Received: 01.12.2025
Accepted: 11.03.2026
Published Online: 29.06.2026
DOI: 10.18613/deudfd.1833355
Research Article

Dokuz Eylül University
Maritime Faculty Journal
Vol:18 Issue:1 Year:2026 pp:34-59
E-ISSN: 2458-9942

THE ROLE OF CYBERSECURITY CAPACITY IN CONTAINER SHIPPING: AN ECONOMETRIC ANALYSIS OF SELECTED COUNTRIES*

BURCU YILMAZ[1]

ABSTRACT

With the widespread diffusion of digital technologies, cybersecurity has become a critical concern for international trade and logistics operations. In this context, container transportation, which occupies a central position in global trade, emerges as a field that is directly exposed to cyber threats. Accordingly, this study aims to analyze the effects of the indicators included in the Global Cybersecurity Index on container transportation. The analysis employs container transportation data for 2023 from the OECD, alongside Global Cybersecurity Index data published by the International Telecommunication Union based on observations from 2023–2024. In the empirical model, container transportation is specified as the dependent variable, while legal measures, technical measures, organizational measures, capacity development, and cooperation measures are included as independent variables. Within this framework, regression analysis is conducted using cross-sectional data for 29 countries. The findings reveal that the variable of legal measures has a negative and statistically significant effect, indicating that an excessive regulatory burden constrains container volume. By contrast, capacity development is found to have a positive and significant impact. This result suggests that investments in infrastructure, human capital, and technology in the field of cybersecurity contribute positively to container transportation. Consequently, prioritizing capacity-building investments, particularly through the training of a qualified cybersecurity workforce, is projected to be a strategy that can enhance container transportation volumes.

Keywords: *Container transportation, International trade, Logistics, Cybersecurity, Cyber risk*

---

[1] Dr., Kayseri University, Faculty of Applied Sciences, Department of International Trade and Logistics, burcukaya107@gmail.com, ORCID: 0000-0002-6004-0640.

*This study is an extended version of the paper that was presented orally and published in abstract form at the 2nd Foreign Trade Summit held on 7–10 November 2025.

KONTEYNER TAŞIMACILIĞINDA SİBER GÜVENLİK KAPASİTESİNİN ROLÜ: SEÇİLMİŞ ÜLKELER İLE EKONOMETRİK BİR ANALİZ

ÖZ

Dijital teknolojilerin yaygınlaşmasıyla birlikte siber güvenlik konusu, uluslararası ticaret ve lojistik faaliyetler açısından kritik bir boyut haline gelmiştir. Uluslararası ticarette önemli bir yere sahip olan konteyner taşımacılığı, siber tehditlerden doğrudan etkilenen bir alan olarak öne çıkmaktadır. Bu doğrultuda çalışma Küresel Siber Güvenlik Endeksi'nde yer alan göstergelerin konteyner taşımacılığına etkilerini analiz etmeyi amaçlamaktadır. Araştırmada, OECD'nin 2023 yılına ait konteyner taşımacılığı verileri ile Uluslararası Telekomünikasyon Birliği tarafından 2023–2024 yıllarında toplanan verilere dayanılarak hazırlanan Küresel Siber Güvenlik Endeksi raporundaki veriler kullanılmıştır. Konteyner taşımacılığı bağımlı değişken olarak; hukuki tedbirler, teknik tedbirler, kurumsal düzenlemeler, kapasite geliştirme ve iş birliği tedbirleri ise bağımsız değişkenler olarak analize dâhil edilmiştir. Bu çerçevede 29 ülkeye ait yatay kesit verisi üzerinden regresyon analizi uygulanmıştır. Elde edilen bulgular, hukuki tedbirler değişkeninin negatif ve anlamlı olduğunu, bu doğrultuda aşırı regülasyon yükünün konteyner hacmini sınırladığını göstermektedir. Buna karşın, kapasite geliştirme değişkeninin pozitif ve anlamlı olduğu tespit edilmiştir. Bu bulgu, siber güvenlik alanındaki altyapı, insan kaynağı ve teknoloji yatırımlarının konteyner taşımacılığına olumlu yönde etki ettiğini göstermektedir. Bununla birlikte siber güvenlik alanında nitelikli iş gücü yetiştirilmesi yoluyla kapasite geliştirme yatırımlarına öncelik verilmesinin, konteyner taşımacılığı hacmini artıracak bir strateji olacağı öngörülmektedir.

Anahtar Kelimeler: *Konteyner taşımacılığı, Uluslararası ticaret, Lojistik, Siber güvenlik, Siber risk*

1. INTRODUCTION

Approximately 80% of international merchandise trade worldwide is carried by sea, and this share is known to be even higher for many developing economies (UNCTAD, 2025). Disruptions in maritime logistics ripple through supply chains, driving up trade costs and ultimately influencing price levels. The severe dislocations experienced in global supply chains during the COVID-19 pandemic have vividly underscored this vulnerability. Consequently, the smooth functioning of maritime trade and logistics plays a pivotal role in supporting economic development. Container ships have transformed global trade by providing a cost-effective, reliable, and efficient means of transporting goods. Designed to carry standardized shipping containers, these vessels have revolutionized logistics by enabling seamless intermodal transport across ships, trucks, and trains. As international trade activities have expanded, container and

cargo ships have continued to knit together markets and economies across the globe. For this reason, container shipping constitutes the backbone of global supply chains.

The increase in global trade volume and the growing complexity of transport networks have made the integration of digital technologies into maritime transport indispensable for ensuring both competitiveness and sustainability. The effective management of logistics processes and the uninterrupted functioning of supply chains are now closely intertwined with the deployment of digital technologies in maritime transport systems. In an era marked by accelerating digital transformation, the incorporation of automation, artificial intelligence, and smart systems into all stages of commercial activity from production and marketing through to logistics management substantially shortens the time required for products to reach end consumers. While this development has intensified competition and heightened operational risks in maritime transport, it has simultaneously rendered key capabilities such as efficiency, optimization, resilience, predictability, sustainability, and reliability strategic imperatives for the sector (UNCTAD, 2022).

However, this increasing digital integration within maritime processes also brings with it a number of challenges, most notably cyber threats and attacks that adversely affect ports and maritime operations. Onboard computers and software systems are now extensively relied upon to ensure efficient operational management (Kaštelan et al. 2024). As the use of digital tools expands, the risk of cyber threats likewise escalates, giving rise to significant security vulnerabilities across the maritime sector. The use of unsupported operating systems on ships (Svilicic et al. 2019), the creation of fictitious vessels through Automatic Identification System (AIS) spoofing, and the manipulation of vessel positions by transmitting false signals via GPS spoofing (Tam and Jones, 2019; Androjna et al. 2021; Amro and Gkioulos, 2022) all contribute to heightened cyber risk exposure. In addition, the infiltration of ship systems by ransomware (Meland et al. 2021; Meland et al. 2022) further exacerbates these vulnerabilities. Such attacks disrupt cargo flows in maritime transport, thereby laying bare the far-reaching implications of cyber risks for international trade and logistics activities.

Given that the cybersecurity risks brought about by increasing digitalization pose a direct threat to operational continuity and the smooth flow of trade in maritime transport, analyzing the impact of countries' cybersecurity capacities on container shipping is crucial for ensuring that container transport remains secure, uninterrupted, and efficient. Such an analysis is significant not only from a theoretical standpoint, but also in

terms of formulating informed policy recommendations for the sector. A substantial proportion of existing studies, however, primarily focuses on the deployment of technologies needed to identify threats targeting information and communication technology components that affect ship operations (Potamos et al. 2024: 2).

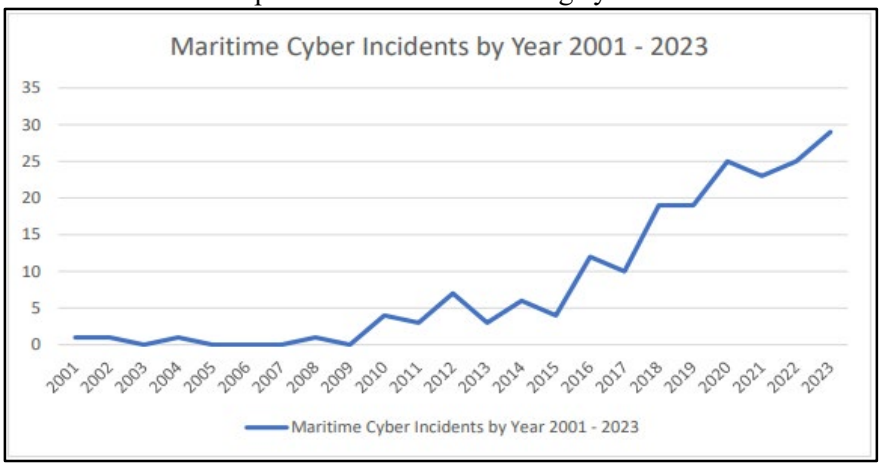
Although some studies in the literature have examined certain implications of cybersecurity for logistics activities using survey-based analyses, multi-criteria decision-making methods, and systematic literature reviews (Karahalios, 2020; Nguyen, 2021; Senarak, 2021a; Senarak, 2021b; Ilyas et al. 2023; Oral and Paker, 2023; Adhikari and Baidya, 2024; Senarak, 2024; Yue and Mangan, 2024; Yilmaz, 2025), there appears to be a lack of empirical research that directly investigates the relationship between countries' cybersecurity capacity and container shipping performance. Accordingly, this study seeks to fill this gap in literature and, in doing so, offers a novel contribution to ongoing scholarly and policy-oriented debates in this field. Against this backdrop, the present study aims to analyze, through cross-sectional data methods, the effects of the indicators included in the Global Cybersecurity Index (GCI) on countries' container transport performance. To this end, the second section reviews the body of literature that addresses the implications of cybersecurity for the maritime sector and container shipping. The third section sets out the data set employed, and the methodological approach adopted in the analysis. The fourth section presents and interprets empirical findings in tabular form. Finally, the fifth section discusses the results in light of the existing literature and puts forward a set of policy recommendations related to the topic.

2. CONCEPTUAL FRAMEWORK AND LITERATURE REVIEW

With the intensification of globalization and international competition, countries have increasingly sought to integrate Industry 4.0 technologies into the logistics sector, as in many other industries. Through the growing use of digital technologies and the acceleration of automation, it is aimed to reduce delays and, in turn, enhance operational efficiency in various processes such as port security, cargo handling, and ship navigation (Senerak, 2021: 347; Mesa et al. 2024: 2). Maritime transport is thus undergoing a significant transformation driven by technological advances associated with Industry 4.0. However, this transformation simultaneously makes port operations and ship navigation more exposed and vulnerable to cyber risks (Potamos, 2024: 5). Accordingly, in the contemporary context, protecting maritime transport operations against

cyberattacks that may disrupt critical processes and building up countries' cybersecurity capacities has become a crucial necessity.

According to the International Maritime Organization (IMO), maritime cyber risk denotes the potential for a technology asset to be affected by a circumstance or event which, through the corruption or compromise of information or systems, may give rise to operational disruptions or safety-related problems in maritime activities (IMO, 2025). In this regard, maritime cyber risk management may be understood as the implementation of measures and practices designed to ensure resilient and secure maritime transport in the face of evolving cyber threats.



Graph 1: Maritime Cyber Incidents by Year 2001-2023
Source: Fenton, 2024.

The importance of enhancing cybersecurity capacity and implementing effective cyber risk management in maritime transport is further underpinned by empirical evidence illustrating the evolution of cyber threats in the maritime sector over time. Figure 1 displays the annual change in the number of reported cyber incidents in the maritime industry for the period 2001–2023. As shown in the Figure 1, the number of cyber incidents remained relatively stable between 2001 and 2008 compared with more recent years. However, from 2009 onwards and particularly from 2015 there is a noticeable upward trend. Between 2018 and 2023, this trend becomes a sharp escalation in reported cyber events. Taken together, the figure demonstrates that cyberattacks targeting the maritime sector have clearly intensified over the last five to six years. In other words, while the diffusion of digital transformation in seaborne trade has undoubtedly boosted speed and efficiency in operational processes, it has simultaneously brought about a rise in cybersecurity risks. Consequently, the pattern observed in the figure helps to explain why ensuring

cybersecurity in maritime transport has emerged as a critical and rapidly growing field of inquiry in recent years.

When literature is examined as a whole, it becomes evident that cybersecurity has emerged as an increasingly strategic factor in the context of maritime and container transport. Existing studies consistently emphasize that a country's cybersecurity capacity directly influences the reliability and efficiency of its transportation systems. However, the nature and magnitude of these effects vary across studies, depending on the methodological approaches adopted, the types of analyses conducted, and the specific cybersecurity components or indicators under investigation.

Yue and Mangan (2024) argue that, in container shipping, elements such as network reliability and the effectiveness of information sharing significantly influence overall system performance, while cyberattacks pose a direct threat to this reliability. In a similar vein, Ben Farah et al. (2022) demonstrate that digitalization renders ship and port operations increasingly vulnerable, with shortcomings in crew training and software vulnerabilities emerging as particularly salient sources of risk. Likewise, Senarak (2024) underscores that ransomware attacks represent the most critical threat in port environments, primarily due to weak procedural safeguards and low levels of staff awareness. Taken together, these findings indicate that cybersecurity capacity must be approached not only through technical measures, but also by systematically addressing human and institutional dimensions.

Capacity development is not only one of the GCI components employed in this study, but also one of the most frequently emphasized dimensions in the literature. The UNIWA Cyber Range platform developed by Chouliaras et al. (2023) has emerged as an innovative tool aimed at narrowing the cybersecurity skills gap across Europe. Similarly, Putra et al. (2023) and Senarak (2021a; 2021b) argue that staff training and awareness play a pivotal role in preventing cyberattacks. Ilyas et al. (2023) likewise show that, during the pandemic period, errors in information flow and human-induced risks adversely affected transport security. Collectively, these studies indicate that cybersecurity is closely intertwined with the availability of a well-trained workforce and with organizational preparedness.

Studies that draw attention to legal and institutional arrangements highlight the importance of institutional coordination and regulatory compliance in the field of cybersecurity. Senarak (2021b) underscores the necessity of aligning port operators' internal policies with international standards, whereas Karahalios (2020) and Ben Farah et al. (2022) point out

that regulatory gaps tend to exacerbate operational security vulnerabilities. These findings are particularly noteworthy for the present study, as they provide a meaningful basis for interpreting the empirical results associated with the *legal measures* variable through different methodological lenses.

Adhikari and Baidya (2024) argue that encryption practices and identity management protocols constitute the primary line of defense in containerization technologies, while Kayişoğlu et al. (2024) demonstrate that standards such as ISO/IEC 27001 are effective in mitigating cyber risks associated with ECDIS systems. However, a substantial body of work also notes that these measures often have only limited scope for implementation in developing countries, chiefly because they are costly and require advanced technical expertise (Putra et al. 2023; Yilmaz, 2025).

From a methodological standpoint, the existing research exhibits considerable diversity. Multi-criteria decision-making (MCDM) techniques have been widely employed in analyses in this field, with the AHP method most frequently preferred, often in combination with survey data and SWOT analyses (Karahalios, 2020; Nguyen, 2021; Oral and Paker, 2023; Putra et al. 2023; Karahalios 2025). Beyond these approaches, systematic literature reviews and bibliometric analyses stand out as the most used methods in the domain (Ben Farah et al., 2022; Chouliaras et al. 2023; Adhikari and Baidya, 2024; Yue and Mangan, 2024; Yilmaz, 2025).

In the existing literature, cybersecurity is widely acknowledged as a key factor influencing the maritime sector and the performance of container transport. However, a substantial proportion of current studies is predominantly based on literature reviews rather than empirical modelling. To date, no study has been identified that explicitly incorporates the components of the Global Cybersecurity Index (GCI) and evaluates the impact of cybersecurity on container shipping through an econometric framework. Accordingly, the present study is expected to make a meaningful contribution to literature by addressing this gap.

Table 1: Literature Review on the Impact of Cybersecurity on Maritime and Container Shipping

Author(s) & Year	Aim and Methodology	Key Findings
Yue and Mangan (2024)	The study formulates a set of research questions to identify which factors influence the concept of reliability in container shipping networks and, to this end, employs the Critical Appraisal Skills Program (CASP) to guide the selection and evaluation of relevant studies. Within this framework, 136 scientific publications are analyzed by means of a systematic literature review.	It is found that the security of port infrastructure strongly influences the reliability of container shipping, the reliability of ports and their connections, the degree of integration across different transport modes, and the effectiveness of information sharing among stakeholders. The study also notes that cyberattacks constitute critical threats in container shipping networks, as they may lead to operational disruptions and a loss of reliability.
Chouliaras et al. (2023)	The study aims to evaluate a container-based cyber range platform developed for cybersecurity training, research, and capacity-building activities. To this end, a literature review was conducted, the system was designed and developed, and its performance was examined through experimental testing.	The proposed cyber range platform offers a low-cost alternative to traditional approaches and provides a container-based cloud infrastructure, scenario management, advanced network isolation, and robust authentication mechanisms. As such, the study makes a significant technical contribution to reducing the cybersecurity skills gap in Europe.
Karahalios, (2020)	The study evaluates the impacts of cyber threats on ship operations by applying the STPA-SafeSec Analysis (Systems-Theoretic Process Analysis for Safety and Security) in conjunction with the Fuzzy AHP method.	An examination of 15 vessels revealed that their cybersecurity management systems remained at only a basic level, with substantial deficiencies identified in software updates, data encryption, intrusion prevention, and crew training. Interruptions to communication services and the compromise of vessel tracking emerged as major threats, indicating that critical information such as a ship's position, route, speed, port schedule, or movement data could potentially be intercepted and exploited.
Nguyen (2021)	The study employs content analysis using NVivo software to evaluate operational risks in container shipping.	According to the analysis, ports and maritime transport companies emerge as the primary carriers of risk. Issues related to information security and cyberattack-induced risks are also addressed in a substantial proportion of the reviewed articles. In this line of research, methods such as Bayesian Networks, Monte Carlo simulation, and

		the Analytic Hierarchy Process have been widely employed.
Adhikari and Baidya (2024)	The study assesses the security measures required to enhance cybersecurity in containerization technologies, the challenges encountered in this process, and the best practices implemented in the field, drawing on evidence from a comprehensive literature review and a series of case analyses.	The findings indicate that attackers primarily gain system access by exploiting vulnerabilities in container runtimes and targeting image registries. Encryption mechanisms, alongside the protection of credentials and other sensitive data, constitute the fundamental line of defense in this context.
Ben Farah et al. (2022)	The study investigates cybersecurity threats, types of attacks, and corresponding defense measures in the maritime domain by employing a systematic literature review approach.	The review suggests that digitalization has amplified the incidence of cyberattacks. Incidents targeting companies such as Maersk, HMM, and MSC between 2017 and 2021 have resulted in financial losses amounting to millions of dollars. Moreover, factors such as the use of shared passwords by crew members, insufficient training, and reliance on portable media for software updates make these organizations particularly vulnerable to attackers.
Putra et al. (2023)	The study employs the AHP and TOPSIS methods to identify and rank maritime cybersecurity threats in Indonesia according to their level of importance.	The analysis reveals that deficiencies in training and a lack of awareness are key determinants of rising cyber risks, and that economic fraud features prominently among maritime cyberattacks. It is further concluded that, in developing economies, there is a pressing need to strengthen national cybersecurity policies.
Yilmaz (2025)	The study examines cybersecurity practices in the maritime sector by means of a bibliometric analysis.	The findings indicate that cyber threats have increased in tandem with digitalization. Autonomous ships, port cybersecurity, and cyber risk management have emerged as the most extensively researched topics, whereas in developing countries, both cybersecurity awareness and the volume of related research remain insufficient.
Kayişoğlu et al. (2024)	The study analyses the cybersecurity risks associated with the Electronic Chart Display and Information System (ECDIS) on board ships and identifies the preventive barriers to mitigate these risks by applying the UCOM-F	The analysis identifies the infection of systems with malicious software via the internet or intranet as the most critical threat. Intrusions through remote access and human errors also emerge as major risk factors. The use of up-to-date antivirus solutions and contemporary information technologies, coupled with enhanced staff awareness and

	(Fuzzy Full Consistency Method) approach.	compliance with international standards are found to constitute effective preventive barriers.
Ilyas et al. (2023)	The study employs the Delphi method to identify the impacts of the COVID-19 pandemic on the security of the maritime container supply chain.	Human resources were identified as the domain most prone to error. Failures in information flows also emerged as a major source of risk, while port congestion was found to constitute the most critical security issue. In addition, threats such as information leakage, the sabotage of operations, and data theft were reported to have a negative impact on transport activities.
Senarak (2024)	The study aims to analyze port-related cyberattacks by employing a systematic literature review approach.	Ransomware has emerged as the most prominent form of cyberattack. The cases examined indicate that weak cybersecurity procedures and inadequate staff training play a decisive role in increasing vulnerability to such attacks. By contrast, collaboration with external stakeholders and the strengthening of technological infrastructure are found to mitigate these risks.
Senarak (2021b)	The study aims to develop policies and preventive strategies to address cybersecurity vulnerabilities in ports. To this end, survey data collected from 243 firms were analyzed using both exploratory and confirmatory factor analysis.	Human errors and inadequate staff training are found to heighten the likelihood of cyberattacks, while shortcomings in security infrastructure and procedural deficiencies create a conducive environment for such incidents. Accordingly, the study concludes that aligning risk management and emergency response procedures with international standards is of critical importance.
Oral and Paker (2023)	Threats to container shipping along the trade corridor between Türkiye and the Far East were analyzed using the Delphi method, SWOT analysis, and the AHP technique.	Cyberattacks were identified as the highest-risk factor, followed by war and piracy activities. The findings further indicate that, in order to ensure cybersecurity in port and ship operations, it is essential to implement protocols that comply with the International Maritime Organization (IMO) guidelines and to pay close attention to the timely updating of software.
Karahalios (2025)	It was aimed to assess the risk of cyberattacks on autonomous vessels during their within-port maneuvers. Threat scenarios were developed, and expert judgments were elicited using the Delphi method. The	The analyses indicated that vessel-related information is excessively exposed through AIS. In addition, it was determined that the close proximity of ports and canals to urban areas in the UK facilitates attacks on wireless networks. The human factor was also found to be critical in such incidents, as poor

	weights of the identified threats were then analyzed using Fuzzy AHP.	communication or inattentiveness can increase the level of risk.
Stępień, (2025)	It was aimed to examine how regulatory gaps in the cybersecurity governance of autonomous vessels influence cyberattacks. To this end, a conceptual assessment was conducted alongside an evaluation of the relevant legal framework.	The assessments indicate that, as the level of autonomy increases, reliance on artificial intelligence also increases, thereby making vessels more vulnerable to cyberattacks. It was further determined that gaps in existing regulations heighten the risk of attacks on autonomous vessels and fail to adequately address the vessel-specific requirements of autonomous maritime operations.

3. DATA SET and METHODOLOGY

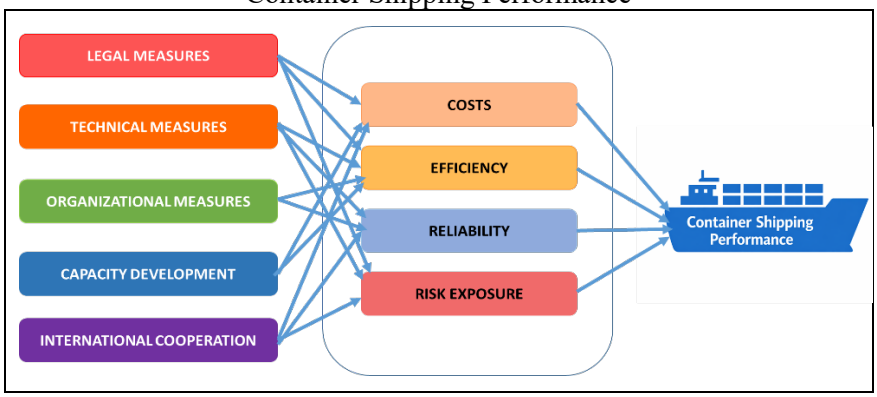
This study aims to examine the impact of cybersecurity capacity on container transportation by employing a cross-sectional data analysis. To this end, a regression model was constructed using cross-sectional data, in which one dependent variable is explained by a set of independent variables. Through this model, the direction and magnitude of the effects of the independent variables on the dependent variable were statistically identified. Although panel data analysis allows the joint consideration of both cross-sectional and time dimensions, a cross-sectional approach was adopted in this study because the Global Cybersecurity Index (GCI) components used as independent variables are available only for a single reporting year (2024). Nevertheless, the potential channels through which the GCI components may influence container shipping performance are analytically justified within the conceptual framework presented below.

The Global Cybersecurity Index comprises five primary indicators. These indicators are legal measures, technical measures, organizational measures, capacity development, and cooperation. These components, in the context of cybersecurity, which is an area that has gained importance alongside the digital transformation experienced in international trade and logistics activities, reflect the capacities of countries in terms of institutional preparedness and implementation. Legal measures cover the laws and regulations of countries in the field of cybersecurity regarding the protection of personal data, privacy, breach notifications and the punishment of cybercrimes; technical measures include computer incident response teams, security operation centers, national and international cyber exercises and the adoption of standards; organizational measures express national cybersecurity strategies, the establishment of institutions responsible for cybersecurity, and the protection of critical information infrastructure; capacity development indicates strengthening the

institutional-level preparedness of countries by increasing R&D activities in the field of cybersecurity and by training qualified human resources; and cooperation measures, by covering public–private partnerships, bilateral and multilateral international agreements, regional cooperations and inter-institutional coordination, express the capacity for acting jointly against cyber threats (ITU, 2024).

The potential impacts of the components addressed on container shipping should also be evaluated through four key factors: costs, efficiency, reliability, and risk exposure (Figure 1). In this context, it is anticipated that legal measures may enhance long-term resilience in risk management due to data protection requirements and sanctions against cybercrime. In the short term, however, compliance costs may arise for firms or ports; the need to align reporting processes accordingly may increase costs and is also expected to have adverse effects by reducing operational efficiency. Technical measures enable faster detection of cyber incidents by increasing incident response capacity and facilitating the adoption of standards through the conduct of cyber exercises. This may mitigate operational disruptions resulting from cyber threats or attacks. Accordingly, by enhancing efficiency and reliability in port operations and reducing risk exposure, such measures may support logistics flows. Organizational measures may facilitate more efficient and secure operations by strengthening cybersecurity strategies and improving the information infrastructure and coordination among ports, carriers, and customs stakeholders. This may also reduce risk exposure in operational processes. Capacity development supports the development of qualified human resources with greater knowledge to respond to cyber threats or attacks. Considering that a substantial portion of risks and cost losses stemming from attacks is attributed to insufficient personnel training (Ilyas et al., 2023), employing a skilled workforce may reduce risk exposure and increase operational efficiency. Cooperation measures ensure coordination between the public and private sectors and enhance information sharing. In this regard, international agreements and regional collaborations among institutions may provide the opportunity to respond to cyber threats at an earlier stage. This may ensure reliability along international routes and reduce cost losses resulting from operational disruptions and improve container shipping performance.

Figure 1: Relationship between Cybersecurity Factors and Container Shipping Performance



Source: This framework was developed by the author based on the GCI components.

When these indicators are considered from the perspective of international trade and logistics activities, legal measures, through data protection and cybercrime legislation, are assumed to safeguard the security of digital documents and customs procedures, thereby enhancing the overall reliability of trade. Technical measures, in turn, help to ensure the continuity of port operations, while organizational measures, by prioritizing the port and logistics sectors within national cybersecurity strategies, contribute to keeping maritime transport running without disruption. Moreover, capacity development are expected to enhance digital security awareness among employees in international trade and logistics, and to increase their sensitivity to fraudulent documents and cyberattacks. Finally, cooperation measures implemented through public–private partnerships and international agreements are thought to play a critical role in detecting and responding to cyber threats in maritime transport. For this reason, countries' cybersecurity capacities are expected to affect transit times in container shipping, the likelihood of operational disruptions, and costs arising from potential delays and from attacks/threats. However, given the data employed, this study has a cross-sectional design. Therefore, the findings reveal statistical relationships between variables rather than causal relationships.

Within this framework, the present study draws on container shipping data for 2023 (measured in TEUs) obtained from the OECD database, together with cybersecurity indicators reported in the Global Cybersecurity Index 2024, published by the International Telecommunication Union (ITU). In the analysis, the Global Cybersecurity Index indicators are specified as independent variables, whereas container shipping volumes constitute the dependent variable.

Based on these variables, a cross-sectional regression analysis is conducted using data for 29 countries. The countries included in the sample are those that are jointly available in the OECD's 2023 container shipping statistics and the GCI reports.

The countries included in the analysis are presented in Table 2.

Table 2: Countries Included in the Analysis

Azerbaijan	Ireland	Mexico
Albania	Sweden	United Kingdom
Estonia	Finland	İtaly
Bulgaria	New Zealand	Türkiye
Croatia	Poland	Germany
Latvia	Portugal	Belgium
Georgia	Chile	Netherlands
Norway	Greece	Spain
Slovenia	France	Korea
Lithuania	Canada	

The study aims to measure the impact of the cybersecurity capacities of the countries in the dataset on container shipping and to provide empirical evidence on this relationship. In this regard, the variables included in the model, based on container shipping data and the indicators obtained from the GCI, are presented in Table 3.

Table 3: Variables Included in the Model

Variable Name	**Variable Code**	**Source**
Container Shipping Volume	TEU	OECD
Legal Measures	LM	The International Telecommunication Union (ITU)
Technical Measures	TM	The International Telecommunication Union (ITU)
Organizational Measures	OM	The International Telecommunication Union (ITU)
Capacity Development	CD	The International Telecommunication Union (ITU)
Cooperation Measures	CM	The International Telecommunication Union (ITU)

In the model, container shipping volume obtained from the OECD database is used as the dependent variable. The independent variables consist of the subcomponents of the GCI. Legal measures capture the legal framework a country establishes through laws, regulations, and criminal provisions concerning cybersecurity-related issues; technical measures refer to the technological infrastructure that underpins the capacity to prevent, detect, respond to, and recover from cyber threats; organizational measures denote the capacity to plan, coordinate, and oversee cybersecurity governance at the national level; capacity development

reflects the extent to which a country enhances its human resources, awareness, and institutional capability in the field of cybersecurity; and cooperative measures represent information sharing, joint action, and coordination among countries in the area of cybersecurity. Drawing on these variables, the impact of countries' cybersecurity capacities on container shipping has been analyzed. In this context, the econometric model is specified as follows:

$$TEU_{i=}\beta_0+\beta_1 LM_{it}+\beta_2 TM_{it}+\beta_3 OM_{it}+\beta_4 CD_{it}+\beta_5 CM_{it}+\varepsilon_i$$

In the equation above, β_0 denotes the constant term, while β_1, β_2, β_3, β_4 and β_5 represent the coefficients to be estimated; ε_{it} corresponds to the error term. By means of this model, the impact of countries' cybersecurity capacities on container shipping has been empirically examined.

The data used in the study were obtained from the GCI report published in 2024, which is based on data collected during 2023–2024. Container shipping volume (measured in TEUs) was drawn from the OECD database.

4. FINDINGS

In this section, the findings of the cross-sectional regression analysis conducted for 29 countries are presented. The analysis draws on GCI data compiled for the 2023–2024 period together with annual container transport data for 2023 obtained from the OECD database. The emergence of multicollinearity in the regression model, resulting from high correlations among the explanatory variables, makes it difficult to estimate the coefficients reliably and, in turn, diminishes the credibility of the results derived from the model (Topal et al. 2010: 54). This situation may cause a variable that is, in fact, influential to appear statistically insignificant, thereby weakening the model's explanatory power and making it more difficult to interpret the results accurately. Multicollinearity is a problem that may arise in both time-series data and cross-sectional analyses (Özel and Gezer, 2020: 83). Therefore, in order to ensure the reliability of the parameter estimates, it is crucial to eliminate multicollinearity from the model.

Beyond this, another critical issue that may compromise the underlying assumptions of regression models is heteroskedasticity. When the variance of the error terms is not constant, coefficient estimates may become biased and unreliable (Bozkaya, 2024: 36). Consequently, this situation can give rise to misleading inferences regarding the statistical significance of the regression coefficients.

In order to prevent such issues from distorting the empirical results, several diagnostic procedures were performed prior to conducting the regression analysis. First, the correlation matrix was reported, and the Variance Inflation Factor (VIF) test was carried out. Subsequently, to examine the validity of the constant variance assumption of the error terms, the Breusch–Pagan/Cook–Weisberg heteroskedasticity test was implemented. In light of the outcomes of these diagnostics, the model was estimated using the Ordinary Least Squares (OLS) method, and the resulting coefficients were evaluated with respect to their effects on the dependent variable, namely container transport volume. The corresponding test results are presented below.

Table 4. Correlation Matrix

	lnTEU	**Legal Measures**	**Technical Measures**	**Organizational Measures**	**Capacity Development**	**Cooperation Measures**
lnTEU	1,000					
Legal Measures	-0,0853	1,000				
Technical Measures	0,3609	0,3492	1,0000			
Organizational Measures	0,2269	0,7221	0,3432	1,0000		
Capacity Development	0,4694	0,4210	0,5871	0,6143	1,0000	
Cooperation Measures	0,2191	0,1821	0,4811	0,3232	0,6915	1,0000

Table 4 reports the correlation coefficients among the variables included in the model. The correlation coefficient indicates both the direction and the strength of the linear relationship between two variables. Accordingly, values approaching 1 point to a strong positive association, those approaching -1 indicate a strong negative association, whereas values close to 0 reflect a weak relationship. According to the correlation table, there is generally a positive relationship between the dependent variable, container transport volume, and the independent variables representing cybersecurity indicators. Most of the coefficients reported in the table take positive values. In this regard, it may be inferred that, as cybersecurity capacity increases, container transport volume tends to rise. Among these indicators, the variable with the highest correlation with container transport volume is capacity development. This finding suggests that, as qualified human capital in the field of cybersecurity is strengthened and training activities are expanded, container transport can be carried out more efficiently and securely. The variable of technical measures also exhibits a moderately positive relationship with container transport volume. This result may be interpreted to mean that reinforcing countries' cybersecurity infrastructure at the technical level supports the continuity of port

operations and may, in turn, contribute to an increase in transport volume. A weak yet positive relationship has been identified between organizational measures and container transport. In this respect, the presence of national strategies and institutional arrangements can be regarded as a key factor in preparing for cyber threats. Likewise, there is a weak but positive association between cooperation measures and container transport. Accordingly, public–private and international collaborations may be said to enhance data security and operational coordination in cross-border trade in particular, thereby supporting the security of container flows. By contrast, the relationship between container transport and legal measures is weak and negative. This result indicates that legal regulations on cybersecurity, on their own, do not directly increase transport volume; however, when considered together with other structural factors, they may generate an indirect effect.

Table 5 presents the Variance Inflation Factor (VIF) values for the independent variables included in the regression model. The VIF value indicates the extent to which a given independent variable is linearly related to the other independent variables. In the literature, it is generally acknowledged that when the VIF value exceeds 10, the presence of multicollinearity in the model can be inferred (Sulaiman et al. 2021: 7; Abeysiriwardana, 2022: 484; Karaca, 2025: 85).

Table 5. VIF Test Results

Variable	VIF Value	1/VIF Value
Legal Measures	3,23	0,309235
Technical Measures	2,85	0,351003
Organizational Measures	2,21	0,453280
Capacity Development	2,03	0,492621
Cooperation Measures	1,63	0,614282
Mean VIF	**2,39**	

The results reported in Table 5 indicate that the VIF values range between 1.63 and 3.23. Accordingly, there is no evidence of a severe multicollinearity problem in the model. In this sense, the VIF test results suggest that the simultaneous inclusion of the independent variables in the model is statistically appropriate.

Table 6. Breusch-Pagan/Cook-Weisberg Heteroskedasticity Test Results

Test Statistic	p-value
0,00	0,9579

Table 6 reports the results of the Breusch–Pagan / Cook–Weisberg heteroskedasticity test, which was conducted to examine the validity of the constant variance assumption of the error terms in the regression model.

According to the results, the probability (p) value of the test is 0.9579. Since this p-value is greater than the 0.05 significance level, it indicates that the variance of the error terms is constant and that there is no heteroskedasticity problem in the model. In line with this finding, the model was estimated using the Ordinary Least Squares (OLS) method. The results obtained from the regression analysis are presented below.

Table 7. Regression Analysis Results

lnTEU	**Coefficients**	**t-statistic**	**p-value**
Legal Measures	-0.8609241	-2,47	0,021**
Technical Measures	0,1945447	1,30	0,206
Organizational Measures	0,2968843	1,09	0,287
Capacity Development	0,3678782	2,07	0,050*
Cooperation Measures	0,1866199	-1,35	0,191
F: 3,35 (0,0000)			
R^2: 0,4215			

Note: ** indicates statistical significance at the 5% level; * indicates statistical significance at the 10% level.

The F-test value reported in Table 7 indicates that the independent variables in the model, legal measures, technical measures, organizational measures, capacity development and cooperation measures jointly make a statistically significant contribution to explain container transport volume. The overall significance test of the model, F (5, 23) = 3.35, together with its corresponding p-value (0.0000), is below the 0.05 significance threshold; therefore, the model is statistically significant. This finding demonstrates that the selected cybersecurity indicators possess a meaningful explanatory power for container transport performance. The model's R^2 value is calculated as 42.15%. Accordingly, the model explains approximately 42% of the variation in container transport volume. In other words, around 42% of the changes in the dependent variable container transport volume are accounted for by the independent variables included in the model. The remaining 57% may be attributed to other factors not incorporated into the model, such as port infrastructure, trade volume, economic size, investments in digital logistics, or geographical location.

When the coefficients are examined, the variable Legal Measures is found to be negative and statistically significant. This result suggests that legal regulations implemented in the field of cybersecurity may, in the short run, generate certain compliance costs rather than directly increasing container transport volume. Put differently, increasing regulatory stringency and the tightening of sanctions may constrain operational flexibility in the short term. However, in the long term, such regulations may generate indirect benefits for sustainable trade security by mitigating systemic risks. The variable Capacity Development is positive and

statistically significant at the 10% level. This finding indicates that the broader dissemination of awareness-raising initiatives, training programs and incentive policies in the field of cybersecurity enhances operational efficiency, security awareness and digital adaptation capacity in the port and logistics sectors. Therefore, enhancing human and institutional capacity plays a crucial role in ensuring the secure and uninterrupted operation of container transport. By contrast, the variables Technical Measures, Organizational Measures and Cooperation Measures are not found to be statistically significant. In light of these findings, it may be argued that improvements in technical infrastructure and international cooperation initiatives are more likely to bolster transport performance over a longer time horizon.

5. DISCUSSION AND CONCLUSION

Given that a substantial share of global trade is carried by sea, a country's cybersecurity capacity emerges as a strategically critical determinant of the continuity and reliability of maritime transport, particularly container shipping. As digital technologies have increasingly permeated the maritime domain, port operations, vessel navigation systems, and cargo planning and tracking processes have progressively been migrated to and integrated with digital platforms. This, in turn, allows cyberattacks to disrupt operations, cause delays throughout supply chains, and lead to substantial financial losses. Accordingly, countries with weak cybersecurity capacity remain more vulnerable to cyber threats in maritime transport and, at the same time, put the uninterrupted functioning of global supply chains at risk. Therefore, a robust cybersecurity capacity plays a pivotal role in ensuring security and predictability in maritime and, in particular, container shipping. In this context, the present study examines the impact of cybersecurity capacity on the container shipping industry. The empirical findings indicate that the capacity development variable exerts a positive impact on container transport. This result is consistent with, and further corroborated by, the evidence reported in Senarak (2021a; 2021b), Chouliaras et al. (2023), Putra et al. (2023), and Senarak (2024). These studies likewise underscore that staff training, the availability of certified experts, and institutions that prioritize capacity development are all critically important for ensuring cybersecurity. Taken together, these findings suggest that a highly skilled workforce and sustained institutional capacity-building efforts rank among the most decisive factors in enhancing container transport performance. In a similar vein, Ilyas et al. (2023) demonstrate that errors in information flows and human-induced risks negatively impact transport security. This, in turn, suggests that well-

trained personnel and strong organizational awareness play a crucial role in enhancing resilience against cyberattacks in the maritime domain.

Legal regulations affect the impact of cybersecurity capacity on container shipping negatively and in a statistically significant manner in the short term. This finding indicates that as cybersecurity legislation becomes more stringent, operational costs and administrative burdens in container shipping may increase in the short run. This adverse effect may reflect transitional costs arising from short-term compliance requirements and reporting or auditing obligations imposed by regulations (Wang et al., 2024). At this point, it is important to distinguish between regulatory stringency and regulatory quality. While stricter rules may create cost pressures in the short term, a higher level of regulatory quality may enable the achievement of the same objectives with lower compliance costs. Nevertheless, Karahalios (2020) argued that a lack of regulatory compliance may lead to operational disruptions, while Ben Farah et al. (2022) stated that regulatory deficiencies increase cybersecurity vulnerabilities. Similarly, Senarak (2021b) demonstrated that the harmonization of port policies with international standards reduces risks in the long term. When the results of this study are evaluated from this perspective, the identified negative short-term effect may be interpreted as a temporary increase in costs that could generate long-term benefits in terms of security and sustainability. This underscores the need to assess short-term compliance costs together with long-term resilience gains.

The fact that the variables for technical measures, organizational measures, and cooperation measures are not statistically significant indicates that regulatory efforts in these domains do not exert a direct short-term impact on container transport performance. The insignificance of these indicators further suggests that the immediate effects of investments in technical infrastructure and multi-stakeholder coordination remain rather limited in the short run. In the long term, however, these dimensions can reasonably be expected to play a pivotal role in strengthening cyber resilience and enhancing operational efficiency in the container shipping industry.

5.1. Limitations

This study has several limitations. Its cross-sectional data structure reveals the association between cybersecurity capacity and container shipping performance. However, because the time dimension of the cybersecurity-related data is restricted to a single year, dynamic effects cannot be observed. Accordingly, the long-term effects of capacity development or regulatory compliance cannot be captured within this

analysis; instead, these effects are discussed with reference to insights from the existing literature. In addition, as the number of countries included in the GCI is 29, the analyses were conducted on this subset of countries. Therefore, to enable a more robust assessment of causal and dynamic effects, future research is recommended to employ panel data analysis if more countries are added to the GCI and multi-year data become available.

5.2. Policy Recommendations

Building on the empirical findings of this study, a multidimensional strategic approach should be adopted to enhance cybersecurity capacity in the container shipping industry. First and foremost, human resources need to be systematically trained in cybersecurity, and coherent policy frameworks should be designed to foster institutional capacity development in this field. In the maritime sector, it is essential to enhance the cybersecurity awareness of personnel and ensure their systematic participation in relevant training programs. Second, legal regulations should be strengthened; however, such rules must not unduly hinder the operational functioning of the transport industry. In other words, the regulatory framework needs to be implemented in a balanced manner so that it enhances security while avoiding unnecessary disruption to firms' operations. Third, in order to foster the development of digital infrastructure, particularly in developing countries, targeted incentives should be introduced to bolster technical capacity. National cybersecurity strategies in developing countries should, moreover, focus not only on technological investments but also on cultivating a pool of human capital capable of effectively deploying and managing these technologies. Finally, strong emphasis needs to be placed on international cooperation and information sharing. Strengthening these channels will, in turn, help countries develop more robust early warning systems, particularly against ransomware attacks and data breaches.

Accordingly, for policymakers and industry stakeholders, the key implication is that the cybersecurity governance required to ensure the uninterrupted functioning of maritime transport must be designed as a balanced, long-term strategy that, beyond merely providing technical infrastructure and regulatory frameworks, simultaneously addresses human resources, institutional capacity, and multi-stakeholder collaboration. Once such an approach is embraced, both cyber resilience and container transport performance can reasonably be expected to improve in the medium to long run.

AUTHOR CONTRIBUTION

CONTRIBUTION RATE	EXPLANATION	CONTRIBUTORS
Idea	Pointing out the research idea or forming hypotheses	Author 1
Review of Literature	Conducting the literature review for the study	Author 1
Research Design	Forming the research design, including research methodology, deciding on scales and samples	Author 1
Data Collection and Editing	Data collection, editing, and analyzing	Author 1
Findings and Discussion	Reporting and discussing the findings	Author 1

Conflict of Interest

No conflict of interest was reported by the authors.

Financial Support

The author(s) has not received any financial support for this study.

REFERENCES

Abeysiriwardana, H. D. and Gomes, P. I. (2022). Integrating vegetation indices and geo-environmental factors in GIS-based landslide-susceptibility mapping: using logistic regression. *Journal of Mountain Science*, 19(2), 477-492. https://doi.org/10.1007/s11629-021-6988-8.

Adhikari, S. and Baidya, S. (2024). Cyber security in containerization platforms: A comparative study of security challenges, measures and best practices. *Computer Science & IT Research Journal*, 5(2), 270–292. https://doi.org/10.51594/csitrj.v5i2.757.

Amro, A. and Gkioulos, V. (2022). From click to sink: Utilizing AIS for command and control in maritime cyber attacks. In V. Atluri, R. Di Pietro, C. D. Jensen and W. Meng (Eds.), *Computer security – ESORICS 2022* (pp. 535–553). Cham, Switzerland: Springer Nature Switzerland. https://doi.org/10.1007/978-3-031-17143-7_26.

Androjna, A., Perkovič, M. and Pavić, I. (2021). Cyber security challenges for safe navigation at sea. *14th Annual Baška GNSS Conference: Technologies, Techniques and Applications Across PNT and The 1st Workshop on Smart, Blue and Green Maritime Technologies*, 47–62.

Ben Farah, M. A., Ukwandu, E., Hindy, H., Brosset, D., Bures, M., Andonovic, I. and Bellekens, X. (2022). Cyber security in the maritime industry: A systematic survey of recent advances and future trends. *Information,* 13(1), 22. https://doi.org/10.3390/info13010022.

Bozkaya, Ş. (2024). Yeşil bir dünya hedefinde: Kırılgan beşli ülkelerinin çevresel kalitesi üzerine ampirik bir inceleme. *Anadolu Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 25(4), 21-50. https://doi.org/10.53443/anadoluibfd.1448240.

Chouliaras, N., Kantzavelou, I., Maglaras, L., Pantziou, G. and Ferrag, M. A. (2023). A novel autonomous container-based platform for cybersecurity training and research. *PeerJ Computer Science,* 9, e1574. https://doi.org/10.7717/peerj-cs.1574.

Clavijo Mesa, M. V., Patino-Rodriguez, C. E. and Guevara Carazas, F. J. (2024). Cybersecurity at sea: A literature review of cyber-attack impacts and defenses in maritime supply chains. *Information*, 15(11), 710. https://doi.org/10.3390/info15110710.

Fenton, A. J. (2024). 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(3), 510. https://doi.org/10.20944/preprints202401.1609.v1.

Ilyas, M., Jin, Z., Ullah, I. and Jafri, A. A. (2023). Investigation of risk factors influencing the safety of maritime containers supply chain: In the period of the pandemic. *Sustainability,* 15(11), 8803. https://doi.org/10.3390/su15118803.

International Maritime Organization (IMO) (2025). *Maritime Cyber Risk*. https://www.imo.org/en/ourwork/security/pages/cyber-security.aspx, Access Date: 02.11.2025.

International Telecommunication Union (ITU). (2024). *Global Cybersecurity Index*. https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf, Access Date: 16.09.2025.

Karaca, C. (2025). Finansal kriz ve COVID-19 etkisi altında finansal risklerin firma değeri üzerindeki dinamikleri: MMQR ve nedensellik analizlerinden yeni kanıtlar. *Bingöl Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 9(1), 79-98. https://doi.org/10.33399/biibfad.1575319

Karahalios, H. (2020). Appraisal of a ship's cybersecurity efficiency: The case of piracy. *Journal of Transportation Security,* 13(3–4), 179–201. https://doi.org/10.1007/s12198-020-00223-1.

Karahalios, H. (2025). Cybersecurity threats of remote autonomous ships while approaching ports. *Journal of Transportation Security*, 18(1), 2. https://doi.org/10.1007/s12198-024-00289-1.

Kaštelan, N., Vidan, P., Assani, N. and Miličević, M. (2024). Digital horizon: Assessing current status of digitalization in maritime industry. *Transactions on Maritime Science*, 13(1). https://doi.org/10.7225/toms.v13.n01.w13.

Kayişoğlu, G., Güneş, B. and Bolat, P. (2024). ECDIS cyber security dynamics analysis based on the fuzzy-FUCOM method. *Transactions on Maritime Science (ToMS),* 13(1), 1–28. https://doi.org/10.7225/toms.v13.n01.w09.

Meland, P. H., Nesheim, D. A., Bernsmed, K. and Sindre, G. (2022). Assessing cyber threats for storyless systems. *Journal of Information Security and Applications*, 64, 103050. https://doi.org/10.1016/j.jisa.2021.103050.

Meland, P. Há., Bernsmed, K., Wille, E., Rødseth, Ø. J. and Nesheim, D. A. (2021). A retrospective analysis of maritime cyber security incidents. *TransNav, the International Journal on Marine Navigation and Safety of Sea Transportation*, 15(3), 519–530. https://doi.org/10.12716/1001.15.03.04.

Nguyen, S., Chen, S.-L. and Du, Y. (2021). Container shipping operational risks: An overview of assessment and analysis. *Maritime Policy & Management,* 48(8), 1109–1136. https://doi.org/10.1080/03088839.2021.1875142.

Oral, F. and Paker, S. (2023). Risk assessment for maritime container transportation security. *Journal of ETA Maritime Science,* 11(4), 304–316. https://doi.org/10.4274/jems.2023.80148.

Özel, S. Ö. and Gezer, F. (2020). Çoklu doğrusal bağlantı problemi altında tahmin edicilerin karşılaştırılması: Genelleştirilmiş maksimum ENTROPİ, RİDGE, LİU. *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi*, (66), 82-96.

Potamos, G., Stavrou, E. and Stavrou, S. (2024). Enhancing maritime cybersecurity through operational technology sensor data fusion: A comprehensive survey and analysis. *Sensors*, 24(11), 3458. https://doi.org/10.3390/s24113458.

Putra, I. N., Octavian, A., Heikhmakhtiar, A. K., Tjahjadi, H. and Susilo, A. K. (2023). Cyber threat analysis of maritime cybersecurity using AHP-TOPSIS. *Journal of Maritime Research,* 20(2), 13–24.

Senarak, C. (2021a). Cybersecurity knowledge and skills for port facility security officers of international seaports: Perspectives of IT and security personnel. *The Asian Journal of Shipping and Logistics*, 37(4), 345-360. https://doi.org/10.1016/j.ajsl.2021.10.002.

Senarak, C. (2021b). Port cybersecurity and threat: A structural model for prevention and policy development. *The Asian Journal of Shipping and Logistics,* 37(1), 20–36. https://doi.org/10.1016/j.ajsl.2020.05.001.

Senarak, C. (2024). Port cyberattacks from 2011 to 2023: A literature review and discussion of selected cases. *Maritime Economics & Logistics,* 26(1), 105–130. https://doi.org/10.1057/s41278-023-00276-8.

Stępień, B. (2025). Defending the fleet: Cybersecurity and autonomous ships. *In 40 Years of the United Nations Convention on the Law of the Sea* (pp. 334-344). Routledge. https://doi.org/10.4324/9781003492566-33.

Sulaiman, M. S., Abood, M. M., Sinnakaudan, S. K., Shukor, M. R., You, G. Q. and Chung, X. Z. (2021). Assessing and solving multicollinearity in sediment transport prediction models using principal component analysis. *ISH Journal of Hydraulic Engineering*, 27(sup1), 343-353. https://doi.org/10.1080/09715010.2019.1653799.

Svilicic, B., Kamahara, J., Rooks, M. and Yano, Y. (2019). Maritime cyber risk management: An experimental ship assessment. *The Journal of Navigation*, 72(5), 1108–1120. https://doi.org/10.1017/S0373463318001157.

Tam, K. and Jones, K. (2019). MaCRA: A model-based framework for maritime cyber-risk assessment. *WMU Journal of Maritime Affairs*, 18(1), 129–163. https://doi.org/10.1007/s13437-019-00162-2.

Topal, M., Eyduran, E., Yağanoğlu, A. M., Sönmez, A. and Keskin, S. (2010). Çoklu doğrusal bağlantı durumunda ridge ve temel bileşenler regresyon analiz yöntemlerinin kullanımı. *Atatürk Üniversitesi Ziraat Fakültesi Dergisi*, 41(1), 53-57.

UNCTAD (2025). *Review of Maritime Transport*. https://www.un-ilibrary.org/content/periodicals/22253459?utm, Access Date: 09.10.2025. United Nations Conference on Trade and Development, (2022). *Review of maritime transport 2022*. New York: United Nations Publications.

Wang, F., Wang, H., & Li, J. (2024). The effect of cybersecurity legislation on firm cost behavior: Evidence from China. *Pacific-Basin Finance Journal*, 86, 102460. https://doi.org/10.1016/j.pacfin.2024.102460.

Yilmaz, B. (2025). Cybersecurity applications in the maritime industry: A scientometric approach. *Scientific Journal of Maritime Research (Pomorstvo),* 39(2), 254–278. https://doi.org/10.31217/p.39.2.6.

Yue, Z. and Mangan, J. (2024). A framework for understanding reliability in container shipping networks. *Maritime Economics & Logistics,* 26(4), 523–544. https://doi.org/10.1057/s41278-023-00269-7.