Jurnal Pembaharuan Hukum
Volume 12, Number 1, April 2025
E-ISSN : 2355 – 0481 (Print)
ISSN : 2580 – 3085 (Online)

PROTECTING VICTIMS OF CYBERCRIME IN THE MARITIME SECTOR: LEGAL CHALLENGES AND THE ABSENCE OF SPECIFIC CYBERSECURITY LAWS IN INDONESIA

Carlo Gambino Hutahayan
Universitas Mpu Tantular, Jakarta, Indonesia
carlogambinohutahayan@gmail.com

Yesarela Easyca
Universitas Mpu Tantular, Jakarta, Indonesia
yesarela.easyca@gmial.com

Junifer Dame Panjaitan
Universitas Mpu Tantular, Jakarta, Indonesia
junifer_panjaitan@mputantular.ac.id

ARTICLE INFO

Keywords:
Cyber Crime; Cybersecurity; Legal Framework; Victim Protection.

ABSTRACT

Indonesia's shipping sector faces substantial risks from cyberattacks in the ever-evolving digital landscape, which threaten navigation systems, ship operations, and critically impact victims, including shipping companies, crews, and passengers. This paper examines the legal challenges encountered by Indonesia's maritime industry in addressing cybercrime, with a particular focus on the lack of dedicated cybersecurity laws that explicitly protect victims. The research findings reveal that Law No. 11 of 2008 on Information and Electronic Transactions and Law No. 17 of 2008 on Shipping are inadequate in addressing the specific cyber threats and victim protection needs within the maritime sector. This study advocates for the establishment of specialized regulations incorporating clear definitions and scope, detailed obligations and responsibilities, robust victim protection measures, appropriate security standards, and effective enforcement mechanisms and sanctions. By integrating these elements, the research offers both theoretical and practical guidance for policymakers to develop a more comprehensive and adaptive regulatory framework that not only secures Indonesia's maritime infrastructure but also ensures justice and support for victims of maritime cybercrime.

A. INTRODUCTION

In the rapidly evolving digital era, cybersecurity has become a crucial concern across various industries, including the maritime sector.[1] The integration of information and communication technology plays a central role in maritime operations, covering navigation systems, cargo management, and communication networks.[2] For instance, a 2023 report by the Indonesian National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara*/BSSN) noted a 35% increase in cyberattacks targeting maritime infrastructure in Indonesia, underscoring the sector's vulnerability.[3] However, the digitalization of maritime activities has led to significant exposure to cybercrime threats. These threats not only endanger operational safety and financial stability but also have profound impacts on individuals and organizations who fall victim to cyberattacks. Indonesia, as the world's largest archipelagic country, relies heavily on the maritime sector for its economic development and national security.[4] With increasing dependence on digital systems, Indonesia's maritime industry has become increasingly vulnerable to cybercrimes such as hacking, data breaches, and system sabotage.

Cyber-attacks in the maritime sector can lead to severe consequences for victims, including loss of sensitive data, financial losses, operational disruptions, and psychological harm.[5] The victims may range from shipping companies and port authorities to individual crew members and passengers whose personal data is compromised. Despite these risks, Indonesia's legal framework, particularly Law No. 11 of 2008 on Information and Electronic Transactions (amended by Law No. 19 of 2016) and Law No. 17 of 2008 on Shipping, fails to adequately address the specific needs of maritime cybercrime victims. A notable case in 2022, where a ransomware attack disrupted

[1] Imran Ashraf, Yongwan Park, Soojung Hur, Sung Won Kim, Roobaea Alroobaea, Yousaf Bin Zikria, and Summera Nosheen. "A survey on cyber security threats in IoT-enabled maritime industry." *IEEE Transactions on Intelligent Transportation Systems* 24, no. 2 (2022): 2679. See also, Mohamed Amine Ben Farah, Elochukwu Ukwandu, Hanan Hindy, David Brosset, Miroslav Bures, Ivan Andonovic, and Xavier Bellekens. "Cyber security in the maritime industry: A systematic survey of recent advances and future trends." *Information* 13, no. 1 (2022): 22.

[2] Georgios A Giannopoulos. "The application of information and communication technologies in transport." *European journal of operational research* 152, no. 2 (2004): 305.

[3] Badan Siber dan Sandi Negara (BSSN), "Laporan Tahunan Keamanan Siber Indonesia 2023" (Jakarta: BSSN, 2023), 45.

[4] Adam James Fenton. "Preventing catastrophic cyber–physical attacks on the global maritime transportation system: A case study of hybrid maritime security in the Straits of Malacca and Singapore." *Journal of Marine Science and Engineering* 12, no. 3 (2024): 510.

[5] Maria Valentina Clavijo Mesa, Carmen Elena Patino-Rodriguez, and Fernando Jesus Guevara Carazas. "Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains." *Information* 15, no. 11 (2024): 710. See also, Steve Symes, Eddie Blanco-Davis, Tony Graham, Jin Wang, and Edward Shaw. "Cyberattacks on the Maritime Sector: A Literature Review." *Journal of Marine Science and Application* 23, no. 4 (2024): 689-706.

operations at a major Indonesian port, highlighted the lack of legal recourse for affected stakeholders, leaving victims without clear remedies.[6]

Furthermore, the absence of specialized cybersecurity laws creates significant obstacles for law enforcement in addressing cybercrime cases effectively.[7] Victims often face challenges in accessing justice, including difficulties in reporting incidents, inadequate investigation processes, and limited support systems for recovery.[8] Jurisdictional challenges compound these issues, as cyber-attacks often involve cross-border elements, making it difficult to identify perpetrators and enforce legal consequences.[9] As a result, victims are left vulnerable, and cybercriminals operate with minimal risk of prosecution.

This study critically examines the deficiencies of Indonesia's current legal framework in protecting victims of maritime cybercrime and proposes a new, victim-centered legislative approach grounded in Hans Kelsen's Pure Theory of Law, which emphasizes a hierarchical system of norms to ensure legal coherence and justice.[10] Although cybersecurity has been widely studied, research specifically addressing the victimology of maritime cybercrime in Indonesia remains limited. Most existing studies focus on technical cybersecurity measures or broader legal frameworks without delving into the victim's perspective and the legal remedies available to them.[11] This study positions itself as a critique of the existing legal shortcomings while offering a novel perspective by advocating for targeted regulations that prioritize victim protection in the maritime sector. This research seeks to fill that gap by emphasizing the importance of legal protection for victims and proposing legislative improvements that can enhance both security and justice in the maritime sector. The study addresses the following explicit research questions: What are the legal challenges faced by victims of cybercrime in Indonesia's maritime sector? How does the absence of specific cybersecurity legislation

[6] Chalermpong Senarak, "Port Cyberattacks from 2011 to 2023: A Literature Review and Discussion of Selected Cases," *Maritime Economics & Logistics* 26, no. 1 (2024): 115.

[7] M. A. A. M. Al-Amaireh. "The Role of Cybersecurity in Enhancing the Effectiveness of Law Against Cybercrimes." *Revista de Gestão Social e Ambiental* 18, no. 8 (2024): e06508-e06508.

[8] Mary P. Koss. "Restoring rape survivors: Justice, advocacy, and a call to action." *Annals of the New York Academy of Sciences* 1087, no. 1 (2006): 206-234. See also, Deirdre Healy. "Exploring victims' interactions with the criminal justice system." *Ireland Department of justice and equality report* (2019).

[9] Beatrice A. Walton. "Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law." *Yale LJ* 126 (2016): 1460.

[10] Joanna Diane Caytas, "The Unconquerable Domain of Discretion in Kelsen's Pure Theory of Law," *Washington Undergraduate Law Review* 6, no. 1 (2012): 10.

[11] Mohammad Fadil Imran. "Cyber Criminology: An analysis of the Indonesian and the United States Police Perception." *International Journal of Cyber Criminology* 17, no. 2 (2023): 250-261.

impact victim protection and access to justice? What legislative reforms are needed to ensure comprehensive victim protection?

This study aims to identify and examine the legal challenges faced by victims of cybercrime in Indonesia's maritime sector, focusing on the urgent need for specific legislation that ensures comprehensive protection. Through normative legal analysis, this research will evaluate the shortcomings of the existing legal framework and its impact on the prevention, investigation, and redress of cybercrime incidents. By integrating Kelsen's normative hierarchy, the study provides a theoretical foundation for developing a coherent legal system that addresses modern cyber threats. The study seeks to provide practical recommendations for policymakers to develop robust and victim-centered cybersecurity regulations tailored to the maritime industry. By highlighting the pressing need for targeted cybersecurity legislation, this paper makes a significant contribution to the development of cyber law and victimology theory. It also offers practical insights for policymakers, legal practitioners, and stakeholders in the maritime industry to strengthen the protection of victims and improve the resilience of Indonesia's maritime sector against cyber threats.

B. RESEARCH METHODS

This study adopts normative legal research to critically analyze the adequacy of Indonesia's legal framework in protecting victims of cybercrime within the maritime sector. Normative legal research is chosen because it is best suited to evaluate the existing legal framework and identify gaps in legislation, which is central to addressing the lack of specific cybersecurity laws for the maritime sector.[12] This method is relevant to the issue at hand, as it allows for a systematic examination of legal norms and their application to the unique challenges of maritime cybercrime, ensuring a focus on victim protection within Indonesia's legal system. The research examines primary legal materials, including Law No. 11 of 2008 on Electronic Information and Transactions, Law No. 17 of 2008 on Shipping, and relevant implementing regulations, alongside international legal instruments such as the Budapest Convention on Cybercrime and IMO Guidelines on Maritime Cyber Risk Management. Secondary materials include scholarly books, journal articles, and legal commentaries on cybersecurity, maritime law, and victimology.

The research employs a doctrinal approach within the normative framework, specifically focusing on statutory and conceptual analysis, as it enables a detailed examination of existing legislation and theoretical constructs like Hans Kelsen's Pure Theory of Law to assess the coherence of Indonesia's

[12] Le Cheng, Jiaxuan Qiu, and Yi Yang, "Constructing Cybersecurity Discourse via Deconstructing Legislation," *International Journal of Legal Discourse* 8, no. 2 (2023): 275.

legal system in addressing cybercrime victims.[13] The doctrinal approach is selected because it facilitates the identification of legal gaps in statutory provisions and provides a theoretical basis for proposing victim-centered legislative reforms, which is critical given the absence of specific maritime cybersecurity regulations. Primary legal materials were collected through official government databases, such as the Ministry of Law and Human Rights and the International Maritime Organization, while secondary materials were sourced from academic databases like Scopus, JSTOR, and Google Scholar. The analysis process involves three key steps: first, identifying relevant legal provisions and their scope; second, evaluating their effectiveness in protecting victims through doctrinal interpretation and comparison with international standards; and third, formulating normative recommendations based on identified gaps and best practices.

This study is limited to analyzing Indonesia's national legal framework, particularly Laws No. 11 of 2008 and No. 17 of 2008, and their application to maritime cybercrime, with a focus on victim protection within Indonesia's jurisdiction. It does not cover technical cybersecurity measures or empirical data on cybercrime incidents due to the normative focus and limited access to real-time incident data. The research also excludes in-depth analysis of international jurisdictions beyond referencing best practices, as the primary objective is to propose reforms tailored to Indonesia's legal and maritime context. Through a doctrinal approach, this study identifies gaps and limitations in current legislation regarding victim protection, assesses legal challenges in enforcement and remedies, and provides normative recommendations to enhance Indonesia's maritime cybersecurity law, ensuring comprehensive protection and legal certainty for victims.

C. RESULTS

1. Cyber Crime in the Maritime Sector

In the maritime sector, cybercrime refers to illegal activities conducted through digital means or computer networks that specifically target the information systems and technologies used in shipping operations.[14,15] These unlawful acts compromise the integrity, confidentiality, and availability of maritime digital infrastructures, directly impacting both organizational victims, such as shipping companies and port authorities, and individual victims,

[13] Joanna Diane Caytas, "The Unconquerable Domain of Discretion in Kelsen's Pure Theory of Law," *Washington Undergraduate Law Review* 6, no. 1 (2012): 10.

[14] Mohamed Amine Ben Farah, Elochukwu Ukwandu, Hanan Hindy, David Brosset, Miroslav Bures, Ivan Andonovic, and Xavier Bellekens. "Cyber security in the maritime industry: A systematic survey of recent advances and future trends." *Information* 13, no. 1 (2022): 23.

[15] Andrej Androjna, Tanja Brcko, Ivica Pavic, and Harm Greidanus. "Assessing cyber challenges of maritime navigation." *Journal of Marine Science and Engineering* 8, no. 10 (2020): 776.

including crew members and passengers whose data or safety may be jeopardized. Cybercrime in this context not only threatens the operational continuity of maritime activities but also exposes victims to significant financial, reputational, and personal harm.[16]

Cybercrime in the maritime industry includes attacks on shipboard navigation systems, cargo management databases, and communication channels between ships and onshore facilities. Such crimes can result in major operational disruptions, data breaches, financial losses, and, crucially, can place human lives at risk when critical maritime operations are compromised. Common types of maritime cybercrime include:

(1) Hacking is the unauthorized access to computer systems or networks. In the maritime context, hackers may infiltrate navigation systems, communication platforms, or logistics databases, leading to the theft of sensitive data, manipulation of ship routes, and potential accidents, all of which indirectly victimize shipping companies, crews, and even passengers.[15]
(2) Malware: Malicious software designed to damage or disrupt computer systems, including viruses, worms, and trojans. Infected maritime systems can malfunction, resulting in operational paralysis, loss of critical data, and increased vulnerability of victims who rely on these systems for safety and efficiency.[17]
(3) Ransomware is a type of malware that encrypts victims' data and demands payment to restore access. In the maritime sector, ransomware can paralyze entire fleets or ports by locking essential operational files, leaving companies, workers, and clients as victims of extortion, with potentially severe economic and safety consequences.[18]
(4) Phishing: Deceptive attempts to obtain sensitive information by masquerading as trustworthy entities. Maritime personnel, from administrative staff to crew members, may fall victim to phishing scams, unknowingly disclosing login credentials that enable

[16] David Miranda Silgado, *Cyber-Attacks: A Digital Threat Reality Affecting the Maritime Industry* (Dissertation, World Maritime University, 2018).
[17]Mohammed N. Alenezi, Haneen Alabdulrazzaq, Abdullah A. Alshaher, and Mubarak M. Alkharang. "Evolution of malware threats and techniques: A review." *International journal of communication networks and information security* 12, no. 3 (2020): 326-337.
[18] Mamoona Humayun, N. Zaman Jhanjhi, Ahmed Alsayat, and Vasaki Ponnusamy. "Internet of things and ransomware: Evolution, mitigation and prevention." *Egyptian Informatics Journal* 22, no. 1 (2021): 105-117.

broader cyberattacks, placing both the individuals and their organizations at risk.[19]

Each type of cyber-attack poses significant hazards to the safety, security, and well-being of victims in the maritime sector. A notable case is the 2017 ransomware attack on Maersk, which caused massive financial losses and disrupted global shipping operations, affecting countless stakeholders and highlighting the sector's vulnerability. These incidents underscore the urgent need not only for robust cybersecurity measures but also for clear legal frameworks that ensure adequate protection and remedies for victims affected by maritime cybercrime.

The maritime sector faces significant risks from cybercrime, as demonstrated by numerous international cases that highlight the industry's vulnerability and the wide-ranging impact on victims.[20] These incidents not only disrupt business operations but also inflict serious harm on victims including shipping companies, business partners, employees, and customers through financial losses, compromised data, and operational chaos.[21] Importantly, these cases expose critical gaps in victim protection and underline the need for robust legal frameworks to ensure that victims can seek effective remedies. Significant Global Case Studies

(1) NotPetya Attack on Maersk (2017): In June 2017, the NotPetya ransomware attack crippled Maersk's IT systems, severely disrupting its global operations. The attack encrypted data across Maersk's network, making vital operational information, such as cargo booking systems and internal communications, inaccessible. As a result, the victims included not only Maersk itself but also its global customers and partners who faced delays, financial losses, and supply chain breakdowns. The absence of clear legal recourse for victims at multiple levels exposed the industry's vulnerability.[22]

[19] Aaron Zimba, Zhaoshun Wang, and Mumbi Chishimba. 2019. "Addressing Crypto-Ransomware Attacks: Before You Decide Whether To-Pay or Not-To." *Journal of Computer Information Systems* 61 (1): 56.

[20] Massoud Mohsendokht, Huanhuan Li, Christos Kontovas, Chia-Hsun Chang, Zhuohua Qu, and Zaili Yang. "Decoding dependencies among the risk factors influencing maritime cybersecurity: Lessons learned from historical incidents in the past two decades." *Ocean Engineering* 312 (2024): 119078. See also, A. Y. Mai-inji, K. E. Ukhurebor, and L. O. Babatope. "Impending maritime cyberspace threats: An educational research perspective." *Journal of Infrastructure, Policy and Development* 8, no. 8 (2024): 4146.

[21] Shipra Pandey, Rajesh Kumar Singh, Angappa Gunasekaran, and Anjali Kaushik. "Cyber security risks in globalized supply chains: conceptual framework." *Journal of Global Operations and Strategic Sourcing* 13, no. 1 (2020): 103-128.

[22] Rory Macfarlane. "Cyber-risk in shipping and its management." In *Ship Operations*, pp. 69-83. England: Informa Law from Routledge, 2020.

(2) COSCO Cyber-Attack (2018). In July 2018, COSCO Shipping Lines experienced a cyber-attack that paralyzed its email and internet systems across North America. Operational disruptions lasted for days, forcing the company and its clients to revert to manual processes. At the same time, data loss was not reported; the victims employees, customers, and business partners suffered from communication breakdowns, delayed shipments, and additional logistical costs.[23]

(3) Phishing Attack on Clarksons (2017): In November 2017, Clarksons fell victim to a phishing attack, which allowed attackers to access confidential company data. This breach posed a significant threat to the privacy of trade secrets and potentially harmed clients whose sensitive information may have been exposed. Both the company and its clients became victims of data compromise, underscoring the need for stronger legal safeguards and victim support mechanisms.[24]

The impact of cybercrime on victims in the maritime sector is profound and multifaceted. Financially, the NotPetya attack on Maersk in 2017 resulted in losses of approximately $300 million, encompassing IT system recovery, lost revenue, and extensive crisis management efforts.[25] Beyond the immediate financial toll on the company itself, a ripple effect was felt by customers and business partners who experienced indirect financial losses due to disrupted logistics and delayed shipments. These financial setbacks not only affect corporate balance sheets but also strain business relationships across global supply chains.

Operational disruptions constitute another significant consequence of maritime cybercrime. Cyber-attacks have led to the shutdown of port terminals, interruptions in shipping schedules, and delays in cargo handling, which directly impact the operational continuity of shipping companies and their clients.[26] These disruptions cause dissatisfaction among customers and

[23] Chalermpong Senarak. "Port cyberattacks from 2011 to 2023: a literature review and discussion of selected cases." *Maritime Economics & Logistics* 26, no. 1 (2024): 105-130.

[24] Zainab Alkhalil, Chaminda Hewage, Liqaa Nawaf, and Imtiaz Khan. "Phishing attacks: A recent comprehensive study and a new anatomy." *Frontiers in Computer Science* 3 (2021): 563060.

[25] Iris Malone, Anastasia Strouboulis, and National Counterterrorism Innovation. "Technology, and Education Center". *Emerging Risks in the Marine Transportation System (MTS), 2001–2021*. Reports, Projects, and Research, no. 27. 2022.

[26] Gabriel A. Weaver, Brett Feddersen, Lavanya Marla, Dan Wei, Adam Rose, and Mark Van Moer. "Estimating economic losses from cyber-attacks on shipping ports: An optimization-based approach." *Transportation Research Part C: Emerging Technologies* 137 (2022): 103423. See also, Chronis Kapalidis, Stavros Karamperidis, Tim Watson, and Georgios Koligiannis. "A vulnerability centric System of Systems Analysis on the maritime transportation sector most

may lead to breaches of contractual obligations, further exacerbating the harm suffered by victims.[27]

Reputational damage is equally critical, as demonstrated by the phishing attack on Clarksons.[28] The breach compromised sensitive information and raised serious concerns regarding the company's capability to protect client data. Incidents like this erode trust between companies and their stakeholders, posing long-term risks to business sustainability.[29] Loss of reputation can be even more damaging than immediate financial losses, as it undermines future business opportunities and investor confidence.[30]

In the aftermath of cyberattacks, victims often bear substantial costs to rebuild and strengthen their cybersecurity frameworks.[31] This includes upgrading IT infrastructure, retraining employees to improve cyber awareness, and developing a robust incident response protocol.[32] These post-attack burdens add further financial and operational strain on victims, highlighting the absence of systemic support structures or compensation mechanisms within the existing legal framework.[33]

These cases collectively underscore not only the severe and widespread harm inflicted by maritime cybercrime but also the urgent need for stronger legal protections for victims. The lack of specific cybersecurity legislation, particularly provisions focusing on victim protection, leaves affected parties with limited avenues for redress and recovery. Comprehensive legal reform is essential to ensure that victims of maritime cybercrime are adequately protected, supported, and empowered to seek justice through clear legal remedies and enforceable cybersecurity standards.

---

valuable assets: Recommendations for port facilities and ships." *Journal of Marine Science and Engineering* 10, no. 10 (2022): 1486.

[27] Julia Hartmann, Sebastian Forkmann, Sabine Benoit, and Stephan C. Henneberg. "A consumer perspective on managing the consequences of chain liability." *Journal of Supply Chain Management* 58, no. 4 (2022): 60.

[28] Srinath Perera, Xiaohua Jin, Alana Maurushat, and De-Graft Joe Opoku. "Factors affecting reputational damage to organisations due to cyberattacks." In *Informatics*, vol. 9, no. 1, p. 28. Multidisciplinary Digital Publishing Institute, 2022.

[29] John D'Arcy, Idris Adjerid, Corey M. Angst, and Ante Glavas. "Too good to be true: Firm social performance and the risk of data breach." *Information Systems Research* 31, no. 4 (2020): 1200-1223.

[30] Robert G. Eccles, Scott C. Newquist, and Roland Schatz. "Reputation and its risks." *Harvard Business Review* 85, no. 2 (2007): 104.

[31] Meysam Tahmasebi. "Cyberattack Ramifications, The Hidden Cost of a Security Breach." *Journal of Information Security* 15, no. 2 (2024): 90. See also, Safitra, Muhammad Fakhrul, Muharman Lubis, and Hanif Fakhrurroja. "Counterattacking cyber threats: A framework for the future of cybersecurity." *Sustainability* 15, no. 18 (2023): 13369.

[32] Atif Ahmad, Kevin C. Desouza, Sean B. Maynard, Humza Naseer, and Richard L. Baskerville. "How integration of cyber security management and incident response enables organizational learning." *Journal of the Association for Information Science and Technology* 71, no. 8 (2020): 939-953.

[33] Shai Farber. "Trauma, truth, and testimony: analysing terrorism survivors' victim impact statements." *International Journal of Comparative and Applied Criminal Justice* (2024): 1-19.

2. Legal Framework in Indonesia

Cybersecurity governance in Indonesia's maritime sector is currently regulated through a patchwork of laws and regulations that broadly address information technology and maritime operations. However, a closer examination reveals that these legal instruments lack specificity, particularly in ensuring comprehensive protection for victims of cybercrime in the maritime context. The primary legal framework is Law No. 11 of 2008 on Information and Electronic Transactions (ITE Law), which governs various aspects of digital activity, including cybercrimes such as unauthorized access, data breaches, and the distribution of malicious software. While this law establishes penalties for cyber offenses, its provisions are general and do not specifically cater to the unique characteristics and risks associated with maritime cybercrime. However, Article 30's broad definition of unauthorized access fails to address maritime-specific risks, such as breaches of navigation systems, leading to normative ambiguity that complicates prosecution and leaves victims without tailored remedies. Even with amendments under Law No. 19 of 2016, which strengthened data protection and expanded penalties, the law still falls short in outlining victim-centered remedies or specific measures aimed at protecting shipping companies, crew members, and passengers who may become victims of cyber incidents.

Meanwhile, Law No. 17 of 2008 on Shipping serves as the foundational legal instrument for regulating Indonesia's maritime activities, covering safety, environmental protection, and technical standards for ships and ports. Notably, this law does not address cybersecurity issues at all. Its focus remains on the physical and operational dimensions of maritime safety, overlooking the digital vulnerabilities that modern maritime operations face. This omission creates a critical normative gap, as maritime operations increasingly rely on digital systems, yet victims lack legal safeguards, contrary to Kelsen's Pure Theory of Law, which requires a coherent normative hierarchy to ensure legal certainty.[34] The authors assert that this gap leaves victims vulnerable to prolonged harm without clear mechanisms for redress, undermining the legal system's coherence.

Other relevant regulations include Government Regulation No. 71 of 2019 on the Implementation of Electronic Systems and Transactions, which provides guidelines for securing electronic systems across both public and private sectors. However, its scope is generic and lacks detailed provisions specific to the maritime sector. The regulation does not articulate victim protection measures or prescribe specific duties for maritime stakeholders in safeguarding digital systems that directly affect operational and personal

[34] Joanna Diane Caytas, "The Unconquerable Domain of Discretion in Kelsen's Pure Theory of Law," *Washington Undergraduate Law Review* 6, no. 1 (2012): 10.

safety. The National Cyber and Crypto Agency's National Cybersecurity Strategy aims to enhance cybersecurity readiness across various sectors, including maritime. However, its implementation remains in the early stages, and its impact on victim protection within the maritime industry has been minimal so far. The absence of detailed, enforceable standards hampers the practical application of this strategy, leaving victims vulnerable and often unsupported.

In summary, Indonesia's current legal framework exhibits significant gaps in addressing cybersecurity in the maritime sector, particularly concerning the protection and redress of victims. The lack of explicit legal provisions hampers effective prevention, enforcement, and victim recovery following cyber incidents. Moreover, law enforcement faces challenges due to unclear mandates and limited technical capacity to handle maritime-specific cyber threats. To enhance the protection of victims and strengthen overall cybersecurity resilience, there is an urgent need for the development of comprehensive, sector-specific legislation that not only defines cyber risks but also ensures robust remedies and support systems for those adversely affected by cybercrime.

A comprehensive analysis of Indonesia's regulatory landscape reveals significant gaps and deficiencies, particularly concerning the protection of victims of cybercrime in the maritime sector. While Law No. 11 of 2008 on Information and Electronic Transactions and Law No. 17 of 2008 on Shipping provide foundational regulation for cyber activities and maritime operations, both fall short in addressing the increasingly sophisticated and sector-specific cyber threats and critically, in offering concrete protections and remedies for victims.

One of the most glaring weaknesses is the absence of explicit cybersecurity provisions in Law No. 17 of 2008. This law focuses primarily on physical safety and operational protocols for ships and ports, but neglects digital risks that arise from the growing reliance on information technology in maritime management. As a result, victims whether shipping companies, employees, or passengers affected by cyber incidents are left without clear legal safeguards or avenues for redress when maritime cyberattacks occur.

Although Law No. 11 of 2008 addresses a broad spectrum of cybercrimes, its generalized scope does not cater to the maritime industry's specific vulnerabilities. While it provides basic frameworks for data protection and the prosecution of cyber offenders, it lacks tailored provisions that deal with the unique dynamics of maritime cybercrime, such as attacks on navigation systems or cargo databases. This gap complicates law enforcement's efforts to effectively identify, investigate, and prosecute cybercrimes that directly impact maritime victims. The weaknesses in

enforcement and oversight exacerbate these challenges. Coordination among regulatory bodies such as the National Cyber and Crypto Agency (*Badan Siber dan Sandi Negara*/BSSN), the Ministry of Communication and Information Technology, and the Ministry of Transportation is often fragmented, hindering swift and effective responses to maritime cyber incidents. Victims, therefore, face prolonged exposure to risk and delays in obtaining justice or compensation.

Moreover, resource limitations and a lack of specialized expertise within law enforcement and regulatory agencies further undermine the ability to protect victims. Maritime cybercrime requires niche technical knowledge, yet many authorities lack adequate training and tools to manage sector-specific threats. This gap leaves victims vulnerable, as even when breaches are reported, the responses are often insufficient or delayed. Compounding these issues is the insufficient cybersecurity infrastructure in many shipping enterprises, where minimal investment in robust security systems makes them easy targets for cybercriminals. Victims bear the brunt of these systemic weaknesses, facing financial losses, operational disruptions, and reputational harm with little recourse under existing laws.

In sum, the current legislative framework fails to provide a comprehensive and victim-centered approach to maritime cybersecurity. Without precise legal provisions and coordinated enforcement, victims of maritime cybercrime remain inadequately protected. Addressing these gaps is critical to enhancing not only the security of maritime operations but also the legal rights and protections of those adversely affected by cyberattacks. Developing specialized legislation, improving inter-agency collaboration, and investing in technical capabilities are essential steps toward ensuring that victims receive the protection and remedies they rightfully deserve.

3. Comparison with International Practices

Several countries have developed specific legislation and regulatory frameworks that focus not only on cybersecurity in the maritime industry but also emphasize the protection of victims affected by cyber incidents[35]. The experiences of the United States, Singapore, and the European Union offer valuable insights and practical models that Indonesia can adopt to strengthen both cybersecurity infrastructure and victim protection in its maritime sector[36].

In the United States, the Marine Transportation Security Act (MTSA) provides a proactive framework requiring maritime businesses to develop and

[35] Mohamed Amine Ben Farah, Elochukwu Ukwandu, Hanan Hindy, David Brosset, Miroslav Bures, Ivan Andonovic, and Xavier Bellekens. "Cyber security in the maritime industry: A systematic survey of recent advances and future trends." *Information* 13, no. 1 (2022): 22.

[36] Adam James Fenton. "Preventing catastrophic cyber–physical attacks on the global maritime transportation system: A case study of hybrid maritime security in the Straits of Malacca and Singapore." *Journal of Marine Science and Engineering* 12, no. 3 (2024): 510.

implement cybersecurity strategies, which are overseen by the U.S. Coast Guard.[37] Notably, the National Institute of Standards and Technology (NIST) has issued detailed guidelines for cybersecurity in maritime industrial control systems.[38] These guidelines not only assist shipping organizations in mitigating cyber risks but also include protocols for protecting stakeholders affected by cyber incidents, ensuring that victims have access to timely information and assistance following an attack.[39] The MTSA's mandatory cybersecurity plans ensure legal certainty for victims, unlike Indonesia's Law No. 11 of 2008, which lacks maritime-specific provisions. The authors argue that adopting similar mandatory plans would enhance victim protection in Indonesia by ensuring timely support and legal recourse.

Singapore, as a leading maritime hub, enforces the Maritime Cybersecurity Code, which sets rigorous cybersecurity standards for shipping companies and port authorities. The code mandates essential cyber risk management and requires regular audits to ensure ongoing compliance. Importantly, Singapore has established the Maritime Cyber Security Operations Centre (MSOC), which plays a pivotal role in real-time monitoring and rapid response.[40] Through MSOC, victims of cyberattacks whether corporate or individual stakeholders receive immediate assistance and clear guidance, significantly reducing recovery time and minimizing harm.[41]

The European Union, through the European Maritime Safety Agency (EMSA), has issued robust guidelines aimed at enhancing cybersecurity within the shipping industry.[42] These include best practices for managing cyber risks, safeguarding critical infrastructure, and educating maritime personnel. The NIS Directive obliges member states to strengthen cybersecurity capacities in the shipping sector and mandates swift reporting of significant cyber events.[43]

---

[37] Ian B. Finley, and Nicholas Harkiolakis. "Cybersecurity policies and supporting regulations for maritime transportation system in the USA." *International Journal of Teaching and Case Studies* 9, no. 2 (2018): 89-108.

[38] Anastasia Dimakopoulou, and Konstantinos Rantos. "Comprehensive Analysis of Maritime Cybersecurity Landscape Based on the NIST CSF v2. 0." *Journal of Marine Science and Engineering* 12, no. 6 (2024): 919.

[39] Georgios Kavallieratos, and Sokratis Katsikas. "Managing cyber security risks of the cyber-enabled ship." *Journal of Marine Science and Engineering* 8, no. 10 (2020): 768.

[40] Allan Nganga, George Nganya, Margareta Lützhöft, Steven Mallam, and Joel Scanlan. "Bridging the gap: Enhancing maritime vessel cyber resilience through security operation centers." *Sensors* 24, no. 1 (2023): 146.

[41] Nganga, Allan, Margareta Lützhöft, Joel Scanlan, and Steven Mallam. "Timely Maritime Cyber Threat Resolution in a Multi-Stakeholder Environment." *CYBER 2022 : The Seventh International Conference on Cyber-Technologies and Cyber-Systems*. (2022): 89.

[42] Oleksiy Melnyk, Oleksandr Drozdov, and Serhii Kuznichenko. "Cybersecurity in Maritime Transport: An International Perspective on Regulatory Frameworks and Countermeasures." *Lex Portus* 11 (2025): 7.

[43] Alkiviadis Giannakoulias. "NIS 2 Directive: implications for system and infrastructure security." (Master's thesis, Πανεπιστήμιο Πειραιώς, 2023).

Victim protection is integral to this framework, ensuring that those affected by maritime cyberattacks receive prompt notification, support, and access to legal remedies.

From this comparative analysis, several key strategies emerge that Indonesia could adopt to enhance both cybersecurity and victim protection in its maritime sector:

(1) Comprehensive Legislative Frameworks: Successful jurisdictions implement proactive, detailed regulations that address not only technical security standards but also include clear procedures for assisting victims of cybercrime.[44]
(2) Centralized Response Systems: The establishment of operations centers, such as Singapore's MSOC, demonstrates the effectiveness of having a centralized platform for incident monitoring, victim assistance, and coordinated response efforts.[45]
(3) Mandatory Training and Capacity Building: Regular cybersecurity training and drills help ensure maritime personnel are prepared to prevent cyber incidents and respond effectively when victims are impacted.[46]
(4) Victim-Centric Policies: Laws and regulations in these jurisdictions emphasize the importance of protecting affected parties by mandating incident reporting, transparency, and access to compensation or remedial measures.[47]
(5) Robust Incident Response and Recovery Plans: Effective regulations compel maritime businesses to develop, maintain, and regularly test incident response plans that prioritize minimizing harm to victims and restoring operations swiftly.[48]

[44] Ifeoluwa Elegbe. "Cybercrime legislation: A comparative analysis of legal frameworks, policy responses and recommendations." *International Journal of Education and Social Science Research* 7, no. 02 (2024): 200. See also, Angelyn Flowers, Sherali Zeadally, and Acklyn Murray. "Cybersecurity and US legislative efforts to address cybercrime." *Journal of Homeland Security and Emergency Management* 10, no. 1 (2013): 32.

[45] Alfred Basta, Nadine Basta, Waqar Anwar, and Mohammad Ilyas Essar. *Open-source Security Operations Center (SOC): A Complete Guide to Establishing, Managing, and Maintaining a Modern SOC*. John Wiley & Sons, 2024.

[46] Aybars Oruc, Nabin Chowdhury, and Vasileios Gkioulos. "A modular cyber security training programme for the maritime domain." *International Journal of Information Security* 23, no. 2 (2024): 1478. See also, Erlend Erstad, Rory Hopcraft, Avanthika Vineetha Harish, and Kimberly Tam. "A human-centred design approach for the development and conducting of maritime cyber resilience training." *WMU Journal of Maritime affairs* 22, no. 2 (2023): 250.

[47] Daniel Pascoe, and Marie Manikis. "Making sense of the victim's role in clemency decision making." *International Review of Victimology* 26, no. 1 (2020): 18.

[48] Paul Barnes, and Richard Oloruntoba. "Assurance of security in maritime supply chains: Conceptual issues of vulnerability and crisis management." *Journal of international Management* 11, no. 4 (2005): 522.

Implementing these best practices in Indonesia would not only fill the existing legal gaps but also ensure that victims of maritime cybercrime, whether companies, employees, or customers are adequately protected and supported. A holistic and coordinated approach is crucial for enhancing both the resilience of Indonesia's maritime infrastructure and the protection of all parties affected by cyberattacks.

4. Supervision Through Code of Ethics

In recent years, the maritime industry has witnessed a marked increase in both the frequency and severity of cyberattacks, including hacking, ransomware, and malware assaults targeting navigation systems, cargo management, and communication infrastructures. These attacks have resulted in operational paralysis, substantial financial losses, and, in some cases, endangered the safety of vessels and their crews. Importantly, these incidents have also inflicted significant harm on victims, ranging from shipping companies and port authorities to individual employees and customers, highlighting the urgent need for explicit legal protections and remedies.

Hans Kelsen's Pure Theory of Law (Reine Rechtslehre) asserts that law constitutes a hierarchical system of norms, with each lower-level norm deriving its legitimacy from a higher one, ultimately anchored in the Grundnorm, or basic norm.[49] From this perspective, the absence of precise cybersecurity regulations within Indonesia's maritime legal framework reveals a critical normative gap that undermines the consistency and effectiveness of the legal system, particularly in safeguarding victims of maritime cybercrime).

The growing scale and sophistication of cyberattacks underscore the inadequacy of existing legal standards and the pressing need to establish new, detailed norms that address these emerging threats.[50] Specific cybersecurity regulations would not only clarify the obligations of shipping enterprises but also lay out concrete mechanisms for victim protection, ensuring that victims have access to legal remedies, compensation, and structured support in the aftermath of cyber incidents.[51] In line with Kelsen's theory, these new norms would strengthen the hierarchical legal system by introducing explicit standards that address real-world technological challenges and victim vulnerabilities.[52]

[49] Joanna Diane Caytas. "The unconquerable domain of discretion in Kelsen's pure theory of law." *Washington Undergraduate Law Review* 6, no. 1 (2012): 10.

[50] John Babikian. "Navigating legal frontiers: exploring emerging issues in cyber law." *Revista Espanola de Documentacion Cientifica* 17, no. 2 (2023): 101.

[51] Tyler Moore. "The economics of cybersecurity: Principles and policy options." *International Journal of Critical Infrastructure Protection* 3, no. 3-4 (2010): 111.

[52] Eyal Benvenisti. "Upholding democracy amid the challenges of new technology: what role for the law of global governance?." *European Journal of International Law* 29, no. 1 (2018): 20.

Moreover, the repercussions of maritime cyberattacks extend beyond individual companies, posing threats to national security and economic stability. Given that the maritime industry is responsible for approximately 90% of global trade, disruptions have far-reaching effects, including delays, shortages of essential goods, and increased logistics costs. Victims at every level whether corporate or individual face cascading consequences that current regulations fail to mitigate adequately.

From Kelsen's standpoint, introducing specific cybersecurity regulations serves to fill gaps in the existing normative framework, thereby reinforcing legal certainty and ensuring a coherent system of protections. These regulations would define proactive, reactive, and remedial measures that shipping companies must adopt, not only to prevent cyber incidents but also to ensure that victims receive timely support and compensation when breaches occur. In doing so, the law would evolve into a more organized and logical system, better aligned with both technological realities and the fundamental principles of justice and victim protection.[53]

In conclusion, given the escalating cyber threats and their severe consequences for victims in the maritime sector, there is an urgent imperative to enact targeted legislation. From the lens of Hans Kelsen's Pure Theory of Law, this legislative development represents a necessary evolution of Indonesia's legal system, one that addresses current deficiencies by establishing clear, practical, and enforceable standards. Such regulations would enhance victim protection, fortify national security, and ensure that the legal system remains a cohesive and responsive framework capable of confronting modern cyber risks.

Hans Kelsen's Pure Theory of Law (Reine Rechtslehre) conceptualizes law as a hierarchical system of norms, where each norm derives its authority from a superior norm, culminating in the Grundnorm or fundamental norm.[54] In developing effective cybersecurity legislation for the maritime industry, it is crucial to incorporate critical components that uphold this normative hierarchy while ensuring comprehensive protection, especially for victims of cybercrime.

(1) Definitions, Scope, and Victim Protection: The law must provide clear and precise definitions of cybersecurity within the maritime context, explicitly identifying systems and assets that require safeguarding, such as navigation, communication, and cargo management systems. Importantly, the law should also define who qualifies as a victim whether corporate entities or individuals and

[53] Le Cheng, Jiaxuan Qiu, and Yi Yang. "Constructing cybersecurity discourse via deconstructing legislation." *International Journal of Legal Discourse* 8, no. 2 (2023): 275.

[54] L. Sree Harrish, I. Monisha, and G. Kavi Bharathi. "A Study on Kelsen's Pure Theory of Law." *Issue 1 Indian JL & Legal Rsch.* 5 (2023): 1.

articulate their rights, remedies, and access to support mechanisms following cyber incidents.

(2) Duties, Liabilities, and Victim Assistance: The legal framework should delineate the duties and liabilities of all involved parties, including shipping companies, port operators, technology providers, and regulatory bodies. These duties should not only encompass the implementation of preventive measures but also mandate prompt reporting of incidents, transparent communication with affected victims, and coordination with authorities to provide immediate assistance and compensation where applicable.

(3) Security and Victim Support Standards: The regulation should establish mandatory cybersecurity standards, such as data encryption, multi-factor authentication, and real-time network monitoring, aligned with global best practices. Additionally, it must include victim support standards, ensuring victims are informed promptly, given access to legal remedies, and supported through recovery processes, thereby reducing their long-term exposure to harm.

(4) Enforcement, Remedies, and Sanctions: Strong enforcement mechanisms are essential, including routine cybersecurity audits, compliance inspections, and clear sanctions for non-compliance. The legislation should stipulate penalties ranging from financial fines to suspension of operations. Crucially, it must also outline protocols for managing cyber incidents that prioritize victim protection, covering reporting procedures, investigation timelines, operational recovery, and restitution mechanisms for affected parties.

These key elements are essential to ensure that the legislation is holistic, effective, and consistent with Kelsen's Pure Theory of Law. By embedding victim protection at its core, the regulatory framework will contribute to a well-structured and logical legal system where each rule not only addresses technical security but also enshrines the rights and interests of victims. In operationalizing these regulations, several strategic measures are necessary:

(1) Developing a Comprehensive Legal Framework: Regulations should be carefully crafted to align with existing legal norms, drawing legitimacy from superior laws to ensure internal consistency and avoid legal conflicts. Thus, they should reinforce the coherence of the legal hierarchy.

(2) Capacity Building and Victim-Centered Training: The government must invest in training programs for law enforcement, regulators, and industry stakeholders, with specific modules focused on victim identification, protection, and legal remedies, alongside technical cybersecurity measures.
(3) Enhanced Interagency Coordination: Effective victim protection requires seamless coordination between cybersecurity agencies, maritime regulators, and law enforcement bodies. Establishing a central authority to oversee compliance, manage incident responses, and facilitate victim support services will be crucial.
(4) Industry Engagement: Collaboration with maritime industry stakeholders is vital to ensure that the regulations are both practical and enforceable. Stakeholder input can help tailor victim support provisions to the real-world needs of those at risk.
(5) Monitoring, Evaluation, and Victim Impact Assessment: A robust monitoring system should be implemented to track cyber incidents and assess the effectiveness of victim protection measures. Periodic reviews and updates to the regulations will ensure continuous improvement based on evolving cyber threats and victim experiences.

By integrating these components into dedicated cybersecurity legislation, Indonesia can establish a robust legal structure that not only fortifies maritime cybersecurity but also prioritizes the protection and support of victims. This approach aligns with Hans Kelsen's Pure Theory of Law, emphasizing the importance of a coherent, hierarchical legal system that effectively addresses modern cyber risks while safeguarding societal and individual interests.

D. CONCLUSION

Indonesia’s maritime sector remains highly vulnerable to cybercrime due to the absence of specific legislation that comprehensively governs cybersecurity and, critically, ensures protection for victims. While the Information and Electronic Transactions (ITE) Law and the Shipping Law provide a foundational legal framework, they fall short in addressing the complex, evolving nature of maritime cyber threats and fail to offer explicit safeguards and remedies for victims affected by such incidents.

Drawing upon Hans Kelsen’s Pure Theory of Law, the necessity for precise and structured legislation becomes evident. A robust legal framework should include clear definitions, well-defined duties and liabilities, stringent security standards, and effective enforcement mechanisms, all while placing victim protection at its core. Such laws would not only strengthen maritime

cybersecurity but also ensure that victims whether companies, employees, or customers receive timely support, legal remedies, and compensation following cyber incidents.

Implementing these comprehensive regulations, alongside capacity-building initiatives and enhanced interagency coordination, will fortify Indonesia's legal system, ensuring that it operates as a coherent, hierarchical, and responsive structure. This approach will significantly enhance victim protection, safeguard maritime infrastructure, and contribute to national security and economic stability in the face of increasing cyber threats.

This study recommends that the Indonesian government urgently develop and implement specific legislation that not only regulates cybersecurity in the maritime industry but also prioritizes the protection of victims affected by cybercrime. The proposed regulations should include key components such as precise definitions and scope that clearly identify victims and their rights, well-defined duties and liabilities for all relevant stakeholders, security standards aligned with international best practices, and robust enforcement mechanisms and penalties. Additionally, it is crucial to strengthen capacity through targeted training and human resource development in cybersecurity, with an emphasis on victim support protocols. Enhanced interagency cooperation is also essential to ensure a swift, coordinated response to cyber incidents, minimizing harm to victims and expediting recovery.

This research provides both a theoretical and practical foundation for policymakers to design comprehensive and adaptable regulations that address not only the technical aspects of cybersecurity but also the legal remedies and protections necessary for victims of maritime cybercrime. By drawing on Hans Kelsen's Pure Theory of Law, this study emphasizes the importance of a coherent and hierarchical legal system that is responsive to emerging cyber risks and ensures justice for affected parties. The anticipated outcomes of this study aim to strengthen the resilience of Indonesia's maritime sector against cyberattacks, enhance victim protection and recovery mechanisms, and ultimately contribute to national security and economic stability.

BIBLIOGRAPHY

Dissertation:

Miranda Silgado, David**.** *Cyber-Attacks: A Digital Threat Reality Affecting the Maritime Industry*. Dissertation, World Maritime University, 2018.

Journal:

Ahmad, Atif, Kevin C. Desouza, Sean B. Maynard, Humza Naseer, and Richard L. Baskerville. "How integration of cyber security management and incident response enables organizational learning." *Journal of the Association for Information Science and Technology* 71, no. 8 (2020): 939-953.

Al-Amaireh, M. A. A. M. "The Role of Cybersecurity in Enhancing the Effectiveness of Law Against Cybercrimes." *Revista de Gestão Social e Ambiental* 18, no. 8 (2024): e06508-e06508.

Alenezi, Mohammed N., Haneen Alabdulrazzaq, Abdullah A. Alshaher, and Mubarak M. Alkharang. "Evolution of malware threats and techniques: A review." *International journal of communication networks and information security* 12, no. 3 (2020): 326-337.

Alkhalil, Zainab, Chaminda Hewage, Liqaa Nawaf, and Imtiaz Khan. "Phishing attacks: A recent comprehensive study and a new anatomy." *Frontiers in Computer Science* 3 (2021): 563060.

Androjna, Andrej, Tanja Brcko, Ivica Pavic, and Harm Greidanus. "Assessing cyber challenges of maritime navigation." *Journal of Marine Science and Engineering* 8, no. 10 (2020): 776.

Ashraf, Imran, Yongwan Park, Soojung Hur, Sung Won Kim, Roobaea Alroobaea, Yousaf Bin Zikria, and Summera Nosheen. "A survey on cyber security threats in IoT-enabled maritime industry." *IEEE Transactions on Intelligent Transportation Systems* 24, no. 2 (2022): 2677-2690.

Babikian, John. "Navigating legal frontiers: exploring emerging issues in cyber law." *Revista Espanola de Documentacion Cientifica* 17, no. 2 (2023): 95-109.

Barnes, Paul, and Richard Oloruntoba. "Assurance of security in maritime supply chains: Conceptual issues of vulnerability and crisis management." *Journal of international Management* 11, no. 4 (2005): 519-540.

Basta, Alfred, Nadine Basta, Waqar Anwar, and Mohammad Ilyas Essar. *Open-source Security Operations Center (SOC): A Complete Guide to Establishing, Managing, and Maintaining a Modern SOC*. John Wiley & Sons, 2024.

Ben Farah, Mohamed Amine, Elochukwu Ukwandu, Hanan Hindy, David Brosset, Miroslav Bures, Ivan Andonovic, and Xavier Bellekens. "Cyber security in the maritime industry: A systematic survey of recent advances and future trends." *Information* 13, no. 1 (2022): 22.

Benvenisti, Eyal. "Upholding democracy amid the challenges of new technology: what role for the law of global governance?." *European Journal of International Law* 29, no. 1 (2018): 9-82.

Caytas, Joanna Diane. "The unconquerable domain of discretion in Kelsen's pure theory of law." *Washington Undergraduate Law Review* 6, no. 1 (2012): 1-46.

Cheng, Le, Jiaxuan Qiu, and Yi Yang. "Constructing cybersecurity discourse via deconstructing legislation." *International Journal of Legal Discourse* 8, no. 2 (2023): 273-297.

Clavijo Mesa, Maria Valentina, Carmen Elena Patino-Rodriguez, and Fernando Jesus Guevara Carazas. "Cybersecurity at Sea: A Literature Review of Cyber-Attack Impacts and Defenses in Maritime Supply Chains." *Information* 15, no. 11 (2024): 710.

D'Arcy, John, Idris Adjerid, Corey M. Angst, and Ante Glavas. "Too good to be true: Firm social performance and the risk of data breach." *Information Systems Research* 31, no. 4 (2020): 1200-1223.

Dimakopoulou, Anastasia, and Konstantinos Rantos. "Comprehensive Analysis of Maritime Cybersecurity Landscape Based on the NIST CSF v2. 0." *Journal of Marine Science and Engineering* 12, no. 6 (2024): 919.

Eccles, Robert G., Scott C. Newquist, and Roland Schatz. "Reputation and its risks." *Harvard Business Review* 85, no. 2 (2007): 104.

Elegbe, Ifeoluwa. "Cybercrime legislation: A comparative analysis of legal frameworks, policy responses and recommendations." *International Journal of Education and Social Science Research* 7, no. 02 (2024): 199-207.

Erstad, Erlend, Rory Hopcraft, Avanthika Vineetha Harish, and Kimberly Tam. "A human-centred design approach for the development and conducting of maritime cyber resilience training." *WMU Journal of Maritime affairs* 22, no. 2 (2023): 241-266.

Farber, Shai. "Trauma, truth, and testimony: analysing terrorism survivors' victim impact statements." *International Journal of Comparative and Applied Criminal Justice* (2024): 1-19.

Fenton, Adam James. "Preventing catastrophic cyber–physical attacks on the global maritime transportation system: A case study of hybrid maritime security in the Straits of Malacca and Singapore." *Journal of Marine Science and Engineering* 12, no. 3 (2024): 510.

Finley, Ian B., and Nicholas Harkiolakis. "Cybersecurity policies and supporting regulations for maritime transportation system in the USA." *International Journal of Teaching and Case Studies* 9, no. 2 (2018): 89-108.

Flowers, Angelyn, Sherali Zeadally, and Acklyn Murray. "Cybersecurity and US legislative efforts to address cybercrime." *Journal of Homeland Security and Emergency Management* 10, no. 1 (2013): 29-55.

Giannakoulias, Alkiviadis. "NIS 2 Directive: implications for system and infrastructure security." Master's thesis, Πανεπιστήμιο Πειραιώς, 2023.

Giannopoulos, Georgios A. "The application of information and communication technologies in transport." *European journal of operational research* 152, no. 2 (2004): 302-320.

Harrish, L. Sree, I. Monisha, and G. Kavi Bharathi. "A Study on Kelsen's Pure Theory of Law." *Issue 1 Indian JL & Legal Rsch.* 5 (2023): 1.

Hartmann, Julia, Sebastian Forkmann, Sabine Benoit, and Stephan C. Henneberg. "A consumer perspective on managing the consequences of chain liability." *Journal of Supply Chain Management 58*, no. 4 (2022): 58-89.

Healy, Deirdre. "Exploring victims' interactions with the criminal justice system." *Ireland Department of justice and equality report* (2019).

Humayun, Mamoona, N. Zaman Jhanjhi, Ahmed Alsayat, and Vasaki Ponnusamy. "Internet of things and ransomware: Evolution, mitigation and prevention." *Egyptian Informatics Journal* 22, no. 1 (2021): 105-117.

Imran, Mohammad Fadil. "Cyber Criminology: An analysis of the Indonesian and the United States Police Perception." *International Journal of Cyber Criminology* 17, no. 2 (2023): 250-261.

Kapalidis, Chronis, Stavros Karamperidis, Tim Watson, and Georgios Koligiannis. "A vulnerability centric System of Systems Analysis on the maritime transportation sector most valuable assets: Recommendations for port facilities and ships." *Journal of Marine Science and Engineering* 10, no. 10 (2022): 1486.

Kavallieratos, Georgios, and Sokratis Katsikas. "Managing cyber security risks of the cyber-enabled ship." *Journal of Marine Science and Engineering* 8, no. 10 (2020): 768.

Koss, Mary P. "Restoring rape survivors: Justice, advocacy, and a call to action." *Annals of the New York Academy of Sciences* 1087, no. 1 (2006): 206-234.

Macfarlane, Rory. "Cyber-risk in shipping and its management." In *Ship Operations*, pp. 69-83. England: Informa Law from Routledge, 2020.

Mai-inji, A. Y., K. E. Ukhurebor, and L. O. Babatope. "Impending maritime cyberspace threats: An educational research perspective." *Journal of Infrastructure, Policy and Development* 8, no. 8 (2024): 4146.

Malone, Iris, Anastasia Strouboulis, and National Counterterrorism Innovation. "Technology, and Education Center". *Emerging Risks in the Marine Transportation System (MTS), 2001–2021*. Reports, Projects, and Research, no. 27. 2022.

Melnyk, Oleksiy, Oleksandr Drozdov, and Serhii Kuznichenko. "Cybersecurity in Maritime Transport: An International Perspective on Regulatory Frameworks and Countermeasures." *Lex Portus* 11 (2025): 7.

Mohsendokht, Massoud, Huanhuan Li, Christos Kontovas, Chia-Hsun Chang, Zhuohua Qu, and Zaili Yang. "Decoding dependencies among the risk factors influencing maritime cybersecurity: Lessons learned from historical incidents in the past two decades." *Ocean Engineering* 312 (2024): 119078.

Moore, Tyler. "The economics of cybersecurity: Principles and policy options." *International Journal of Critical Infrastructure Protection* 3, no. 3-4 (2010): 103-117.

Nganga, Allan, George Nganya, Margareta Lützhöft, Steven Mallam, and Joel Scanlan. "Bridging the gap: Enhancing maritime vessel cyber resilience through security operation centers." *Sensors* 24, no. 1 (2023): 146.

Nganga, Allan, Margareta Lützhöft, Joel Scanlan, and Steven Mallam. "Timely Maritime Cyber Threat Resolution in a Multi-Stakeholder Environment." *CYBER 2022 : The Seventh International Conference on Cyber-Technologies and Cyber-Systems*. (2022): 86-92.

Oruc, Aybars, Nabin Chowdhury, and Vasileios Gkioulos. "A modular cyber security training programme for the maritime domain." *International Journal of Information Security* 23, no. 2 (2024): 1477-1512.

Pandey, Shipra, Rajesh Kumar Singh, Angappa Gunasekaran, and Anjali Kaushik. "Cyber security risks in globalized supply chains: conceptual framework." *Journal of Global Operations and Strategic Sourcing* 13, no. 1 (2020): 103-128.

Pascoe, Daniel, and Marie Manikis. "Making sense of the victim's role in clemency decision making." *International Review of Victimology* 26, no. 1 (2020): 3-28.

Perera, Srinath, Xiaohua Jin, Alana Maurushat, and De-Graft Joe Opoku. "Factors affecting reputational damage to organisations due to cyberattacks." In *Informatics*, vol. 9, no. 1, p. 28. Multidisciplinary Digital Publishing Institute, 2022.

Qian, Xu. "Redefining International Law Paradigms: Charting Cybersecurity, Trade, and Investment Trajectories within Global Legal Boundaries." *The Journal of World Investment & Trade* 25, no. 3 (2024): 295-333.

Safitra, Muhammad Fakhrul, Muharman Lubis, and Hanif Fakhrurroja. "Counterattacking cyber threats: A framework for the future of cybersecurity." *Sustainability* 15, no. 18 (2023): 13369.

Senarak, Chalermpong. "Port cyberattacks from 2011 to 2023: a literature review and discussion of selected cases." *Maritime Economics & Logistics* 26, no. 1 (2024): 105-130.

Symes, Steve, Eddie Blanco-Davis, Tony Graham, Jin Wang, and Edward Shaw. "Cyberattacks on the Maritime Sector: A Literature Review." *Journal of Marine Science and Application* 23, no. 4 (2024): 689-706.

Tahmasebi, Meysam. "Cyberattack Ramifications, The Hidden Cost of a Security Breach." *Journal of Information Security* 15, no. 2 (2024): 87-105.

Walton, Beatrice A. "Duties Owed: Low-Intensity Cyber Attacks and Liability for Transboundary Torts in International Law." *Yale LJ* 126 (2016): 1460.

Weaver, Gabriel A., Brett Feddersen, Lavanya Marla, Dan Wei, Adam Rose, and Mark Van Moer. "Estimating economic losses from cyber-attacks on shipping ports: An optimization-based approach." *Transportation Research Part C: Emerging Technologies* 137 (2022): 103423.

Zimba, Aaron, Zhaoshun Wang, and Mumbi Chishimba. 2019. "Addressing Crypto-Ransomware Attacks: Before You Decide Whether To-Pay or Not-To." *Journal of Computer Information Systems* 61 (1): 53–63.

Regulation:

Law Number 11 of 2008 on Electronic Information and Transactions

Law Number 17 of 2008 on Shipping

Law Number 19 of 2016 on Amendments to Law Number 11 of 2008 on Electronic Information and Transactions (ITE Law).