sciendo

Management
2022
Vol. 26, No. 1

DOI: **10.2478/manment-2019-0092**

MICHAŁ IGIELSKI

A model for managing the security of maritime critical infrastructure under the conditions of the fourth industrial revolution

„In science, nothing is so bad that it is completely rejected, and nothing is so good to completely accept it".
Kozielecki

„The structure of our minds limits both the range of questions we ask nature, and the understanding of the answers it gives us".
Kant

1. Intoduction

Currently, the world is in a phase of transition from the third industrial revolution to the fourth, referred to as Industry 4.0. The pillars of Industry 4.0 are concepts such as the global megatrend (includes the integration of advanced computing and automation systems), the Internet of Things, and artificial intelligence - all of which allow for global access to data. This integration enables widespread use of „machine intelligence" - this is primarily aimed at the autonomization of analytical, production and service processes. Thus, the potential of dynamic civilizational changes makes it necessary to forecast new challenges and threats to the management of maritime infrastructure, which requires

Michał Igielski Ph.D.,
Faculty of Management
and Quality Science Gdynia,
Maritime University,
Poland,
ORCID: 0000-0003-4680-3733.

a more detailed study for the sake of state security. Therefore, in-depth analysis, due to the potential of threats and the progress of informatization, we must subject the existing development of a dynamic model of security system solution, which takes into account the harmonization of the National Program for Critical Infrastructure Protection with the planned solutions.

The so-called technological forecasting applied in the study means exemplification in its content, technologies mainly future-oriented through rational and scientific prediction on the basis of logical conclusions - from premises to conclusions. Therefore, another assumed direction of the author's analysis for such forecasting is the suggestion to conduct research in the field of Technology Demand Forecasting - it is needed to predict and study the development of management of maritime critical infrastructure. In addition, the article contains the results of a preliminary exploration of a new problem field in the area of maritime critical infrastructure security, covering a broad spectrum of complex threats and system risks facing a maritime economy undergoing a rapid transformation towards cyber-physical systems.

Therefore, the aim of this article is to propose a preliminary and theoretical model of security management of maritime critical infrastructure along with the specification of selected issues. The author does not want to focus on those issues about which we have already had some knowledge, but on those which, in the necessity of a new look, cause problems and, because of the management of the safety of the maritime infrastructure, should find a solution preceded by their scientific examination.

The set of objectives adopted by the author determined the further course and nature of the study. The author used, as a research method, the analysis of the literature on the subject - for systematizing the language of concepts, and comparison for indicating the characteristics and ways of understanding the defined concepts.

Therefore, the analysis of the literature on the subject is important for the author's standpoint presented here, because the analysis of the standpoints presented in the past by their authors constitutes a potential ability to forecast the development of civilization and in many cases confirms the correctness of their earlier assumptions.

Moreover, the information available in publications on safety management of maritime infrastructure, refers mainly to technical and formal aspects. Meanwhile, empirical studies clearly indicate the reality of threats resulting directly from information security. These are threats present in the everyday reality of organizations responsible for critical maritime infrastructure.

Therefore, in the author's opinion, the management of this area is a potential to maintain and improve security - in accordance with legal requirements.

2. A review of the driving forces and barriers to development for maritime infrastructure management

Critical infrastructure in Polish legislation means systems and functionally related facilities, including construction facilities, equipment, installations, services that are important for the security of the state and its citizens. Within these critical infrastructure systems, it is possible to distinguish systems, facilities and services that can be classified as maritime critical infrastructure (Bursztyński, 2020):

1. Power plants that use ocean and marine energy to generate electricity.
2. Wind farms located in offshore areas.
3. Over-water power cables.
4. Offshore production facilities - drilling, production and storage platforms.
5. Transhipment terminals for fuels and energy resources.
6. Maritime communication, navigation and technical observation systems.
7. Data communications networks.
8. Desalination and seawater treatment plants.
9. Port transshipment terminals.
10. Shipping routes.
11. Maritime offices.
12. Port warehouses and transmission pipelines.
13. Production facilities located in or adjacent to ports.

Contemporary issues related to the management of maritime infrastructure concern the designed integration and harmonization of information systems in an information-saturated environment with a dominant share of artificial intelligence. From the point of view of security of such infrastructure, undoubtedly important are IT solutions concerning integration of distributed IT systems and their security and use of artificial intelligence for wider support of human decision-making processes.

Further challenges for the management of maritime critical infrastructure are investments in the digitalization of the national and European maritime economy, which contribute to:

1. Smart growth in the areas of data infrastructure quality, connectivity and security.

2. Development of new trends: artificial intelligence (AI) and distributed ledger technologies (e.g. blockchain).
3. The development of robotics and the use of big data.
4. The use of advanced digital skills their implementation and the optimal use of digital capabilities and their interoperability.

In general, the maritime information infrastructure, understood as a constituent modular, blockchain technology and information system that supports integrated port processes, is based on three technologies: information acquisition, information processing, and data and information use in identified silos, sets, and subsets of information. Thus created Information Infrastructure architecture, assumes integration and harmonization of information systems and their security in a distributed environment and with information saturated systems (Hoffmann, 2017).

We can also see that the contemporary experience of social sciences boils down to the fact that many people see chaos, confusion and uncertainty in the world, including deep social inequalities, armed conflicts or mass migrations - this is relevant for the security management of critical infrastructure. Nonetheless, we can observe today the striving towards integration progress of digital technical innovations. These innovations deliver new products and services, changing processes, shaking up markets and ultimately altering the maritime environment. Under these conditions, however, there is a disruption of the cyclical crisis that is growing, a trend that is supported by a developmentally inadequate lack of regulation and alternating between nationalization and economic liberalization, deepening social divisions and access to capital (von Weizseker & Wijkman, 2018). The main challenges for modern society related to the progress of civilization are presented by the author in figure 1.

Today, capital and its financial systems are geared towards maximizing short-term profit, which are a source of conflict between private and public interests leading to an insufficient supply of money. Especially the supply is important in areas serving important social investment needs, which certainly includes the management of maritime infrastructure. (Potejko, 2019). In this situation, certainly the security management of this infrastructure will be related to, among others:

1. The generic and qualitative planning of development investments, including but not limited to maritime infrastructure (e.g., seaports).
2. The necessity to analyse global investments, e.g. in the sector of strategic resources extraction and the planned commercial expansion of this sector with the involvement of sea transport.

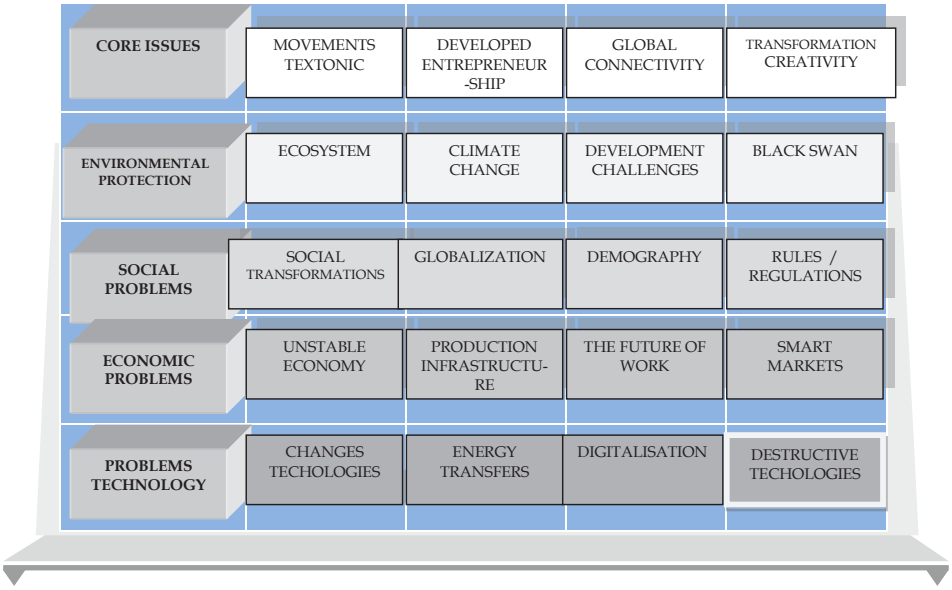

Figure 1. Matrix of challenge areas and threats, barriers and driving forces of civilizational development

Source: own study based on Raich and all, 2018

Therefore, the assumed economic criteria of profitability of innovative solutions and the so-called time objectives (waiting for the ship, occupancy of the berth and turning back) will be of significant importance for the safety management (e.g. in port infrastructure). Their importance also arises from the need to design new, IT-based procedures in the area of target times and infrastructure changes that improve the efficiency of e.g. the port. With the direct operation of port infrastructure is related to the estimation of risks associated with the energy security of the country, which includes, among others, security of supply, including the aforementioned concentration of supply of energy resources.

The issue of security management, which occurs for this problem, is related to the continuity of the logistical supply chain, which includes their concentration, social, political and economic stability of the region. In addition, according to the author of the study, it also includes the possibility of influencing this balance on the security of ports of supplier and recipient of such raw materials

(Babenko and all, 2017). Therefore, research and, on its basis, the development of platforms for security management of critical infrastructure will be of significant importance. In this particular case, for example, it may be about port infrastructure, where next-generation machine learning will be used, by defining new rules and indicators that maximize the port's potential against such threats.

Currently, such a manifestation of the changing environment is, although not yet sufficiently effective, but a great intentionality in seeking benefits from the cooperation of entrepreneurs and academic research communities or support for innovative activities by non-governmental social organizations involved in the development of the maritime sector. This manifests itself in undertaking innovative research and development initiatives on the basis of economic activity of entities and preparation of the environment and maritime infrastructure for a new stage of shipping development based, for example, on unmanned floating objects with a high degree of autonomy.

In today's global economy we also observe a significant reevaluation of the principles of business management, which is related to the computerization of information processed in them and its security. There are risks associated with the lack of information security, which in a broad sense is a certain state, negatively valued and achieved as a result of the action, which causes the loss of the assumed level of their: confidentiality, integrity, availability, accountability, authenticity and reliability. In the case of e.g. business entities understood as enterprises operating in the maritime infrastructure, and especially constituting critical infrastructure, their essential feature is that:

1. All types of threats, and including those arising from the management of their production or services, create risks of loss of operability threatening the security of their strategic customers, as well as serious material losses.
2. The need to clarify the concept of critical infrastructure or the company itself having such infrastructure, which is further complicated by the problem of the company in a situation of international ownership structure, which includes here, due to civilization 4.0, its own information systems, is still a current problem.

The rationale for the relevance of this issue stems from the aforementioned specificities of information security system management in such enterprises, including, for example:

- national distinctiveness, through the legal and functional peculiarities of such infrastructure, which result from such enterprise's maintenance of necessary social functions;

- specifics of information protection in such an enterprise, which result from their obligatory protection;
- peculiarities of construction and functioning of elements of the information security management system considered in relation to the functional criterion of distinction;
- peculiarities of management within the framework of crisis management engineering - that is, management of security organization through implementation of useful applications.

In the literature itself, there is general agreement on the basic meaning of the concept and functions of critical infrastructure management. Thus, for example, B. Kosowki (2014) believes that it is the management of basic facilities and institutions necessary for the proper functioning of the State. In turn, J. Sadowski (2018) believes that in Poland the term critical infrastructure is used primarily to refer to resources that are essential for the functioning of the State and its citizens. However, attempts at its continental unified definition are proving quite difficult. This is understandable, given the affiliation function indicated in normative acts - there is still a need for broad beyond definition cooperation in the field of critical infrastructure security management both at the national and international levels. The above relates to the fact that in the current solutions, although we are dealing with a logical operator in the form of a defined membership function, but there is an overly broad lack of a defined set boundary due to the functions it performs. Therefore, in this view, the prospect of widespread computerization and related security of intelligent maritime critical infrastructure will be a predominantly object-oriented environment capable of communicating, visualizing, receiving commands or transmitting information with little or no human intervention.

To sum up, in order to manage the security of maritime infrastructure, its security needs to be particularly emphasized in view of the development challenges of maritime-related enterprises. Therefore, it will be necessary to support the economic decision-making process in the real and virtual world with the help of artificial intelligence at the global and regional level. An example of this state of the art is blockchaim technology. According to the World Economic Forum (WEF) in 2018, this technology as a development challenge, has become one of the most important for use in the so-called „banks of the future" where most transactions will take place in the virtual world. This technology is also an answer to the global needs of companies that generate a lot of documents and transactions. It allows for accurate and very fast verification of both business partners and the documentation related to economic cooperation.

3. Managing the information infrastructure of the fourth developmental level

Nowadays it becomes a problem to profile information sources that provide users with access to a coherent and common set of data and their flow enabling integration of specific processes of business management and technical catalog of services. Efficient circulation of up-to-date information makes it possible to organize the functioning of an organization and provides a basis for increasing the quality of taken decisions, and thus increasing the efficiency as a result of actions derived from the implementation of integrated IT software supporting this management. The purpose of such activities is to support and optimize value-generating processes, including: teams designing, producing, selling, providing services or serving and talking to customers (Senge, 2008).

Today, the IT environment is crucial in most businesses. This is perhaps especially true for small companies, which often do not have as large a budget as large corporations. For them, backup facilities and data centers with failover systems are simply not an option. IT infrastructures are becoming too complex and prone to failure to keep up with the pace and dynamics of modern companies. 70% of current investments in IT infrastructure are for related to maintenance, resulting in few resources being allocated to innovation. Users expect shorter response times and executives expect lower costs, so a better strategy for using IT resources is essential. Cloud computing environments represent a new model that reduces IT system complexity by efficiently pooling on-demand, self-managed virtual infrastructure into pools of resources available as a service (Szyjko, 2012).

The learning experience shows that artificial intelligence, learns from information and interacts with the outside world. Machine intelligence, on the other hand, using data from various silos, data containers including current operational and so-called „Proxy" data, can recognize causal patterns so that it can preemptively shut down a threatening element. Using an actuation sensor in a safety system in combination with a lock sensor, for example, is nothing more than the functional experience of events by machines and devices. Thus, machine learning becomes a collective consciousness in which each element learns and acts in a synchronized, collective manner ordering the effectiveness of the system according to set parameters. Moreover, the system too can study the behavior of the user of such a system, also analyzing its prediction in the decision-making process, thus optimizing harmony and safety in an anomaly-free environment. In addition, machine learning models make it possible to assign a risk index to each employee - this determines their job competencies

and verifies assumptions related to future competencies. As S. Zubboff (2020) states, in this scenario the whole is not greater than the sum of the parts, for there are no parts and there is a whole.

This is where the term machine knowledge comes in, which according to researchers of the topic, will be the new gateway to a safe reality - it eliminates and organizes ignorance, nullifies risks and the emergence of faults. Instead, using a library of algorithms and deep machine learning (deep learning), intelligence here could mean, for example, that sensors in marine technological processes can also be „actuators" whose purpose will be to intervene, act and control (Babenko and all, 2017).

The technological foresight already mentioned makes the use of artificial intelligence and machine learning (especially deep learning), additionally, will enable (Barrat, 2013):

1. To make decisions in the absence of all data.
2. To apply robotics and advanced automation effectively to the process.
3. Will enrich the expert and diagnostic systems using the knowledge base with data and information (will activate the mechanisms of reasoning to solve problems, point to areas related to the needs of information and knowledge acquisition, increase the possibility of waiting for specific results, enable the use of intelligent interfaces and enable real-time analysis, in monitoring systems, technological process management systems and forecasting the safety of such a process).

In the opinion of the author of the study, currently in Poland, due to the costs, at the stage of preliminary studies, modernized and adapted to a specific situation IT applications can be based on existing backbone systems, but only those which meet the basic requirements for the scale of progress, - this allows to assess the scope of necessary modernization changes. Moreover, such action streamlines the implementation process and profiles the needs for custom-built detailed IT modules. Bearing in mind the professional experience and beliefs adopted on this basis profiling the cognitive system, we can state that the data collected in the IT system already today often becomes the basis for the introduction of comprehensive optimization of management processes. Moreover, with appropriate authorizations, access to information allows analyzing threats more easily and in many dimensions - this becomes a basis for conscious shaping of safety of maritime infrastructure, for example: on the basis of matrix analysis. Besides, in terms of basic research it becomes useful to build a rectangular cage matrix, in which such a picture of columns and rows best forms a coherent, transformable system. The matrix also allows profiling of

data and information transfer channels for the so-called algorithmic machine language (software).

In response to information security threats, organizations have made efforts to implement and improve their information security measures. In doing so, these organizations are developing: organizational security management systems and strategies, information security policies, and a huge variety of recommendations/ standards/technologies that are related to security management. The multiple and asymmetric nature of these solutions has contributed to organizations looking for other models of security policy development. However, given that threats can arise from differently configured situations, we can assume that a threat to maritime critical infrastructure (including information) is a situation in which there is, whether realized or not, restriction or abuse of lawful access and free use of current, reliable, integral and properly protected property (Stanik & Kiedrowicz, 2016).

In summary, the identification of contemporary selected threats and challenges to the security of civilizational development in the 21st century, taking into account the management of maritime information infrastructure of the fourth developmental level, cannot ignore, in the area of strategic raw materials, the exploited areas of information warfare, which is the basis of multigenic conflicts.

4. Proposed Maritime Critical Infrastructure Security Management Model

Systemic threats and risks have been increasingly included in security research and infrastructure risk analysis for more than a dozen years, but the real impetus for the reactivation of systems theory and in-depth research on systemic risks was the financial crisis in the US. However, the concept of system hazards and system risks is further imprecise due to the vagueness, ambiguity of its components. There is no universally valid definition of systemic threats and systemic risks - they are understood in an intuitive way, and further research is needed to theoretically ground these concepts and develop methods and tools for analyzing this new type of threats and risks (Michalski, 2020).

A prerequisite for creating a model of maritime critical infrastructure security management is effective and active identification of threats, assessment of their risk and undertaking actions aimed at their elimination or reduction. In figure 2 below, the author of the article has attempted to identify the main threats to critical infrastructure security.

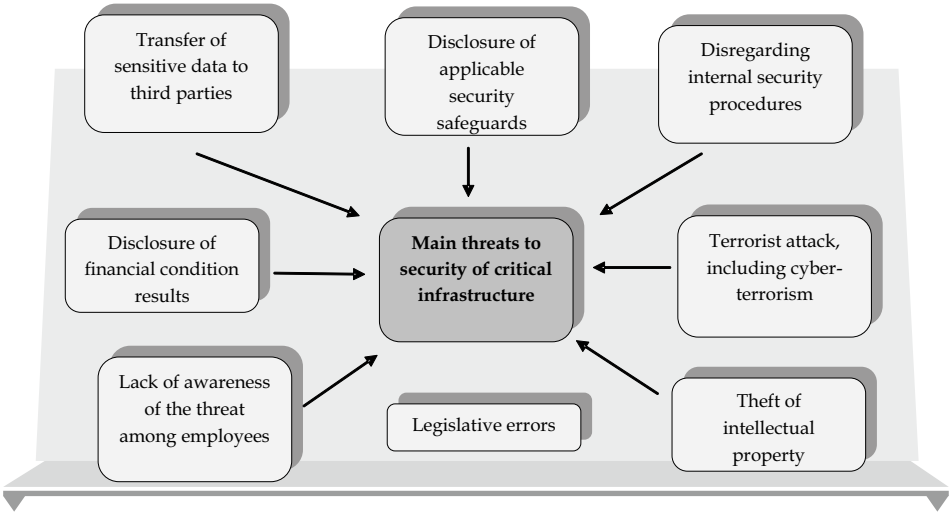

Figure 2. Threats to the security of modern critical infrastructure

Source: own study

Therefore, in the proposed management model, we can distinguish the typical components of this process: hazard identification, action planning (goal setting), implementation and control. Threat identification means having and continuously improving knowledge about potential threats and the necessity of implementing the adopted security strategy. Developing an action plan, which is its implementation, is the responsibility of those responsible for overseeing the proper functioning of the organization. Action planning may be carried out with the participation of experts in the field of security and should be oriented towards achieving the main objectives, for the implementation of which it is necessary to define specific objectives. The overriding goal, in the case of a safety system, is always to ensure and maintain the organisation's ability to evacuate safely. In turn, the implementation of planned activities should include the following elements (Pecio, 2018):

1. Determining the necessary resources needed to achieve the stated objectives.
2. Designing the organizational structure of the undertaking.
3. Allocation of tasks with identification of responsible persons.
4. Provision of authority and organization of training.
5. Determining the principles of communication and documentation of activities.

Whereas the last element, i.e. control, is in the author's opinion the key element in the safety management model. Based on the analysis of the available literature, in this particular case, the author concluded that there should be at least two levels of control. Thus, we start with the current monitoring of work and ad hoc response in situations requiring it and in emergency situations. This allows us to move on to so-called periodic actions, i.e. planned controls that end with conclusions to be implemented. This approach allows for continuous improvement of the model adopted for implementation (figure 3).

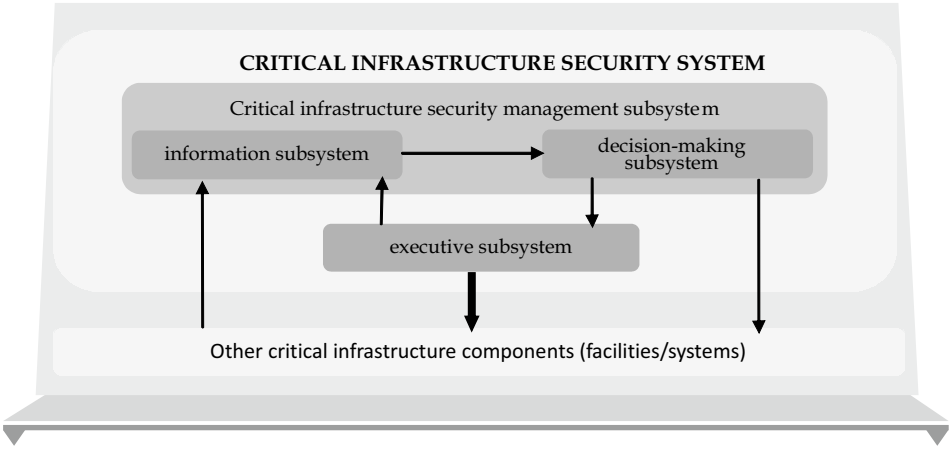

Figure 3. Critical infrastructure security system model

Source: own study based on Stanik & Kiedrowicz, 2016

Going further, under the conditions of civilization development 4.0., organizations understood as maritime infrastructure, have to integrate available data to a much greater extent, analyze it and process it into useful knowledge. In general, we should state that the sets of information for decision making, taking into account their entropy, should be as abundant and extensive as possible. The larger the information base is, the more the decisions generated from it are relevant to the current situation and represent higher utility and usefulness in the management process. The most effective

in the process of marine infrastructure safety management turns out to be the set obtained from the links between management levels, derived from planning information, operational information and control information. Therefore, in the developmental evolutionary process of such infrastructure, the use of expert support model in the management structure based on data collection and its analytical processing and effective use becomes important. In addition, in the structure of such a model, due to the knowledge bases, its functions will change. This is necessary because in global access to information, processes of information exchange, sources of collected data or control of appropriateness and readiness of resources for reporting, are very necessary for decision support.

Therefore, the architecture of such a model, shown in figure 4, in each element, must take into account, among other things: editing of databases and knowledge and the so-called in banking - rules engine, i.e. security shaped alerts and notifications and „nodes", which are needed for external databases regulated by information protection. Depending on threats and needs, the subsystem support modules can be expected with high probability. Examples of this are scenario alternatives to identified threats, or business continuity and contingency plans carried out with the help of artificial intelligence.

Under these conditions, we must also take into account the problem of redundancy of information in the model (redundancy), which, based on quantitative and qualitative criteria, by definition exceeds the minimum required to solve the problem. At the same time, due to the particular for the safety of maritime critical infrastructure its use in software, is justified in terms of:

1. Identified and precisely defined data, information in their sets and information silos, the occurrence and reliability of transmission of which plays a key role during the technological process.
2. dentification of redundant communication routes, which can be used interchangeably (a kind of hot reserve) - it affects the costs of the system, but profiles the so-called backup route to the information.
3. Restoring data after its partial loss or damage or to detect e.g. damage (CRS checksum).
4. Data compression, i.e. the possibility of verifying the information to detect possible errors originating from its use (checksums).

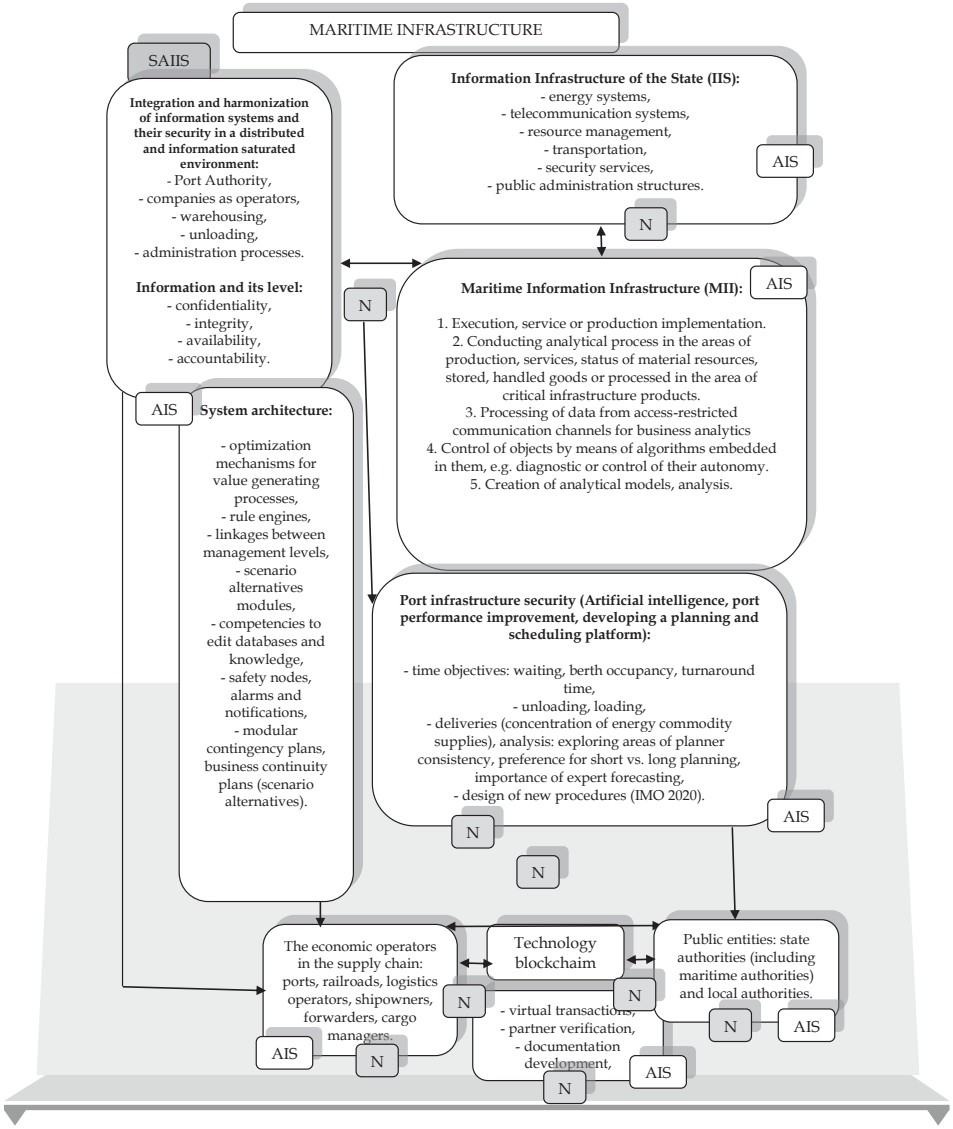

Figure 4. Maritime critical infrastructure security management model

Source: own study

Explanation of the symbols used in the model:
SAIIS - system area of integrated information software (operational level)
AIS - autonomous information silo (profiled information sources and their collections).
N - nodes (internal and external data rationing, information and database protection).

An important aspect that we must analyze in designing and implementing a critical infrastructure security management model is the Security Management Systems (SMS). A Security Management System (SMS) is a global system that integrates all security systems in an organization. It is one of the basic elements of managing automatic control systems and integrates other safety systems, including the fire alarm system, which is the main fire safety system - after all, there is an obligation to use such systems in maritime critical infrastructure (Stanik &Kiedrowicz, 2017).

In summary, the proper design and implementation of a professional safety system and its management requires, first of all, an understanding of the organization (in this case, the essence of critical infrastructure), its context, and a case-by-case analysis of the risks arising from the nature of the activity, the topography of the site, and the size and shape of the infrastructure.

5. Conclusion

As already mentioned by the author, the subject matter of the issues analyzed in the study is a fragmentary proposal for a new multidisciplinary and combined look at the possible choice of the research area - and on the basis of typology of selected issues and phenomena that should be further investigated. necessary. This process is forced on us primarily by the progress of civilization.

As it follows from the doctrine, the civilizational transformations have always been accompanied by processes verifying the scientific correctness of the old paradigms and their relevance to the change, under the conditions of the assumed structural balance of the elements of social cybernetics. Despite the growing awareness of the transformations, the complexity of the contemporary world and the lack of its ultimate prediction, causes that the contemporary environment of knowledge environments, in the dynamic innovative and fuzzy space of research, may be accompanied by a harmful subjective anti-intellectualism. Its power is intensified by the perceived impermanence of social integration mechanisms and axiological

disorientation in the modern anthropogen, i.e. the era of human domination, which determines new threats.

Making a summary, taking into account its praxeological relevance to the subject matter undertaken in the author's study, it should be pointed out that:

1. Managing the security of maritime critical infrastructure under the conditions of the fourth industrial revolution, enforces the necessity of new competences of those dealing with its security;
2. Effective crisis and conflict management in this infrastructure in the future will be, mainly in these conditions, related to the qualitative and quantitative dimension of information with the participation of artificial intelligence;
3. The fundamental importance of information, as a tool for recognizing and combating valued states, is now and will be due to the potential of its importance.

In conclusion, the primary intention of the author of this paper was to open a discussion on the security management model of the maritime infrastructure and the related study of critical infrastructure under the conditions of the fourth industrial revolution. As is evident from numerous scientific studies, the awareness of the negative consequences of progress, is essential to take correct actions to minimize their impact. Therefore, an important issue and, at the same time, a threat becomes the problem of current and future cognitive representation in which we must take into account the fact that, in general, when studying security culture we study it using cognitive categories brought from our own culture - this means that, in fact, we study our own relation to the studied new culture and its new components. For it seems that this knowledge will remain a permanent part of management, as physical assets, organizational structures, strategies, processes, systems, financial, human or information resources have become. In science, in turn, it can be hoped that the need to develop conceptual frameworks and methods for studying this area will not disappear. One can also hope that the research presented in this paper is being conducted in the right direction.

In this connection, it will become important that while civilization 4.0 means a new kind of power over the world (today knowledge is power), will ignorance still not mean lack of power? In other words, what will be crucial for the development of civilization is to what extent the lack of scientific reflection or cognitive optimism, suppressed by conservative anxiety about new things, will benefit from the terror not of the things themselves, but of the subjective belief and imagination about those things (Pais, 2006).

Summary

A model for managing the security of maritime critical infrastructure under the conditions of the fourth industrial revolution

The primary objective of the author of this paper is to propose a preliminary and theoretical model of security management of maritime critical infrastructure under the conditions of the fourth industrial revolution. The proposed model in the definition is to be comprehensive in terms of shaping information security management. The article is also an attempt to capture the main threats in the sphere of information security management during the management of critical infrastructure. In addition, the author's intention is to provoke/open a discussion on this topic, because as is evident from numerous scientific studies, the awareness of the negative consequences of progress is essential to take correct actions to minimize their impact.

Keywords: *fourth industrial revolution, critical infrastructure, security management.*

Streszczenie

Model zarządzania bezpieczeństwem morskiej infrastruktury krytycznej w warunkach czwartej rewolucji przemysłowej

Podstawowym celem autora opracowania jest zaproponowanie wstępnego i teoretycznego modelu zarządzania bezpieczeństwem morskiej infrastruktury krytycznej w warunkach czwartej rewolucji przemysłowej. Zaproponowany model w definicji ma mieć charakter kompleksowy jeśli chodzi o kształtowanie zarządzania bezpieczeństwem informacyjnym. Artykuł stanowi również próbę ujęcia głównych zagrożeń w sferze zarządzania bezpieczeństwem informacyjnym podczas zarządzania infrastrukturą krytyczną. Dodatkowo zamiarem autora jest wywołanie/otwarcie dyskusji na ten temat, ponieważ jak wynika z licznych opracowań naukowych, świadomość negatywnych konsekwencji postępu jest niezbędna dla podejmowania prawidłowych działań w celu zminimalizowania ich wpływu.

Słowa kluczowe: *czwarta rewolucja przemysłowa, infrastruktura krytyczna, zarządzanie bezpieczeństwem.*

JEL: F52, L10, M15, O32

References

Babenko, D., Marmanis, H., Walczak, T. (2017). *Inteligentna sieć. Algorytmy przyszłości*. Gliwice: Helion Press.

Barrat, J. (2013) *Our Final Invention: Artificial Intelligence and the End of the Human Era*. New York: Thomas Dunne Books.

Bursztyński, A. (2020). Safety of Maritime Critical Infrastructure Facilities in the Aspect of Contemporary Threats. *Rocznik Bezpieczeństwa Międzynarodowego*, Vol. 14, No 1, pp. 167-182.

Hoffmann, R. (2017). A multi-faceted methodology for business process risk analysis and management. *Ekonomiczne Problemy Usług*, Vol. 1, No 126, pp. 339–354.

Kaplan, A., Haenlein, M. (2019) Siri, Siri in my Hand, who's the Fairest in the Land? On the Interpretations, Illustrations and Implications. *Intelligence Business Horizons*, Vol. 62, No 1, pp. 15-25.

Kosowki, B. (2014). *Elements of critical infrastructure protection in crisis management.* Katowice: WSZOP Press.

Michalski, K. (2020). Protecting electricity infrastructures from system threats and risks - a new paradigm in energy security management. *Rocznik Bezpieczeństwa Międzynarodowego*, Vol. 14, No 1, pp. 200-220.

Pais, A. (2006). *Czas Nielsa Bohra. W Fizyce, filozofii i polityce.* Warszawa: Prószyński i S-ka Press.

Pecio, M. (2018). Safety management model. *Zeszyty naukowe SGSP*, No 65, pp. 77-96.

Potejko, P. (2019). Information Security Management. In: Wojtaszczyk, K.A., Materska- Sosnowska, A. (eds..), *Bezpieczeństwo państwa* (pp. 209-220). Warszawa: ASPRA JR Press.

Raich, M., Eisler, R. (2014). *Cyberness; The Future Reinvented Paperback*. Karolina Południowa: Createspace Independent Publishing Platform.

Sadowski, J. (2018). Critical infrastructure protection. Genesis of the problem. *Organizacja i Zarządzanie*, No 6, pp. 1237-1241.

Senge, P. (2008). *Piąta dyscyplina*. Gdańsk: Wolters Kluwer Press.

Stanik, J., Kiedrowicz, M. (2017). Business process risk model. *Ekonomiczne Problemy Usług,* Vol.1, No 126, pp. 325–338.

Szyjko, T.C. (2012). Innovative management in a virtual environment. *Zarządzanie innowacyjne w gospodarce i biznesie*, Vol. 14, No 1, pp. 119-129.

von Weizseker, E., Wijkman, A. (2018). *Kapitalizm, krótkowzroczność, populacja i zniszczenie planety*. Warszawa: Politechnika Warszawska Press.

Zuboff, S. (2020). *Wiek kapitalizmu inwigilacji, walka o przyszłość na nowej granicy władzy*. Poznań: ZYSK i S-ka Press.