AL-BIRUNI

Al-Biruni Journal of Humanities and Social Sciences
Vol. 03, No. 10, 2025, pp. 1-12
ISSN 3104-8900
https://al-biruni-journal.jo

Cyber-Terrorism Crimes And Their Impact On Maritime Transport Operations

JAMAL AWWAD ALKHARMAN

[a] Assistants professor, Department of law, Faculty of law, Jadara university, Email: j.alkharman@jadara.edu.jo , Orcid: https://orcid.org/0000-0002-5438-0673

DOI: https://doi.org/10.64440/BIRUNI/BIR005

ARTICLE INFO

Article history
Received June 19, 2025
Revised June 22, 2025
Accepted Oct 20, 2025

Keywords
Cyber-Terrorism;
Crimes;
Maritime;
Transport operations.;

ABSTRACT

The maritime transport sector, integral to global trade, has embraced advanced digital technologies for operational enhancement, yet this transformation has exposed vulnerabilities, making it a prime target for cyber-terrorism. Defined as using the use of information technology to disrupt critical infrastructure for political or ideological motives, cyber-terrorism threatens navigation systems, causes financial losses due to downtime and ransomware, and endangers human safety and the environment. Despite the critical importance, research gaps persist in understanding and mitigating these threats. This study aims to explore cyber-terrorism's impact on maritime operations, propose countermeasures, expand academic knowledge, identify vulnerabilities, develop security models and influence policy. Practically, it enhances security, reduces financial losses, protects the environment, and develops human capabilities, advocating for robust cybersecurity measures and international cooperation to safeguard maritime transport.

1. Introduction

In an era of advanced technology and hyperconnectivity, the world's critical infrastructures have become more susceptible to cyber-attacks. One such critical infrastructure that stands out is the maritime transport sector. Maritime transport is considered a vital artery for global trade, with approximately 90% of the world's goods transported across oceans and seas. With increasing reliance on digital systems and advanced communications to enhance efficiency and safety, the risks associated with Cyber-terrorism are also on the rise.

Cyber-terrorism refers to the deliberate use of information technology and communications to achieve political, religious, or ideological objectives by causing considerable damage or destruction to electronic systems and critical infrastructure. This type of terrorism involves attacks on electronic networks, the spread of malicious software, and causing operational disruptions that may result in substantial financial losses, environmental damage, and even loss of life.

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 03, No. 10, 2025, pp. 1-12
ISSN 3104-8900

The potential impact of Cyber-terrorism on maritime transport operations is significant. Cyber-attacks can disrupt navigation and ship management systems, hindering the movement of vessels, causing shipment delays, and increasing costs. They can also result in massive financial losses due to operational disruptions, the need to repair damaged systems, and ransom payments in cases of ransomware attacks. In scenarios where cyber-attacks target navigation or control systems, the safety of crew members, ships, and cargo can be at risk, potentially leading to catastrophic maritime accidents. Furthermore, cyber-attacks can cause oil spills or other maritime incidents, resulting in severe environmental damage, affecting marine life and coastlines.

Despite the growing awareness of the importance of cybersecurity in the maritime sector, there is still a lack of in-depth research on this topic. Enhancing cybersecurity in maritime transport requires the development of modern technologies, improved defense strategies, and training for industry personnel to effectively address cyber threats.

2. Problem Statement

The maritime transport sector, a cornerstone of global trade, is increasingly reliant on advanced digital technologies and interconnected systems to enhance operational efficiency and safety. However, this digital transformation has simultaneously introduced new vulnerabilities, making the sector a prime target for cyber-terrorism. Cyber-terrorism, defined as the deliberate use of information technology to disrupt, damage, or destroy critical infrastructure for political, ideological, or religious motives, poses a significant threat to maritime operations.

The problem is multifaceted, involving potential disruptions to navigation and ship management systems; financial losses from operational downtime and ransom payments; and risks to human safety and the environment. Despite the critical importance of this issue, there remains a substantial gap in comprehensive research addressing the specific threats, vulnerabilities, and mitigation strategies related to cyber-terrorism in the maritime domain.

2.1. Research objective

This research aims to explore the nature and extent of cyber-terrorism threats to maritime transport operations, assess the potential impacts on the industry, and propose effective countermeasures to enhance resilience against such threats. Understanding and addressing these challenges is crucial for safeguarding the future of maritime transport and maintaining the integrity of global trade networks.

2.1.1. Research Significance

- **Scientific Significance:**

Δ **Expanding Knowledge:** This research contributes to expanding the body of knowledge on cyber-terrorism within the maritime transport sector, a field that remains underexplored. It adds to the academic literature and encourages further studies in this critical area.

Δ **Identifying Vulnerabilities and Threats:** The research provides a detailed analysis of the cyber vulnerabilities and threats specific to maritime systems, helping to pinpoint the weakest points that cyber-terrorists might exploit.

Δ **Developing New Theories and Models:** The findings can contribute to the development of new security theories and models based on data and analysis from case studies and real-world examples, thereby creating a comprehensive academic framework.

∆**Stimulating Future Research:** This study opens avenues for further research on cybersecurity issues in the maritime sector, encouraging scholars to explore new topics and develop innovative solutions.

- **Practical Significance:**

∆ **Enhancing Security and Safety:** The research helps develop effective strategies and measures to enhance security and safety in maritime transport operations, reducing the risk of cyber-attacks and increasing confidence in the digital systems used.

∆ **Reducing Financial Losses:** By identifying and implementing appropriate preventive measures, the research can help minimize financial losses due to operational disruptions and cyber-attacks, ensuring the sustainability of maritime operations.

∆ **Protecting the Environment:** The study contributes to preventing maritime incidents that could cause severe environmental damage, such as oil spills, by improving cybersecurity measures.

∆ **Developing Human Capabilities:** The research aids in training and developing the capabilities of personnel in the maritime sector to handle cyber threats, enhancing their readiness and quick response in case of attacks.

∆ **Influencing Policies and Legislation:** The research can impact the formulation and development of policies and regulations related to cybersecurity in maritime transport, ensuring the implementation of high security standards at an international level.

3. Study Methodology

Based on the study's title and problem statement, a descriptive, inductive, and analytical methodology is most appropriate. This methodology examines the study topic to provide clarifications related to it, as well as other relevant aspects. Additionally, this study employs a descriptive-analytical method to address cyber-terrorism crimes and their impact on maritime transport operations.

3.1. Concept of Cyber-terrorism

Some argue that cyber-terrorism is "the use of information technology systems to attack critical infrastructures or government and public institution systems with the aim of coercion and intimidation." The FBI defines it as "the premeditated, politically motivated attack against information systems, computer programs, and data stored by various actors." It is also described as "the unlawful threat or attack on computers, information systems, programs, and data to intimidate or coerce governments to achieve various objectives." Hence, cyber-terrorism refers to terrorist acts committed through information technology systems and can be considered a new technological tool for traditional terrorism. (1)

In this sense, cyber-terrorism can transcend national borders, impacting various countries and communities. Its main objectives are to attract attention, spread panic and fear among civilians, and coerce governments into unwanted policies.

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 03, No. 10, 2025, pp. 1-12
ISSN 3104-8900

Cyber-terrorism is the intersection of terrorism and cyberspace, differing from cybercrimes (such as data theft and bank fraud).

This type of terrorism can target individuals, property, or infrastructure, causing damage that may result in death, physical injuries, or severe economic losses. Due to the lack of a precise definition of cyber-terrorism, two distinct aspects of the terrorist use of information technology are intertwined: the use of computers to facilitate terrorist activities and the use of information technology as a weapon or target. (2)

Therefore, a distinction has emerged between two types of cyber-terrorism: pure cyber-terrorism and hybrid cyber-terrorism. The former refers to direct attacks on the cyber infrastructure of the victim (such as computers, networks, and information) to achieve political, religious, or ideological goals. The latter refers to the use of the internet in various terrorist activities such as propaganda, recruitment, radicalization, fundraising, data extraction, communications, training, and planning actual terrorist attacks. Terrorists and terrorist organizations use the internet to disseminate their propaganda, promote their ideology, wage psychological warfare, radicalize individuals, and recruit new members through terrorist websites, electronic magazines, and social media platforms. (3)

Additionally, "destructive cyber-terrorism" refers to manipulating or corrupting the functions of information systems to damage or destroy virtual and physical assets. This includes introducing viruses into vulnerable data networks, hacking servers to disrupt communications and steal sensitive information, defacing websites to make them inaccessible to the public, intercepting communications platforms to stop communications, issuing terrorist threats using the internet, or attacking financial institutions to transfer funds and spread panic. This type of terrorism is described as hacking designed to shut down websites and undermine normal life by deliberately damaging the critical infrastructure that supports medical facilities, transportation, financial systems, and more (4).

However, there is no globally accepted definition of cyber-terrorism, despite the extensive use of the internet in various aspects of life and the increasing tendency of different terrorist organizations to use it to achieve their goals. Some definitions focus on the aim of cyber-terrorism, others on its perpetrators, the nature of the losses it can cause, or the tactics, objectives, and methods used. Despite the diversity of these definitions, the common denominator is the exploitation of information technology by terrorist organizations to achieve their goals, which is the meaning adopted by this study. By using the internet and electronic media, terrorist organizations can conduct their activities on a large scale, enabling them to reach millions of people, convey their message, and justify their actions. (5)

In other words, cyberspace has become an attractive arena for terrorist organizations as it enables them to carry out their activities on a broad scale. Through cyber-terrorism, terrorists can inflict physical and moral damage on targeted states that exceeds that of traditional terrorism. In the latter, the impacts are confined to specific geographical locations and limited physical and human casualties, with media and public attention primarily focused on the losses rather than the underlying causes and extremist ideologies. Conversely, the ability of cyber-terrorism to affect large groups of people enables terrorist organizations to achieve their strategic objectives with increasing ease. (6)

Therefore, it can be argued that cyber-terrorism has become attractive to various terrorist organizations because it requires fewer people and resources, allows them to target large-scale objectives, and maintains the anonymity of the terrorists, especially as they can be located far from the actual target sites. Terrorists can also choose from a wide range of targets that can be quickly compromised without the need for extensive intelligence, preparations, physical barriers to cross, or checkpoints to pass through. (7)

4. Cyber-terrorism characterized

Cyber terrorism is characterized by several features that distinguish it from other forms of cybercrime. These characteristics include: (8) (9)

Δ **Political or Ideological Objectives:** Cyber terrorism aims primarily to achieve political or ideological goals by influencing governments, institutions, or communities.

Δ **Psychological and Social Impact:** Cyber terrorism aims to create a state of fear and chaos in targeted communities, instilling instability and distrust in cybersecurity.

Δ **Strategic Targeting:** Targets are carefully selected to achieve significant strategic impact, such as critical infrastructure, government systems, and vital sectors like energy and transportation.

Δ **Technological Complexity:** Cyber terrorism employs advanced and complex techniques such as sophisticated malware, Distributed Denial-of-Service (DDoS) attacks, and large-scale database breaches to achieve its goals.

Δ **Collaboration:** Cyber terrorism may involve collaboration among diverse groups of hackers and cyber extremists who share knowledge and resources to execute high-impact attacks.

Δ **Wide-ranging Impact:** The damage resulting from cyber terrorism can be extensive, affecting economies, infrastructure, essential services, and the safety of individuals.

These characteristics make cyber-terrorism a serious threat that requires international response and collaborative efforts to mitigate its negative impacts on targeted communities and economies.

- **Cyber threats in maritime transport**

Cyber threats in maritime transport refer to the various risks posed by cyber-attacks on the systems, networks, and operations within the maritime industry. These threats have increasingly become a concern due to the digitalization and interconnectedness of maritime infrastructure, vessels, and port operations. Here are some key aspects and types of cyber threats in maritime transport:

Key Aspects of Cyber Threats in Maritime Transport

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 03, No. 10, 2025, pp. 1-12
ISSN 3104-8900

Δ **Vulnerabilities in Ship Systems:** Ships today heavily rely on digital systems for navigation, communication, engine control, and cargo management. These systems are vulnerable to cyber-attacks that can manipulate navigation data, disrupt communication channels, or even take control of critical ship functions.

Δ **Port Operations:** Ports are crucial nodes in global maritime logistics; cyber-attacks can disrupt container handling systems, customs procedures, and logistics management. Such disruptions can lead to delays, financial losses, and impacts on global supply chains.

Δ **Supply Chain Security:** The interconnected nature of global supply chains makes them susceptible to cyber-attacks aimed at disrupting cargo tracking, inventory management, and shipment scheduling. Attackers may target sensitive data related to cargo contents or shipment routes.

Δ **Financial Transactions:** Maritime companies engage in extensive financial transactions related to cargo payments, insurance, and port fees. Cyber-attacks can target financial systems to divert funds, manipulate transactions, or cause financial losses.

Δ **Environmental Risks:** Cyber-attacks on maritime systems can also pose environmental risks, such as manipulating ballast water management systems or causing oil spills through unauthorized access to vessel control systems. (10) (11) (12)

- **Types of Cyber Threats:**

Δ **Malware and Ransomware:** These are malicious software programs designed to infiltrate systems, encrypt data, and demand ransom payments for decryption. They can disrupt vessel operations or compromise sensitive information.

Δ **Phishing and Social Engineering:** Cyber-attackers may use phishing emails or social engineering tactics to trick maritime personnel into divulging sensitive information, providing access to credentials, or inadvertently downloading malware.

Δ **Denial-of-Service (DoS) Attacks:** These attacks aim to overwhelm maritime systems or networks with excessive traffic, rendering them inaccessible or disrupting normal operations.

Δ **Insider Threats:** Employees or contractors with access to maritime systems may pose a threat by intentionally or unintentionally compromising security protocols, sharing sensitive information, or facilitating unauthorized access.

Δ **IoT Vulnerabilities:** Internet-of-Things (IoT) devices onboard ships, in ports, or within maritime infrastructure may have security vulnerabilities that cyber-attackers can exploit to gain unauthorized access or manipulate operations. (13)

- **Impact of Cyber Threats:**

Δ **Operational Disruption:** Cyber-attacks can disrupt vessel operations, leading to delays in cargo delivery, port congestion, and increased operational costs.

Δ **Financial Losses:** Loss of revenue due to operational downtime, financial fraud, or ransom payments can significantly impact maritime companies' profitability.

Δ **Reputation Damage:** Public perception and trust in maritime companies can be damaged by cyber incidents, affecting customer relationships and business partnerships.

Δ **Safety Risks:** Manipulation of navigation systems or critical vessel controls poses safety risks to crew members, vessels, and cargo, potentially leading to accidents or environmental disasters.

Δ **Regulatory Compliance:** Maritime companies must adhere to international regulations and cybersecurity standards. Failure to comply due to cyber incidents may result in legal penalties or restrictions on operations. (14)

Organized Crime and Opportunists:

Worldwide criminal syndicates are increasingly leveraging cybercrime as a lucrative revenue stream. Through methods such as direct extortion, theft, or trafficking, hackers exploit digital vulnerabilities to extract diverse and innovative sources of wealth.

In 2011, hackers breached the Port of Antwerp's terminal operating system, gaining access to a database containing precise location data of every container within the facility. Exploiting this breach, drug traffickers smuggled narcotics concealed within legitimate shipments of timber and bananas. The stolen information allowed them to pinpoint and retrieve their contraband from amidst thousands of containers, avoiding detection by the rightful owners until their operations grew too bold, resulting in discovery by authorities. (15)

Similarly, in 2016, hackers infiltrated the content management system of a major container carrier's website, obtaining access to global cargo manifests. They sold this valuable data on the dark web to Somali piracy syndicates, who then targeted ships carrying high-value cargo. This coordinated effort allowed the pirates to quickly locate and seize specific containers before fleeing, a series of attacks that continued for months until the vulnerability was identified and secured. (16)

While smuggling and cargo theft yield profits, they entail significant risk. In contrast, ransomware presents a low-risk, high-reward alternative for criminals. Ransomware attacks, facilitated by the rise of cryptocurrencies, encrypt critical computer networks, locking out legitimate users until a ransom is paid. This form of cyber extortion has become increasingly prevalent in the shipping industry, exemplified by the 2022 attack on Swire Pacific Offshore, impacting their operations and compromising sensitive data such as employee information and financial details. (17)

The evolution of ransomware tactics in 2021 highlighted two alarming trends for the maritime sector. First, there is an increasing focus on targeting systems with operational technology, potentially compromising critical equipment and safety. The ransomware attack on the Colonial Pipeline illustrated this vulnerability, forcing a shutdown until a substantial ransom was paid. Second, ransomware actors are targeting supply chain organizations to access and extort their customers, a tactic that saw a significant rise in incidents throughout 2021, affecting companies like SolarWinds and Kaseya, whose software is integral to maritime operations and logistics. (18)

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 03, No. 10, 2025, pp. 1-12
ISSN 3104-8900

These developments underscore the urgent need for robust cybersecurity measures across the maritime industry to mitigate the growing threat posed by cybercriminals exploiting digital vulnerabilities for financial gain and operational disruption.

While cybercriminals perpetrate a massive portion of cyber-attacks, nation-states wield the capability to execute far more perilous forms of cyber warfare. As of the current writing, the world is grappling with the repercussions of Russia's full-scale invasion of Ukraine. During January and February 2022, a series of successful cyber-attacks targeted Ukrainian organizations, drawing global attention. Particularly alarming are reports of new destructive "wiper" malware deployed in these attacks, attributed to Russian state actors. (19)

In contrast to ransomware, which encrypts systems with the intent to decrypt upon payment of a ransom, wiper malware is designed to irreversibly destroy networks and files, often in an indiscriminate manner. These incidents underscore the evolving tactics of state-sponsored cyber operations, posing severe threats not only to targeted entities but also to international cybersecurity and stability.

Spoofing Positioning Systems

Spoofing Global Navigation Satellite Systems (GNSS) poses significant threats to maritime navigation systems, particularly GPS, which plays a crucial role in ship navigation. GPS vulnerabilities arise because receivers interact with low-energy signals from space, making them susceptible to manipulation through false information, a technique known as spoofing. This issue has escalated globally and presents varying levels of risk depending on the scale and sophistication of the attack (17). Small-scale disruptions are easily achievable even by amateurs who can acquire basic spoofing equipment for less than US$100. However, with the resources of a nation state, sophisticated spoofing attacks capable of affecting entire regions or seas have become a reality rather than just a possibility. (20)

Instances of large-scale GPS spoofing incidents are increasingly reported. For example, during a 2017 Russian military exercise, over 50 commercial vessels experienced interference with their positioning systems. The inconsistencies were so severe that some ships' digital charts erroneously displayed their locations far inland near a regional airport. While this incident caused minimal disruption due to its blatant nature, subtle spoofing attacks can evade detection by ship navigation teams, leading to potentially severe consequences (21). The Strait of Hormuz, a critical and challenging waterway shared between Iran and Oman, illustrates the dangers of GPS spoofing in maritime navigation. On July 19, 2019, the UK-flagged vessel Stena Impero encountered unusual deviations from its intended voyage path while transiting the strait. Despite typically sailing within Omani waters, the vessel's GPS reported positions inconsistent with its actual course and speed, as indicated by raw Automatic Identification System (AIS) data from Lloyd's List Intelligence. While there is no official confirmation from Iranian or UK authorities, experts widely speculate that the vessel's GPS was spoofed, potentially leading it to unintentionally enter Iranian waters. This incident sparked an international diplomatic crisis, with Iran's Revolutionary Guard boarding and detaining the Stena Impero for two months. (22)

In conclusion, GPS spoofing represents a critical threat to maritime security, capable of causing operational disruptions and geopolitical tensions. Mitigating these risks requires advanced detection technologies, improved authentication methods for GNSS signals, and heightened awareness among maritime operators to detect and respond effectively to spoofing attacks.

Mitigation Strategies

To mitigate cyber threats in maritime transport, industry stakeholders can implement several strategies: (23) (24) (25)

Δ **Intrusion Detection and Prevention Systems (IDS/IPS):** These systems are critical for mon Ports are crucial nodes in global itoring unauthorized activities and malicious cyber attempts within maritime transport networks, aiding in early detection of attacks and immediate response.

Δ **Antivirus and Malware Protection Software:** These provide essential protection against viruses and malicious software targeting computer systems and networks in maritime transport.

Δ **Firewalls:** Firewalls contribute to preventing unauthorized access to maritime transport networks and filtering network traffic based on specified rules.

Δ **Network Behavior Analysis:** This technology aims to monitor unusual behavior patterns within networks, enabling detection of cyber-attacks that may evade traditional intrusion detection systems.

Δ **Data Encryption:** Encryption protects sensitive data during transmission over networks, reducing the risk of interception and unauthorized access.

Δ **Identity and Access Management (IAM):** IAM systems help regulate access permissions for individuals and systems in maritime environments, minimizing the chances of breaches by defining access to sensitive information.

Δ **Cybersecurity Training and Awareness:** Continuous training of employees on cybersecurity risks and how to handle them is essential to enhance awareness and effective response in the event of an attack.

Δ **Cybersecurity Incident Response:** Establishing plans and procedures for rapid response to cyber-attacks helps mitigate damage and quickly restore systems.

These tools and technologies constitute part of cybersecurity strategies that maritime companies can implement to protect their systems and data from increasing cyber threats.

By proactively addressing these aspects and types of cyber threats, the maritime industry can enhance its resilience against cyber-attacks and safeguard critical operations, ensuring the safety of personnel, vessels, and cargo while maintaining the efficiency of global supply chains.

5. Conclusion

Cyber-terrorism crimes pose significant threats to maritime transport operations, leveraging advanced technologies to disrupt, infiltrate, or manipulate critical systems. The interconnected nature of global shipping networks and reliance on digital infrastructure make the industry susceptible to various cyber threats, ranging from data breaches to operational disruptions and even physical safety risks.

Al-Biruni Journal of Humanities and Social Sciences
https://al-biruni-journal.jo
Vol. 03, No. 10, 2025, pp. 1-12
ISSN 3104-8900

The evolution of cyber-terrorism tactics, such as ransomware attacks, GPS spoofing, and sophisticated malware, underscores the growing sophistication and malicious intent of cyber actors targeting maritime transport. These incidents not only jeopardize operational continuity but also raise concerns about maritime safety, environmental impact, and economic stability.

Effective cybersecurity measures are imperative to mitigate these risks. Implementing robust intrusion detection systems, antivirus software, firewalls, and encryption technologies can fortify defenses against cyber intrusions. Additionally, ongoing cybersecurity training and awareness programs for maritime personnel are crucial to enhance readiness and response capabilities in the face of evolving cyber threats.

Furthermore, international cooperation and regulatory frameworks are essential for addressing cyber-terrorism challenges collectively. Collaborative efforts among maritime stakeholders, governments, and cybersecurity experts are pivotal in developing proactive strategies, sharing threat intelligence, and fostering resilience against cyber-terrorism in maritime transport.

In conclusion, safeguarding maritime transport operations from cyber-terrorism requires a multifaceted approach that integrates technological defenses, human vigilance, and global cooperation to uphold the security, reliability, and integrity of maritime infrastructure in an increasingly digital world.

Author Contribution: All authors contributed equally to the main contributor to this paper. All authors read and approved the final paper.

Funding: This research received no external funding"

Conflicts of Interest: "The authors declare no conflict of interest."

References

[1] Weimann, G. (2004, December). *Cyber-terrorism: How real is the threat?* United States Institute of Peace, Special Report No. 119. Available at https://shorturl.at/ektIO

[2] El Bahi, R. (2019, September 30). *Cyber terrorism: Concept, characteristics, and patterns.* Egyptian Center for Strategic Studies. Available at https://ecss.com.eg/7141/

[3] Zerzri, M. (2017). *The threat of cyber terrorism and recommendations for countermeasures.* C·A· Perspectives on Tunisia, No. 4. Available at https://shorturl.at/uwIMR

[4] Wigan Council. (n.d.). *Cyber terrorism.* Available at https://shorturl.at/ewRS7

[5] Achkoski, J., & Dojchinovski, M. (2012, June 9). *Cyber terrorism and cyber crime – Threats for cyber security.* In *Proceedings of the First Annual International Scientific Conference.* MIT University–Skopje, Makedonski Brod, Macedonia. Available at https://shorturl.at/oEJU0

[6] Charvat, J. P. I. A. G. (2009). *Cyber terrorism: A new dimension in battlespace. The Virtual Battlefield: Perspectives on Cyber Warfare*, (3), 77–87.

[7] Dogrul, M., Aslan, A., & Celik, E. (2011). *Developing an international cooperation on cyber defense and deterrence against cyber terrorism.* In *3rd International Conference on Cyber Conflict* (p. 10). Tallinn, Estonia.

[8] Tawfiq, S. (2025). *The role of the Great Arab Revolt in shaping Jordanian national identity. Al-Biruni Journal of Humanities and Social Sciences, 3*(6). https://doi.org/10.64440/BIRUNI/BIR002

[9] Grabosky, P. (2006). *Computer crimes: Global dimensions.* In *Internet Networks and Their Social and Security Impacts* (p. 338). General Directorate of Abu Dhabi Police, Center for Security Research and Studies.

[10] Alcaide, J. I., & Llave, R. G. (2020). *Critical infrastructures cybersecurity and the maritime sector. Transportation Research Procedia, 45*, 547–554.

[11] Fell, J. (2015). *Mayflower tribute set to sail unmanned [automated marine transport]. Engineering & Technology, 10,* 42–44.

[12] Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I., & Bellekens, X. (2022). *Cybersecurity in the maritime industry: A systematic survey of recent advances and future trends. Information, 13,* 22.

[13] Almarabeh, H., & Sulieman, A. (2019). *The impact of cyber threats on social networking sites. International Journal of Advanced Research in Computer Science, 10*(2).

[14] Ghelani, D. (2022). *Cyber security, cyber threats, implications, and future perspectives: A review. Authorea Preprints.*

[15] Abouyounes, M. W. A. (2025). *The legal underpinnings of Jordanian and Iraqi law's administrative penalty systems. Al-Biruni Journal of Humanities and Social Sciences, 3*(9). https://doi.org/10.64440/BIRUNI/BIR003

[16] Polikarovskykh, O., Daus, Y., Larin, D., & Tkachenko, M. (2023). *Systematization of cyber threats in maritime transport. Security of Infocommunication Systems and Internet of Things, 1*(1), 01008–01008.

[17] Simola, J., & Pöyhönen, J. (2022, March). *Emerging cyber risk challenges in maritime transportation.* In *International Conference on Cyber Warfare and Security* (Vol. 17, No. 1, pp. 306–314).

[18] Metalla, O., Golgota, A., Pupa, K. S., Ndokaj, E., Beqiraj, P., Thana, E., & Çerma, U. (2023). *Cyber security in the maritime transport. Interdisciplinary Journal of Research and Development, 10*(2), 74–74.

[19] Silgado, D. M. (2018). *Cyber-attacks: A digital threat reality affecting the maritime industry.*

[20] Melnyk, O., Onyshchenko, S., Onishchenko, O., Shumylo, O., Voloshyn, A., Koskina, Y., & Volianska, Y. (2022). *Review of ship information security risks and safety of maritime transportation issues. TransNav: International Journal on Marine Navigation and Safety of Sea Transportation, 16.*

[21] Ashraf, I., Park, Y., Hur, S., Kim, S. W., Alroobaea, R., Zikria, Y. B., & Nosheen, S. (2022). *A survey on cyber security threats in IoT-enabled maritime industry. IEEE Transactions on Intelligent Transportation Systems, 24*(2), 2677–2690.

[22] Simola, J., & Pöyhönen, J. (2022, March). *Emerging cyber risk challenges in maritime transportation.* In *International Conference on Cyber Warfare and Security* (Vol. 17, No. 1, pp. 306–314).

[23] Lagouvardou, S. (2018). *Maritime cyber security: Concepts, problems, and models.* Kongens Lyngby, Copenhagen.

[24] Ahmad, R. W., Hasan, H., Jayaraman, R., Salah, K., & Omar, M. (2021). *Blockchain applications and architectures for port operations and logistics management. Research in Transportation Business & Management, 41,* 100620.

[25] Bechtsis, D., Tsolakis, N., Bizakis, A., & Vlachos, D. (2019). *A blockchain framework for containerized food supply chains.* In *Computer Aided Chemical Engineering* (Vol. 46, pp. 1369–1374). Elsevier, Amsterdam, The Netherlands.