Miroslav Kelemen[*]
Volodymyr Polishchuk[**]
Martin Kelemen[***]
Andriy Polishchuk[****]

Reflection of the Act on Cybersecurity in aviation education

Abstract

The paper presents knowledge in the field of professional and legal implementation of building a strong cyber security of the European Union at the national level of a Member State, in the context of the implementation of a new legal norm on cyber security of the state. Part of the expert knowledge is the implementation of the law and the response to the praxeological problems of cyber security in the critical infrastructure sectors, including the TRANSPORT sector, resp. Air transport, as part of flight education.

Key words: hybrid threats, cyber security, protected interests, civil aviation, cybernetic security of aviation network traffic aviation education

* Prof. dr hab. Miroslav Kelemen, Technical University of Kosice, Faculty of Aeronautics, e–mail: miroslav.kelemen@tuke.sk.
** Prof. dr hab. Volodymyr Polishchuk, Faculty of Information Technology, Uzhgorod National University, Uzhgorod, Ukraine, volodymyr.polishchuk@uzhnu.edu.ua.
*** Martin Kelemen, Technical University of Kosice, Faculty of Aeronautics, martin.kelemen@tuke.sk.
**** Andriy Polishchuk, Faculty of Information Technology, Uzhgorod National University, Uzhgorod, Ukraine, andriy.polishchuk@uzhnu.edu.ua.

Introduction

Today's phenomenon is o.i. hybrid threats to society, in the public and private spheres, in the national and international dimension. Not only information activities have dangerous potential, but also cyber threats and attacks on selected entities / critical infrastructure / state. Cyber security has therefore become a priority for the international community.

In this area, the European Union set out in a joint communication to the European Parliament and the Council „Resilience, deterrence and defense: building strong cyber security for the EU". The document emphasizes the key idea that „Cyber security is essential for our prosperity and security"[1]. „Our future security depends on transforming our ability to protect the EU from cyber threats: civilian infrastructure as well as military capabilities depend on secure digital systems. This was recognized by the European Council in June 2017"[2] as well as in the Global Strategy for Foreign and Security Policy of the European Union[3].

At the national level of the Slovak Republic, we find a reaction in the form of the legal norm of Act no. 69/2018, Coll. On Cyber Security and on Amendments to Certain Acts, with effect from 1 April 2018. Professional and legal aspects of legally protected interests are therefore the subject of systematic and long-term examination[4].

The main legislative basis of the new law was the Strategy for Information Security in the Slovak Republic (Government Resolution no. 270/2008), the Legislative Intent of the Information Security Act (Government Resolution no. 136/2010) and Government Resolution no. 328/2015 on the Concept of Cyber Security. The draft Act on Cyber Security and on Amendments to Certain Acts was prepared by the National Security Office of the Slovak Republic in cooperation with the Office of the Deputy Prime Minister for Investments and Informatization.

1 Spoločné oznámenie Európskemu parlamentu a Rade „Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti EÚ", Brusel 13.9.2017, JOIN (2017) 450 final.
2 http://www.consilium.europa.eu/sk/press/press–releases/2017/06/23–euco–conclusions/.
3 http://europa.eu/globalstrategy/.
4 M. Kelemen, *Problems of protected interests in the security sectors: Professional and criminal law aspects of the protection of interests*, Banská Bystrica 2017, p. 11.

Problem identification

In its 2017 Joint Communication, the European Commission announced its intention to support the creation of a network of Cyber Security Competence Centers to stimulate the development and deployment of cyber security technologies. As a first step in this direction, the European Commission has mapped existing centers of expertise in cyber security (eg university department, research center, etc.).

The result of this mapping is the so-called „Cybersecurity Atlas" (index of existing EU cyber security centers). The aim of this Atlas is to become a valuable tool and reference for the cybersecurity community, which is looking for potential partners and pooling European resources.

According to the information provided by the Slovak Liaison Office for Research and Development in Brussels[5] in addition, as early as 2018, the european commission came up with a pilot project under Horizon 2020 to network national centers and create a new impetus in cyber security and technology development competences.

The solution to the problem at the national level is the identification of the „National Competence Center for Cyber Security of the Slovak Republic" at the National Security Office of the Slovak Republic, and possibly the creation of a consortium for its professional and legal support in implementing this agenda.

The resilience of networks and the stability of the information system is a prerequisite for the smooth and smooth functioning of the EU's internal market and a prerequisite for credible international cooperation. „Networks and information systems play a vital role in free movement and are often interconnected and interconnected by the Internet as a global tool. 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 of the new lawmaker, the National Security Office[6].

This problem cannot be comprehensively solved by one state, but by consistent and professional international cooperation based on high-quality national capabilities. The Cyber Security Act transposed into Slovak law the European Directive on measures to ensure a high common level of security of networks and information systems in the Union (NIS). The NIS Directive is the

5 Slovak Liaison Office for Research and Development, Brussels, e–mail 24. januára 2018.
6 LP/2017/407 *Dôvodová správa*, p. 1. URL: https://www.slov–lex.sk/legislativne–procesy/–/SK/dokumenty/LP–2017–407.

first pan-European cybersecurity legislation aimed at strengthening the powers of national competent authorities, increasing their coordination between them and providing security conditions for key sectors as a methodological guide for Member States.

Analysis of selected problems

The experience of the security community confirms that due to the mutual inconsistency of existing legal norms, in which the issue of cyber security was partially addressed in the Slovak Republic, the level of protection was diverse and incompatible, as a result of which it did not reach the required level of EU member states. The result is a failure to ensure an adequate level of cyber security against existing threats, resulting in irreparable losses and undermining the credibility of organizations and the state.

„The goal of cyber security is therefore to minimize the possibility of such threats and, in the event of the consequences, to minimize their impact, which is a necessary condition for both public administration and the private sector"[7].

Already during the legislative process LP-2017-407, the comment procedure on the draft law, 706 comments were received, of which 236 were fundamental comments on the draft law. Z analýzy návrhu právnej normy a z pripomienok vyplynuli nasledovné, vybrané zásadné výstupy: 1) the proposal repeatedly referred to vague legal concepts which it does not define itself and which are not established in the current legislation. There was a requirement that the submitter of the law, in accordance with the valid Legislative Rules of the Government of the Slovak Republic, reduce the degree of uncertainty of these terms in order to prevent later problems of interpretation in the application of the law after its approval; 2) uncertainty of concepts brings other problems in application practice; 3) the wording of the draft law was objected to "For the purposes of ensuring the fulfillment of tasks under this Act, the Office may enter into a cooperation agreement with a natural person or a legal entity. The cooperation agreement must contain the specific form and conditions of cooperation. The cooperation agreement is not a compulsorily published agreement". It completely violated any security measures of

7 LP/2017/407 Doložka vybraných vplyvov. *Dôvodová správa k návrhu zákona o kybernetickej bezpečnosti*, s. 8.

the basic service operator in the area of personnel and physical security. According to the proposal, any person who has entered into an agreement with the Office will have the competence to consult any information. If the applicant maintains the possibility of concluding a cooperation agreement, it is necessary to set out the specific conditions that a natural or legal person as a contracting party must meet, including the provision of the obligation to demonstrate knowledge of security and technical standards, qualifications and cyber security skills. The scope of the information with which such a person will be entitled to consult the basic service provider should also be laid down in a written agreement and the obligation to maintain confidentiality of the facts which that person has become aware of in the implementation of such an agreement should be laid down. Also, if the agreement is not excluded from the mandatory publication of contracts under Act no. 211/2000 Coll. as amended, non-disclosure of this agreement is a violation of this law. Even in the case of unpublished contracts, however, there is an obligation to publish information on its conclusion (the so-called notification obligation); 4) the remaining problem in the case of new legal norms is to achieve compliance with other valid legal norms; 5) objected to the bill that „Members of the Office are authorized to enter the communication and information systems to the level of system administrator, including the right to temporarily change the hardware or software configuration, in connection with the performance of control and to the extent necessary for its performance.". The proposed wording of § 29 par. 6 of the bill provides disproportionate competencies to members of the Office, including disproportionate interventions in communication and information systems. Pursuant to § 3 par. 4 of Act 275/2006 Coll. on public administration information systems, obligated persons who are IS administrators are obliged to ensure the smooth, secure and reliable operation of public administration information systems under their administration, including organizational, professional and technical support, and to secure the public administration information system against misuse. In the event of a change in hardware or software configuration, the provision of these obligations may be compromised or directly disrupted. At the same time, there may be a violation of the provisions of Act no. 122/2013 Coll. on the protection of personal data, as the right to enter the information system at the level of the system administrator may result in the disclosure of personal data of the data subjects, provided that personal data have been processed in the given information system. If the proposed wording of § 29 par. 6 of the Act on Cyber Security will not be repealed, the IS administrator cannot ensure the fulfillment

of obligations imposed on him by Act no. The bill should also determine who will be responsible for the malfunction or disruption of IS functionality after a change in hardware or software configuration and who will bear the adverse consequences associated with it, including compensation for damage caused to third parties; 6) definition of cyber security incident in § 3 letter f) of the draft law largely overlaps with the facts of the criminal offenses specified in § 247 – § 247d of the Criminal Code. However, the bill in this provision, or elsewhere, does not address the interaction with criminal proceedings, does not refer to obligations in criminal proceedings and does not take into account in several places, such as the need to secure evidence (response to a security incident should be conducted evidence for subsequent criminal proceedings). This is the complexity of the assessment of the proposed legislation[8].

Legislative solution of selected outputs and problems: 1) for the purposes of ensuring the fulfillment of tasks pursuant to this Act, the Office may enter into a written agreement on cooperation with a natural person. The cooperation agreement must contain the specific form and conditions of cooperation and the natural person must be entitled to become acquainted with classified information of the appropriate classification level, if the performance of tasks requires it; 2) in exercising control over compliance with the provisions of this Act and its implementing regulations, the Office shall proceed in accordance with the basic rules of control activities established by a special regulation. For the purposes of the inspection, the basic service operator and the digital service provider have the rights and obligations of the inspected entity pursuant to a special regulation. The Office shall carry out an inspection at the digital service provider if there is a reasonable suspicion that the digital service provider does not meet the requirements set out in this Act; 3) cyber security incident means any event which, as a result of a breach of network and information system security, or a breach of a security policy or binding methodology, has a negative impact on cyber security or which results in: a) loss of data confidentiality, destruction of data or breach of system integrity, b) restrict or deny the availability of a basic service or digital service, c) a high probability of compromising the activities of the basic service or the digital service – or threats to information security.

8 LP/2017/407 *Vznesené pripomienky v rámci medzirezortného pripomienkového konania* [cit.2018–03–04]. URL: https://www.slov–lex.sk/legislativne–procesy/–/SK/LP/2017/407.

Implementation of knowledge on cyber security in the transport sector, in the subsector Air transport, in aviation education

In addition to commercial successes, possible failures, modern air transport, its management and security also generate risks, such as potential danger to persons, property and other legally protected interests. The current danger, in the form of security threats, manifests itself in the form of security incidents or other anti-social phenomena, which may also have a criminal law level. Huge amount of data within the network operation of information systems and data repositories of civil aviation is an attraction and a potential target of cybercrime.

Cyber security in civil aviation operations is one of the important praxeological issues in examining the security and resilience of one of the elements of critical infrastructure. The topic has its limits and specifics at the national and European level. In an era of globalization, the free movement of people, goods, services, finance and information, its importance in international aviation, police and judicial cooperation is global. Cyberspace erases „natural boundaries and obstacles" to illegal activity on the road for political or ideological purposes, as well as material enrichment at the cost of violating the fundamental rights and freedoms of others or other legally protected interests in the public and private sectors. We have two introductory questions: what methodology and tool in the prevention of cybercrime we can use and what are the forensic purposes for surveillance in civil aviation network operations?

To process and examine the majority of the issue, we use an analytical-synthetic method based on critical thinking, shaped by the conceptual tools of „situational management of complex systems", i. situation management methodology[9].

The method of situational management in the field of cyber security of civil aviation network operations, as a complex adaptive system, creates preconditions on the basis of the application of information technologies and analytical activities, especially for: 1) the situational superiority of managers in decision-making compared to classical linear decision-making; 2) shortening the decision-making and management process in the management and operation of air traffic; 3) increasing the effectiveness of the intervention (s) in the system in case of deviation from the standards, or in case of non-compliance

9 L. Madarász, *Metodika situačného riadenia a jej aplikácie*, Košice 2003, s. 73.

with the required parameters; 4) providing up-to-date information (feedback) for the participants of the manager; 5) improving the quality of internal processes and the interoperability of components; 6) increasing the efficiency of the use of available human, financial, material and technical resources, within the national system, in cooperation with organizations abroad.

Findings from the implementation of knowledge and the law on cyber security within the agenda of safety and security in aviation are reflected in the study programs for the training of new aviation professionals: 1) in the study program of the first level of higher education (Bc., 3 years) „Air Transport Management", for the specialization „Security in Air Transport", primarily in subjects such as: a) Comprehensive airport protection, b)Security legislation, c) Safety equipment technology, d) Airport security documentation.; 2) in the study program of the second level of higher education (Ing., 2 years) „Air Transport Management", for the specialization „Safety and Security in Air Transport", primarily in subjects such as: a) Security management, b) Aviation operational safety, c) Security legislation, d) Air carrier security program, e) Solving aviation emergencies, f) Design of security systems in aviation; 3) in the study program of the third degree (Ph.D., internal study 3 years, external study 4 years) „Air traffic management", primarily in subjects such as: a) Air safety, b) Information systems in air transport, c) Airport security, d) Air traffic control, e) Sensors and electronics of security and safety systems, f) Integration and use of RPAS – Remotely Piloted Aircraft systems to protect objects against unauthorized systems, g) Aerospace surveillance and security systems.

Conclusion

The Slovak Republic in the process of guaranteeing security, creating a security strategy, creating 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, Central Europe and its own territory.

The company's attention has always been focused on two basic areas of security, namely internal security and external security, and the corresponding sources of threats, which in the basic understanding were presented mainly natural and civilized sources of threats or their combinations. It is precisely the area of civilizational threats associated with armed violence that has become, in the historical development of mankind, an area that has experienced

grandiose growth and provided humanity with tools for self-destruction, destruction of the world and human civilization. The state uses available tools of the security system to eliminate them, in the context of collective defense and securing protected interests, in individual security sectors.

At the national level, we expect that the work of the „National Competence Center for Cyber Security of the Slovak Republic" will ensure the implementation of EU intentions in the field of strengthening cybersecurity, as well as the implementation of the provisions of the Act on Cyber Security of the Slovak Republic: 1) Coordination and methodological guidance of activities from the level of national authority; 2) Promoting the synergistic effect of the potential of relevant actors at national level (within and outside the Cyber Security Knowledge Alliance); 3) Supporting research, technology innovation, production as well as cyber security education (at professional level, in civil society education, participation in the national curriculum at primary and secondary schools, implementation of prevention programs, university and other lifelong learning for critical sectors/subsectors) state infrastructure, etc.); 4) Developing training capacities and capabilities for forensic crime investigation and cyber prevention, and developing cybercriminology for theory and practice in critical infrastructure sectors.

Non-standard behavior in the civil aviation network operation can take the form of unlawful conduct in a specific cyberspace, with criminal liability for damage to protected interests. In the field of aviation security, the professional community recognizes 4 segments of vulnerability: 1) air traffic management / civil aviation network operation; 2) aeronautical / on-board control systems; 3) airport / internal information network, passport control systems, etc.; 4) the Internet of Things.

The detection, monitoring and analysis of such non-standard behavior in civil aviation network operations in the context of security incident prevention can act as an effective prevention tool in this cyberspace, for the following key purposes of forensic surveillance: 1) leakage of information; 2) network traffic tunneling; 3) anomalies indicating long-term port scanning and other attacker activities; 4) preparation for data theft and data theft; 5) unauthorized, automated data collection; 6) foreign equipment in the network; 7) violation of internal security rules.

To cope with these safety challenges even in aviation conditions, there is quality professional training in aviation education, which reflects the knowledge of science and real safety practice.

Bibliography

Joint Communication to the European Parliament and the Council „Resilience, deterrence and defense: building a strong EU cyber security", Brusel 13.9.2017, JOIN (2017) 450 final.
Kelemen M., *Problems of protected interests in the security sectors: Professional and criminal law aspects of the protection of interests*, Banská Bystrica 2017.
Slovak Liaison Office for Research and Development, Brussels, e-mail 24. januára 2018.
LP/2017/407 Explanatory memorandum. p. 1. Available on the internet: https://www.slov-lex.sk/legislativne-procesy/-/SK/dokumenty/LP-2017-407.
LP/2017/407 Selected effects clause. Explanatory memorandum to the bill on cyber security, p. 8.
LP/2017/407 Comments raised in the interdepartmental comment procedure [cit.2018-03-04]. Available on the internet: https://www.slov-lex.sk/legislativne-procesy/-/SK/LP/2017/407.
Madarász L, *Situation management methodology and its application*, Košice 2003.

Spostrzeżenia dotyczące ustawy o cyberbezpieczeństwie w edukacji lotniczej

Streszczenie

W artykule przedstawiono wiedzę na temat zawodowych i prawnych aspektów kształtowania silnego cyberbezpieczeństwa Unii Europejskiej na poziomie państwa członkowskiego, w kontekście wdrażania nowej normy prawnej dotyczącej cyberbezpieczeństwa państwa. Wiedza fachowa obejmuje wdrażanie przepisów prawa i reagowanie na prakseologiczne problemy cyberbezpieczeństwa w sektorach infrastruktury krytycznej, w tym w sektorze TRANSPORTU, a szczególnie transportu lotniczego, w ramach edukacji lotniczej.

Słowa kluczowe: zagrożenia hybrydowe, cyberbezpieczeństwo, interesy chronione, lotnictwo cywilne, cybernetyczne bezpieczeństwo ruchu sieciowego w lotnictwie, edukacja lotnicza