SILESIAN UNIVERSITY OF TECHNOLOGY PUBLISHING HOUSE

SCIENTIFIC PAPERS OF SILESIAN UNIVERSITY OF TECHNOLOGY 2024
ORGANIZATION AND MANAGEMENT SERIES NO. 197

SECURITY MANAGEMENT IN THE FACE OF CIVILIZATIONAL AWARENESS OF THE DIGITAL WORLD – A THEORETICAL APPROACH

Michał IGIELSKI

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

Purpose: The purpose of the study is a fragmentary proposal for a new interdisciplinary combined view of the problem of security management on the basis of selected and specified issues involving, among other things, the integration of scientific knowledge and the combination of methodologies of two or more research strategies with implications of interdisciplinary unification.
Design/methodology/approach: The methodical approach chosen by the author of the study is a thinking guided by preconceived conclusive and explanatory sentences. Research methodology, mainly on the potential of information and its elements shaping security, is a description dedicated to the author's approach to the adopted solution of the research problem. In this way, based on methodological considerations, considerations structure the organisation of the research subject.
Findings: The proposal for the components of the security management model presented in the publication is an example of universal system engineering based on integrated and advanced information systems that support the management of information resources. According to the author, in the face of new economic challenges, it should take into account: the competence of the future, the study of security in the dynamic fuzzy space of research, risk and risk intelligence, and quantification of the cognitive approach to security management.
Practical implications: The practical nature of the study derives from the objective the author intends to achieve by fulfilling the principles of generality, accuracy, informative content, epistemological certainty and logical simplicity.
Social implications: In addition, issues related to the decision-making process vis-à-vis the identification of collective and individual discretion and the role of the subject as an interoperable integrator of the potential of partner competencies in the field of security management become essential.
Originality/value: The developmental nature of the work, is due to the importance of internal and external factors of cognitive activities and awareness conditions of the community organised into the organisation. The internal factors of the research conducted can include the variables empirically obtained in the organisations studied for the causes of events. The external factors that the author considered in his work are: social, economic and cultural determinants of safety, based on information potential.
Keywords: digital transformation, artificial intelligence, decision-making, information infrastructure.
Category of the paper: Research paper.

1. Introduction

In the anthropological approach, civilization and its security, is identified with political wisdom and mutual aid, which allow societies to self-organize to ensure their persistence, improvement and development Such an organized society, here the secure environment of a given organization and its management, should operate in the area of the only constant certainty for it, which is development. Therefore, according to the author, since it is inevitable, it is in our interest to learn how to reach it most effectively (Greber, Wengrow, 2021) - which is the main thesis of this article.

The modern progress of civilization, which is associated with the awareness of the digital world, makes the characteristic of management science the question of resolving the direction of scientific doubt, that is, the source of the decision about what understanding of the problem is appropriate (Kahneman, 2012). The modern division of the world causes conflicts and threats in global politics to fulfill the integrative function of these communities, but should also include areas of advanced research in the area of scientific formation of security management. The rationale for this is that the ongoing globalization of various forms of economic circulation, implies political-economic processes that take on the characteristics of complex systems. It is becoming increasingly difficult for us to globally forecast and scientifically determine the probabilities of possible directions of change, trends and threats. In addition, the imperfection of our knowledge causes difficulties in studying various phenomena due to the qualitative difference between, for example, the sciences and social sciences, which describe the relationship between explanation and understanding.

Therefore, the primary intention of the author of the study is to initiate a discussion on security management under the conditions of civilization progress. As evidenced by numerous studies and scientific papers, awareness of the negative consequences of progress is essential for taking correct measures to minimize its negative impact (Banach, 2022). Therefore, an important issue and, at the same time, a threat is 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 through cognitive categories derived from our own culture. And this means that we study our own relation to the studied new culture and its new components (Koźmiński, Piotrowski, 2011). In this situation, the analysis of the introduction for these trends of the problems of interdependence, relevance and legitimacy of the use of the terms management and security, requires the verification of the existing circulating patterns of interpretation of these phenomena. The presence of a conscious environmental routine, a certain type of social and intellectual mentality, and the presence of doctrinal biases cause limitations to development opportunities. In this situation, the socio-scientific environment of expert knowledge in - the influence of this environment on the formation of the contemporary limits of scientific rationality in it - becomes essential (Shapiro, 2003).

The solution optics presented in this study were directed at increasing the level of security of operations of any organization - in each case could be developed for a specific addressee. Its detailed elements and their derivatives to the structure of the solution model depend, among other things, on the business profile of the organization, the adopted competitive strategy and also the functional-organizational structure (Grobler, 2016).

Therefore, in this situation, for the progress of civilization and its study, the construction of definitions of the essence of the management, forecasting or research decision, which include, at the present stage of consideration, the constitutive features of the doctrine, gains importance. Therefore, the rationale for the selection of these issues is due to:

- The changing functions of political systems, which include new rules of world politics in the face of global security problems, and economic and social issues that affect the potential of the driving forces and barriers to development.
- Contemporary and global civilizational development trends.
- Occurring contemporary complex legal problems as a result of the emergence of innovative objects.

It is also worth noting at the outset that the terms ontology and phenomenology used in the following section of the study mean, for the author, respectively, the criterion of distinction - the cognition of reality and its nature, and the pursuit of grasping the essence of what is given (materiality vision), the use of the relationship of the mind to things.

2. Literature Review

Framing the problem in an ontological and phenomenological way allows combining scientific knowledge of the essence of the problem with the possibility of practical application (Zięba, 2018). Accordingly, a full analysis of a given type of individual and collective security confronted with threats, must take place in the context of its adjectival definition, which determines a variety of criteria depending on the purpose and object of research.

Security in the face of the problems of an organization oriented to social interaction, which includes in society its organization, structure, ties and dependencies, is to ensure its continuance, improvement and development. Despite the growing awareness of technological transformations, security research can still be accompanied by confusion and information noise, which determine the new threat of the so-called “tunnel of secure reality” (von Weizseker, Wijkman, 2018). Therefore, an important role in creating the concept of security is played by the actions of a given environment at a certain time. In addition to this, the level of culture, political forms or geographical location also remains an important element.

The rationale for the adopted position stems from the fact that a contemporary overview of the driving forces and development barriers for security management boils down to the inclusion of issues relating to the integration and harmonization of information systems in an information-saturated environment with the dominant participation of artificial intelligence (Bryjka, Zając, 2023). In addition, the security-required harmonization of information systems makes it necessary to apply artificial intelligence to the current need for broader support of human decision-making processes.

According to the author's observations, the essence of such projects is an interactive information infrastructure as the basis for decision-making based on profiled information sources and content, which enable the management of a catalog of tasks in security management elements. Thus, they will ensure their integration, optimization of value-generating processes and applied processes. The information infrastructure architecture thus created, implies the integration and harmonization of information systems and their security in this environment. Therefore, from this perspective, the prospect of widespread computerization and its associated security, will be a mainly object-oriented environment that can communicate, visualize, receive commands or transmit information with negligible human participation and mediation. From this area, such accumulated data and knowledge, on the basis of data sets and information, it will be possible to use it to conduct the analytical process towards the areas of production or ty services.

Therefore, the research and, based on it, the development of a planning and scheduling platform that will take advantage of the so-called "machine learning" of the new generation becomes important. It is dedicated to security management by defining new rules and indicators that maximize security potential against identified threats. Here, the analysis and methodology for studying the areas of planner consistency, preference for short and long planning, or the praxeological importance of human forecasting becomes essential. Predicted with high probability subsystem support can be, depending on the threats and needs, a module that supports the decision-making process - such as scenario alternatives carried out with the help of artificial intelligence in the face of identified threats or business continuity and contingency plans. Their use in security management is justified, for example, when identifying redundant digital communication routes. This has an impact on the so-called backup route to information and data compression, i.e. the ability to verify information to detect possible errors from their use (checksums). Therefore, according to the author, further research is needed, the results of which will allow, in the security management space, to reduce the occurrence of anomalies or significantly eliminate the occurrence of failures, errors and general randomness (Kaplan, Haenlein, 2019).

The process of digital transformation of society and an economy with algorithms deeply saturated with data are fundamental development challenges in the 21st century. The data-driven economy is changing the previous rules of secure development. Artificial intelligence is a fast-growing group of innovative technologies that requires novel forms of regulatory

oversight and a safe space for experimentation, while ensuring responsible innovation and incorporating appropriate safeguards and risk mitigation measures. Artificial intelligence (AI)-based solutions enable better forecasting, optimisation of operations and resource allocation, and personalisation of digital solutions. According to the author, nothing in the foreseeable future will be more transformative for our economy, our society and our entire lives than this technology. Given Europe's digital, data-driven future and the potential for new technologies, in security management it is the information infrastructure that will underpin all decision-making. This will manifest itself:

- Building an open, cross-sectoral and single data market for common European information spaces - this will enable collaboration using artificial intelligence (AI).
- Data management will take place in the common information space defined for this activity - through data collection standards and their use.
- The abolition of data fragmentation in the data space used for security awareness.
- Identifying the necessary selection of new specialists for the analysis of large data sets (increase of personal digital competences).
- Taking into account the rights of legal and natural entities with respect to their data.
- The emergence of common European data spaces in strategic sectors of the economy, together with the tools and their infrastructure.

Furthermore, in the structure of such a system, due to the knowledge bases, its functions will change. This is necessary due to global access to information, information sharing processes, sources of data collected or control of resources.

The subsystem support envisaged, with a high probability, will be, depending on the threats and needs, support modules - e.g. scenario alternatives to identified threats guided by artificial intelligence.

In this situation, the emergence and occurrence of subjective and objective mental phenomena in humans is of particular relevance to this process - information evaluation is the most general purpose of information processing in human activity. It is here that discrepancies in interpretation can occur, which imply the magnitude of errors as a result of opposing overlapping claims to rationality. Moreover, the dynamics of civilisational progress mean that we cannot also speak of the predictability of risks as they are produced, and the problem of their unpredictability is mainly due to the difference based on lack of skill between estimation and calculability (Beck, 2014). Under these conditions, the criterion of functional, individual and subjective management of security becomes important, in the face of the individual and collective decision-making freedom of the entity managing it. The distinction in terms of adopted couplings and information loops in the procedural, implementation and maintenance stages of its security is also important in this regard. In this situation, an example of the conditions for the safe operation of artificial intelligence algorithms interacting with the human

environment is mainly enforcement in a unified system of legal frameworks. Currently, this boils down to:

- Identifying the system by level of risk (systems: posing an unauthorised risk, high risk, limited risk, not belonging to any other category).
- Introducing rules in the designed artificial intelligence system that should apply regardless of the classification of the system in question and that meet safety standards.

Thus, agility and safety under the conditions of the fourth industrial revolution necessitates the need for new competences for those dealing with this problem. Effective future crisis and security management will mainly be linked to the qualitative dimension of information under these conditions. Consequently, the fundamental importance of information, as a tool for identifying and combating negatively valued conditions, is now and will continue to be driven by the potential of its importance.

Safety management always takes place when the decision-maker(s) is always in one of two states: the desire to make a decision or the compulsion to make a decision. Decision-making under risk conditions results in the uncertainty arising from these actions being assessed by the individual decision-maker in relation to the assumed benefit function (objective assessment - procedures; subjective assessment - individual perception). The theory 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, we will assume that risk is, the estimated probability of a particular type of hazard or loss occurring, as well as the gains and benefits associated with decisions made, relevant to the future. In this situation, the intended objectives of safety management, implemented in the decision-making process, should take into account the strategy for the situation of their destruction within the specified risk tolerance band (Ficoń, 2007).

It is worth noting at this point that systems thinking is very important in the design of such structures. R.D. Arnold and J.P. Wade (2015) write that systems thinking is a set of synergistic analytical skills used to improve the ability to identify and understand systems, predict their behaviour and develop modifications. It is intended to help achieve desired outcomes. A researcher who uses this approach identifies the root causes of a hazard and determines their dynamics in a more robust way. He considers and analyses the complexity and non-linearity of the threat and potential solutions through the lens of the whole system. This is based on the assumption that complex problems are better solved when decision-makers understand the subsystems and their interdependencies. This requires managers to move away from reactive and adopt creative organisational cultures (Brown, Martin, 2015). Design thinking, on the other hand, emphasises the need to develop empathy with users, involving them in the processes of problem definition, solution creation, prototyping and in iterations to improve solutions (Grohs et al., 2018).

Risk acceptance, on the other hand, is risk tolerance on the basis of resource and relational discretion. The rationale for this statement stems from the fact that integral to the analysis of each risk (risk receiver, risk issuer) are the determinants of the decision-making process that create and determine the decision-making situation (e.g. legal determinants). Such relationships can arise from the assessment of the decision-making freedom made at the stage of building the options for solving the decision issue and selecting the option for solving the decision issue.

The analysis of the concept of risk carried out in the publication takes into account the realisation that, today, the unravelling of risk is becoming a scientific problem in its own right, and it is necessary in this situation to reveal the contradictions and difficulties that exist in the interrelationships between practice and disciplines in an interdisciplinary reality. We should take into account that:

- In a technologically and innovatively advanced reality, the creation of occurring risks and hazards shows a dependence on knowledge as its product.
- It dynamics of civilisational progress mean that we cannot also speak of the predictability of risks as they are produced and defy rational conditions of acceptability.
- In the security space, there is the so-called intelligence of risk, which has a fundamental impact on the theoretical content of risk and its relation to the proliferation of its varieties. It also influences the so-called risk content (extent, intensity, causality, damage) (Falencikowski, 2008).

Under these conditions, safety management performance risk dictates that:

- Operational risks, resulting from inadequate and malfunctioning internal processes, occurring e.g. in the environment of the people employed at the facility.
- Economic risks, which may be caused by changes in economic conditions.
- Event risk, which may be caused by the occurrence of specific events or natural disasters.
- Model risk, or the risk of theoretical error in the real world.

In this situation, security management is utilitarian in nature and is realised in the informational dimension, as a process of making effective decisions that guarantee the fulfilment of the mission of a given system under existing conditions and constraints (Jajuga, 2007). On the other hand, in the substantive sense, risk management in the implementation of such management is essentially based on the appropriate management of information and its attributes of completeness, completeness, reliability, certainty, accuracy and timeliness. Therefore, due to the subject-matter relationship, IT security, related to the estimation and control of risks arising from the use of computers, computer networks and data transmission, becomes essential. These processes and issues should be assigned a subject-matter character, the components of which are: devices, systems, ICT networks, paper documents or content on other media. Accordingly, the risk analysis should include: the identification of the entities' information assets, the identification of threats and their consequences for each organised asset,

and the identification of the IT system's vulnerability. In addition, such an analysis should also incorporate into IT systems standards for security system design, 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 over the authorisation of access to information.

The author's analysis presented in this way, which is based on literature research and the author's professional experience, makes it necessary to analyse risks on an ongoing basis in order to quickly grasp the problem in which the risk created turns into a crisis.

In summary, as the learning experience shows, the fundamental issue in considering risk intelligence is to determine the difference between our degree of understanding of a given risk and that of others - this is mainly due to our awareness and our predisposition. Understanding risk requires two conditions: in order to fully comprehend risk, it is necessary to identify possible solutions to the problems created by the risks, as well as the factors that determine them. 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 of the determinants for understanding risk intelligence. Thus, risk intelligence refers to the ability to select the right type of risk by applying the rules of risk intelligence, which we will be able to manage effectively through our experience, e.g. by (Apgar, 2016):

- A tentative measure of uncertainty - determining the upper limit of expected losses.
- Assessing the risk and its impact on the safety management of a given system/facility.
- Estimating risk intelligence, which is the relative ability to understand and know the determinants of risk.

3. Materials and methods

Modern research related to security management, is really the awareness of what is needed for the duration and development, through knowledge and legitimate human activity, understood as value-justified decision-making. Therefore, in the research conducted, it should be borne in mind that the process of organizing safety management is always a set of activities performed to achieve the main objective and intermediate objectives at a certain time, which include the object and scope of the activity, the time to undertake and execute the system, the cost of the system and the risk (Czekaj, 2012). In addition, the organizational activities that shape the security system are harmonized planning, scheduling and execution with control of security tasks.

The author based the process of mental cognition in his research on analysis, deduction and comparison, justification, proof, and generalization and inference (Kotarbiński, 1990). In the process of analysis, the author used the research method of recorded security incidents - the investigated incidents were decomposed into established causes. This resulted in the extraction of basic factors and the correlation between them as dependent variables in the security system. On the other hand, the cognitive approach to the problem was an attempt to explain the circumstances and describe the causes that cause changes in the subject under study, which are the sources of decision-making in security management.

The methodical outlook selected by the author of the study is thinking guided by preconceived conclusive and explanatory sentences. The content of the study, in the author's intention, is epistemological cognition, which is understood as practically verifiable and socially useful knowledge, and gnoseological outlook, which is understood as conceptual knowledge in the intentional and cognitively rational area of human consciousness (Nowak, 2024). Research methodology, mainly on the potential of information and its elements, shaping security is a description dedicated to the approach of the author of the publication to the adopted solution to the research problem. Thus, based on methodological considerations, considerations organize the organization of the subject of research (Kotarbiński, 1994). On this basis, it will be possible in the future to design a model of the potential of information used for security management, preliminarily verified empirically. At the same time, it should be emphasized that nowadays in this type of conducted research of interdisciplinary knowledge, the fundamental research problem lies in the development of concepts and methodologies for designing hybrid systems, harmonizing predictive research methods, which in complex areas of security management research should ensure methodological unambiguity without being dominated by one of the detailed methodologies.

The scientific nature of the study stems from the goal that the author intends to achieve by fulfilling the principles of generality, accuracy, informative content, epistemological certainty and logical simplicity. The realization of the goal, that is, the research methodology used, will boil down to:

- the possible construction of a model of the sources of information potential shaping security;
- the solution and knowledge of unknown facts;
- to describe, seek and explain new phenomena and methods;
- development of new patterns and model of security management on the basis of the information potential used.

The developmental nature of the work, from the point of view of science, is due to the importance of internal and external factors of cognitive activities and awareness conditions of the community organized into an organization. Among the internal factors of the research conducted, we can include the variables obtained empirically in the studied organizations for the causes of events - they are the subject of the study and the theoretical considerations carried

out on their basis are aimed at obtaining the closest possible theoretical justifications. The external factors that the author considered in his work are: social, economic and cultural determinants of security, based on the potential of information.

Thus, scientific cognition is presented, described in the interdisciplinary area, the results of which, as a design of a new solution, will enable its confirmation in practical application. In addition, the author's definition of the concept of security as an ontological category, implies the openness of the dispute about the principals of this process and makes it possible to predict unfavorable phenomena for the conducted activity - this indicates the possibility of resolving events not yet known. Contemporary scientific writing on this issue is mainly reduced to presenting a position on a fragmentary view of this problem. Other scientific positions focus on a general approach to the problem of security of processed information. Especially with regard to issues related to the security of personal data processed in information systems as well as issues related to specific elements of the ICT infrastructure.

4. Results and discussion - assumptions for designing a security management model

From an analysis of the literature on the subject and the author's practical experience, the relationship between risk and crisis management problems implies managing security by having to make choices about strategies for action under high risk conditions. In terms of security management, decisions are in the nature of an assumed positive prediction based on identified incidents and established and identified vulnerabilities of the (information protection) system. These decisions should be understood as the act of consciously choosing one of the many identified and considered acceptable options for action, chosen on the basis of knowledge, experience and the aforementioned intuition to which a high degree of utility is attributed (Dąbrowski et al., 2016) Decisions in security management should be the result of an assumed way of solving a problem, and their making should fulfil a methodological pattern that boils down to:

- Gathering the necessary information about the decision situation and analysing it (data correctness).
- Characterising the problem and formulating the conditions of the decision situation.
- Developing options and ways of obtaining a solution.
- Make a selection of the optimal decision.
- Justify the choice and estimate the decision risk (decision optimality).

In addition, the management engineering necessary to consider is, first and foremost, the practical ability to build efficient and useful organisational and functional structures and to effectively control their operation in the context of various conditions. This is needed to

maintain the right balance and the right relationship with the environment of a given system and its internal development in terms of its safety. For the engineering of the security management system, its key elements and concepts are the working system and the emergency response system. The latter, as a deliberate action, was based on the identification of threats, elimination of causes and levelling of consequences. The crisis response system has its application during identified cases of at least information disclosure and therefore:

- security management is about making effective decisions based on a set of selected, organised and analysed information;
- security management is the practical skill of building organisational and functional structures and directing their operation in the surrounding relative reality;
- practically, the risk of decision-making is present in every situation and increases in direct proportion to the time (in which these decisions materialise), the consequences and the probability of the premises on which the decisions are based;
- crisis safety management, is a complex know-how for a specific organisation (Denning, 2022).

Therefore, when detailing the security management processes in question, we cannot omit:

- the management described by the standard and the information security system used;
- the management of the personnel-verified distribution of information;
- conducting audits and controlling the effectiveness of the applied solutions, which have a decisive impact on information security (Juchniewicz, 2017).

Thus, we must base the organisation of the management system, as well as security management itself, on information management embedded in the classic organisational cycle of the management process, the components of which are:

- Forecasting and identification of threats, specification of their types, scope and scale.
- Programming the consequences and repercussions of possible risks and their effects.
- Planning and inspiring remedial procedures to minimise risks or maintain risks at an acceptable level.
- Controlling and supervising risk indicators (Jajuga, 2007).

In characterising the decision functions in safety management, it should be stated that it is an activity-based management, which is realised in the form of decision streams. Therefore, we can conclude that the functions fulfilled by such decisions can be grouped into two (analogous to management functions) sets: morphological (planning, organising, controlling) and organic (anticipatory, transformational, benefit and predictive functions). On the other hand, in cybernetic terms, a decision is a function, i.e. an assignment according to which its content is influenced by a set of the following interrelated dependent elements (Skrzypek, 2000).

Thus, when characterising a system in relation to a security organisation, it turns out that it should be (Maliszewski, 2022):

- strict - because it designates what belongs to it;
- relatively unchanging - because possible changes fall within its definition;
- functional - because it fulfils the functions assigned to it.

We must also remember that the root causes of the weaknesses of such a system must be sought in the manner and quality of management. Moreover, any systemic security management is a function of the conjunction of the management of the elements of the classical stream and the psycho-sociological stream of selected basic variables. The classical scheme of organising an organisation's safety system assumes management based on a management system and an executive system. The management system is formed by two basic subsystems: decision-making and information. The decision-making subsystem implements the decision-making process necessary for the rational (efficient) operation of the organisation. The information subsystem implements the processes of collecting, transmitting, processing, storing and sharing information according to the needs of the decision-making system. The executive system carries out the task processes mandated by the management system, and the management system carries out the management, information and decision-making processes and organises the operation and course of executive processes. The management system is subordinated to the superior management system (Koźmiński, Jemielnik, 2007).

Thus, the safety management model is a set of activities performed to achieve the main objective and intermediate objectives in a specific period of time, which includes: the object and scope of the activity, time to undertake and execute the system, system costs and risks. In addition, the organisational activities that shape the model are: planning, scheduling and implementation and control of the protective tasks that make up the achievement of these objectives.

To sum up, as a result of the analyses of the holistically viewed problem, it turned out that information is crucial for the subject criterion of security management. Its dualistic understanding and use stemmed from the fact that it was firstly an object of protection and secondly a tool used for protection. Its first and second forms reflected the essence of efficient management in the decision-making process. Furthermore, information is an element of reconnaissance and a source of forecasting and analysis. Information is also, in the security management process, the internal legal standards assigning competences, describing standards and sanctioned standards. Thus, it should be stated that the implementation of security in the field of information protection constitutes its management through subject and object management. This means that a fundamental scientific problem is the (permanently analysable and digitally designable) complexity of the systems.

Conclusions

It was the intention of the author of the study to specify the problems and issues which, within the framework of an important view of security management, determine the functioning of many organisations in the market in the era of civilisation changes. In addition, the so-called technological foresight and the resulting risks applied in the study. On the basis of logical inference, we come to the conclusion regarding the necessity of research primarily in two aspects. Firstly, the prediction and study of a secure future must take place on the basis of the integration of scientific knowledge by means of triangulation research, which is characterised by the combination of methodologies of two or more research strategies of the same empirical objects. Secondly, the setting and prioritisation of such research must aim to maximise the benefits for economic and social security.

In the era of digital transformation and cognitive industry, weaving a consideration of security management (using IT tools, cognitive science methods and cognitive technologies), we come to the conclusion that these are methods, techniques and tools, supporting decisions for this management. The experience of interdisciplinary science shows that the above-mentioned activities, which are in fact information processing systems, use cognitive science departments to explain and model conscious, but also abstract thought processes.

Another problem in the cognitive view of security management boils down to the analysis of propositional attitude structures and intentionality - often understood as ‘planting attitudes’. This is otherwise a necessary research attempt to explain the processes of individual and collective mental models and the formation of broadly oriented cognitions of perception, emotion and awareness of discretion.

In summary, it is clear from the research issues described in the content that, under these conditions, the relationship between the most general principles of cognition and verified rationales is of great importance for the conduct of research and the use of results.

Under these conditions, it is still necessary to realise that the creation of a rationale for the design of a safety management model, according to which types of safety can be built in view of their changing functionality, will be based on:

- The statement that man is an anthropocentric entity (the first determinant of forms of existence).
- The concepts of threat, risk, emergency and its characteristics.
- Information and its parameters in the area of systemic security.
- Constitutional foundations-secure and organised communities (positive law).

References

1. Apgar, D. (2016). *Inteligencja ryzyka.* Gliwice: Helion, pp. 25-28.
2. Arnold, R.D., Wade, J.P. (2015). A Definition of Systems Thinking: A Systems Approach. *Procedia Computer Science, Vol, 44,* pp. 668-674.
3. Banach, D. (2022). *Rozwój i postęp techniczny na tle ogólnych prawidłowości gospodarczych i cywilizacyjnych, wybrane problemy*. Kraków: Księgarnia Akademicka.
4. Beck, U. (2014). *Społeczeństwo ryzyka, w drodze do innej nowoczesności.* Warszawa: Scholar, pp.29-48.
5. Brown, T., Martin, R.L. (2015). Design for action. *Harvard Business Review, September,* pp. 58-63.
6. Bryjka, F., Zając, T. (2023). *Wzmocnienie ochrony infrastruktury krytycznej państw UE i NATO*. Retrieved from: https://www.pism.pl/publikacje/wzmocnienie-ochrony-infrastruktury-krytycznej-panstw-ue-i-nato, 13.02.2024.
7. Czekaj, J. (2012). *Podstawy zarządzania informacją*. Kraków: Wydawnictwo Uniwersytetu Ekonomicznego w Krakowie.
8. Dąbrowski, A., Schumann, A., Woleński, J. (2016). *Podejmowanie decyzji: pojęcia, teorie, kontrowersje*. Kraków: Copernicus Center Press.
9. Denning, D.E. (2022). *Wojna informacyjna i bezpieczeństwo informacji*. Warszawa: WNT.
10. Falencikowski, T. (2008). *Kształtowanie swobody decyzyjnej w zarządzaniu grupami kapitałowymi.* Toruń: Dom organizatora, pp. 194-199.
11. Ficoń, K., (2007). *Inżynieria Zarządzania Kryzysowego. Podejście systemowe*. Warszawa: BEL Studio, pp. 16-19.
12. Greber, D., Wengrow, D. (2021). *Narodziny wszystkiego, nowa historia ludzkości*. Poznań: Zysk i S-ka, pp. 441-444.
13. Grobler, A. (2016). *Metodologia nauk.* Kraków: Ureus i Znak, pp. 36-41.
14. Grohs, J.R., Kirk, G.R., Soledad, M.M., Knight, D.B. (2018). Assessing systems thinking: A tool to measure complex reasoning through ill-structured problems. *Thinking Skills and Creativity, Vol. 28,* pp. 110-130.
15. Jajuga, J. (2007). *Zarządzanie ryzykiem.* Warszawa*:* PWN, pp. 26-32.
16. Juchniewicz, M. (2017). Koncepcje doskonalenia organizacji – ewolucja, krytyka, perspektywy rozwoju. *Prace Naukowe Uniwersytetu Ekonomicznego we Wrocławiu, No. 463,* pp. 34-44.
17. Kahneman, D. (2011). *Pułapki myślenia.* Poznań: Media Rodzina, pp. 39-40.
18. Kaplan, A., Haenlein, M. (2019). Siri, Siri in my Hand, who's the Fairest in the Land? On the Interpretations, Illustrations and Implications of Artificial Intelligence. *Business Horizons, Vol. 62, No. 1,* pp. 15-25.

19. Kotarbiński, T. (1990). *Elementy teorii poznania, logiki formalnej i metodologii nauk*. Wrocław: Ossolineum.
20. Kotarbiński, T. (1994). *Ontologia, teoria poznania i metodologia nauk*. Wrocław: Ossolineum.
21. Koźmiński, A.K., Jemielnik, D. (2008). *Zarządzanie od podstaw*. Warszawa: WAiP, pp. 73-79.
22. Koźmiński, A.K., Piotrowski, W. (2011). *Zarządzanie teoria i praktyka*. Warszawa: PWN.
23. Maliszewski, M. (2022). Koncepcja modelowego systemu zarządzania kryzysowego obiektu infrastruktury krytycznej na przykładzie Rafinerii w Gdańsku. *Przegląd naukowo-metodyczny edukacja dla bezpieczeństwa, Vol. 55, No. 2,* pp. 117-121.
24. Nowak, S. (2024). *Metodologia badań społecznych*. Warszawa: PWN, pp. 49-51.
25. Skrzypek, E. (2018). *Nowoczesne trendy w zarządzaniu a doskonalenie zarządzania*. Retrieved from: https://depot.ceon.pl/bitstream/handle/123456789/16400/Skrzypek_El%C5%BCbieta, 6.02.2024.
26. von Weizseker, E., Wijkman, A. (2018). *Club of Rome report. Capitalism, short-sightedness, population and the destruction of the planet.* Warszawa: Instytut Badań Stosowanych Politechniki Warszawskiej, pp. 7-11.
27. Zięba, R. (2018). *Instytucjonalizacja bezpieczeństwa europejskiego*. Warszawa: Scholar.