Cybersecurity in the Context of Criminal Law Protection of the State Security and Sectors of Critical Infrastructure

Miroslav KELEMEN[1], Stanislav SZABO[2], Iveta VAJDOVÁ[3]

[1]Department of Flight Preparation, Faculty of Aeronautics, Technical University in Kosice, Rampová 7, 041 21 Kosice, Slovakia
[2,3]Department of Air Transport Management, Faculty of Aeronautics, Technical University in Kosice, Rampová 7, 041 21 Kosice, Slovakia
E-mails: [1]miroslav.kelemen@gmail.com; [2]stanislav.szabo@tuke.sk; [3]iveta.vajdova@tuke.sk

Abstract

The protection of state security by the legal standards of the criminal law is one of the key, the legally protected interests including the cybersecurity in the sectors of critical infrastructure transport (road, air transport, ship, and rail), electronic communications, energy, information and communication technologies, post, industry, water and atmosphere, health. Today's empirical empowerment confirms that the security is a significant multidimensional factor of the quality of society and citizen's life, which we have to systematically examine, forecast and ensure. The contribution presents the defined security interests of the state in the framework of new strategic documents of the Slovak Republic in the comparison with the current standards of the criminal law for the protection of state security within the material and non-material components of the defence potential of the state.

KEY WORDS: *cybersecurity, legal norms, criminal law, protection, protected interests, state security, cooperation*

1. Introduction

The protection of state security by the legal standards of the criminal law is one of the key, the legally protected interests including the cybersecurity in the sectors of critical infrastructure: transport (road, air transport, ship, and rail), electronic communications, energy, information and communication technologies, post, industry, water and atmosphere, health. An important period of strengthening the security and defense capabilities of the Slovak Republic is the practical implementation of the provisions of the New Cyber Security Act of 30 January 2018 [1]. The draft of law on the Cyber Security and Amendments to some acts no. 69/2018 Coll. was prepared by the National Security Office of the Slovak Republic in cooperation with the Deputy Prime Minister for Investment and Informatization. We also regard the cyber-security issues as an important part of protecting state security within the material and immaterial components of defense and protection.

The resilience of networks and the stability of the information system is a prerequisite for a smooth and the uninterrupted functioning of the EU internal market and a prerequisite for the credible international cooperation. Networks and information systems play a crucial role in free movement and are often interconnected and connected to the Internet as a global tool. The disruption of the network and information systems in one Member State therefore affects other Member States and the EU as a whole, explained the key issue the National Security Authority [2].

2. Method of Investigation

This problem cannot be solved by one country in a comprehensive way, but a rigorous and professional international co-operation that relies on high-quality national capabilities.

The New Act transposes into the Slovak legal order a European directive on measures to ensure a high common level of network security and information systems in the Union (NIS). The NIS Directive is the first pan-European legislative regulation on cyber security that aims to strengthen the competences of the relevant national authorities, increases their mutual coordination and constitutes safety conditions for key sectors as a methodological guide for Member States. This article uses the historical and content legal analysis to explore the issue.

3. Investigation Results

The experience of the security community confirms that the level of protection was heterogeneous and incompatible due to the mutual inconsistency of the current legal norms in which the cyber-security issue was solved partially in the conditions of the Slovak Republic, thus failing to reach the required level of EU member states. As a result, there is no

Corresponding author.
E-mail address: 1miroslav.kelemen@gmail.com

adequate level of cyber security against existing threats, resulting in irreparable losses and disruptions in the credibility of organizations and the state. The goal of cyber security is therefore to minimize the potential for such threats and, in the event of the consequences, to minimize their impact, which is a prerequisite for both public administration and the private sphere.

The article presents:

- Analysis of selected praxeological problems;
- The legislative solutions of selected problems of cyber security;
- The cybersecurity as part of the security interests of the state protected by the criminal law standards.

Already during the legislative process LP-2017-407, commenting on the draft law, 706 comments came, of which 236 were essential. From the analysis of the draft legal standard and from the comments, the following selected key outputs resulted:

– The proposal has repeatedly identified vague legal concepts which it does not itself define and which are not settled in the current legislation. A request was made for the law-bearer to reduce the uncertainty of these concepts in accordance with the applicable Legislative Rules of the Slovak Government in order to prevent later interpretative problems in the application of the Act after its approval;

– The uncertainty of terms brings other problems in application practice;

– The draft law was objected. "In order to ensure fulfillment of the tasks under this Act, the Office may conclude a cooperation agreement with a natural person or a legal person. The cooperation agreement must include a specific form and terms of cooperation. The cooperation agreement is not necessarily a public contract ". It completely disrupted any security measures of the basic service provider in the area of personnel and physical security. According to the proposal, any person who will have an agreement with the Authority will have the power to learn about any information. If the applicant remains in a position to conclude a cooperation agreement, it is necessary to specify the specific conditions that a natural person or a legal person as a contracting party must fulfill, including a requirement to demonstrate security and technical standards, qualifications and skills in cyber security. Also, a written agreement should specify the extent of the information that such a person will be entitled to acquaint himself, with the basic service operator and a duty to keep confidential about the facts that that person has become aware of when implementing such an agreement. Also, if the agreement is not excluded from mandatory disclosure of contracts under Act No. 211/2000 Coll. as subsequently amended, the non-disclosure of this Agreement constitutes a breach of this Act. However, in the case of unpublished contracts, exist the obligation to disclose information on its conclusion (the so-called notification obligation);

– The continuing problem is to reach a compliance with other applicable legal standards in the case of new legal standards;

– The draft law was objected that "The officers of the Office shall, in relation to the performance of the control and to the extent necessary for its execution, to enter the communication and information systems to the level of the System Administrator, including the authority to temporarily change the Hardware or Software Configuration". The proposed wording of § 29 par. 6 of the draft law provides inadequate competencies to the Office's officers, including inappropriate interventions in communication and information systems. Under § 3 par. 4 of Act 275/2006 Coll. on the information systems of the public administration of the obliged persons, who are administrators of the information system, are obliged to ensure the smooth, secure and reliable operation of the public administration information systems in their administration, including organizational, professional and technical security, and to provide the public administration information system against abuse. In the event of a change in the hardware or software configuration, the assurance of these obligations may be compromised or directly impaired. At the same time, may violation of the provisions of Act no. 122/2013 Coll. on the protection of personal data, since the entitlement to enter the information system at the level of the system administrator may result in the disclosure of the personal data of the persons concerned, provided that personal information is processed in that information system. If the proposed wording of Article § 29 par. 6 of the Cyber Security Act will not be abolished, the IS administrator cannot ensure the fulfillment of the obligations imposed by Act no. 275/2006 Coll. The draft law would also determine who will be responsible for malfunction or disruption IS functionality after changing the hardware or software configuration, and who will bear the adverse consequences associated with it, including damages caused to third parties;

– Definition of a cyber security incident in § 3 (f) of the draft law largely overlaps with the facts of the offenses set forth in § 247 - § 247d of the Criminal Code. However, the bill does not refer to criminal obligations in this provision or elsewhere, it does not refer to obligations in criminal proceedings and does not look at several places, such as the necessity of providing evidence (the response to a security incident should be conducted in such a way as to avoid devaluation evidence of subsequent criminal proceedings). This is a complexity of the assessment of the proposed regulation[4].

Legislative solution of selected outcomes and problems:

– In order to ensure fulfillment of the tasks under this Act, the Office may conclude a written cooperation agreement with a natural person. The cooperation agreement must contain the specific form and terms of the cooperation and the natural person must be entitled to have access to classified information of the relevant classification level if required to do so;

– When exercising control over observance of the provisions of this Act and its implementing regulations, the Office shall proceed according to the basic rules of the control activity stipulated by a special regulation. For the purpose of performing the control, the basic service provider and the digital service provider have the rights and obligations of the audited entity under a separate regulation. The Office will check the Digital Service Provider if it is reasonable to suspect

that the digital service provider does not meet the requirements of this Act;

– A cyber security incident is any event that has a negative impact on cyber security due to a disruption of network and information security or a breach of security policy or a binding methodology, or which has the following consequences:

1. loss of data confidentiality, destruction of data or compromise of system integrity,
2. limit or deny the availability of a basic service or digital service,
3. high probability of compromising basic service or digital service activities, or
4. threats to security of information.

4. Cybernetic Security as Part of the Security Interests of the State Protected by Criminal Law Standards

The Slovak Republic in the process of guaranteeing security, creating a security strategy, building its security policy and creating an adequate security system is based on historical experience, available scientific analyzes and forecasts of the security situation in the world, Europe, the Central European Space and its territory [5].

Company attention has always focused on two basic areas of security, namely internal security and external security, and the corresponding sources of threats that have been basically presented by natural and civilization sources of threats or combinations of them. It is precisely the area of civilization threats associated with armed violence that has become an area of great development in mankind's historical development which has provided humanity with instruments of self-destruction, destruction of the world, and human civilization. The state uses the available tools of the security system to eliminate them, in the context of collective defense and safeguard of protected interests, in individual security sectors.

The protection of state security by the standards of criminal law is one of the key, legally protected interests. Today's empirical empowerment confirms that security is a significant multidimensional factor of the quality of society and citizen's life, which we have to systematically examine, forecast and ensure.

The Slovak Republic is currently experiencing a new stage of defining security interests from its autonomy, which mirrors the newly formed Security Strategy of the Slovak Republic under the authority of the Ministry of Foreign Affairs and European Affairs of the Slovak Republic and their implementation in parallel strategic documents such as the Defense Strategy of the Slovak Republic and the Military Strategy of the Slovak Republic, in charge of the Ministry of Defense of the Slovak Republic. The paper presents an introductory part of the first stage of the scientific assessment of the problem - the identification of security interests in the newly proposed Security Strategy of the SR (2017) and relevant standards of criminal law.

5. Discussion to Protect the Security Interests of the State

5.1. The current, initial situation

We perceive the security strategy as the theory and practice of the functioning of the State - the Community of States, aimed at achieving general and long-term security objectives. The previous approaches and opinions as well as the basic postulates of security and defense are contained in the Security Policy Documents, discussed and approved by the National Council of the Slovak Republic in September 2005 - "The Security Strategy of the Slovak Republic" and the "Defense Strategy of the Slovak Republic"[6]. Country Strategy Documents were in the process of updating to respond to changes in the security environment by all available means of the Slovak Republic, based on the "Strategic Defense Assessment" in 2011 and a broad professional and layout debate. A key pillar of our direction was the "Strategic Concept of Security and Defense of North Atlantic Treaty Organization Members", adopted by the Heads of State and Government in Lisbon in 2010, to replace the 1999 Strategic Alliance concept. "The strategic concept must offer freedom with regard to the foreseeable development but with sufficient precision to be useful to Allied officials responsible for policy implementation."[7].

The security interests of the Slovak Republic are based on the principle of guaranteeing the security of the citizen in accordance with international legal standards and constitution and fundamental civil and democratic values. The Slovak Republic recognizes and protects the values of freedom, peace, democracy, the legal state, law, and justice, pluralism, prosperity, solidarity, respect for human rights and freedoms[8].

Slovakia's security interests are based on the following values:

- Guaranteeing the security and protection of the fundamental human rights and freedoms of citizens;
- The guarantee of territorial integrity, sovereignty, the integrity of borders, political independence, identity;
- Democratic state establishment, legality and market economy;
- Economic, social, environmental and cultural development of society;
- Transatlantic Strategic Partnership, allied security;
- The effectiveness of the international organizations to which Slovakia is a member, supporting the expansion of NATO and the EU;
- Developing good partnerships and forms of cooperation with countries with which we share common interests;
- Promoting the spread of freedom and democracy, respect for human rights, rule of law, international order, peace and stability in the world.

5.2. New Reality

The new Security Strategy defines the security interests of the Slovak Republic, the basic objectives of the SR's security policy and the ways of their implementation in the various areas of Slovak security. Strengthening the interconnection of security interests with the expression of objectives, procedures and tools of the Slovak Security Policy in key areas of security in their enforcement, in line with a comprehensive approach to security (integrated action of a wide range of instruments). It also takes into account the limits of international organizations to address current issues, giving greater importance to regional organizations based on a common value basis and capacity development of the SR[9].

The expert community notes that, in view of the continuation of the draft of the Security Strategy of the SR of 2017 on the Security Strategy of the Slovak Republic in 2005, there has been no significant shift in the determination of security interests. The preservation of state existence, sovereignty and integrity, the development of democratic foundations and the rule of law, sustainable development and security remained almost identical in terms of text and order. Compared with the 2005 Slovak Republic Security Strategy, a good environment, cultural development and safe cyber space have been added. The security, stability and capability of the EU and NATO as a security interest have remained (this has brought about the continuation of the integration core - the response to the changes in the EU). If the Transatlantic Partnership in the 2005 Slovak Republic's Security Strategy was the fifth, in the document of 2017 is the penultimate one and it is included in the area of security and stability in the European Neighbourhood. [10]. The debate on the new Security Strategy of the Slovak Republic is expected by the end of 2017.

5.3. Material and non-material components of the defense potential of the state

The scientific examination of the material and non-material components of the defense potential of the state constitutes the starting platform for the assessment of the current scientific problem of criminal law protection of state security[11]. The historical experience of many war conflicts and the defense of autonomy, civil liberty and ideals of democracy as well as national values have confirmed the synergistic effect of bringing together material means of defense and patriotic conduct and determination to bring sacrifices for their freedom, the nation and the state. Even military science (defense and military science) considers military force and military potential to be a sum of the real material and spiritual possibilities of society, military coalitions that it uses to lead a war or other external or internal activities, in accordance with their security interests using armed forces.

Among the forms of development of unity of material and spiritual components of defense we can include:

- Facts that develop parts of the social consciousness, activity and commitment of citizens to actively engage in defensive activities;
- Facts that directly or indirectly create optimal conditions for defense and defense activities.
- The core of the material components of the defense potential of the state and its regions consists mainly of economic potential, military-economic potential, scientific potential, and military-scientific potential. Material potential is the source and foundation of the spiritual forces of the citizens and the armed forces. Spiritual elements are not the passive reflection of the material elements, nor their mechanical consequences. They always play an active role in changing the military force, in the efficiency of its use, increasing or decreasing the size or effectiveness of the material elements. While the material elements of the military force act on the enemy immediately physically and morally psychologically, the spiritual elements act primarily morally and psychologically.

5.4. Identification of criminal law protection of state security in the legal order of the Slovak Republic

Key instruments of criminal law protection of legitimate interests in the subject matter of investigation are the criminal law standards set out in a specific part of the Criminal Code[12], such as:

- Criminal offenses against property (primary legal regulation the fourth chapter of a special section of the Criminal Code: in the area of cybernetic security § 247-247d; property rights and interests are also protected in some other sections of a special part of the Criminal Code
- Criminal offenses against the Republic (legal regulation the Chapter 7 of the Criminal Code: § 311-320).
- Criminal offenses against the defense capacity, against civilian service, against service in the armed forces and against the defense of their homeland (legal regulation of the tenth chapter of a special section of the Criminal Code: § 379-392).
- Crime offenses against peace, against humanity, terrorist offenses, extremism and war crimes (legal regulation of the twelfth chapter of a special section of the Criminal Code).

Further scientific work within analyzing and assessing the potential of tools of criminal law protection of selected, legitimate interests in the subject matter, including cybernetic security of the state, will be the second and third stage of assessment and legal argumentation [13], the investigation of security law, the use of relevant legal case- as well as the experience of building the National Competence Center for Cyber Security of the Slovak Republic with the professional support of the "consortium" of the national ecosystem of cyber security from the academic, research and IT environment of the Slovak Republic (the Knowledge Alliance of Cyber Security of the Slovak Republic).

Conclusions

The following results of our investigation were obtained:

The protection of state security by the criminal law standards is one of the key of the legally protected interests, and the cyber security is an important and indispensable part of it. Today's social empiricism confirms us that security is an important multidimensional factor of the quality of society and citizen's life, which we must systematically examine, forecast and ensure.

The importance of the topic and the use of the national defense potential is mirrored in the latest initiative under the ongoing structured EU security and defense cooperation - PESCO, with the emphasis on the cooperation and strengthening the cybersecurity capabilities. Due to the topicality and multidisciplinary, the solution of the problem will be supported also in the form of a national research project with partners. The priority is given to the security in the critical infrastructure sectors such as the transport (road, air, water, and rail transport), electronic communications, energy, information and communication technologies, post, industry, water and atmosphere, and health.

Acknowledgements

This work was conducted within the framework of the Establish a national risk assessment and management of the security risks strategy. The authors are thankful for the cooperation provided by the Ministry of Foreign Affairs of the Slovak Republic.

References

1. Law no. č. 69/2018 on cybersecurity.
2. LP/2017/407 Dôvodová správa. p. 1. Available at: https://www.slov-lex.sk/legislativne-procesy/-/SK/dokumenty/LP-2017-407.
3. LP/2017/407 Doložka vybraných vplyvov. Dôvodová správa k návrhu zákona o kybernetickej bezpečnosti, p.8.
4. LP/2017/407 Vznesené pripomienky v rámci medzirezortného pripomienkového konania. [2018-03-04]. Available at: https://www.slov-lex.sk/legislativne-procesy/-/SK/LP/2017/407.
5. **Kelemen, M., Blažek, V.** Obrana a krízový manažment vo verejnej správe I. L. Mikuláš: AOS GMRŠ, 2011, 268 p. ISBN 978-80-8040-423-9.
6. LP/2017/627 Návrh Bezpečnostná stratégia Slovenskej republiky. [2018-03-04]. Available at: https://www.slov-lex.sk/legislativne-procesy/SK/LP/2017/627.
7. **Nečas, P., Kelemen, M.** War on insecurity: calling for effective strategy! : Scientific monograph. Kiev: The Center of Educational Literature, 2010. 158 p. ISBN 978-611-01-0023-6.
8. Art. 4 a 5 Bezpečnostnej stratégie SR 2005.
9. http://www.rokovania.sk/Rokovanie.aspx/BodRokovaniaDetail?idMaterial=25849. [2018-03-04].
10. **Nečej, E., Žilinčík, S.** Analýza návrhu Bezpečnostnej stratégie SR 2017: Porovnanie so strategickými dokumentmi Českej republiky a Poľskej republiky. Bratislava: STRATPOL – Strategic policy institute, 2017. 17 p. [2017-11-04]. Available at: http://stratpol.sk/wp-content/uploads/2017/08/BSSR-2017-SVK-v-final-OND-final.pdf, s.5.
11. **Kelemen, M., Blažek, V.** Obrana a krízový manažment vo verejnej správe I. L. Mikuláš: AOS GMRŠ, 2011, 268 p. ISBN 978-80-8040-423-9.
12. Law NR SR č. 300/2005 Coll. Criminal Code, as amended. Available at: http://www.epi.sk/zz/2005-300
13. **Mašľanyová, D**. et al. Trestné právo hmotné. Všeobecná a osobitná časť. 2. vyd. Plzeň: Aleš Čeněk, 2016. 623 p. ISBN 978-80-7380-618-7.
14. **Šimovček, I.** et al. Trestné právo procesné. Plzeň: Aleš Čeněk, 2016. 479 s. ISBN 978-80-7380-617-0
15. **Kelemen, M.** Problems of protected interests in the security sectors: Professional and criminal law aspects of the protection of interests. 2nd. suppl. ed. Banská Bystrica: Belianum. Matej Bel University Press, 2017. 112 p. ISBN 978-80-557-1261-1.