

THE OBJECTS OF CRITICAL INFRASTRUCTURE OF THE STATE AND ESTABLISHMENT OF THEIR SECURITY

¹LENKA PALAŠČÁKOVÁ

*Armed Forces Academy of M. R. Štefánika,
Demänovská cesta 393, 031 01 Liptovský Mikuláš,
email: "palascakova.lenka@gmail.com"*

Abstract: Critical infrastructure has become a modern phenomenon and the problem of its security is very actual topic nowadays. For understanding mutual causalities among particular sectors of critical infrastructure, it's necessary to deal with their commitments or relations under which we can imagine a mutual influence and dependency of these sectors. The main aim of the article based on law regulation and strategic document analysis modifying the protection of critical infrastructure EU and analysis the critical infrastructure in SR through the use of pinpoint method, is to point out to the objective need of defense and act security of important national infrastructure objects against the traditional imminence.

Keywords: security, threat, critical infrastructure, risk, strategy

1 Scopes of the need to define a critical infrastructure

Critical infrastructure – the notion which is the subject of discussion in the field of academies, central bodies of public administration, at national and multinational level. Resourcing the contemporary security risks, the need to define critical infrastructure as itself in developed countries of the world has appeared within the field of infrastructure where destruction will cause serious political and economic consequences. More European countries are considered by terrorists as potential targets and Europe is one of the base of their operation. Terrorism is focused on the attacks against civilian population as well as critical infrastructure of the state with the goal to cause massive victims, damages, develop fear and feeling of danger.¹

The Slovak Republic is likewise a subject to similar threats and challenges the other countries in Euro-Atlantic region face. Analysis of the risks is necessary assumption to understand the threats in more global world. Therefore, we elaborated a short analysis of critical infrastructure in the Slovak Republic in order to understand mutual relations among particular sectors of critical infrastructure in our article. We included nine sectors of critical infrastructure into the analysis, according to the National Program adopted in 2007 which we analyzed based on three factors of interaction, namely: the factor of the consequences scope, the factor of the number of affected sectors and the factor of space-time. In order to prove the practical way of understanding the sensitive elements of critical infrastructure and its sectors, we performed the comparison at the level of the Slovak Republic in comparison to other V4 countries (The Czech Republic, Poland and Hungary).

The main aim of this article is: *“Based on the analysis of legal regulations and strategic documents modifying the protection of critical infrastructure of EU and the analysis of critical infrastructure in the Slovak Republic with the help of point method, to point out the objective need of the security of the protection and the defense of important objects of national infrastructure against traditional threats.”*

Basic background documents are sourced from relevant legislation of EU and the Slovak Republic as well as from available domestic and foreign literature. Research methods we used come from the information on the past and present and apply heuristic approaches towards the future in order to achieve the prognosis how the following development will look like, thus what events or occasions can appear in future. There are a lot of various methods, processes available which are mostly focused on the revision of risks and on the evaluation of particular parameter of critical infrastructure. According to the selected

criteria, we chose point method from the great number of methods and processes. By the analysis of the protection of critical infrastructure in the Slovak Republic, we evaluated particular sectors (transport, water, food, health, energetics, ICT, public order and internal security, industry and financial sector) according to factors from the point of view of their importance for the operation of critical infrastructure as a whole, based on that the vulnerability of critical infrastructure in these sectors can be predicted.

We decided for the topic of critical infrastructure because of the fact that mentioned problem is understood as very significant and important field for keeping elementary functions of the state as well as keeping important needs for population, during crisis situations. We consider it as the field which still should search new possibilities, ways and effective solutions for the minimization of the threats of contemporary world.

2 Development of critical infrastructure in EU

European Union with its global position and population cares about the protection of the most important infrastructures of particular states. Terrorist attacks in Madrid, London, Paris emphasized the threat of terrorism. The need for the improvement of protection, readiness and the response of Europe to terrorist attacks focused on critical infrastructure was established, based on which the proposal to elaborate *European Program for Critical Infrastructure Protection* was adopted. The response of EU was to elaborate several documents solving the prevention, readiness and responses to threats threatening critical infrastructure focusing on the threat of terrorism.²

The elaboration of *European Program for Critical Infrastructure Protection* (hereinafter just “EPCIP”) and *Critical Infrastructure Warning Information Network* (hereinafter just “CIWIN”) belong among the significant documents. After the reflection of member states of EU and particular industrial communities, *Green Book on European Program for the Most Important Infrastructure Protection* (hereinafter just “Green Book”) has been elaborated by The Commission of the European Communities (hereinafter just “the Commission”) in 2005.³ Document finds the opinions of member states of EU in the field of criteria on the review of critical infrastructure and it also emphasizes that there should be public administration together with private sphere included into critical infrastructure, while the significant responsibility for critical infrastructure protection must be taken by state.

It consists of alternative possibilities which the Commission can use for application of EPCIP and CIWIN. It specifies that the goal of EPCIP is to ensure to have the same levels of protective security of the most important infrastructure within the whole EU that should consist of the least number of weak points and fast and proved renewal mechanisms. The level of protection should not be the same for all the elements, but derived from possible impact that could cause the failure.⁴

The Council Directive 2008/114/ES (hereinafter just “the Council Directive”)⁵ is of a particular significance, it modifies

² *Predbežné stanovisko k návrhu smernice Rady o identifikácii a označení európskej kritickej infraštruktúry a o zhodnotení potreby zlepšiť jej ochranu – EÚ*. Tlač: 2006/0276 (CNS), Brusel 2006.

³ Komisia európskych spoločenstiev. *Zelená kniha o európskom programe na ochranu najdôležitejšej infraštruktúry*. Brusel, 17.11.2005, KOM (2005) 576 as final amendment. [on line]. [cit. 2013. 6. 16]. Available on: http://eur-lex.europa.eu/LexUriServ/site/sk/com/2005/com2005_0576sk01.pdf.

⁴ Komisia európskych spoločenstiev. *Zelená kniha o európskom programe na ochranu najdôležitejšej infraštruktúry*. Brusel, 17.11.2005, KOM(2005) 576 as final amendment. [on line]. [cit. 2013. 6. 16]. Available on: http://eur-lex.europa.eu/LexUriServ/site/sk/com/2005/com2005_0576sk01.pdf.

⁵ The Council Directives 2008/114/EC from December 8th 2008 on identification and marking European critical infrastructures and evaluation of the need to improve their (U. v. EÚ, L 345/75, 23.12.2008), Brussels 2008.

¹ *Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany*. [on line]. [2008-03-11]. Available on: <http://www.economy.gov.sk/pk/2130-2006-1000/ma.doc>.

the duties and the progress for each member state in identification of the elements of European critical infrastructure (hereinafter just "ECI"), which fulfills three cross-sectional and sector-specified criteria. It also set the cross-sectional criteria and subsectors of energetics and transport. It does not exclude the application even to other identified sectors by other member states.

If we sum it up, there were following threats identified in strategic documents within EU:

1. Terrorism;
2. Mass destruction weapons propagation;
3. Regional conflicts;
4. State operation failure;
5. Organized crime.

Presented threats are more or less related to every member state of EU and, thus, its critical infrastructure. Directive does not exclude identification and classification of national threats and security risks regarding the elements of the system of ECI or national elements of critical infrastructure. Concurrently, it creates a sufficient legal environment for the elaboration of own generally obligatory legal regulations modifying the identification and protection of sectors and elements of critical infrastructure. Particular states of EU responded to the directive in various ways. Some of them adopted unique laws, some of them did not elaborate the directive deeper.

Within the North Atlantic Treaty Organization, the problem of critical infrastructure is dealt with the Senior Civil Emergency Planning Committee (SCEPC) of NATO which authorized its subcommittees by the research on general aspects of the protection of critical infrastructure as well as possible consequences in case of the violation. They publish more documents and studies with the recommending character, while the choice of the approach to these recommendations and their overall implementation is in the operation of every member state.

3 Analysis of critical infrastructure protection in the Slovak Republic

The first document which established the term "critical infrastructure" and defined it for the conditions of the Slovak Republic is *the Concept of critical infrastructure in the Slovak Republic and its protection and defense*.⁶ Its resource is *Security strategy of the Slovak Republic*⁷ authorized by the National Council of the Slovak Republic which declares that the Slovak Republic guarantees the security of critical infrastructure prior to terrorist attacks and also focuses on the minimization of the vulnerability of information and communication systems, especially systems necessary for the safe performance of basic state operations.

It is necessary to be aware that except of the current threat number one – terrorism – there is a range of other natural risks and threats such as: floods, earthquakes, wide-area fires or new mutations of diseases. Further on, risks result from: usual operation of industry, operation of economy, production, transport, consumption of goods and services.

By now, *Law no. 319/2002 Col. of Laws on Defense of the Slovak Republic* as amended, dealt with this problem, where the term defense infrastructure has been applied, which according to § 26 sec. 1 of this law consists of: "*The complex of real estates, buildings and facilities, telecommunication, communication and transport systems, which serves to secure defense of the state at the time of war or warfare*".

Currently, we often meet the polemics among central authorities of public administration in Slovakia, of the members of academic grounds, regarding the identification of the element of the system of critical infrastructure. Even though, that *Law no. 45/2011 Col. of Laws on Critical Infrastructure* identifies such an elements (fulfills sector and sectional criteria), there is not more significant shift/development of the Slovak Republic in this field. It is worth to look for the reasons of this stagnation. Related central authorities of public administration under the coordination of Ministry of Defense of the Slovak Republic deal with the fields of critical infrastructure from 1999 (established *Coordination Center for the Protection of National Infrastructure - CPNI*)⁸, or from 2002 when the objects of personal importance (strategic objects of defense infrastructure, which, when damaged or destroyed, can limit the protection of the state's defense) and other important objects (objects of defense infrastructure, which, when damaged or destroyed, limit the activity of military forces or the operation of economy of the Slovak Republic) were identified by *Law no. 319/2002 Col. of the Law on the Defense of the Slovak Republic* as amended.

National Program for the Protection and Defense of Critical Infrastructure in the Slovak Republic (hereinafter just "National Program")⁹ adopted in 2007 determined the following nine sectors of critical infrastructure: *water, food, health, energetics, information and communication technologies* (hereinafter just "ICT"), *transport, public order and internal security, industry, financial sector*. The *Law no 45/2011 on Critical Infrastructure*¹⁰, which has been published in February 8th, 2011, adopted eight modified sectors. It adopted almost all sectors from the National Program, except of these sectors: *public order and internal security, food and financial sector*. The list has been extended in the sectors: *electronic communication and post office*.

If we sum it up, we deal with the problem of the protection of critical infrastructure in the Slovak Republic from 1999. It is 17 years so far and the result of so long effort is scant. Adopted government documents resulted just into *The Law on Critical Infrastructure* from 2011. In the following part, we characterize the sector of critical infrastructure based on factors.

3.1 Characteristics of particular sectors of critical infrastructure according to the factors

For the understanding of mutual causalities between particular sectors of critical infrastructure, it is necessary to deal with their relations (under which we can imagine mutual activity and dependency of these sectors). However, in order not just to state that sectors depend on each other, we need to assess the relationships between sectors quantitatively as well as their qualitative factors working between sectors.

We used "*point method*" for quantitative expression of the interaction we used, which consisted in counting the points added on the basis of the review of three various aspects of the interaction of each sector. It is obvious that the failure of any sector will result in the limitation in sectors depending in it. However, these consequences can present not only *restrictions*, but even *threats*. When analyzing, this characteristics of sector has significant importance, therefore, we need to evaluate this area from the point of view of particular sectors and register it as the first aspect.

When analyzing the mutual interaction, we considered three factors of the interaction of sector:

1. *Factor of the range of consequences* – the way, how one sector can influence other sectors, how other sector can threaten the failure of one sector;

⁶ Koncepcia kritickej infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany. Vláda Slovenskej republiky, uznesenie č. 120/2007, Bratislava, 2007.

⁷ *Bezpečnostná stratégia Slovenskej republiky*. Národná rada Slovenskej republiky, Bratislava, 2005.

⁸ The main task of the center was to develop and coordinate the activities necessary for the protection of critical infrastructure.

⁹ *Národný program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike*. [on line]. [cit. 28.6.2013]. Available on: <http://www.minv.sk/?ochrana-kritickej-infrastruktury>.

¹⁰ *Zákon č. 45/2011 Z. z. o kritickej infraštruktúre*.

2. *Factor of the number of stricken sectors* – we consider subjective revision; in case that sector A does not influence sector B, it is not proved that sector B won't influence sector A.
3. *Factor of the space-time* – time, during which the failure of one sector is proved in other sectors locally and globally.

We included all nine sectors (transport, water, food, health, energetics, ICT, public order and internal security, industry and financial sector) of critical infrastructure into this analysis according *National Program* adopted in 2007.

Based on the analysis of nine sectors according to three factors of interaction in Tables 1 – 4, we bring the results we got. In the following Table 1, we bring the range of interaction in sectors according to *restriction* and *threat*.

Table 1: Range of interaction in sectors

Sector	Restriction	Threat
Water	1	1
Food	1	1
Health	1	1
Energetics	1	1
Transport	1	0
ICT	1	1
Public order and internal security	1	0
Industry	1	1
Financial sector	1	1

We mark by:

1 point – existing relation in certain range,

0 point – non-existing relation in certain range.

Source: own elaboration based on the *National Program* data

In Table 2, as next aspect, we assessed sectors according to the number of other sectors of critical infrastructure influenced by them, as we added 1 point for each influences sector.

Table 2: Number of influenced sectors

Sector	Number of influenced sectors
Water	8
Food	3
Health	5
Energetics	8
Transport	5
ICT	8
Public order and internal security	2
Industry	7
Financial sector	8

Source: own elaboration based on the *National Program* data

As we can see in Table 2, the most influential sectors of critical infrastructure are: water, energetics, ICT and financial sector. The last aspect of revision is the factor of time-space.

In Table 3, we reviewed the speed of impact of failure of sector on other sectors in local and global measure. We added 2 points for fast impact, 1 point for slow impact.

Table 3: Evaluation of time-space factor

Sector	Time-space factor	
	Local	Global
Water	fast	fast
Food	slow	slow
Health	slow	slow
Energetics	fast	fast
Transport	fast	slow
ICT	fast	fast
Public order and internal security	fast	slow
Industry	slow	slow
Financial sector	slow	slow

Source: own elaboration based on the *National Program* data

Based on the elaborated analysis, we finally assessed particular sectors from the point of view of their significance for the operation of critical infrastructure as a whole. From the presented, we can further suppose the vulnerability of critical infrastructure in its particular sectors. After counting the points, we got the final Table 4 which says what range of the interaction between given sector and other sectors is, thus what share in the operation of critical infrastructure as a whole can we predict.

Table 4: Final assessment of analysis according to sectors

Sector	Number of points
Water	14
Food	7
Health	9
Energetics	14
Transport	9
ICT	14
Public order and internal security	6
Industry	11
Financial sector	12

Source: own elaboration based on the *National Program* data

Presented information are especially significant within the questions of the protection of critical infrastructure against terrorism. Any of the sectors cannot be neglected, neither underestimated. Analysis supposes how to choose priorities and the rate of investments to the protection of sector correctly. It requests stability, partnership cooperation among owners and operators of critical infrastructure and representatives of the governments of member states. The protection of particular elements of critical infrastructure is fully organized by legal person, owner or operator as a part of own arrangements for the protection of property. Governments of member states are responsible for the coordination of important political responses to the needs of the protection of critical infrastructure.

3.2 Comparison of the Slovak Republic to other V4 countries

For the purpose of verification of practical way of understanding the sensitive elements of critical infrastructure and its sectors, we did their comparison at the level of the Slovak Republic in comparison to other V4 countries (the Czech Republic, Poland and Hungary). The aim was not to name the right and complete names of the sectors of critical infrastructure of particular countries. The goal was to point out the sectors of critical infrastructure, which V4 countries consider important at national level. Other goal was to find out whether particular V4 countries are similar regarding their security threats and social-economic conditions. At the same time, we wanted to identify the same or close sectors of critical infrastructure based on how the Slovak Republic has identified them. We can see the comparison of the sectors of critical infrastructure at the level of V4 countries in Table 5 (own elaboration based on Vidriková, Broc, 2013).

Table 5: Sectors of critical infrastructure of the Slovak Republic in comparison with V4 countries

Sector	SK	CZ	PL	H
Banking and financial sector	√	√	√	√
Industry	√	√	√	√
Energetics	√	√	√	√
Public health	√	√	√	√
Governmental institutions, security and state protection	√	√	√	√
ICT and telecommunication systems	√	√	√	√
Transport and logistics systems	√	√	√	√
Water supply	√	√	√	√
Food	√	√	√	√
Science and research				
Building infrastructure and facilities				
Information services, media, cultural landmarks			√	
Emergency services		√	√	
Storage of hazardous substances			√	
Mail and postal services	√			

We can see in Table 5 that the intersection of the sectors of V4 countries are sectors regarding Banking and financial sector; Energetics; Public health; ICT and telecommunication systems; Transport and logistics systems and Water supply. The closest common sector are even Governmental institutions, security and state protection, sector marked even as Public order and internal security. Further on, as we can see in Table 5, except of Slovakia, other stated V4 countries consider it as the sector of critical infrastructure. The reason why the Law on Critical Infrastructure in the Slovak Republic do not exclude this sector, is not known. Although, it was identified in the *National Program*.

From the analysis of security situation during five years (since adopting the *National Program* and adopting the *Law on Critical*

Infrastructure), there are no changes/amendments regarding the security interests of the Slovak Republic or the security environment of the Slovak Republic or security threats, which were identified in *the Security Strategy* which was approved by the National Council of the Slovak Republic on September 27th, 2005. Based on this statement, we can assume that the changes in determination of sectors were not conditional by this document. We suppose, that the scope in determination of the sectors of critical infrastructure should not be just the recommendations of *the Council Directives*, but even the questions solved within security strategy.

For the purpose of finding the possible motives in determination of sectors of critical infrastructure, it is possible to use even causal relations. One of the possibilities of the research is even the use of cluster hierarchical agglomeration analysis by the method of the closest neighbor. We could perform the analysis of social-economic data of selected states of EU, or V4 countries, in our case, by mentioned method as a certain time period (according to the topicality and availability of data).¹¹ For the purpose of finding the similarities of particular states (with the use of presented social-economic data), we could find out e.g. Euclidian distances expressing the range of relationship or similarity. However, it was not the goal of our article.

4 Discussion and conclusions

Infrastructure of Slovakia is similar to other countries: transport, energetics, chemical industry, defense industry, production and transport of dangerous goods, information technologies and telecommunication, financial institutions and insurance companies, drinking water supply, food supply, health and emergency services, waste removal, state and public administration, courts, police, armed forces, customs administration, media, research and education institutions and national cultural landmarks. Every part of infrastructure falls under the sphere of some of central state authorities and bodies, or bodies of local administration.¹²

Law no 45/2011 Col. of Law on the Protection of Critical Infrastructure creates the basic scope for the solution of the problem of the protection of critical infrastructure in the Slovak Republic. It objectively codifies new terminology and sets the parts of critical infrastructure. It has a priori goal focused on improving present protection of a part of critical infrastructure, which when corrupted or damaged could cause serious negative consequences only on regular operation of economy of the Slovak Republic.¹³

As a consequence, that the law sets the organization and the operation only of the bodies of public administration within a division of critical infrastructure, it does not set the obligatory criteria for the determination of an element of sector of critical infrastructure for the element of critical infrastructure, does not set the tools for the protection and defense of elements of critical infrastructure, the level of the security of particular components will vary and the overall level of the protection of critical infrastructure, except of the objects of defense infrastructure, will be insufficient.

The tasks of the management are of different character, range and significance at particular levels of management and during particular periods of time of crisis situation solution. That is the reason why particular levels of crisis management differ to each other in contents and range of fulfilled tasks, the range of

competencies and the possibilities of the use of powers and means, as well as the relationship to particular periods of crisis situations.¹⁴

Therefore, these levels of management are absent in identification and protection of critical infrastructure:

1. *International* – multinational level of crisis management (UN, NATO, OSCE, EU);
2. *National* – state level of crisis management;
3. *Regional* – county, district level of crisis management;
4. *Local* – municipal, metropolitan level of crisis management.

What does it consist of or what is the source of retardation factors which impede the Slovak Republic from more significant progress in this field? We think that one of possible reasons can be the question of real determination of element of critical infrastructure and its protection. Objects of personal importance and other important objects classified to defense infrastructure have practical identification solved. Even though, they are the part of the system of critical infrastructure, follow unique legal regulation, thus the law on critical infrastructure relates to it just marginally. Set sectors in reference with central authorities /organs of public administration of the Slovak Republic should help the identification of other elements of critical infrastructure by the Law on Critical Infrastructure. Their protection should be focused primarily on security threats set by the state.

Decreasing the vulnerability of the Slovak Republic is task of long-term character and national program together with adopted conception should be the first step to increasing the preparedness of the Slovak Republic to face mentioned threats. Next significant step should be the preparation of the legislation and elaboration of the program itself to particular tasks with quantification of necessary financial impacts on state budget.

Literature:

1. *Bezpečnostná stratégia Slovenskej republiky*. Bratislava: Národná rada Slovenskej republiky, 2005.
2. Hendl, J.: *Přehled statistických metod. Analýza a metaanalýza dat*. Praha: Portá, 2009. 696 p.
3. Hofreiter, L.: Ochrana kritickéj infraštruktúry ako problém národnej bezpečnosti. In *Národná a medzinárodná bezpečnosť 2013*. 4. *Medzinárodná vedecká konferencia. Zborník vedeckých a odborných prác*. Liptovský Mikuláš: Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2013. ISBN 978-80-8040-475-8.
4. *Komisia európskych spoločností. Zelená kniha o európskom programe na ochranu najdôležitejšej infraštruktúry*. Brusel, 17.11.2005, KOM(2005) 576 v konečnom znení. [on line]. [cit. 2013. 6. 16]. Available on: http://eur-lex.europa.eu/LexUriSe rv/site/sk/com/2005/com2005_0576sk01.pdf.
5. *Koncepcia kritickéj infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany*. [on line]. [2008-03-11]. Available on: <http://www.economy.gov.sk/pk/2130-2006-1000/ma.doc>
6. *Koncepcia kritickéj infraštruktúry v Slovenskej republike a spôsob jej ochrany a obrany*. Vláda Slovenskej republiky, uznesenie č. 120/2007, Bratislava 2007.
7. Marchevka, P.: Súčasnosť a budúcnosť kritickéj infraštruktúry v Slovenskej republike. In *Riešenie regionálnych disparít a nerovnovážnych stavov v prírodnom a hospodárskom prostredí. Zborník z vedeckej konferencie s medzinárodnou účasťou*. Veľká Lomnica: Slovenská akadémia pôdohospodárskych vied, 2009. ISBN 978-80-89458-02-8.
8. *Národný program pre ochranu a obranu kritickéj infraštruktúry v Slovenskej republike*. [on line]. [cit. 28.6.2013]. Available on: <http://www.minv.sk/?ochrana-kritickej-infrastruk tury>.

¹¹ Hendl, J.: *Přehled statistických metod. Analýza a metaanalýza dat*. Praha : Portá, 2009, pp. 696.

¹² Marchevka, P.: Súčasnosť a budúcnosť kritickéj infraštruktúry v Slovenskej republike. In *Riešenie regionálnych disparít a nerovnovážnych stavov v prírodnom a hospodárskom prostredí. Zborník z vedeckej konferencie s medzinárodnou účasťou*. Veľká Lomnica: Slovenská akadémia pôdohospodárskych vied, 2009. ISBN 978-80-89458-02-8.

¹³ Tarcsi, G.: Obranné plánovanie v kontexte bezpečnostného systému štátu. In *Národná a medzinárodná bezpečnosť 2013*. 4. *Medzinárodná vedecká konferencia. Zborník vedeckých a odborných prác*. Liptovský Mikuláš: Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2013. ISBN 978-80-8040-475-8.

¹⁴ Hofreiter, L.: Ochrana kritickéj infraštruktúry ako problém národnej bezpečnosti. In *Národná a medzinárodná bezpečnosť 2013*. 4. *Medzinárodná vedecká konferencia. Zborník vedeckých a odborných prác*. Liptovský Mikuláš: Akadémia ozbrojených síl generála Milana Rastislava Štefánika (2013). ISBN 978-80-8040-475-8.

9. *Predbežné stanovisko k návrhu smernice Rady o identifikácii a označení európskej kritickej infraštruktúry a o zhodnotení potreby zlepšiť jej ochranu – EÚ. Tlač: 2006/0276 (CNS), Brusel 2006.*

10. Tarcsi, G.: Obranné plánovanie v kontexte bezpečnostného systému štátu. In *Národná a medzinárodná bezpečnosť 2013. 4. Medzinárodná vedecká konferencia. Zborník vedeckých a odborných prác.* Liptovský Mikuláš: Akadémia ozbrojených síl generála Milana Rastislava Štefánika, 2013. ISBN 978-80-8040-475-8.

11. The Council Directives 2008/114/EC from December 8th 2008 on identification and marking European critical infrastructures and evaluation of the need to improve their (U. v. EU, L 345/75, 23.12.2008), Brussels 2008.

12. Vidriková, D., Broc, K.: Kritická analýza prístupov k problematike ochrany kritickej infraštruktúry v Slovenskej republike. In *Krízový manažment - 2/2013.* Žilina: Žilinská univerzita v Žiline, Fakulta špeciálneho inžinierstva.

13. Zákon č. 45/2011 Z. z. o kritickej infraštruktúre.

14. www.minv.sk.

Primary Paper Section: A

Secondary Paper Section: AG, AQ