ORIGINAL RESEARCH (AR) DOI: 10.4274/jems.2023.80148

Journal of ETA Maritime Science 2023;11(4):304-316

Risk Assessment for Maritime Container Transportation Security

Ferhan Oral[1], Serim Paker[2]

[1]Dokuz Eylül University Faculty of Maritime, Department of Marine Transportation Engineering, İzmir, Türkiye
[2]Dokuz Eylül University Faculty of Maritime, Department of Maritime Business Administration, İzmir, Türkiye

Abstract

Container shipping is the backbone of the global supply chain, and its security is directly linked to the global economy. Disruptions in container transportation could have severe consequences, such as an increase in transport and insurance costs and damage to the environment and cargo. The first aim of this study is to identify, assess, and prioritize the security risks associated with maritime container transportation using the Delphi technique and to draw a risk map accordingly. The second aim is to identify the strengths, weaknesses, opportunities, and threats to using SWOT analysis from a security perspective. Maritime container transportation between Türkiye and the Far East serves as a case study for this purpose. As a conclusion of the first part of the study, the risk of cyber-attacks has one of the highest probability factors scored first, war and warlike conditions having the highest impact factor scored second, and piracy and armed robbery scored third in general. In the second part, the SWOT factors are determined and prioritized using the Analytic Hierarchy Process. Strengths scored the highest among the main SWOT factors, which indicates that it is more prominent than other factors. Weaknesses, opportunities, and threats to. The overall conclusion drawn is that security risk assessment has become essential given recent technological changes, such as the increasing risk of cyber-attacks on electronic navigational aids, and geopolitics, such as tensions in the Middle East and the South China Sea.

Keywords: Transportation security, Risk assessment, Delphi, SWOT, AHP

1. Introduction

"Transportation security" is defined as "the combination of preventive measures and human and material resources intended to protect transport infrastructure, vehicles, systems, and workers against intentional unlawful acts" [1]. Transport security is concerned with the security of cargo transported by various modes of transportation. The need for security during transportation stems from the desire to avoid unwanted negative disruption in the flow of goods. Such disruption, whether physical (terrorist attacks, piracy) or virtual (cyber-attacks), may result in fatalities-the primary concern-as well as delays and cancelations among other problems. In this context, "security risk" refers to the likelihood that an individual or organization may encounter a negative consequence because of a security breach.

The perception of transportation security has significantly changed over recent decades, particularly in the wake of the 9/11 terrorist attacks. The concepts of security, resilience, and systemic vulnerabilities must be reexamined and rediscovered in a new political, economic, social, and technological environment [2]. The first of the changes is the necessity to take measures not only against cargo theft but also against terrorism. The other is the shift in the field of interest from national to global issues. The last one is that security has emerged as an issue that interests all actors in the supply chain rather than being a problem only on the basis of companies [1].

Nowadays, the container trade takes center stage in transportation security concerns because of its evolution as an ideal means to smuggle drugs, weapons, and

*This article is derived from a thesis titled "Risk Assessment of Turkey and the Far East Trade in Terms of Transportation Security" (Dokuz Eylül University, İzmir, Türkiye).

Address for Correspondence: Ferhan Oral, Dokuz Eylül University Faculty of Maritime, Department of Marine Transportation Engineering, İzmir, Türkiye
E-mail: ferhan.oral@gmail.com
ORCID ID: orcid.org/0000-0003-3249-5266

Received: 06.09.2023
Last Revision Received: 13.11.2023
Accepted: 30.11.2023

To cite this article: F. Oral, and S. Paker. "Risk Assessment for Maritime Container Transportation Security" *Journal of ETA Maritime Science*, vol. 11(4), pp. 304-316, 2023.

people. Technological developments and recent changes in geopolitics are another factor affecting transportation security. For instance, blockchain technology can completely transform maritime security by improving accountability, traceability, and transparency in the sector. It offers a decentralized, unchangeable ledger that securely documents and validates transactions, making it the perfect solution to problems such as fraud, smuggling, and piracy [3]. Geopolitical tensions such as those in the Black Sea, Middle East, and South China Sea negatively affect shipping trade either directly by affecting merchant ships and their crew or indirectly by increasing insurance premiums.

Terrorist attacks on container transportation include the 2013 attack on China's COSCO Asia, at al-Qantarah, 30 miles south of Port Said, after it had departed Suez at the southern entrance to the Canal [4] - an attack that prompted China to consider alternative routes bypassing the Suez Canal-and recent assaults carried out against merchant traffic off the coast of Yemen or at ports along the Gulf of Aden [5].

For the past 20 years, the major illicit activity that threatens the security of the world's maritime transport routes has been piracy and armed robbery. In particular, in the Gulf of Aden, the Indian Ocean, the Straits of Malacca and Singapore, the South China Sea, and the Gulf of Guinea, dozens of merchant ships have been hijacked, with hundreds of seafarers held and even injured or killed, and tons of cargo forcibly detained.

Containers can be used to smuggle people, narcotics, weapons, and radioactive, chemical, and biological materials. This can be accomplished by altering cargo paperwork or by concealing the presence of unlawful people or substances in any area of the transportation without the consent of transportation authorities, carriers, consignees, and cargo owners.

Unlawful smuggling of people into shipping containers endangers both seafarers' and national security. Stowaways outnumbering crew members or behaving violently is a risk that could result in injury to crew members; one recent incident was the Turkish cargo ship, sailing from Türkiye to France, which was attacked by armed stowaways off Naples and secured by Italian special forces [6].

Many incidents of cyber risks in maritime transportation can be cited. In addition to the cyber-attack carried out against the Danish shipping company AP Moller-Maersk, in which their IT systems were completely shut down for ten days in 2017, several incidents have been reported of unauthorized persons gaining access to conventional ship control systems [7]. Since Automatic Identification System (AIS) spoofing scenarios can disrupt maritime traffic and interfere with a vessel's ability to navigate safely [8], dependable precision navigation is more important than ever because of the increase in the size and number of vessels at sea.

Another risk area in transportation security includes war and warlike conditions, internal conflicts, and geopolitical instabilities through maritime routes. In recent years, several incidents originating from the civil war in Yemen, including assaults on ships off the Yemeni coast, tensions between Iran and the US in the Persian Gulf, and between China and the US in the South China Sea and off the coast of Taiwan and the Eastern Mediterranean after the Israel-Hamas war, are regions of crises that may impact merchant traffic between Türkiye and the Far East. The Russian-Ukrainian war that began in February 2022 also had direct and indirect impacts on the structure of the global supply chain.

Moreover, the coronavirus disease-2019 pandemic-although not a security but a safety risk, because it was not a deliberate incident, which is a prerequisite for a security risk [9] - also had indirect security effects due to its impact on the global supply chain. These effects include increasing risks from container shortages, blank sails, delays, and lay times, in addition to the increase in cargo theft of medical equipment (masks, suits, sanitizer, etc.) [10]. The pandemic also expedited digitization and created new digital opportunity structures that increased cyber risks [11].

In this study, no safety-related risk factors are examined because additional issues around security are gradually taking center stage in terms of technological advancements as new types of security risks emerge (e.g., cyberattacks, autonomous transport etc.) [12]. Another reason for dealing purely with security issues is that security breaches are considered more dangerous than safety issues because their results are far more severely damaging than safety issues, despite arguably occurring less frequently. Additionally, the occurrence of security breaches is associated with a high level of uncertainty and is frequently beyond the company's control.

Hence, the primary objective of this study is to examine the security risks associated with container trade, focusing specifically on the trade between Türkiye and the Far East. The objective of this study is to address three research questions: Research Question 1: What are the security risk factors associated with container trade between Türkiye and the Far East? Research Question 2: Among the identified risk factors, which ones hold relatively greater significance in terms of security? Research Question 3: What are the strengths, weaknesses, opportunities, and threats of container trade between Türkiye and the Far East? To address these questions, a comprehensive examination of existing literature, followed by four iterations of Delphi surveys, and a thorough SWOT analysis are employed as the chosen methodological approach.

The following section presents a review of the literature. Section 3 discusses the methodology, data collection, and calculation of risk and SWOT factors. Section 4 presents the results and a discussion of the study. The last two sections provide concluding thoughts on the study and recommendations for future research.

2. Literature Review

It is imperative to define risk and risk assessment before discussing research in that area. "The combination of the frequency and severity of the consequence" is the definition of "risk" in the IMO circular [13], while risk assessment is "the process of gathering data and synthesizing information to develop an understanding of the risk of a particular enterprise" [14]. Many risk assessments have the primary goal of identifying the dangers associated with a certain process or system and developing appropriate measures to prevent or mitigate undesirable consequences.

Various safety and security risk assessment studies have been conducted that could help to manage the corresponding threats [14-25]. Different methodologies were used when conducting this research, such as quantitative risk assessment (QRA), failure mode and effects analysis (FMEA), and risk mapping. The examined studies on risk assessment are summarized in Table 1.

Mousavi et al. [14] provided a brief introduction to risk analysis methods and emphasized the importance of identifying hazards before conducting risk analysis techniques or risk-reducing measures. Zhang [15] introduced two case studies in the Yangtze River-China's largest and the world's busiest inland waterway-to illustrate the application of several approaches in maritime risk assessment. Jiang et al. [16] analyzed the risk factors influencing maritime supply chains along the Maritime Silk Road, and their assessment results revealed that fuel price is the most significant risk factor.

Goerlandt and Montewka [17] studied and analyzed risk definitions, views, and scientific risk analysis methodologies in maritime transportation, with a focus on applications addressing the accidental risk of shipping. Cieśla et al. [18] analyzed foundations associated with risk management for a company performing multimodal transportation services of intermodal transport units (ITU). Among the 24 threats, they concluded that the two most important threats were overturning the ITU stack on the terminal yard and collision or accident involving the ITU during its shipment process

Table 1. *Literature review*

Author/Year	Subject	Method	Country/Case study
Mousavi et al. [14] (2017)	Risk assessment in the maritime industry	Literature review	Iran
Zhang [15] (2014)	Challenges and new developments in marine risk assessment	Combined AHP with discrete fuzzy sets	China/Yangtze River
Jiang et al. [16] (2022)	Risk assessment of maritime supply chains in the context of the Maritime Silk Road (MSR)	QRA	China/The 21st Century MSR
Goerlandt and Montewka [17] (2015)	Maritime transportation risk analysis: Review and analysis considering foundational issues	Literature Review	Finland
Cieśla et al. [18] (2017)	Multimodal transport risk assessment with risk mapping	Risk Mapping	Poland/Intermodal Transport Units
Roh et al. [19] (2018)	Risk assessment of maritime supply chain security in ports and waterways	Risk/loss exposure matrix	Malaysia/ Malaysia's ports and waterways
Nguyen et al. [20] (2022)	Methodological framework for quantitative risk analysis in container shipping operations	QRA	Vietnam/Three Container Shipping Companies
Nguyen and Wang [21] (2018)	Prioritizing operational risks in container shipping systems using cognitive assessment techniques	FMEA and its integration into a fuzzy rules Bayesian network	Vietnam: An Anonymous Container Shipping Company
Wan et al. [22] (2019)	Analysis of the risk factors influencing the safety of maritime container supply chains	Delphi	China/Selected Maritime Stakeholders in China
Chang et al. [23] (2015)	Risk analysis for container shipping from a logistic perspective	Risk scale average likelihood and consequence and average risk scale	Taiwan/Taiwan Container Shipping Industry
Zhou et al. [24] (2022)	Holistic Risk Assessment of Container Shipping Services based on Bayesian Network Modelling	Hybrid Method Comprising FMEA, Evidential Reasoning, and Rule-Based BN	China/Maritime Experts from China
Wan et al. [25] (2019)	Advanced fuzzy Bayesian-based FMEA approach for assessing maritime supply chain risks	Fuzzy Belief Rule Approach using Bayesian Networks	China/Container Shipping Company

AHP: Analytical hierarchy process, QRA: Quantitative risk assessment, FMEA: Failure mode and effects analysis

[18]. Roh et al. [19] analyzed the risk to Malaysia's maritime supply chain security in ports and waterways using piracy and terrorism, government intervention, cyber security, and facility as risk assessment factors and concluded that Malaysian ports are vulnerable to attacks and crime due to various factors.

Different authors examined container-specific works. Nguyen et al. [20] proposed a methodological framework to strengthen the quality and reliability of the QRA of container shipping in Vietnam in diverse risk scenarios. Nguyen and Wang [21] identified container shipping operational risks using multivariate risk evaluation mechanisms such as the fuzzy rules Bayesian network and FMEA. Wan et al. [22] identified the primary risk factors of substantial safety concerns using a Delphi survey and a risk matrix approach from different viewpoints. Chang et al. [23] investigated the hierarchical classification of risks in container shipping operations from a logistics standpoint.

Zhou et al. [24] examined container shipping service risks using a hybrid method and found that economic, political, and technical risks pose the greatest threats to resilient container shipping service. Wan et al. [25] created a novel model to assess the risk factors of maritime supply chains and investigated a container shipping company, revealing that the most significant risk factors are "transportation of dangerous goods, fluctuation of fuel prices, fierce competition, unattractive markets, and change of exchange rates," in that order.

The above papers shed important light on the safety and security risks facing container transportation businesses. While safety studies focused on hazards related to transportation systems, security studies focused on threats that have a negative impact on transportation systems. Little research has strictly discriminated between safety and security [19] because of the nature of those two concepts, which are indivisible in many ways [26]. Apart from the conceptual papers on risk assessment [14,17], while most studies focused solely on safety issues [15,18], some studies discussed both safety and security together [16,20-25].

This research is one of the pure security risk assessments among the literature examined. Although some studies have made an integrated analysis of safety and security, which is called "Safety and Security Co-Analysis (SSCA)" [27], modeling security risk using safety analysis approaches is difficult because security is an activity involving a higher level of uncertainty and is influenced more by external factors. Therefore, this study may help fill the research gap in this area. Moreover, the results of this study can also contribute to the idea that safety and security studies can be divided in some cases or for specific patterns of container transport different from traditional risk assessment studies.

A risk assessment is the foundation of a comprehensive risk management strategy, and a risk analysis is a component of the assessment process in which the likelihood and criticality of each risk are calculated and a score is assigned to each risk based on the findings. A risk assessment is a more comprehensive process that involves conducting assessments, determining the choices for risk mitigation, and informing stakeholders. To improve corporate strategy development against risks and simplify complicated problems, another approach is SWOT analysis [28,29]. SWOT analysis with an analytical hierarchy process (AHP) helps rank and prioritizing risks; several studies have been conducted in this area.

Amin et al. [30] used a SWOT matrix to identify the strengths, weaknesses, opportunities, and threats to different transportation modes in Cape Breton Island, Nova Scotia, Canada, while evaluating and ranking the factors based on pairwise comparisons in the AHP. Chang and Huang [31] used major container ports in East Asia as a case study and compared them with different criteria using the quantified SWOT analytical method and obtained the weights of key factors using the AHP method. They concluded that the quantified values of the SWOT would help enterprises learn about themselves and can be used as the foundation for developmental strategies. Şenol et al. [32] investigated the strategies associated with autonomous shipping and proposed a strategy based on SWOT-AHP analysis.

3. Research Methodology

The Delphi technique was used for data gathering, whereas QRA/mapping and SWOT AHP were used to analyze the data. The Delphi technique is a method used in complex problems where uncertainty exists and expert opinion is needed to overcome this uncertainty and reach a consensus on the likelihood and consequences of future events by identifying risks, threats, and opportunities with positive and negative consequences.

The fact that SWOT analysis cannot be expressed numerically makes it difficult to access solid and reliable information in strategic management planning. Therefore, SWOT analysis gains a quantitative meaning when integrated with multi-criteria decision making (MCDM) techniques such as AHP. For this reason, the SWOT-AHP method was chosen as the best fit for our research.

To accomplish the goals of the research, analysis processes were structured using the risk management framework. The next sections go into further detail on the steps involved in putting these methods into practice.

3.1. Design of the Methodology

In this study, transportation security risks were identified by content analysis of academic papers and books on

transportation security. As a second step, a Delphi survey was conducted with twelve experts from shipping companies and academia to confirm the security risks found in the literature review. In the third step, a second tour Delphi survey was conducted to determine the likelihood and impacts of the risk areas by eliminating one risk area (smuggling of drugs, weapons, and weapons of mass destruction) with a consensus rate below 70% [33]. The average percentage of majority opinions (APMO) formula is used with the formula [34]:

$$APMO = \frac{Majority\ Agreements + Majority\ Disagreements}{Total\ opinions\ expressed} \quad (1)$$

As a fourth step, risks were calculated by multiplying likelihoods and impacts, prioritized, and a risk map was drawn. In the fifth step of the study, another Delphi was conducted to collect input for a draft SWOT table indicating the strengths, weaknesses, opportunities, and threats of container transportation risks from Türkiye to the Far East. The final SWOT table was formed with experts' input. In the last step, the SWOT AHP technique was used to prioritize SWOT's main and sub-criteria with a fourth round of Delphi survey. The stages of the methodology are shown in Figure 1.

3.2. Data Collection

A comprehensive data collection process is necessary for valid data analysis. The Delphi technique is a useful tool for determining the expert panel's most reliable consensus for a set of sequential questions or rounds separated by controlled feedback [35]. Participants in an expert panel in a Delphi study are seasoned experts who can offer a knowledgeable viewpoint or expert opinion on problems in their particular

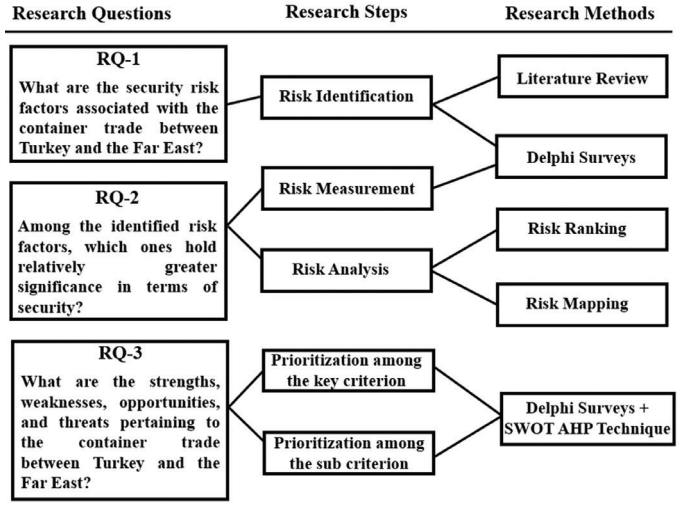

Figure 1. *Methodology for the study*

Source: Authors

field [36]. Therefore, 12 experts in container transportation with at least five years of experience were chosen; and contacted by phone/e-mail/in person conversation. The list of experts is given in Table 2.

3.3. Calculation of Risk Factors and Risk Mapping

The filtered risk area's likelihood and impact factors (Tables 3 and 4) were calculated using the linguistic assessments of the experts (Table 5).

Based on the data acquired through the aforementioned techniques, the risk scale for each risk factor was evaluated, and their relative weights were determined. The following notations are introduced before going into the mechanics of how risk scales are calculated:

- R: the total number of risk areas.
- E: the total number of experts.
- l_{re}: the likelihood of risk area r by the expert, e, $1 \le r \le R$ and $1 \le e \le E$; and
- i_{re}: the impact of risk area r by the expert, e, $1 \le r \le R$ and $1 \le e \le E$.

Note that the risk scale's elements are a risk area's likelihood and impact. One of the two methods can be used to determine the risk scale. In the first strategy, the average likelihood across all experts is multiplied by the average consequence across all experts. This method is known as risk scale average likelihood and impact (RSALI). The formula is as follows:

$$RSALI = \bar{l}_r \times \bar{i}_r \quad (2)$$

where:

$$\bar{l}_r = \frac{1}{E}\sum_{e=1}^{E} l_{re} \text{ and } \bar{i}_r = \frac{1}{E}\sum_{e=1}^{E} i_{re} \quad (3)$$

In the second method, the risk scales for each respondent on each risk component are first obtained, and then the risk scales for all respondents are averaged to create a risk analysis for container transportation. This methodology is known as the Average Risk Scale (ARS). The formula is as follows:

$$ARS_r = \frac{1}{E}\sum_{i=1}^{E}(l_{re} \times i_{re}) \quad (4)$$

For each risk factor, the first technique offers three results: average likelihood, average impact, and risk scale. It is simple to use, and the outcomes can be displayed right in the risk map that calls for them all. However, the fact that the RSALI results include those components derived by multiplying one respondent's likelihood by another respondent's impact could skew the statistical findings.

Table 2. *Profile details of maritime experts*

No	The type of organization	Year of employment	Department/professional area	Position
1	Shipping Industry	8	Intermodal, Railway, and Maritime Transport	Marketing and Sales Manager
2	University*	23	Port Management	Dean
3	Shipping Industry	23	Maritime Transportation	Senior Manager, Port and Terminals
4	University*	14	Logistics and Container Transportation	Lecturer
5	Shipping Industry	11	Dangerous Cargo Transportation: Port Operations	Line Manager
6	Shipping Industry	14	Container-Ship-Port Operation	Operation Manager
7	Shipping Industry	10	Container and maritime transportation	Cargo Operations Officer
8	University*	14	Foreign Trade	Lecturer-General Manager
9	Shipping Industry	18	Equipment and Ship Operation Management	Türkiye Operation Manager
10	Shipping Industry	17	Shipping and Logistics, Training and Development, Project Management	Learning Partner: Global Commercial Team
11	Shipping Industry	5	Export	Customer service assistant specialist
12	University*	22	Management and Strategy	Vice dean

*All of them also had working experience in the shipping industry

Source: Authors

Table 3. *Definitions of the likelihood of risk factors*

Likelihood	Scale	Definition	Numerical value
It is unlikely to happen (High)	5	It didn't happen, or at least once every ten years.	0.85
The probability is very low (Moderately high)	4	It only happens in some extreme environments, or it can happen every few years.	0.70
Less likely (Medium)	3	The probability of occurrence is not high, or at most once a year.	0.50
It can happen (Low)	2	It can happen in some cases or every few months.	0.25
The probability is higher (Very low)	1	It happens in most cases, or every month.	0.10

Source: Adapted from [22]

Table 4. *Definitions of the impact of risk factors*

Impact	Scale	Definition	Numerical value
Catastrophic	4	Cause complete and irrecoverable failures, long-term environmental damage, or death.	1.00
Severe	3	Cause some disruptions, or sometimes failures with severe impacts such as major cost increase and major environmental damage injuries.	0.70
Moderate	2	Cause some disruptions with medium impacts, such as moderate cost increase, delay, and minor environmental damage.	0.50
Minor	1	Cause some inconvenience with minor impacts, such as a small cost increase/schedule change.	0.25

Source: [22]

Since the risk scales are derived by first multiplying the risk likelihood by the risk impact provided by each respondent and then averaged over all respondents, it is concluded that the second method-ARS-is more acceptable in generating risk scales. Consequently, both techniques were employed to assess the risk scale for each risk factor, and both results did not change the overall order (Table 6).

Finally, a security risk map for maritime transportation is created using the risk rankings given above. In Figure 2, red denotes critical risks, orange indicates severe risks, yellow indicates moderate risks, and green indicates sustainable risks.

3.4. SWOT and the AHP Model

Risk assessment is necessary for a shipping company when defining the potential impact of each risk, but it is not enough. For "risk management" which is used to assess, analyze, prioritize, and formulate a strategy for mitigating threats and managing risks to a company's resources and revenue, SWOT is a widely applied tool in strategic

Table 5. *Linguistic assessment of maritime transportation security risks*

Maritime transportation security risks	E-1	E-2	E-3	E-4	E-5	E-6	E-7	E-8	E-9	E-10	E-11	E-12
	Likelihood/impact											
Terrorism and sabotage	L/S	VL/C	M/Mr.	L/S	L/C	L/S	L/C	L/S	L/S	VL/S	M/S	M/C
Piracy and armed robbery	L/M	MH/S	M/Mr.	L/S	M/S	M/S	M/S	L/S	M/M	L/S	M/S	H/S
Human trafficking and stowaways	H/Mr.	MH/Mr.	MH/M	MH/S	MH/Mr.	MH/M	MH/M	M/M	L/M	MH/S	M/Mr.	H/M
Cyber attacks	H/C	M/M	H/S	M/M	VL/Mr.	MH/M	MH/C	M/S	H/C	MH/S	H/C	M/M
War and warlike conditions	H/C	L/M	MH/S	M/S	VL/M	M/M	MH/C	L/S	L/C	L/C	M/C	M/C
Cyber theft	MH/Mr.	H/M	MH/M	L/C	H/Mr.	MH/M	MH/Mr.	M/M	M/Mr.	MH/M	MH/Mr.	H/M
Source: Authors' Delphi survey inputs												

Table 6. *Maritime transportation risk rankings*

Maritime transportation	Risk scale calculated using RSALI	Risk scale calculated by ARS	Ranking
Cyber-attacks	0.440	0.484	1
War and warlike conditions	0.346	0.368	2
Piracy and armed robbery	0.290	0.291	3
Human trafficking and stowaways	0.280	0.258	4
Cargo theft	0.277	0.254	5
Terrorism and sabotage	0.219	0.210	6
Source: Authors' calculations RSALI: Risk scale average likelihood and impact, ARS: Average Risk Scale			

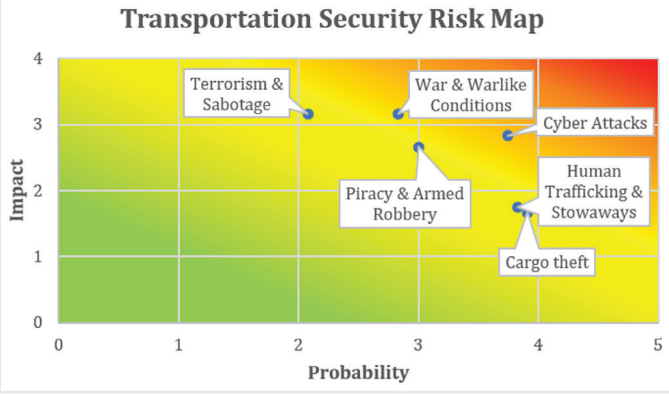

Figure 2. *Risk mapping of container transportation security from Türkiye to the Far East*

Source: Authors

decision support. Therefore, a SWOT matrix is drafted, and another Delphi tour is conducted to collect experts' input to fine-tune the matrix. The final SWOT matrix (Table 7) is disseminated again to experts for prioritization of the main and sub-criteria using the SWOT AHP technique.

The basic goal of a SWOT analysis is to subjectively identify and assess an organizational and operational system's strengths, weaknesses, opportunities, and threats. By identifying these elements, new constitutive strategies based on strengths, weakness, eradication, exploitation of opportunities, and threat to can be devised. Opportunities and threats are identified as external factors, whereas strategies and weaknesses are identified as internal system elements [37].

AHP, a decision-making technique that considers both qualitative and quantitative factors aimed at using professional consultation to derive relative priority on absolute scales from discrete and continuous paired comparisons [38], helps to conduct SWOT more analytically and to elaborate the study. Moreover, the combined use of AHP and SWOT analysis is a promising approach for supporting strategic decision-making processes [39].

Three steps are involved in applying the SWOT AHP technique [38]. The first stage in conducting a SWOT analysis for strategic planning is to make a list of the significant internal (strengths and weaknesses) and external (opportunities and threats) variables. The weights of each SWOT group are captured in the second stage, which employs pairwise comparisons. To determine the relative importance of each element within the SWOT categories, the third phase employs AHP. The local weights of the factors are multiplied by the particular group weight to arrive at the overall factor weight rank.

By selecting a number from a standardized comparison scale of nine levels (Table 8) created by Saaty [40] to indicate the relative relevance of the criteria, the prioritization method is carried out. Pairwise comparison matrices provided the means for calculating the importance of these factors.

Table 7. *SWOT matrix of transportation risk between Türkiye and the Far East*

Strengths (S)	Weaknesses (W)
S1 Need for maritime expertise to perform terrorist attacks or sabotage against sea targets. **S2** Strict rules such as ISPS Code and CSI exist in IMO frameworks. **S3** Regional/international naval support against piracy and human trafficking. **S4** Use of technology enhancing the security of containers (AI, IoT, RFID, etc.).	**W1** Additional risks compared with other transportation modes such as piracy and stowaways. **W2** Increased reliance on communication and information networks renders shipboard power systems more susceptible to covert cyberattacks. **W3** A more potential space for smuggling. **W4** Risk of blocking choke points in case of terrorist attack/sabotage on a container ship, which will have a greater impact on the global economy.
Opportunities (O)	**Threats (T)**
O1 China's policy to bypass sea routes by alternative transport routes and pipelines. **O2** Existence of alternate routes, such as the Arctic route.	**T1** Existence of high-risk areas (HRA) through routes from Türkiye to the Far East. **T2** Increasing cyber-security risks with recent developments in technology. **T3** Territorial disputes in the South China Sea and the Taiwan problem.
Source: Authors' interpretation, including Delphi survey inputs IoT: Internet of Things, RFI: Radio frequency identification	

Table 8. *Pairwise comparison scale*

Importance	Explanation
1	Equally important or preferred.
3	Slightly more important or preferred.
5	Strongly more important or preferred.
7	Very strongly more important or preferred.
9	Extremely more important or preferred.
2,4,6,8	Intermediate values to reflect compromise.
Reciprocals	Used to reflect the dominance of the second alternative as compared with the first.
Source: [40]	

Let $C = \{ C_j | j = 1, 2, ..., n\}$ be the collection of requirements. An (n x n) evaluation matrix A, in which each element is a_{ij} ($i, j = 1, 2, ..., n$) is a quotient of the weights of the criteria (relative importance for i to j in each SWOT group), can be used to summarize the results of a pairwise comparison of n criteria. A square and reciprocal matrix can be used to illustrate this pairwise comparison (see Equation 5).

$$A = (a_{ij}) = \begin{bmatrix} a_{11} & a_{12} & \cdots & a_{1n} \\ a_{21} & a_{22} & \cdots & a_{2n} \\ \vdots & \vdots & & \vdots \\ a_{n1} & a_{n2} & & a_{nn} \end{bmatrix} \quad (5)$$

Each matrix is normalized, and the relative weights are determined in the last step. The right eigenvector (w) corresponding to the largest eigenvalue (λ_{max}) as follows:

$$A_W = \lambda_{max} \times w \quad (6)$$

Matrix A has rank 1 and $\lambda_{max} = n$, if the pairwise comparisons are entirely consistent. Any of the rows or columns of a can be normalized in this scenario to yield weights.

Note that the consistency of the pairwise comparison judgments has an impact on output quality of the AHP. The relationship between the entries of

$A: a_{ij} \times a_{jk} = a_{ik}$ serves as the basis for determining consistency. The following formula can be used to compute the consistency index (CI).

$$CI = \frac{\lambda_{max} - n}{n - 1} \quad (7)$$

The assessment levels of consistency can be determined using the final consistency ratio (CR). According to Equation 8, the CR is determined by dividing the CI by the random index (Table 9).

$$CR = \frac{CI}{RI} \quad (8)$$

The generally acknowledged top limit for CR is 0.1. To increase consistency, the review process must be repeated if the final CR is higher than this.

3.5. Application

AHP is applied to the SWOT matrix. First, pairwise comparisons of the SWOT groups were performed using a comparison scale from 1 to 9 developed by Saaty [40]. Second, each SWOT group is considered while comparing the components of SWOT matrices. The expert team performs all pairwise comparisons in the application. Five of the 12 experts used in the first part of the study made up the expert team, and the first expert's prioritization scores are given below as an example (Table 10).

Table 9. *Random index*

n	1	2	3	4	5	6	7	8	9	10
RI	0.00	0.00	0.58	0.90	1.12	1.24	1.32	1.41	1.45	1.49
Source: [39] RI: Random index										

Table 10. *Pairwise comparisons of the SWOT factors for E1*

SWOT Groups	S	W	O	T	Importance degrees of SWOT groups
Strength (S)	1	3	1/3	1	0.223
Weaknesses (W)	1/3	1	1/3	1	0.129
Opportunities (O)	3	3	1	3	**0.485**
Threats (T)	1	1	1/3	1	0.161
CR=0.05	Source: Authors' calculations				

Table 11. *SWOT rankings of the main criteria based on pairwise comparisons*

SWOT/Expert	E1	E2	E3	E4	E5	Average	Rank
Strengths	0.223	**0.387**	0.183	**0.463**	0.161	**0.283**	**1**
Weaknesses	0.129	0.179	**0.316**	0.272	**0.424**	0.264	2
Opportunities	**0.485**	0.128	**0.316**	0.168	0.044	0.228	3
Threats	0.161	0.304	0.183	0.095	0.369	0.222	4
Source: Authors' calculations							

Table 12. *Comparison matrix of strength groups*

Strengths	S1	S2	S3	S4	Importance degrees
S1 Need for maritime expertise to perform terrorist attacks or sabotage against sea targets.	1	1/3	1/5	1/3	0.076
S2 Strict rules such as ISPS Code and CSI exist in IMO frameworks.	3	1	1/5	1	0.172
S3 Regional/international naval support against piracy and human trafficking.	5	5	1	3	0.559
S4 Use of technology enhancing the security of containers (AI, IoT, RFID, etc.).	3	1	1/3	1	0.191
CR=0.04 Source: Authors' calculations IoT: Internet of Things, RFI: Radio frequency identification					

The procedure is repeated and the results based on the opinions of five experts (E1, E2, E3, E4 and E5) are depicted in Table 11.

Subcriteria are then prioritized based on the same technique (Table 12).

Table 13. *SWOT rankings of strengths based on pairwise comparisons*

Strengths/ Experts	E1	E2	E3	E4	E5	Average	Rank
S1	0.076	0.055	0.061	0.073	0.065	0.066	4
S2	0.172	0.182	0.111	0.234	0.119	0.163	3
S3	**0.559**	0.238	**0.635**	**0.603**	**0.574**	**0.521**	**1**
S4	0.191	**0.522**	0.190	0.087	0.239	0.245	2
Source: Authors' calculations							

The procedure is repeated and the results based on the opinions of five experts (E1, E2, E3, E4 and E5) are depicted in Table 13.

Subcriteria are then prioritized based on the same technique (Table 14).

The procedure is repeated and the results based on the opinions of five experts (E1, E2, E3, E4 and E5) are depicted in Table 15.

Subcriteria are then prioritized based on the same technique (Table 16).

The procedure is repeated and the results based on the opinions of five experts (E1, E2, E3, E4 and E5) are depicted in Table 17.

Subcriteria are then prioritized based on the same technique (Table 18).

The procedure is repeated and the results based on the opinions of five experts (E1, E2, E3, E4 and E5) are depicted in Table 19.

4. Results and Discussion

There are different criteria for transportation mode selection, and safety/security is one of them. Other criteria for mode selection are cost, transport time, product characteristics (type of freight), service quality, market considerations (customers' demand), and carrier considerations [41]. Although there are initiatives such as the ISPS Code [42], which regulates the ship security analysis that must be performed by ship owners and operators, additional tools are needed to assess the security for a specific route, time period, or conditions. For example, the waters off the coast of Somalia were the world's most dangerous maritime channels between 2008 and 2011. During this time period, hundreds of attacks were conducted against ships, numerous seafarers were taken captive by pirates, and billions of dollars were spent by governments as hijacking costs.

Among the identified maritime transportation security risks, cyber-attacks had the maximum score -which is understandable-, considering the dependance on Global Navigation Satellite Systems and their vulnerability to jamming and spoofing. The second scored risk factor is

Table 14. *Comparison matrix of the weakness group*

Weaknesses	W1	W2	W3	W4	Importance degrees
W1 Additional risks compared with other transportation modes such as piracy and stowaways.	1	5	1	1	0.323
W2 Increased reliance on communication and information networks renders shipboard power systems more susceptible to covert cyberattacks.	1/5	1	1/3	1/3	0.082
W3 A more potential space for smuggling.	1	3	1	1/3	0.218
W4 Risk of blocking choke points in case of a terrorist attack/sabotage on a container ship, which will have a greater impact on the global economy.	1	3	3	1	0.375
CR=0.06 Source: Authors' calculation					

Table 15. *SWOT rankings of weaknesses based on pairwise comparisons*

Weaknesses/ Expert	E1	E2	E3	E4	E5	Average	Rank
W1	0.323	0.302	**0.418**	0.110	0.115	0.253	2
W2	0.082	**0.365**	0.217	0.173	0.085	0.184	4
W3	0.218	0.183	0.283	0.056	0.226	0.193	3
W4	**0.375**	0.148	0.080	**0.659**	**0.572**	**0.366**	**1**
Source: Authors' calculations							

Table 16. *Comparison matrix of the opportunities group*

Opportunities	O1	O2	Importance degrees
O1 China's policy to bypass sea routes by alternative transport routes and pipelines	1	5	1
O2 Existence of alternate routes, such as the Arctic route	1/5	1	2
CR=0.00 Source: Authors' calculations			

Table 17. *SWOT rankings of opportunities based on pairwise comparisons*

Opportunities/ Expert	E1	E2	E3	E4	E5	Average	Rank
O1	**0.833**	0.500	**0.833**	**0.833**	**0,866**	**0,773**	1
O2	0.166	0.500	0.166	0.166	0.129	0.225	2
Source: Authors' calculations							

war and warlike conditions, including territorial disputes. Territorial disputes in the South China Sea have not yet had a significant effect on merchant traffic as in the Black Sea, although that may change if the situation worsens. Piracy and armed robbery, the third scored risk factor, are perceived by experts as not as high a risk factor as the first two risk factors because of the modus operandi of the pirates in the Malacca Strait, which generally occurs as petty theft instead of hijacking.

Therefore, policy recommendations for the first part of the study could be to ensure that cyber awareness protocols,

Table 18. *Comparison matrix of the threats group*

Threats	T1	T2	T3	Importance degrees
T1 Existence of high-risk areas (HRA) through routes from Türkiye to the Far East.	1	3	5	0.655
T2 Increasing cyber-security risks with recent developments in technology.	1/3	1	1	0.186
T3 Territorial disputes in the South China Sea and the Taiwan problem.	1/5	1	1	0.157
CR=0.02 Source: Authors' calculations				

Table 19. *SWOT rankings of threats to on pairwise comparisons*

Threats/ Expert	E1	E2	E3	E4	E5	Average	Rank
T1	**0.608**	0.199	**0.607**	**0.655**	0.259	**0.477**	**1**
T2	0.242	0.199	0.302	0.186	0.106	0.207	3
T3	0.101	**0.600**	0.089	0.157	**0.634**	0.313	2
Source: Authors' calculations							

including IMO recommendations [43,44], are followed in addition to some basic precautions, such as the segregation of vessel networks, frequent password changes, or software updates. Another countermeasure could be switching off the AIS in high-risk areas (HRA) upon the lawful decision of the ship's captain [45].

There is not much that can be done about the risk of war and warlike conditions other than to take appropriate security measures, such as staying away from HRAs or taking necessary precautions in ports with ISPS Security Level 3. For piracy risk, complying with IMO and Best Management Practices (BMP) recommendations would be the best option apart from a detailed threat and risk assessment to be conducted by the companies and ships prior to transit through the HRA, as stated in BMP-5 [46].

When analyzing the results of the prioritization of the main SWOT criteria, "strengths" had the highest score,

which indicates that existing tools such as regulatory legislation, naval support, and use of technology together with the need for maritime expertise to perform a terrorist attack are recognized enough for the experts to choose strength as the highest scored SWOT criterion. This can be interpreted as indicating that although there are some hurdles, maritime container transportation's strengths are higher than its weaknesses, which makes it a preferred mode of transportation compared to other modes, in terms of security aspects.

Among the subcriteria within the main SWOT factors, the highest scored "strength" factor is "regional/international naval support against piracy and human trafficking". Operations that help decrease piracy incidents off the Somali coast, such as NATO's Operation Ocean Shield (terminated end 2016), the EU's Operation Atalanta, and Combined Task Force-151 led by the United States, are examples of how this option works. A similar operation, named MALSINDO, has been carried out in the Malacca Strait since 2014 by the Malaysian, Indonesian, and Singaporean navies to manage piracy in the region.

The highest scored "weakness" is "risk of blocking choke points in case of a terrorist attack/sabotage to a container ship that will have a greater impact on global economy". Although the Ever Given accident in 2021 in the Suez Canal was a safety incident, attacks that disrupt choke points can easily be organized by terrorists using remote controlled "kamikaze" unmanned surface vehicles (USV) packed with explosives. It should be remembered that until the stuck ship was rescued, the blockage of the Suez Canal -through which 30% of the world's container ship traffic passes- cost $9 billion per day [47], with hundreds of ships waiting at both entrances of the canal or some preferring the Cape of Good Hope by extending their route by at least 4,000 extra miles, or 6 more transport days (minimum).

Within the subcriteria "opportunities", "China's policy to bypass sea routes by alternative transport routes" is the preferred choice between the two criteria, such as the China-Pakistan Economic Corridor and/or Kra Canal. The former aimed to secure and reduce passage through the Malacca Strait for China's energy imports, and the latter planned to connect the Andaman Sea across southern Thailand. The second opportunity, namely Arctic routes bypassing the Suez route, has recently increased in importance with the expanded time window in which the passage could be accomplished throughout the year without the assistance of icebreakers, as a result of global warming. Furthermore, it is shorter than the Suez route. Although Turkish shipping companies have not yet begun to use that route, they may do so in the future.

Within the "threats" subcriteria, "the existence of HRA through the routes from Türkiye to the Far East" had the highest score. When checking the *International Bargaining Forum's list of designated war risk areas [48] as of September 1, 2023, 12 nm. off the Yemeni Coast including all ports, excluding the Maritime Security Transit Corridor in the Red Sea, is designated as the risk area and the recommendation is to operate at ISPS Level 3. Additionally, considering the developments in Israel, the security level of Turkish flagged ships that will call at Israeli ports and sail off the coast of these ports has been increased to three by the Ministry of Transport and Infrastructure [49].

Although not an HRA, the Straits of Malacca and Singapore (72 incidents), South China Sea (4 incidents), and Arabian Sea (1 incident) are areas of concern in terms of piracy and armed robbery, constituting 58% of all piracy incidents in 2022 throughout the world (131 incidents). In the same year, out of 77 incidents en route to the Far East, 6 were against container ships, in two of which the crew's belongings were stolen, without any injuries [50]. In the first six months of 2023 -for which monthly reports were published by the IMO- of a total 89 incidents, 7 were against container ships in the Straits of Malacca and Singapore, the South China Sea, and the Arabian Sea, 6 were at anchor and 1 was drifting, no crew members were injured, and all resulted in stolen equipment. Most of the attacks in those regions were conducted against bulk carriers and tankers, whose low speed and freeboard compared with container ships make them easier for pirates to board [51].

5. Conclusion

The aim of this study was to understand the perception of security risks in the container trade by choosing the Suez route from Türkiye to the Far East as a case study based on three research questions. The 12 experts selected from shipping companies and academia concluded that among the six identified risk factors, cyber-attacks were the most dangerous. Additionally, SWOT factors are identified and prioritized. Strengths were the highest scored main criterion, and each subcriteria was prioritized as explained above. Although "strengths" scored highest among the SWOT prioritization, recent incidents in the Black Sea could occur in the South China Sea if the situation worsens; if so, they could impact merchant traffic and hence the global supply chain.

The merging of hitherto standalone operational technology (OT) systems -which physically operate several systems

*The International Bargaining Forum (IBF) brings together the International Transport Workers' Federation (ITF) and the international maritime employers that make up the Joint Negotiating Group (JNG).

onboard the ship-with information technology (IT) systems deployed both onboard and ashore has made the marine industry extremely vulnerable to cybersecurity threats today. Cloud computing, the Internet of Things, and autonomous technologies will continue to be adopted by the maritime industry, which will boost the interconnectedness between OT and IT and raise cybersecurity threats. Moreover, maritime pirates can exploit cybersecurity breaches to track ship movements and gather intelligence about possible weaknesses in defenses.

Therefore, more strict legal implications are needed to tackle both cyber security and piracy risks from the viewpoint of governments and international maritime security governance. Creating courts with specific jurisdiction, such as the ones established for piracy crimes in West Africa, may help prevent cybercrimes as well.

On the other hand, climate change affects maritime transportation and its security. The increasing time window for the use of the Arctic route will not only decrease transit time and cost but also eliminate security risks in the Suez route, which increased recently after the Israel-Hamas war.

Finally, the main conclusion is that additional risk assessments are needed by shipping companies for a specific route or a period to increase transportation security.

6. Suggestions for Further Research

Most research in this area takes both safety and security into account, which in a way is understandable because of their close link, but security-specific research assessing a designated route or transportation mode such as intermodal transport could contribute to the literature. Additionally, considering the fast-growing digitalization and automation in our era, recommendations for future research could include a security risk assessment for autonomous ships and security concerns against unmanned underwater vehicles (UUVs) or USVs.

Peer-review: Externally peer-reviewed.

Authorship Contributions

Concept design: F. Oral, Data Collection or Processing: F. Oral, Analysis or Interpretation: F. Oral, and S. Paker, Literature Review: F. Oral, Writing, Reviewing and Editing: F. Oral.

Funding: The authors received no financial support for the research, authorship, or publication of this article.

References

[1] D. Ekwall, *Managing the Risk for Antagonistic Threats Against the Transport Network*. Göteborg: Chalmers Univ. of Technology, 2009.

[2] M. G. Burns, Logistics and Transportation Security: A Strategic, Tactical, and Operational Guide to Resilience, CRC Press, NW: Boca Raton, 2016.

[3] M. Chandra, and S. K. Pandey, *Advancements in Maritime Security: Exploring Emerging Technologies,* 2023.

[4] The Jamestown Foundation, China's Silk Road Strategy: A Foothold in the Suez, China Brief Volume: 14 Issue: 19, 2014. [Online]. Available: https://jamestown.org/wp-content/uploads/2014/10/China_Brief_Vol_14_Issue_19_5.pdf, [Accessed: Aug. 14, 2023].

[5] Dryad Global Annual Report 2022-2023, The State of Maritime Security, [Online]. Available: https://insights.charliecharlieone.co.uk/story/dryad-global-annual-report-2022-2023/page/6/1, [Accessed: Aug. 14, 2023].

[6] Euronews, "Italian forces secure Turkish ship attacked by armed stowaways off Naples", 10, June 2023. [Online]. Available: https://www.euronews.com/2023/06/10/italian-forces-secure-turkish-ship-attacked-by-armed-stowaways-off-naples, [Accessed: Aug. 14, 2023].

[7] V. Bolbot, G. Theotokatos, E. Boulougouris, and D. Vassalos, "A novel cyber-risk assessment method for ship systems," *Safety Science*, vol. 131, pp. 1-14, Jul 2020.

[8] G. Wimpenny, J. Šafář, A. Grant, and M. Bransby, "Securing the Automatic Identification System (AIS): Using public key cryptography to prevent spoofing whilst retaining backwards compatibility," *Journal of Navigation*, vol. 75, pp. 333-345, Oct 2021.

[9] E. Albrechtsen, "Security vs safety", *Norwegian University of Science and Technology Department of Industrial Economics and Technology Management*, Aug 2003.

[10] J. Kubáňová, and I. Kubasáková, "Impact of the pandemic Covid-19 to criminal activity in transport," *International Scientific Journal About Logistics*, vol. 8, pp. 117-122, Dec 2021.

[11] K. Kuhn, S. Bicakci, and S. A. Shaikh, "COVID-19 digitization in maritime: Understanding cyber risks", *WMU Journal of Maritime Affairs*, vol. 20, pp. 193-214, Jun 2021.

[12] S. Fan, and Z. Yang, "Safety and security co-analysis in transport systems: Current state and regulatory development," *Transportation Research Part A: Policy and Practice*, vol. 166, pp. 369-388, Nov 2022.

[13] IMO. Formal safety assessment-consolidated text of the guidelines for formal safety assessment (FSA) for use in the IMO rule-making process (MSC/Circ.1023-MEPC/Circ.392). In: International Maritime Organization; 2007.

[14] M. Mousavi, I. Ghazi, and B. Omaraee, "Risk assessment in the maritime industry," *Engineering, Technology & Applied Science Research,* vol. 7, pp. 1377-1381, Feb 2017.

[15] D. Zhang, "Challenges and new developments in maritime risk assessment," *PSAM 2014 - Probabilistic Safety Assessment and Management*, Jun 2014.

[16] M. Jiang, Y. Liu, J. Lu, Z. Qu, and Z. Yang, "Risk assessment of maritime supply chains within the context of the Maritime Silk Road," *Ocean & Coastal Management*, vol. 231, pp. 1-14, Oct 2022.

[17] F. Goerlandt, and J. Montewka, "Maritime transportation risk analysis: Review and analysis in light of some foundational issues," *Reliability Engineering & System Safety*, vol. 138, pp. 115-134, Feb 2015.

[18] M. Cieśla, B. Mrówczyńska, and T. Opasiak, "Multimodal transport risk assessment with risk mapping," *Zeszyty Naukowe Politechniki Śląskiej*, vol. 105, pp. 31-39, 2017.

[19] S. Roh, J. Tam, S.-W. Lee, and Y.-J. Seo, "Risk assessment of maritime supply chain security in ports and waterways," *International Journal of Supply Chain Management*, vol. 7, pp. 300-307, Dec 2018.

[20] S. Nguyen, P. S.-L. Chen, and Y. Du, "A methodological framework for quantitative risk analysis in container shipping operations," *Maritime Business Review*, vol. 8, pp. 139-155, Apr 2022.

[21] S. Nguyen, and H. Wang, "Prioritizing operational risks in container shipping systems by using cognitive assessment technique," *Maritime Business Review*, vol. 3, pp. 185-206, Aug 2018.

[22] C. Wan, X. P. Pan, D. Zhang, and Z. Yang, "Analysis of risk factors influencing the safety of maritime container supply chains," *International Journal of Shipping and Transport Logistics*, vol. 11, pp. 476-505, Jan 2019.

[23] C.-H. Chang, J. Xu and D.-P. Song, "Risk analysis for container shipping: From a logistics perspective," *The International Journal of Logistics Management*, vol. 26, pp. 147-171, May 2015.

[24] Y. Zhou, X. Li, and K. F. Yuen, "Holistic risk assessment of container shipping service based on Bayesian Network Modelling," *Reliability Engineering & System Safety*, vol. 220, pp. 1-16, Apr 2022.

[25] C. Wan, X. Yan, D. Zhang, Z. Qu, and Z. Yang, "An advanced fuzzy Bayesian-based FMEA approach for assessing maritime supply chain risks," *Transportation Research Part E: Logistics and Transportation Review*, vol. 125, pp. 222-240, May 2019.

[26] M. Blišťanová, P. Koščák, M. Tirpáková, and M. Ondicová, "A cross-comparative analysis of transportation safety research," *Sustainability,* vol. 15. pp. 7609, May 2023.

[27] S. Fan, and Z. Yang, "Safety and security co-analysis in transport systems: Current state and regulatory development," *Transportation Research Part A: Policy and Practice,* vol. 166, pp. 369-388, Nov 2022.

[28] T. Hill, and R. Westbrook, "SWOT analysis: it's time for a product recall", *Long Range Planning*, vol. 30, pp. 46-52, 1997.

[29] H. Shevchenko, S. Shevchenko, Y. Zhdanova, S. Spasiteleva, and O. Negodenko, *Information Security Risk Analysis SWOT*, Open Conference on Cybersecurity Providing in Information and Telecommunication Systems, Jan 2021, Kyiv, Ukraine.

[30] S. H. Amin, N. Yan, and D. Morris, "*Analysis of transportation modes by evaluating SWOT factors and pairwise comparisons: a case study*" in Multi-Criteria Methods and Techniques Applied to Supply Chain Management, V. A. P. Salomon, Ed. Brazil: InTech., 2018, pp. 57-74.

[31] H.-H, Chang, and W.-C. Huang, "Application of a quantification SWOT analytical method," *Mathematical and Computer Modelling*, vol. 43, pp. 158-169, Jan 2006.

[32] Y. E. Şenol, V. Gökçek, and A. Seyhan, "*SWOT-AHP analysis of autonomous shipping*," IV. International Multidisciplinary Congress of Eurasia, Aug. 2017, Roma, Italy.

[33] V. Brett, *The Potential for Clustering of the Maritime Transport Sector in the Greater Dublin Region*. Dublin: National College of Ireland, 2007.

[34] P. Kapoor, *Systems approach to documentary maritime fraud*. Plymouth: Plymouth Polytechnic Institute of Marine Studies, 1987.

[35] C. Powell, "The Delphi technique: Myths and realities," *Journal of Advanced Nursing*, vol. 41, pp. 376-382, 2003.

[36] J. Nworie, "Using the Delphi technique in educational technology research," *TechTrends*, vol. 55, pp. 24-30, Oct 2011.

[37] A. Görener, K. Toker and K. Uluçay, "Application of combined SWOT and AHP: a case study for a manufacturing firm," *Procedia - Social and Behavioral Sciences*, vol. 58, pp. 1525-1534, Oct 2012.

[38] M. J. Sharma, I. Moon, and H. Bae, "Analytic hierarchy process to assess and optimize distribution network," *Applied Mathematics and Computation*, vol. 202, pp. 256-265, Aug 2008.

[39] J. Kangas, M. Pesonen, M. Kurtilla, and M. Kajanus, A'WOT: Integrating the AHP with SWOT Analysis, The International Symposium on the Analytic Hierarchy Process, 6th ISAHP 2001 Proceedings, Berne, Switzerland, 2001.

[40] T. L. Saaty, The Analytic Hierarchy Process, McGraw-Hill, New York. 1980

[41] G. D. Sakar, *Transport Mode Choice Decisions and Multimodal Transport: A Triangulated Approach*, Dokuz Eylul University Publications, Izmir, 2010.

[42] IMO, 2002. The international Ship and Port Facility Security Code. In: SOLAS. International Maritime Organization, London (Chapter XI-2).

[43] IMO Resolution MSC.428(98) with the topic: "Maritime Cyber Risk Management in Safety Management Systems".

[44] IMO Guideline MSC-FAL.1/Circ.3/Rev.2 with the topic: "Guidelines on Maritime Cyber Risk Management".

[45] H. Karahalios, "Appraisal of a ship's cybersecurity efficiency: the case of piracy", *Journal of Transportation Security*, vol. 13, pp. 179-201, Sep 2020.

[46] BMP-5, "Best management practices to deter piracy and enhance maritime security in the Red Sea, Gulf of Aden, Indian Ocean and Arabian Sea.

[47] BBC News Pidgin, Suez Canal blockade: "Ever Given" ship blocking Suez Canal dey cost traders $9.6bn daily, [Online] Available: https://www.bbc.com/pidgin/tori-56541085.

[48] ITF Seafarers, IBF Warlike and High-Risk Areas, London: ITF House, 2023 [Online] Available: https://www.itfseafarers.org/en/resources/materials/ibf-warlike-and-high-risk-areas.

[49] Turkey Posts English, "*Extraordinary' measure for Israeli ports*", October 2023, [Online]. Available: https://turkey.postsen.com/world/394827/%E2%80%98Extraordinary%E2%80%99-measure-for-Israeli-ports.html.

[50] IMO, Piracy Reports, 2022 annual report and monthly reports between January to June 2023 [Online] Available: https://www.imo.org/en/OurWork/Security/Pages/Piracy-Reports-Default.aspx.

[51] H. Liwång, J. W. Ringsberg, N. Martin, "Quantitative risk analysis - ship security analysis for effective risk control options," *Safety Science*, vol. 58, pp. 98-112, Apr 2013.