conduct an independent technical investigation of the incident, interviewing the researchers and involved stakeholders, obtaining information from civilian companies, and EU member state through EU CyCLONe.

(b) Focusing the efforts on developing a transparent information sharing between the parties concerned (Ukraine, Russia, Arctic Council). Endorsing a diplomatic solution to the case at hand. ” [8]

Alternative A)	
Strengths	Weaknesses
Immediate action Direct evidence	Possibly inadequate cooperation
Expanding intersectoral cooperation	Possible escalation
Opportunities	Threats

Alternative B)	
Strengths	Weaknesses
Mediation Preventing escalation	Only diplomatic solution
Broadening international cooperation	No direct evidence
Opportunities	Threats

6. Conclusion

We can draw a conclusion from this case study that a problem which from first view is just a technical problem could escalate to the geopolitical level and the engineers needs to understand that not only the technical details matter. In these sensitive cases we need to navigate through not only just the technical details, but the soft areas of the cyber space as well!

In the era of Industry 5.0 it is really crucial to defend everything in the ship, because in the maritime area. We could see that this is the era of the autonomous vehicle.

In modern ships there are a lot of equipment that help the staff to sail the boat and just in no time due to the increase technology development speed there will be autonomous ships and that is a cyber security threat, because at today, the ships could be hacked easily.

I would like to thanks for Dr. Csaba Krasznay Associate Professor for mentoring our team!

7. Sources

Hivatkozások

- [1] M. Stopford, „Maritime economics (3rd ed.),” Routledge, 2009.
- [2] T. & Y. G. Notteboom, „Handbook of maritime logistics,” Edward Elgar Publishing., 2020.
- [3] „International Maritime Organization (IMO). (2023). Initial strategy for reducing greenhouse gas emissions from ships,” 2023. [Online]. Available: <https://www.imo.org/en/OurWork/Environment/Pages/2023-IMO-Strategy-on-Reduction-ofGHG-Emissions-from-Ships.aspx> .
- [4] I. M. B. (IMB), „ Piracy Reporting Centre: Quarterly Report [Press release].,” (2024, January 22).. [Online]. Available: <https://www.icc-ccs.org/>.
- [5] U. N. O. o. D. a. C. (UNODC)., „Global Study on Homicide 2019.,” (2020). . [Online]. Available: <https://www.unodc.org/documents/data-and-analysis/gsh/Booklet1.pdf>.
- [6] F. a. A. O. o. t. U. N. (FAO)., „The State of World Fisheries and Aquaculture 2022.,” (2023). . [Online]. Available: <https://www.fao.org/documents/card/en?details=cc0461en>.
- [7] N. C. o. T. A. U. t. U. States., „ The 9/11 Commission Report.,” (2004).. [Online]. Available: <https://9-11commission.gov/report/>.
- [8] I. M. O. (. (n.d.), „International Maritime Organization (IMO). (n.d.),” [Online]. Available: <https://imo.org/>.
- [9] I. P. I. (.), „ Private Security Providers and Maritime Security: Regulation and Cooperation.,” 2011. [Online]. Available: <https://www.ipinst.org/>.
- [10] C. a. S. A. (. (n.d.), „Cybersecurity and Shipping Alliance (CSA). (n.d.),” [Online]. Available: <https://csashipping.org/industry-resources/>.
- [11] E. U. A. f. C. (. (2020)., „Cyber threats to the maritime sector.,” 2020. [Online]. Available: <https://www.enisa.europa.eu/topics/critical-information-infrastructures-and-services/maritime> .
- [12] CCDCOE, „Cybersecurity_Considerations_in_Autonomous_Ships,” [Online]. Available: https://ccdcoe.org/uploads/2022/09/Cybersecurity_Considerations_in_Autonomous_Ships.pdf .
- [13] A. COuncil, „9/12,” [Online]. Available: <https://www.atlanticcouncil.org/programs/digital-forensic-research-lab/cyber-statecraft-initiative/cyber-912/>.

- [14] M. Secue, „Current Threats to Maritime Security,” [Online]. Available: <https://www.missionsecure.com/blog/real-world-lessons-learned-from-maritime-cyberattacks-incidents>.
- [15] „dnv,” [Online]. Available: <https://www.dnv.com/maritime/insights/topics/maritime-cybersecurity/>.
- [16] [Online]. Available: <https://www.missionsecure.com/maritime-security-perspectives-for-a-comprehensive-approach>.
- [17] A. Council, „Cyber 9/12 Intelligence Report,” 2024.
- [18] G. Palmer, A beginner's guide to digital forensics: Your essential guide to computer forensics., [S.l.]: Packt Publishing Ltd., 2021.
- [19] S. I. (n.d.), „Introduction to Digital Forensics and Incident Response,” [Online]. Available: <https://www.sans.org/digital-forensics-incident-response/>.
- [20] I. O. o. C. E. (IOCE), „Certified Forensic Computer Examiner (CFCE),” [Online]. Available: <https://uia.org/s/or/en/1100029648>.
- [21] C. 9/12, „Cyber 9/12 Decision Document,” 2024.
- [22] A. council. [Online]. Available: <https://www.atlanticcouncil.org/programs/digital-forensics-research-lab/cyber-statecraft-initiative/cyber-912/>.

AI Usage:

Gemini and Deeple was used for translation purposes!