SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2025
ORGANIZATION AND MANAGEMENT SERIES NO. 231

# RISK IDENTIFICATION PROCESS IN THE MANAGEMENT OF CRITICAL MARITIME INFRASTRUCTURE

Michał IGIELSKI

Gdynia Maritime University; m.igielski@wznj.umg.edu.pl, ORCID: 0000-0003-4680-3733

**Purpose:** The main purpose of the article is to identify the basic groups of risks during the process of managing maritime critical infrastructure.
**Design/methodology/approach**: The methodological approach chosen by the author of the article is thinking guided by preconceived conclusive and explanatory sentences. The methodology of the research was mainly focused on the process of managing maritime critical infrastructure - it was based on the analysis of activities carried out by selected entities in the maritime industry. To achieve the research goal, the author used critical analysis with reference to the collected literature, the observational method (allowed to identify the risk flux in changing external and internal conditions) and the intuitive method (consisted of considering a number of concepts, problems and terms in the field of risk management).
**Findings:** Organizations in the maritime industry that manage maritime critical infrastructure are aware of the challenges they face due to the new risk groups accompanying the above process. According to the author, in the face of new market determinants, organizations, should include in this process unprecedented risks, risk intelligence and quantification of cognitive approaches to critical infrastructure management.
**Practical implications:** The practical nature of the study stems from the author's intended goal of identifying new risks in the process of managing maritime critical infrastructure. In addition, the author of the article is tasked with the fact that these very new risks, which are a consequence of economic changes, will become a permanent part of management.
**Social implications:** For organizations and their employees, properly identified new risk groups should help in their daily work, and in combination with decision-making issues, in this area of management, affect the security of entire societies.
**Originality/value:** Thanks to the research process carried out - the analysis of activities in the area of management of maritime critical infrastructure in selected organizations, the main purpose of the prepared material has been realized. In turn, the conclusions obtained can find theoretical and practical application, in the creation of new methods and tools for risk management.
**Keywords:** critical infrastructure, risk, risk management.
**Category of the paper:** Research paper.

## 1. Introduction

Risk management is a key element in the operation of all modern organizations, regardless of industry. Today's businesses face numerous threats, both internal and external, which can affect their ability to achieve their strategic objectives. This is even more so when considering those with so-called critical infrastructure. It is the management of critical infrastructure that has become a major issue in the area of national security and the stability of economic and social systems, and risk management a fundamental element of their functioning, regardless of the industry. Therefore, the aim of the article is to identify the main risks when managing maritime critical infrastructure.

In the article, the author provides a definition of critical infrastructure and the main types of risks. He also discussed the challenges of managing it in the face of economic and technological uncertainty and presented good practices in the context of protecting, developing and maintaining these assets in the face of various risks. In addition, the author conducted an analysis of the basic principles and techniques of risk management - describing the main types of risks.

The content of the paper covers theoretical and practical aspects, taking into account the latest trends and technological solutions. On the other hand, the author's intention of the paper is to initiate a discussion on risk in the process of security management of critical infrastructure, under the conditions of civilization progress, because, as is evident from numerous scientific studies, awareness of the negative consequences of progress is essential for taking correct actions to minimize their negative impact.

## 2. A definition of risk management in critical maritime infrastructure

Critical infrastructure is a set of resources and systems that are essential to the functioning of society and the economy, and their damage or destruction can lead to serious consequences, both locally and globally. Critical infrastructure includes, but is not limited to, energy, water, transport, telecommunications, information systems, as well as emergency and defense services. Managing such infrastructure requires specialized planning, organizing, monitoring, securing and responding to threats that may damage or destroy it. Critical infrastructure protection encompasses both prevention and response to potential threats, including cyber-attacks, natural disasters, technical failures or terrorist activities (Nowak, 2020).

Today's critical infrastructure is highly complex and many of these systems are interconnected. Problems in one area can lead to disruptions in others. For example, a failure in the power grid can affect the operation of telecommunications systems, which in turn can have a negative impact on the operation of emergency services. These interdependencies mean that

effective management of critical infrastructure requires a holistic approach, taking into account different sectors and systems. Strategies need to be developed that are able to address potential contingency scenarios in different areas of infrastructure (Prabaswari et al., 2024).

With the increasing digitalization of critical infrastructures come new threats of cyber-attack. Hackers can take control of energy, transport or water supply systems, which can lead to major crises. Protecting against cyber threats is crucial, and safeguards must include both hardware and software. Climate change, on the other hand, is leading to an increase in extreme weather events such as hurricanes, floods and heat waves. Such phenomena can have a serious impact on the operation of critical infrastructure, especially with ageing systems. For this reason, it is also becoming necessary to integrate climate change protection aspects into infrastructure management strategies. Depending on the country and the specifics of the infrastructure in question, we can observe a range of management models, some examples of which are described by the author in Table 1.

**Table 1.**
*Main models of critical infrastructure management*

| № | Name | Description |
|---|---|---|
| 1. | Centralized management | In a centralized model, all decisions concerning critical infrastructure are taken centrally. Such a model has its advantages in terms of rapid decision-making and uniform oversight of the entire infrastructure, but may be less flexible in responding to local problems. |
| 2. | Decentralized management | In a decentralized model, responsibility for individual infrastructure sectors is distributed among different local government units, agencies and organizations. Such a system can provide greater flexibility and a faster response to local crises, but involves difficulties in coordinating activities at the national level. |
| 3. | Public-private partnership (PPP) | In the PPP model, the public and private sectors work together, where responsibility for managing critical infrastructure is shared. In this case, private companies are often responsible for the design, construction and operation of the infrastructure, while the government handles its supervision and regulation. Such a model can combine the advantages of both sectors, but requires very precise contracts and strict controls. |

Source: own study based on Prabaswari et al., 2024.

Nor can we forget modern technologies, which are playing an increasingly important role in critical infrastructure management. Among them, it is worth mentioning (Wiśniewski, 2022; Dąbrowski, 2021):

1. Monitoring and data analysis systems, which allow to keep track of the state of infrastructure, detect anomalies and predict potential failures.
2. The Internet of Things (IoT), which enables the integration of different infrastructure components - this allows remote monitoring and control of systems.
3. Artificial intelligence (AI), which is used to analyses large data sets, among other things, which can help detect threat patterns and optimize management.
4. Blockchain, which ensures the secure transfer and storage of data - this can be particularly important in the context of protection against cyber attacks.

In many countries, standards and good practices for critical infrastructure management have been developed based on the above tools. An example is the US CISA[1] (Cybersecurity and Infrastructure Security Agency) guidelines, which include, among other things, preparing contingency plans, conducting regular training and investing in new security technologies.

Given the information on critical infrastructure management presented by the author above, the issue of existing risks and their management cannot be ignored in this area. This process is commonly equated with the process of identifying, assessing and taking action to minimize the negative effects of risks and maximize the benefits associated with potential opportunities. The aim is to create structures and processes that allow an organization to respond to risks and exploit opportunities in a way that does not threaten its stability and growth. Various definitions can be found in the literature, but the aspects of anticipating, monitoring and controlling risks, as well as the adaptability of the organization to a changing environment, are most commonly emphasized). This is probably a result of the fact that this concept covers a wide range of risks that can occur in different areas of an organization's activities. Several key types of risk can be identified in the literature, including (Krzysztofowicz, 2012):

1. Strategic risk - associated with long-term decisions and the direction of the organization's development. This includes the risk of wrong strategic choices, inadequacy of resources, changes in the market or unpredictable technological trends.
2. Operational risk - associated with the day-to-day processes of the organization, including human error, system failures, inadequate quality management or problems with suppliers.
3. Financial risk - associated with the unpredictability of financial markets, changes in exchange rates, interest rates, inflation or credit risk.
4. Legal and regulatory risk - includes the risk of changes in laws, industry regulations or the risk of the organization's activities not conforming to current standards.
5. Market risk - arising from dynamic changes in the market environment, such as changing demand, increased competition, changing consumer preferences or economic crisis.

Therefore, in order to manage risks effectively, methodical approaches should be used together with appropriate tools (described by the author in Table 2). In contrast, the most commonly used model is the so-called risk management cycle, which includes the following stages[2]:

1. Risk identification - involves identifying and understanding the risks that may affect the organization. Various tools are used for this purpose, such as SWOT analysis, PESTLE analysis or risk mapping.

[1] https://www.cisa.gov/critical-infrastructure-security, 31.01.2025.
[2] https://www.iso.org/obp/ui/en/#iso:std:65694:en, 31.01.2025.

2. Risk assessment - in this step, the organization assesses the likelihood of a hazard occurring and the potential impact it may have on the business. An important tool here is a qualitative and quantitative analysis of risks, including a so-called risk matrix that helps to priorities.
3. Risk response - includes taking action to reduce the risk (e.g. through insurance, implementing control procedures), transferring the risk (e.g. outsourcing, working with partners), avoiding the risk (e.g. changing strategy) or accepting it if the cost of counteracting it is too high.
4. Risk monitoring and control - the process of continuously overseeing identified risks, including assessing the effectiveness of actions taken, and adjusting strategies in response to changes in the organization's environment.

**Table 2.**
*The most common tools used in risk management*

| № | Name | Description |
|---|---|---|
| 1. | SWOT analysis | Helps to identify an organisation's internal strengths and weaknesses and external opportunities and threats. |
| 2. | Ishikawa diagram (Fishbone) | Used to analyse the causes of risk, it enables the identification of factors that can lead to problems. |
| 3. | Monte Carlo analysis | Used in the assessment of financial risks, it is based on computer simulations to estimate the probability of various scenarios. |
| 4. | Risk matrix | Allows risks to be classified according to their probability of occurrence and potential impact on the organisation, helping to prioritise actions. |

Source: own study based on Tarczyński (2011).

Below, in Figure 1, the author of the article proposes a risk classification matrix for maritime critical infrastructure (MIC), which includes basic risk categories, examples of risks, potential consequences, and areas of risk management.

In summary, today's organizations face a number of risk management challenges. In an era of globalization, a rapidly changing technological environment and economic uncertainty, identifying and controlling risks has become more difficult. Some of the most significant challenges include:

1. The complexity of risks - risks are becoming increasingly complex, interconnected and difficult to predict.
2. Dynamic technological change - rapid developments in technology are associated with new risks, e.g. cyber-attacks, which pose a serious threat to the security of the organization.
3. Market uncertainty risk - changes in economic policy, trade wars, pandemics and other crises can trigger rapid changes in the market environment that are difficult to predict.
4. Global risk management - organizations operating in multiple international markets must take into account the risks associated with different legal systems, organizational cultures and economic differences.

**RISK CLASSIFICATION MATRIX**

Maritime Critical Infrastructure

| | Category | Sources or threat | Examples | Potential impacts | Risk management |
|---|---|---|---|---|---|
| | **Natural** | Storms, hurricanes, tuunamis, floods, sea-level rise- | Demage to ports, docks, terminals, supply chain disruptions | Damage to ports. docks, terminals, supply chain | Soatial planning protective engineering eatly warning systems |
| | **Technical** | infrastructure san-tem failures, cargo handi-ng equipment failures | Shipment delays, financial losses, accident risk | Paralysis of traffic management systems, | Preventive maintenance technical safety systems contingency plans |
| LONV | **Cyber** | ITIOT attacks, system failures, ransum-mare attacks on port | P20AMscu of traffic, management.systems, delays in handling | Destruction of infrastructure, casualties, economic | Cybersecurity policy network segmentat-tion. setioms, rations |
| | **Physical** | Bombings in ports, subsea cable sabotage maritime route bac | Destruction of infrastructure, casualties economic destabiliza- | Disruptions in energy supply and trade, political esciation | International coopera-tion, strategic monitor-ing, crisis exercises |
| | **Hybrid/ Geopolitical** | State conflicts, hybrid warfare, incortsRerece in subsea pipelines· | Disruptions in energy supply, trade | Unrcupion of energey escala | Route diversification business continuity management, contrac- |
| | **Economic/ Logistic** | Disruptions in global trade and supply chains port-strives | Shipment delays, increased transport costs production stoppages | Accidents, reduced efficiency, increased risk of secondary | Training, safety procedu-res. satety culture: crisis communications |

**Figure 1.** Risk classification matrix for critical maritime infrastructure.

Source: own study.

Therefore, risk management in critical maritime infrastructure is a key element in ensuring its continuity of operation, safety, and resilience to natural, technical, and deliberate threats. In terms of definition, this process includes the identification, analysis, assessment, and control of risk, as well as the implementation of measures to minimize its effects. The essence of risk management is a systemic approach that combines technical, organizational, and legal aspects, enabling effective response to threats and reduction of their potential consequences. This makes it possible not only to ensure the safety of maritime infrastructure, but also to protect the economic, environmental, and social interests of the state.

## 3. Materials and methods

In order to talk about the identification of the main risks in the process of security management of maritime critical infrastructure, it is necessary, according to the author, to "start" from the problem of making decisions and judgements under conditions of uncertainty and cognitive errors. During security management, many decisions are based on beliefs about the probability of uncertain events, which are central to the choices made in the context of risk (Wódkiewicz, 2019). These risks can result in serious and systemic errors due to: a lack of

acknowledged representativeness of the premises, an illusion of the accuracy of one's own predictions, a lack of so-called cognitive strain and giving the outcomes under investigation their own interpretative framework by misstating the problem, e.g. the identified threat (Kahneman, 2022).

On the other hand, the doctrinal position points to the complexity, diversity and relativity of the concept of risk itself, which, in research, makes it difficult to attempt any classification of this problem in definable terms. However, in this situation, for the purposes of the study, on the basis of the definitions cited earlier, let us assume that risk is: the estimated probability of a particular type of hazard or loss occurring, as well as the gain and benefit associated with decisions made, which are relevant to the future. In this situation, the intended objectives of critical infrastructure security management, as implemented in the decision-making process, should include a strategy for situations of their destruction within a certain risk tolerance band (Ficoń, 2007).

The cited definition is closely related to the ontological view of security, from which it follows that the general definition of the formation of any type of security, boils down to the fact that it is the design of a specific state of relatively valued positively ensuring persistence, survival, improvement and development. In contrast, its identical and developed formulation, boils down to (Beck, 2004):

- the shaping of a certain state, through the assessed risks relating to it,
- risk understood as a useful application, which should be balanced by a decision in the management process on the basis of a decision,
- a decision made using the information at hand, information that is relevant to the future, which should refer to a specified object, in a specified meaningful context and the resulting conclusions).

Under these conditions, risk acceptance, is risk tolerance on the basis of resource and relational discretion. The rationale for this statement stems from the fact that an integral part of the analyzed each risk (risk receiver, risk issuer), are the conditions of the decision-making process, creating a decision-making situation, which is determined, among other things, by legal conditions. Among other things, such relations may result from the assessment of decision-making freedom made at the stage of building variants for solving the decision issue in the aspect of advantageousness, completeness and sufficiency of resource wielding, as well as the selection of a variant for solving the decision issue in the aspect of wielding sufficient resources in the period of decision implementation (Walasek, Wojnarowski, 2011).

Summarizing on the basis of an analysis of theoretical research on risk in the maritime sector and a review of strategic documents, the author of the article:

- defines key concepts: risk management, critical infrastructure, maritime critical infrastructure,
- analyzes risk management models in the literature,

- classify risks in maritime infrastructure (natural, technical, cyber, terrorist, and geopolitical threats),
- identify dominant approaches and compare international perspectives.

## 4. Results and discussion

A recurring theme across policy and academic work is the fragmentation of responsibility and the absence of coherent, sector-specific governance frameworks. C. Bueger and T. Liebetrau (2023) emphasizes that high-profile incidents exposed gaps in assignment of roles and coordination between state actors and private operators. Similarly, practitioner reports argue for system-level coordination mechanisms and common procedures to improve situational awareness and response. Together, these analyses suggest that effective MIC risk management requires institutional designs enabling cross-jurisdictional information sharing and joint decision processes rather than ad hoc, reactive arrangements.

Based on an analysis of the literature on the subject and strategic documents, the author identified the main theoretical gaps (described in Table 3), which focus on the lack of uniform definitions and models dedicated to the maritime sector, weak interdisciplinary integration, failure to take into account complex systemic links, underrepresentation of new generation threats, and insufficient development of the concept of resilience and the international perspective.

**Table 3.**
*Theoretical gaps in research on risk management in maritime critical infrastructure*

| № | Area | State of research | Theoretical gap | Directions for further research |
|---|---|---|---|---|
| 1. | Definitions and conceptual frameworks | General definitions of critical infrastructure and risk management exist (ISO 31000, EU directives). | Lack of unified definitions and models dedicated to the maritime sector. | Development of standardized, sector-specific definitions and conceptual frameworks. |
| 2. | Theory–practice integration | Technical and security-oriented studies dominate over managerial and organizational analyses. | Lack of interdisciplinary approaches combining technical, legal, economic, and social aspects. | Development of holistic models integrating multiple research perspectives. |
| 3. | Systemic and cascading risks | Analyses focus on single elements (ports, terminals, cables). | Insufficient research on interdependencies and cascading effects. | Creation of systemic models considering interactions and cross-border consequences of failures. |
| 4. | New Types of Threats | Focus on traditional threats (natural disasters, technical failures). | Low representation of cyber threats, hybrid conflicts, and the impact of climate change. | Expanding analyses to include new generations of threats and their effects on maritime infrastructure. |

Cont. table 3.

| | | | | |
|---|---|---|---|---|
| 5. | Resilience | Dominance of preventive approaches and risk minimization. | Weak development of resilience and adaptability concepts in maritime systems. | Research on adaptability and rapid recovery of infrastructure functions. |
| 6. | International Perspective | Analyses mainly concentrated at the national level. | Lack of comparative studies on regulations and practices at the global scale. | Development of studies on international cooperation and regulatory harmonization. |

Source: own study.

A strong strand of recent research advances the argument that this process must be treated as an interconnected network whose local failures can propagate widely. J. Liupeng, W. Guangsheng, F. Xuejun, Y. Tong and L. Zhiyi (2024) develop quantitative models of cascading failures in maritime networks, demonstrating that disruptions in a single port or chokepoint may trigger broad, nonlinear consequences for global flows. Complementary modeling work using multi-agent simulations (Qu et al., 2024) shows that even short-term port disruptions can create long-tail impacts on supply chains that persist after direct physical operations resume. These studies collectively make the case for embedding network and systems thinking - rather than single-asset risk assessment - into maritime risk frameworks.

On the other hand, work on multiple hazard analysis and flood impact mapping methodology (Arvidsson et al., 2023) highlights the vulnerability of ports and coastal infrastructure to complex hazards. Ports in low-lying areas are exposed to cumulative effects (e.g., storms and simultaneous infrastructure failure) that significantly weaken their resilience. Researchers emphasize that climate risk must be integrated into classic hazard analyses to account for both the increasing frequency of events and the degradation of infrastructure in the long term.

The risk analysis carried out in the publication takes into account the realization that nowadays, the unlearning of risk becomes a scientific problem in itself, where in this situation it will be necessary to reveal the contradictions and difficulties that exist in the interrelationships between practice and disciplines in the interdisciplinary maritime reality, which should take into account that (Falencikowski, 2008):

1. In a technologically advanced innovative economy, the production of occurring risks and hazards shows a dependence on knowledge as its product, based on standards of its own rationality.
2. The dynamics of civilizations progress means that we can no longer speak of the predictability of risks as they are:
   - produced - the problem of unpredictability is mainly due to the difference based on scientific skill between estimation and calculability,
   - contradict rational conditions of acceptability, deforming the rules of universal acceptance.

3. There is a so-called risk intelligence in the maritime safety space that:
   - has a fundamental impact on the theoretical content of risk and its relation to the proliferation of its varieties,
   - has an impact on the so-called risk content (extent, intensity, causality, damage).

Under these conditions, the risk of the effectiveness of the security management of maritime critical infrastructure dictates that we consider:

1. Operational risks, which arise from inadequate and malfunctioning internal processes, occurring, for example, in the environment of those employed at the facility.
2. Economic risks, which may be caused by changes in economic conditions - e.g. the risk of an acceptable financial contribution to the security management organization.
3. Event risk, which may be caused by the occurrence of specific events or natural disasters.
4. Model risk, or the risk of theoretical error in the real world, which includes the model of security management itself (and the risks within it).
5. Model of risk assessment adopted, which most often leads to wrong decisions being made in the face of the risks of their relationship to the social mission of the company.

In this situation, security management of maritime critical infrastructure is utilitarian in nature and is realized in an informational dimension, as a process of making effective decisions that guarantee the fulfilment of the mission of a given system under the existing conditions and constraints (Jajuga, 2018).

On the other hand, in a substantive sense, risk management in the implementation of such governance is essentially based on the appropriate management of information and its attributes of completeness, completeness, reliability, certainty, accuracy and timeliness. Therefore, in view of the subject and object relationships, IT security, which is related to the estimation and control of risks arising from the use of computers, computer networks and data transfer, assumes fundamental importance. These processes and issues should be assigned a subjective character, the components of which are: information and communication equipment, systems and networks, paper documents or content contained on another medium. Accordingly, the risk analysis should include the identification of the entities' information resources. In addition, such an analysis should also take into account the standards of security system design in information systems, which are based on general principles that include: implicit denial of access to information, control of the security system including acceptability of the security system, control of the authorization to access information, implementation of the principle of least privilege, and separation of privileges and minimization of shared protection mechanisms.

At this point, it is also worth mentioning risk intelligence in the management of maritime critical infrastructure. According to the learning experience, the basic issue in risk intelligence is to determine the difference between our degree of understanding of a given risk and that of others, which is mainly due to our awareness and our predisposition. Understanding risk requires two conditions. Firstly, in order to fully understand risk, it is necessary to identify

possible solutions to the problems created by the risks, as well as the factors that determine them. Secondly, understanding risk requires experience that allows us to recognize which of the solutions presented can be effective, which are flawed, and whether we need more options. When talking about risk intelligence, it is important to bear in mind this experience in the safety management process that we have already gained or will gain in the future. This means that the concept of risk refers precisely to the second determinant of understanding risk intelligence. Thus, risk intelligence refers to the ability to choose the right type of risk by applying the rules of risk intelligence, which we will be able to manage effectively thanks to our experience (Apgar, 2016).

In summary, given the variety of causes of the most frequently investigated hazards, we usually have no way of determining their unambiguous origin - in practice, this implies that they cannot be accurately forecast. Therefore, their assignment to system elements should introduce the concept of an elementary incident indicator. Thus, the elementary incident indicator, as a security threat and a measure of danger in a system element, can become a function in which the incident scaling index is assigned to a given number of attempts. This will help us determine the abundance of the set of identified threats as specific features in the scaling elements of the information security system. In this situation, this indicator will indicate and describe the image of the weakest for security, element of the system. On this basis, it will become possible to select security measures that will reduce the identified risks to an acceptable level. In this situation, it is essential to have the necessary knowledge, understood as the ability to understand the relationship between cognition, knowledge and reality, on the basis of which it will become possible to reasonably believe in it.

## Conclusions

Critical infrastructure management is a complex process that requires coordinated action at various levels - from local to international. In the face of increasing threats, both natural and man-made, it is necessary to constantly improve management methods and introduce innovative technological solutions. Effective management of critical infrastructure ensures not only the security of citizens, but also the stability of the economy and the state. Meanwhile, the identification of risks in the process, along with the attempt to manage them, has become an integral part of the strategy of any such organization. The goal here is not just to protect against threats, but also to take advantage of opportunities that may arise as a result of the changing environment. Effective risk management requires the use of appropriate tools and techniques, as well as the ability to adapt quickly to changing conditions. However, the growing complexity of risk and uncertainty remains a challenge for organizations, requiring continuous improvement of risk management processes.

From 2022 to 2025 the field has shifted toward an appreciation of interdependence, hybrid threats and climate-driven vulnerabilities. Future theoretical work should prioritize:

- integrated frameworks that marry network science with governance analysis,
- operational resilience metrics and recovery planning tools,
- more granular studies of cyber–physical coupling in port and subsea systems,
- comparative policy analysis of coordination mechanisms.

Filling these gaps will support risk management approaches capable of both anticipating cascading failures and enabling rapid system recovery - objectives that are essential for sustaining maritime security and global trade.

In summary, the author's study and analysis based on the author's experience makes it necessary to analyze risks on an ongoing basis in order to quickly grasp the problem where the resulting risk turns into a crisis. The crisis in the transfer to the application of management decisions is the growing process of uncertainty in the process of changes and risks that occur under these conditions, which leads to the occurrence of a critical situation. The problematic issue signaled is important because a crisis, understood as a sudden or growing event, causes a threat to the basic values of the functional potential of maritime critical infrastructure. In fact, it can be a specific type of breakthrough period, in which a solstice occurs (usually manifests itself as a strong deterioration in the ability of a maritime critical infrastructure entity to perform its functions), which causes the collapse of the existing line of development, which in turn forces the search for alternative and, most often, innovative solutions.

## References

1. Apgar, D. (2016). *Risk intelligence*. Gliwice: Helion Press.
2. Arvidsson, B., Guldåker, N., Johansson, J. (2019). A methodological approach for mapping and analysing cascading effects of flooding events. *International Journal of River Basin Management*, *Vol. 21(4),* 659-671, https://doi.org/10.1080/15715124.2022.2079655
3. Beck, U. (2004). *Risk Society.* Warszawa: Scholar.
4. Bueger, C, Liebetrau, T. (2023). Critical maritime infrastructure protection: What's the trouble? *Marine Policy, Vol. 155*, https://doi.org/10.1016/j.marpol.2023.105772
5. Cybersecurity and Infrastructure Security Agency (CISA). *Critical Infrastructure Security and Resilience*, https://www.cisa.gov/critical-infrastructure-security, 31.01.2025.
6. Dąbrowski, R. (2021). *Technologies in critical infrastructure management.* Kraków: Technical Publishing.
7. Falencikowski, T. (2008). *Shaping discretion in the management of capital groups.* Toruń: Dom Organizatora.
8. Ficoń, K. (2007). *Crisis management engineering. A systems approach.* Warszawa: PWN.

9. ISO 31000:2018. *Risk management – Guidelines. International Organization for Standardization,* https://www.iso.org/obp/ui/en/#iso:std:65694:en, 1.01.2025.
10. Jajuga, K. (2018). *Risk management.* Warszawa: PWN.
11. Kahneman, D (2022). *The traps of thinking. On thinking fast and thinking slow.* Poznań: Media Rodzina.
12. Krzysztofowicz, R. (2012). *Risk management.* Warszawa: PWN.
13. Liupeng, L., Guangsheng, W., Xuejun, F., Tong, Y., Zhiyi, L. (2024). Study on cascading failure vulnerability of the 21st-century Maritime Silk Road container shipping network. *Journal of Transport Geography, Vol. 177*, https://doi.org/10.1016/j.jtrangeo.2024.103891
14. Nowak, A. (2020). *Critical infrastructure management in Poland.* Warszawa: PWN.
15. Prabaswari, Yusuf, A., Gultom, R.A.G., Simbolon, L., Gunawan, A.A.N. (2024). A Novel Socio-Technical Framework for Enhancing Cyber Crisis Management Capabilities, *International Journal of Safety and Security Engineering, 14/4,* 1181-1193. https://doi.org/10.18280/ijsse.140415
16. Qu, S., She, Y., Zhou, Q., Verschuur, J., Zhao, L.-T., Liu, H., Xu, M., Wei, Y.-M. (2024). Modeling the dynamic impacts of maritime network blockage on global supply chains. *The Innovations, Vol. 5(4),* https://doi.org/10.1016/j.xinn.2024.100653
17. Tarczyński, J. (2011). *Risk management in organizations*. Kraków: Krakow University of Economics.
18. Walasek, R., Wojnarowski, M. (2011). Logistyka 2025: badanie eksperckie metodą delficką. *Folia Oeconomica, Vol. 251,* pp. 193-210.
19. Wiśniewski, W. (2022). Challenges in protecting critical infrastructure in the age of cyber threats. *Engineering Review, 45*, 89-102. https://doi.org/10.33141/po.2022.11.05
20. Wódkiewicz, R. (2019). Critical infrastructure facility- required documentation. Analysis on the example of the Refinery in Gdansk. *New Energy, 1/66*, 35-39.