TRANSPORT PROBLEMS 2021 Volume 16 Issue 3
PROBLEMY TRANSPORTU DOI: 10.21307/tp-2021-047

Keywords: railway system; safety; asymmetric threats

Andrzej CHUDZIKIEWICZ*, Andrzej KRZYSZKOWSKI
Kazimierz Pulaski University of Technology and Humanities in Radom
Malczewskiego 29, 26-600 Radom, Poland
Anna STELMACH
Warsaw University of Technology
Koszykowa 65, 00-682 Warsaw, Poland
**Corresponding author*. E-mail: chudzikiewicz.andrzej@gmail.com

ASYMMETRIC THREATS IN TERMS OF SAFETY OF RAILWAY SYSTEMS

Summary. This article deals with the problem of new threats that appear in areas that have not been affected by them so far. The considerations concern asymmetric threats and the railway system. The analysis of this issue was carried out on the basis of general information on the problem of asymmetric threats and the knowledge of the railway system, its operation and identified threats that can be attributed to the characteristics of asymmetric threats. The aim of the article is to draw attention to new phenomena that are beginning to affect transport on a global basis, including rail transport.

1. INTRODUCTION

The issue of the safety of the railway system is a major one, and although it concerns only the sphere of rail transport, it cannot be assigned only to this sphere of economic activity of the state. The area of security includes issues from such sciences as law, sociology, psychology, technology, and logistics. Generally speaking, the concept of security is an interdisciplinary concept derived from socio-political sciences, and it is in this area that basic research on security theory is developed [1, 2, 20]. One of the many definitions of security that can be found in these studies is as follows: Security is defined in the context of threats to a given entity (individual, group, nation, or society as a whole).

The concept of a threat is related to the notion of security. It can be understood as a subjective or actual occurrence of a danger for a given subject for the values, interests, and goals recognized by him. The reconstruction of the international order and social changes after World War II resulted in a modification of the global security environment, especially the description of contemporary security problems and the threats related to these phenomena. One of the new concepts related to threats, developed in the beginning in Anglo-Saxon countries and borrowed from environments dealing with security research in the aspect of international relations, taking into account the military sphere, is the concept of asymmetric threats [3 - 5, 21]. An asymmetric threat is not only a specific technique or method of operation but also an entity that uses it by unconventional means and techniques. The literature on the subject, including in [6, 22], lists many factors as influencing the environment of the activities of entities that constitute asymmetric threats.

One such factor is the sensitivity and susceptibility of some state structures to asymmetric threats. Among these elements, the most common are transport and telecommunications infrastructure, as well as energy and water networks [23, 24, 33]. The railway system, which is an important component of transport, telecommunications, and energy infrastructure, is particularly sensitive to asymmetric threats, characterized by a lack of predictability both in terms of methods and techniques of operation and entities that are the source of these threats. This paper presents considerations for the safety of the railway system, taking into account the asymmetric threats, which, so far, have not been taken into account as a significant element that may affect the safety of the railway system. An example of an incident where the threat that caused it may be classified as asymmetric is the railway disaster in Santiago de Compostela (Spain) on July 24, 2013, in which 79 people were killed and over 178 persons were injured, including 35 who were seriously injured.

The development of new IT technologies, quickly adapted to new solutions for railway traffic control systems and passenger and goods transport management systems, prompted the authors to take up this subject with a view to the continuous improvement of the safety of the railway system.

2. SECURITY AND ASYMMETRIC THREATS

In the safety literature, one can find at least a dozen definitions and terms of this concept [7, 21, 32]. It is difficult to consider it impartially because each author's approach to any topic is by definition subjective, which, on the basis of the definitions given in the literature, is complete and consistent with the general concept of security. Choosing among many definitions, the definitions given in dictionaries can be adopted from the provision contained in the Dictionary of Social Sciences [8]. In the most literal sense, security is actually identical with safety and means no physical danger or protection against it. In other publications in the field of social sciences, one can find the term security as the ability to survive, independence, identity, or development. Along with the development, at the beginning of the 20th century, of social relations and the formation of new socio-economic systems, the importance of national and social security acquired significant importance, bearing in mind the dynamics of this development. In the mid-twentieth century, the concept of safety was adopted, along with the development of, inter alia, nuclear energy, to study the safety of technical systems and technological processes taking place in them.

There are many new types of threats generated by evolving new phenomena in areas such as IT, new technologies, space exploration, or ecology and defined by analysts involved in research in these areas. Among them, military strategists play a major role, trying to demonstrate the existence of such threats, and justify the need to undertake research in this field. An example of such trends is the formulation of the theory of asymmetric threats and the development of research in this area. There is a lot of controversy among researchers dealing with this issue and there is no currently formulated unambiguously and universally recognized definition of security asymmetry. Nevertheless, numerous research studies are carried out in this area and asymmetric threats are often identified with the phenomenon of terrorism, which narrows the theoretical area of research and analysis, but at the same time extends the scope of practical use of this concept to such areas as energy, transport, telecommunications, and the Internet.

Asymmetry is a concept known from geometry. It means a violation or a lack of symmetry - a situation of some dissimilarity. Researchers dealing with the definition of this term in terms of security and threats pay attention to the different statuses of the parties in relation to the conflict, the existence of large disproportions in the analyzed states of ownership, and the positions of the parties in relation to the conflict. In asymmetric threats, it is possible to observe a significant disproportion of potentials, a clear difference in goals, or a different degree of involvement of the participants in the conflict. Such situations lead to the fact that the "weaker party" looks for unique and maximally unpredictable solutions. As a consequence, the results are unconventional solutions and methods of operation, the advantage of which, from the point of view of the "weaker party," is the difficulty of counteracting with the possible maximization of the effects of the activities carried out. An example of such actions is the attack on the Pentagon and the Word Trade Center on September 11, 2001.

The heuristic, preliminary analysis [9, 26] shows the lack of a systemic approach to the issue and the failure to consider all the causes that evoke effects classified as asymmetric results of conscious activity.

The second aspect of the problem is that it is difficult to unequivocally classify such events as asymmetric from the point of view of national (internal) or global security, and that may be classified as asymmetric during the technical and mathematical system analyses [14, 27] and not within the assumptions of asymmetric actions. On the other hand, symmetry in the mathematical sense does not mean identical or uniform. Critical analysis indicates a non-scientific approach and definition of the issue, and a dialectical–political interpretation of the problem qualified as "asymmetric activities in security."

Due to the multidimensionality of threats, it is difficult to define their asymmetry. Since this problem is most often considered by military strategists, the most developed concepts can be found in the works of strategists and NATO documents. In the NATO Glossary of Terms and Definitions, we find that an asymmetric threat is one "resulting from the possibility of using various means and methods to circumvent or neutralize the enemy's strengths, while taking advantage of his weaknesses in order to obtain disproportionate results."

Each threat, including an asymmetric one, is characterized by the possibility of adverse events, causing concerns about maintaining a state that guarantees safety and certain values. Risk assessment, i.e., the probability of this unfavorable phenomenon, requires the adoption of certain assumptions that allow the use of an appropriate method in the analysis of events.

In the case of asymmetric actions at work [4], in line with the intuitive understanding of this type of threat, the following assumptions were made:
I. asymmetric actions are characterized by the uniqueness of events and
II. the uniqueness of a given event makes it impossible to predict it.

Therefore, while attempting to model [9] phenomena referred to as asymmetric events using the probability theory, let us define the number of possible events. In the first approach, it can be assumed that if we have a set of n elements and the number k is the number of expected events, then the possibility of their occurrence will be as many as there are combinations of k elements on the set of n elements C_n^k, that is:

$$C_n^k = \binom{n}{k} = \frac{n!}{k!(n-k)!} \quad . \tag{1}$$

However, taking into account assumption II, i.e. the uniqueness of events, i.e. the specific order of occurrence, relationship (1) should be modified and the concept of variation without repetition V_n^k should be used:

$$V_n^k = \frac{n!}{(n-k)!} = n \cdot (n-1) \cdot \ldots \cdot (n-k+1) \quad . \tag{2}$$

Using the concept of an n-element permutation P_n on the {n} element set, we can write the relationship between the number of combinations and variations without repetitions built on the n element set in the form:

$$V_n^k = C_n^k \cdot P_k \tag{3a}$$

and

$$V_n^{n-1} = V_n^n = P_n \quad . \tag{3b}$$

From the form of relations (3a) and (3b) it can be concluded that the unpredictability of events increases with the number of events k. The next conclusion is that the event that has taken place will not repeat itself, but: this way of proceeding leads to a situation where the event that has occurred is the least predictable – therefore, at the same time, the most probable according to the assumptions (Annex II) of asymmetric actions.

The contradiction that occurs in this situation shows that the model, and dependencies (1) and (2) are incorrectly adopted and the current literature shows the necessity to replace it with a model from the repetition. Therefore, we can adopt models of eqv. [4]:

$$\boxed{\bar{C}\,{}_n^k = \binom{k+n-1}{k} = \frac{(k+n-1)!}{k!\,(n-1)!}} \tag{4a}$$

$$\overline{V}_n^k = n^k \quad . \tag{4b}$$

Such an approach to the problem of description of threats is possible in the case of the analysis of asymmetric threats in political science [3,10], which links asymmetric threats only with the activity of non-state, trans-, or subnational entities. The most common types of threats of this type are as follows:

- international terrorism,

- transnational organized crime (e.g. drug trafficking),
- use of weapons of mass destruction by non-state actors, and
- hostile use of information technology.

On the other hand, in the case of events associated with asymmetric threats on a smaller, non-global scale, e.g. in the scale of the region and the functioning of the transport system, a different model of description of the phenomenon can be proposed, taking into account the area and time associated with the threat.

In this situation, the most reliable is the mathematical description of the event in the form of a mathematical model presented as a record of the parameter dependence function with the possibility of changing the magnitude of the rank - meaning, (size) of parameters, made by the user depending on changing conditions. Considering a probabilistic space written as:

$$(S, P) \tag{5}$$

where: S is a set of possible random events,
P is the probability of the event occurring,
in the case of asymmetric events, which may occur in a smaller area than a continent or a large country, characterized by a rarity, the Poisson distribution described by the probability distribution function (6) can be used [14]:

$$P\{X = k\} = \frac{\lambda^k}{k!} e^{-\lambda} \tag{6}$$

where:
λ is the expected number of events in a given time interval in a given area and
$P\ \{X = k\}$ is the probability that in a given time interval on a given k events will take place.

The Poisson distribution assumes the temporal and spatial independence of events, which implies an important property of this distribution, taking into account the possibility of its use in the analyses of asymmetric events:

- the number of events occurring in separate, consecutive time intervals shows the properties of the Markov process, in which the knowledge of the current state fully determines the probabilistic relationships for future moments, and additional information about the previous behavior of the system does not add anything new, and
- to assess the future state, i.e., to forecast the number of such events in the future, it is enough to know the current state of the system.

The paper [11] attempts to explain that these properties of the Poisson distribution justify the use of the expected number of events (λ) in this distribution as a measure of the risk of the occurrence of critical incidents of a specific category in a given area. The problem arises in formulating a method for determining the expected number of critical incidents (λ) occurring in the analyzed phenomenon. In work [11], it was proposed to relate the amount of data on the basis of which the accuracy of the determination (λ) could be estimated by determining the confidence intervals. The proposed method can be used in the case of a large number of events, while in the case of a small number of events, such as in the case of asymmetry, this method does not lead to reliable results. Therefore, further research in this area should be carried out. In the case of communication networks and distributed IT systems used in transport systems, an interesting approach to the issue of threat modeling and risk analysis in the case of cyber attacks is presented in [29].

The risk assessment methodology is based on building a trust model[1] based on selected leaders of the analyzed group of potentially endangered means of transport. Risk assessment includes assessing

[1] The trust model proposed by Marsh (1994) is one of the first works that proposed a formal treatment integrating different trust concepts. According to Marsh, major early contributions to understanding trust have come from the areas of sociology, social psychology, and philosophy, mainly in work carried out by Deutsch, Luhman, Berber, and Gambetta. Many attempts have been made to represent trust mathematically and a number of computational trust models, mostly based on Gambetta's definition, have emerged for risk management mechanism in on-line communications. The goal of a computational trust model is to assist users with decision-

the impact and likelihood of attacks relevant to the identified threats, assessment of the trust model design principles, validation of built-in security, and attack mitigation actions. For maritime transport, [28] presents a combined approach using modeling and simulation and data fusion techniques to analyze complex scenarios involving asymmetric hazards in marine environments, in particular, in coastal areas and ports. In the case of air transport, the paper [30] presents a method of dynamic problem-solving related to the allocation of aircraft that may occur on the airport apron, in the case of threats, different types of failures, or unusual events (eg a terrorist attack). The method uses fuzzy logic in the process of assessing the situation and making decisions under conditions of uncertainty. As we can see, the multitude of types of asymmetric threats, in different areas of transport, causes that research is carried out in various directions and with different methods, adequate to the nature of these threats. In addition to quantitative research and analyses, qualitative analyses are also carried out, showing the possibility of threats in areas such as ITS. For example, work [32] presents a comprehensive classification of ITS security and privacy vulnerabilities, discusses the challenges of solving security and privacy issues in ITS, and presents opportunities for future research directions to counter global threats.

3. SAFETY OF THE RAILWAY SYSTEMS

We can say that the railway system, or the rail system, is a structure consisting of railway infrastructure, including both lines and fixed devices functioning in this structure, together with vehicles of all categories and origins. We can say that the railway system, or the rail system, is a structure consisting of railway infrastructure, including both lines and fixed devices functioning in this structure, together with vehicles of all categories and origin, which are moving within this infrastructure The inseparable elements of this structure are legal and organizational conditions and the human factor: the people responsible for the functioning of this system.

As far as the legal regulations concerning the railway system and its operation are concerned, it should be clarified that apart from national law, there is also Community law (EU law), which, from the moment of Poland's accession to the EU, plays an important role in the formulation of national law. In accordance with the provisions of the Directives [16, 17] and the Act [15], the railway system can be divided into the following subsystems:

a) structural:
- infrastructure,
- energy,
- control, and
- rolling stock,

b) operational:
- rail traffic,
- maintenance, and
- telematics applications for passenger and freight services.

The tasks of the system and subsystems have been written in the Act and directives.

Considering the safety of railway transport, the following thesis can be formulated:
- railway infrastructure, its condition, and the level of safety constitute the safety of transport railway.

However, the essential elements of the infrastructure in this regard are:
- rolling stock and its maintenance level,
- train control systems and signaling system, and
- safety management system as a recognized risk control tool.

In the case of rail transport and rail transport, the Ir-8 instruction issued by the infrastructure manager of PKP PLK S.A. Railway traffic safety was defined as: "no unacceptable risk of damage in connection with the implementation of transport processes on the railway infrastructure".

making (Manish Gupta, Raj Sharman. *Handbook of Research on Social and Organization Liabilities in Information Security. State University of New York, USA, 2009, ISBN10: 160566 1325*)

Pursuant to Directive 2004/49 / EC of the European Parliament and of the Council (2009/460 / EC) on safety, the railway system as a whole and its parts must meet the minimum requirements defined as Common Safety Targets (CST). CST are indicators that determine the minimum, expressed in risk acceptance criteria, safety levels set by the European Railway Agency (ERA) on the basis of the so-called National Reference Value (NRV) for each country.. The NRV indicator is calculated in accordance with the procedure set out by the Commission Decision of 5 June 2009, adopting a common safety method to determine whether the safety requirements referred to in 6 of Directive 2004/49 / EC of the European Parliament and of the Council (2009/460 / EC), have been met. The list of NRV indicators for individual countries is included in the Annex to the Commission Decision of 23 April 2012 on the second package of common safety requirements for the railway system [19]. Member States are required to continuously monitor the safety performance of their rail systems, including the achievement of common safety targets (CSTs), defined in a quantitative and qualitative manner. In Poland, the relevant provisions specifying the conditions that should be fulfilled to achieve an appropriate level of safety are contained in the Act on rail transport.

When analyzing the potential threats that may affect the rail system and its individual elements today, it is impossible not to refer to the general considerations in Chapter 2 concerning asymmetric threats. These are related to the development of international relations, but on such levels as, among others, culture, ecology, technology, humanitarianism, or demography. As a result, not only countries but also international systems, non-governmental entities, economic and economic systems, and their elements (energy system, transport system, water system, telecommunications system) are considered as objects and entities influencing security and the relationship with it and others, similar and specific human communities, social groups, or even single people. In this context, the concept of asymmetric risk acquires a new meaning and considering this category of threats in relation to transport safety, and in particular, the rail system, seems to be justified [9]. The transport system, including the rail system within Europe, has already become a global system; thus, globalization, with all the good and bad features accompanying this phenomenon, has already started to affect it. One of the elements is ITS - the area of knowledge and its applications in many areas of transport, not just rail [34], in which the latest research and implementation results in the field of information technologies are currently available.

4. POSSIBILITY OF ASYMMETRIC THREATS IN THE RAILWAY SYSTEM

Along with the development and strengthening of the EU as an economic and political union of 27 European countries, transport, including the rail system, has become one of the important elements determining the development of these countries in practically every area. The EU's transport policy aims to open up transport markets to competition and create trans-European networks that allow freight and passenger transport to be balanced, bearing in mind, inter alia, the use of different modes of transport. However, in the social sphere, an important goal is the sustainable development of regions and environments through, inter alia, increasing the mobility of the inhabitants of the Union. The activities of the EU in this area are an example of the globalization processes taking place in many areas of the modern world. As shown by numerous publications [11], globalization is one of the reasons for the emergence of asymmetric threats and the formation of an "asymmetric enemy", which may be an individual or a supranational organization, and the subject of attack is a functioning element in the global world or even an individual.

In the case of asymmetric threats in political science, their characteristic feature is not only the fact that their source is non-state entities but also features such as [10, 12]:

- *quasi-military in nature*, i.e. threats from non-state actors are not take the form of an attack by regular armed forces, which does not allow them to be considered a threat military in the traditional sense; however, these entities may use for their own purposes typical means of armed struggle, produced for the army,
- *transnationality and territoriality*, i.e., non-state actors posing a threat; they can develop their structures in the territory of more than one state, and in the case of the occurrence of the threat

itself, it is difficult for them to assign a specific area of activity, the theater of combat, or the front, thus blurring the distinction between threats of an external nature and an internal one;

- *unpredictability* of the place and time of occurrence as well as the form and method of implementation specific actions taken by non-state constituting actors posing a threat;
- *low susceptibility of entities being the source of threats to deterrence* or other strategies to prevent and combat dangers through coercion or the threat of its usage.

The methods and forms of operation of an asymmetric enemy may be diverse, and the sphere of action may be military or non-military [10, 11, 12] such as

- terrorism,
- information warfare and activities in cyberspace,
- piracy, or
- even individual forms based on beliefs or a unit's mental state.

The place of action may also be undefined, and its choice is also random.

The above-mentioned features characterizing asymmetric threats correspond to the functions, objectives, and tasks that were set for the EU transport system and thus for the transport systems of the EU countries, including the rail system.

Examples of events in the UE transport system that can be assigned asymmetricity and qualify as asymmetric events can be:

- Spain, March 11, 2004, attack on 4 commuter passenger trains in the center of Madrid and around Atocha station,
- Russia, the train crash of the Nevsky Express, November 17, 2009,
- Spain, a train disaster on July 24, 2013 in the city of Santiago de Compostela,
- Disappearance of the Malaysia Airlines 370 plane, March 8, 2014,
- Plane crash, Germanwings 9525 flight in the Alps, March 24, 2015.

As shown by numerous presentations at conferences devoted to transport safety [13, 33, 34], including rail transport, e.g., Railway Safety Forum, 03/03/2021, the issue of railway transport safety in the context of the implementation of modern traffic control systems is an issue that is becoming increasingly more important.

From the technical point of view, the railway traffic control system (srk) is a collection of computer, relay, or mechanical devices. In the srk technique, one can distinguish, among others, station systems (controlling the movement of vehicles in the area of a single traffic post or multiple related posts), linear systems (controlling the correct sequence of vehicle movement between posts-stations), or special-purpose systems. These systems communicate with each other by means of closed and open transmission standards, creating computer networks. Information from these networks is sent to railway traffic management systems in a given area and constitutes an element of cyberspace, which, by definition, is already subject to asymmetric threats.

Therefore, we can see that in the case of the rail system, apart from the threats that have existed so far, new threats have appeared that should be the subject of research and analysis with a view to broadly understood the safety of the transport system of a region, country, or area such as the European Union.

5. CONCLUSIONS

The development of new technologies as well as new techniques and methods of their implementation in the modern, global world is the reason for the evolution of threats and creation of their new types and kinds. An example of this phenomenon is developing asymmetric threats, initially in the military sphere, and then in other spheres of socio-economic life. As shown in the paper, globalization is one of the causes of the emergence and development of asymmetric threats.

The EU rail system consisting of the subsystems of railways of the Community countries, along with the development of new technologies for the production of rail vehicles, infrastructure elements and systems, and IT solutions, began to fit into the globalization process and take on features that characterize global systems. Asymmetric threats and their symptoms have started to appear for over a dozen years in the transport space, including rail transport. An example would be cyber threats. The authors of these threats, as shown by events from the past, are individuals lost in the global world or groups and individuals generally referred to as terrorist groups.

Symptoms of this type of threats are difficult to recognize; they are unique, which makes it impossible to predict such events. Due to the specificity of these threats, the research undertaken is carried out using mixed methods, i.e., using theoretical and empirical methods and a whole range of techniques and research tools characteristic of these methods. Moreover, as literature research shows, methods and tools depend on the type of transport, and if we consider rail transport, the area to which they apply is important (rolling stock, control systems, or point or line infrastructure). It is also difficult to model and assess the risk in the case of asymmetric threats in this area, because, inter alia, there is no work on this subject. On the other hand, the effects of events resulting from such threats are unpredictable and can be very tragic.

Bearing in mind the safety of railway systems, in the face of asymmetric threats and their specificity, counteracting these threats, it is necessary to take untypical actions, corresponding to the nature of the asymmetric threats. These should be activities, e.g., like the already existing forms of passenger control at airports or forms of protection of airports and airplanes standing on airport aprons.

In addition to non-standard activities, activities should be carried out using already known methods, such as monitoring, but with the use of new ITS technologies (e.g., image recognition methods).

In sum:

- asymmetric threats covering all ranges of human activity on a scale global began to include the rail transport system and the subsystems included within it,
- the specificity of these threats allows the conclusion that in the case of railways, they can be informatics systems and control systems (SRK systems) exposed to threats as one of the systems vulnerable to cyber threats,
- studies and analyses of this type of risk in the case of the rail system, due to uniqueness, unpredictability, and small numbers, are difficult and require experience and knowledge of the specificity of railways,
- analysis of various events that have taken place in the area of transport in the last years of the twenty-first century age, shows that asymmetric threats cannot be ignored in the analysis of threats to which the rail system is exposed.

The negative effects of the ongoing changes and their impact on the rail system cannot be avoided; only actions can be taken to minimize these effects. Therefore, the authors took up this subject, hoping to start a discussion and spur work in this area.

References

1. Stańczyk, J. *Współczesne pojmowanie bezpieczeństwa*. Warsaw, 1996. [In Polish: *Contemporary understanding of security*].
2. Jakubczak, R. *Bezpieczeństwo narodowe w XXI wieku*. Warsaw, 2006. [In Polish. *National security in the 21st century*].
3. Ciekanowski, Z. Działania asymetryczne jako źródło zagrożeń bezpieczeństwa. *BiTP*. 2009. No 3. P. 47-72. [In Polish: Asymmetric activities as a source of security threats].
4. Krzyszkowski, A. Logistyka a bezpieczeństwo asymetryczne. *Logistyka*. 2014. Vol. 4. [In Polish: Logistics and asymmetric security].
5. Madej, M. *Zagrożenia asymetryczne bezpieczeństwa państw obszaru transatlantyckiego*. Warsaw: Polski Instytut Spraw Międzynarodowych. 2007. [In Polish. *Asymmetric threats to the security of the states of the transatlantic area*].
6. *Strategic Assessment - Report*. National Defense University. Waszyngton, 1998.

7. Pokruszyński, W. *Teoretyczne Aspekty Bezpieczeństwa*. Józefów, Poland: Wyższa Szkoła Gospodarki Euroregionalnej im. Alcide De Gasperi. 2010. [In Polish. *Theoretical aspects of security*].
8. *A Dictionary of the Social Sciences*. London, 1964.
9. Krzyszkowski, A. Metody heurystyczne, historia powstania i zastosowanie. In: *Zimowa Szkoła Sportów Wodnych, Ratownictwa, Rekreacji i Rehabilitacji w Wodzie*. Szczyrk, Poland. 2009. [In Polish: *Heuristic methods, history of origin and application*].
10. Urbanek, A. Cyberwojna – Zagrożenie Asymetryczne Współczesnej Przestrzeni Bezpieczeństwa. *Studia Nad Bezpieczeństwem*. 2016. No. 1. P. 5-32. [In Polish: *Cyberwar – Asymmetric threats of contemporary security space*].
11. Prońko, J. *Metodyka Przestrzennej Analizy Zagrożeń Miejscowych*. Bezpieczeństwo. Teoria - Badania - Praktyka. Józefów, Poland: CNBOP-PIB. 2015. P. 88-108. [In Polish: *Methodology of spatial analysis of local hazards*].
12. Rokiciński, K. Wybrane aspekty zagrożeń asymetrycznych na morzu w funkcji wykorzystania sił morskich. *Zeszyty Naukowe Akademii Marynarki Wojennej*. 2005. Rok XLVI. No. 1(160). P. 151-171. [In Polish: Selected aspects of asymmetric threats at sea as a function of the use of naval forces].
13. Pawlik, M. Bezpieczeństwo kolejowe – wyzwania 2021. Nowe podejście do bezpieczeństwa kolejowego w kontekście cyberbezpieczeństwa. *Forum Bezpieczeństwa Kolejowego*. Warsaw. 03.03.2021. [In Polish: Railway safety – the challenges of 2021. A new approach to railway safety in the context of cybersecurity].
14. Findeisen, W. (red.). *Analiza Systemowa – Podstawy i metodologia*. Warsaw: PWN. 1985. [In Polish: *System analysis – Fundamentals and methodology*].
15. *Ustawa z dnia 28 marca 2003 r. o transporcie kolejowym*. [In Polish: *The act of 23 March 28, 2003 on rail transport*].
16. *Dyrektywa Parlamentu Europejskiego i Rady 2008/57/WE z dnia 17 czerwca 2008 r. w sprawie interoperacyjności systemu kolei we Wspólnocie*. DU UE 18.7.2008. [In Polish: *Directive 2008/57/EC of the European Parliament and of the Council of 17 June 2008 on the interoperability of the rali system within the Community*].
17. *Dyrektywa Rady z dnia 29 lipca 1991 r. w sprawie rozwoju kolei wspólnotowych* (91/440/EWG. Dz. Urz. L 237 z 24.8.1991, P. 25. [In Polish: *Council Directive of 29 July 1991 on the development of the Community's railway*].
18. *Decyzja Komisji 2012/226/UE z dnia 23 kwietnia 2012 r*. [In Polish: *Commission Decision 2012/226/EU of 23 April 2021*].
19. *Przewodnik dotyczący opracowywania i wdrażania kolejowego systemu zarzadzania bezpieczeństwem*. European Railway Agency Safety Unit. ERA/GUI/01-2011/SAF. Version 1. 13/12/2010. [In Polish: *Guide to the development and implementation of a railway safety management system*].
20. Kass, L. & Jack, J.P. *Combating Asymmetric Threats: The Interplay of Offense and Defense*. Spring 2014. No. 248. Published for the Foreign Research Institute by Elsevier Ltd. DOI: 10.1016/j.orbis.2014.02.004.
21. Brzica, N. Understanding contemporary asymmetric threats. *Croatian International Relations Review*. 2018. Vol. XXIV(83). P. 34-51. DOI: 10.2478/ cirr-2018-0013.
22. Singh, S. & Tu, H. & Allanach, J. & Pattipati, H. & Willett, P. Modeling threats. *IEEE Potentials*. 2004. Vol. 23. No. 3. P. 18-21.
23. Kaewunruen, S. & Alawad, H. & Cotruta, S. A decision framework for managing the risk of terrorist threats at rail stations interconnected with airports. *Safety*. 2018. Vol. 4. P.36.
24. Matsika, E. & O'Neill, C. & Battista, U. & Khosravi, M. & Laporte, A. & Munoz, E. Development of risk assessment specifications for analysing terrorist attacks vulnerability on metro and light rail systems. *Transp. Res. Procedia.* 2016. Vol. 14. P. 1345-1354.
25. Pejic, I. Impact of Terrorism as an Asymmetrical Threat on the State's Conventional Security Forces. *World Academy of Science. Engineering and Technology International Journal of Law and Political Sciences.* 2018. Vol. 12. No 5.

26. Verma, B.K. Long range identification and tracking. *Journal of National Maritime Foundation of India.* 2009. No. 5. P. 39-56.
27. Krdeepak Kumar. *Asymmetric threats and their challenges to freedom of navigation*. Dissertation, World Maritime University. Malmo. Sweden 2010.
28. Tremori, A. & Massei, M. & Madeo, M. & Reverberi, A. Interoperable simulation for asymmetric threats in maritime scenarios: a case based on virtual simulation and intelligent agents. *International Journal of Simulation and Process Modelling*. 2013. Volume 8. Issue 2-3. DOI: 10.1504/IJSPM.2013.057546.
29. Hasrouny, H. & Bassil, C.& Samhat, A.& Laouiti, A. Security Risk Analysis of a Trust model for Secure Group Leader-based communication in VANET. *Adv. Intell. Syst. Comput*. 2017. Vol. 548. P. 71-83.
30. Skorupski, J. & Żarów, P. Dynamic management of aircraft stand allocation. *Journal of Air Transport Management.* 2021. Vol. 90.
31. Motamedian, E. & Nouri, M. Assessing Sub-factors of Superiority Factors with Asymmetric Threats Approach. *Quarterly Journal Scientific Research of Strategic Defense Studies*. 2019. Vol. 17. Issue 76. P. 79-96.
32. Dalton, A. Hahn, & Munir, A. & Vahid Behzadan. Security and Privacy Issues in Intelligent Transportation Systems: Classification and Challenges. *IEEE Intelligent Transportation Systems Magazine*. 2021. DOI: 10.1109/MITS.2019.2898973.
33. Qian Chen & Azizeh Khaled Sowan & Shouhuai Xu. Safety and Security Architecture for Reducing Accidents in Intelligent Transportation Systems. In: *2018 IEEE/ACM International Conference on Computer-Aided design (ICCAD)*. San Diego. USA. 2018. DOI: 10.1145/3240765.3243462.
34. Wilkerson, S. & Korpela, C. & Chang, K. & Lee, A. & Gadsden, A. Aerial wars as Asymmetric Threats. In: *2016 International Conference on Unmanned Aircraft Systems (ICUAS)*. June 7-10. 2016. Arlington. VA USA.

Received 15.06.2020; accepted in revised form 13.09.2021