CYBER SECURITY IN THE CRITICAL INFRASTRUCTURE SECTOR INCLUDING CIVIL AVIATION – KNOWLEDGE ALLIANCE PROJECT

Antoni OLAK
Wyższa Szkoła Biznesu i Przedsiębiorczości w Ostrowcu Świętokrzyskim
Jaroslav JEVČÁK*, Ladislav CHOMA
Faculty of Aeronautics of Technical University of Košice, the Slovak Republic
**Corresponding author.* E-mail: jaroslav.jevcak@syteli.sk

Summary. The specialized article presents the project intent and input analysis in the field of professional and legal implementation of the building of the strong computer security of the European Union at the national level of the member state in the context of the implementation of the new legal norm on the cyber security of the state. Part of the project consortium's activities would be the praxeological problems of cyber security in the critical infrastructure sectors, including the TRANSPORT sector, respectively the Air Transport.

Keywords: hybrid threats; cybernetic security; protected interests and subjects; civil aviation

1. INTRODUCTION

The phenomenon of today are the hybrid threats to the society, the public and private sphere, the national and international dimension. Dangerous potential has not only information activities but also cyber threats and attacks on selected entities / critical infrastructure / state. Cybernetic security has become a priority for the international community.

The European Union in this area plans to implement the intentions expressed in the Joint Communication to the European Parliament and the Council "Resilience, deterrence and defense: building strong cyber security for the EU". The document highlights the key idea that "The Cyber security is an essential to our prosperity and security" [1]. "Our future security depends on the transformation of our ability to protect the EU from the cyber threats: the civilian infrastructures as well as the military capabilities depend on the secure digital systems, as recognized by the European Council in June 2017" [2] as well as in the global strategy for the foreign and security policy of the European Union [3].

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

2. PROBLEM IDENTIFICATION

In its 2017‘s joint Communication, the European Commission announced its intention to support the establishment of a network of computer security competence centers to stimulate the development and deployment of the cyber security technologies. As a first step in this direction, the European Commission has mapped the existing cyber security expertise centers (e.g. the University Departments, the Research Centers, etc.).

The results of this mapping will be translated into the so-called "the Cybersecurity Atlas" (the existing EU Cyber Security Center index), which will be publicly available. The aim of this „Atlas“ is

to become a valuable tool and reference for the cyber security community that seeks potential partners and brings together European resources.

According to information provided to Slovakia by the Liaison Office for Research and Development in Brussels [5]. In addition, the European Commission comes with a Horizon 2020 pilot project in 2018 to connect national centers to the network and create a new impetus for cyber security and technology development competences.

The solution of the problem at the national level is, according to our intention, to identify the "National Competence Center for Cyber Security of the Slovak Republic" and to create a consortium for its professional and legal support for the implementation of this agenda.

Our knowledge base for the finding of solutions to the subdivision of Air transport is also supported by the results of exploring the synergy of civil, national, international security and the new challenges of military science [6], as well as the exploring procedural and situational management of an asymmetric opponent as a possible effective access implementation tool action-based operations to overcome the current and future security problems, the comprehensive use of state-owned instruments in the defense of its security interests [7], and the development of the Slovak Air Force's capabilities for an effective participation in the allied air operations [8]. The issue finds partial mirroring as well as complex solutions within the airport security management [9].

3. OBJECTIVE AND METHODOLOGY OF PROBLEM SOLVING

The National Competence Center for Cyber Security in the Slovak Republic could probably be the workplace of the National Security Authority of the Slovak Republic (decision belongs to the state).

The aim of the new project entitled "the Knowledge Alliance of Cyber Security – the Consortium for the Professional and Legal Support of the National Competence Center for Cyber Security of the Slovak Republic" is to create a consortium for professional and legal support and implementation of the agenda.

The structure of the consortium's partners should consist of:

- Actors in the public sphere;
- Actors in the private sphere.

The consortium's partner character should represent:

- Academic community (primarily in ICT education - Information and communication technologies, law);
- Public and private research organizations;
- Manufacturers and system integrators in ICT, security technologies;
- Relevant public authorities;
- Representatives of the critical infrastructure sector of the state (including universities that prepare experts for individual sectors / sub-sectors of the state KI, e.g. TRANSPORT / Air transport);
- The security and legal community;
- SMEs in the field of security education, cyber industry.

A key tool for the examining the issue will be the application of the situational management method in the area of cyber security and the protection of economic mobilization / critical infrastructure subjects. Our inspiration to address the issue is also in the security monitoring and network traffic analysis [10].

4. SELECTED PROBLEMS IN THE TRANSPORT SECTOR, SUBSECTOR AIR TRANSPORT AND ACADEMIC DISCUSSION

The selected cyber security issues in the TRANSPORT sector, in the sub-sector Air transport: both the economic mobilization / critical infrastructure subjects

The modern air transport, its management and security, generate, in addition to the commercial successes, the potential failures, risks as a potential danger to persons, property and the other legitimate interests. The current danger, in the form of security threats, is manifested in the form of security incidents or other anti-social phenomena, which may also have a criminal law platform. The huge amount of data in the network traffic of information systems and data storages of civil aviation is an attraction and potential target of the cybercrime.

The cybernetic security in the civil aviation is one of the most important praxeological issues of examining the protection and resilience of one of the elements of critical infrastructure. The topic has its limits and specifics at the national and European level. At the time of globalization, the free movement of people, goods, services, finances and information, its importance in the international aviation, the police and judicial cooperation is worldwide. The cybernetic space is wiping out the "natural boundaries and obstacles" of unlawful conduct on the road for political or ideological purposes, as well as the material enrichment at the cost of violating the fundamental rights and the freedoms of others or other legally protected interests in the public and private sectors. We have the two preliminary questions: what methodology and tool in the framework of cybercrime prevention can we use and what are forensic purposes for the oversight in the civil aviation network?

To analyze and explore the majority of the problem, we will use the analytical-synthetic method based on the critical thinking, shaped by the concept of "situational management of complex systems", ie the situational management methodology [11].

The method of situational management in the field of computerized security of civil aviation network as a complex adaptive system will create, based on the application of information technologies and analytical activities, the prerequisites especially for:

- situational predominance of decision-makers versus the classical linear decision-making,
- reduction of the decision and control process in the management and the provision of air traffic,
- increasing the effectiveness of the intervention (s) in the system in the case of deviations from the standards, or in the case of failure of the required parameters,
- providing up-to-date information for the control,
- improving the quality of internal processes and interoperability of components,
- increasing the efficiency of the available human, financial, material and technical resources, within the national system, in cooperation with organizations abroad.

Research and development on a given topic in an international scale

The emergence of a comprehensive concept of critical infrastructure and its protection within the EU was set in 2004 at the European Council, which asked the European Commission to prepare an overall strategy known as "Critical Infrastructure Protection in the Fight against Terrorism". The document that specifically addresses the issue of Critical infrastructure is the so-called "Green Paper on a European Program for Critical Infrastructure Protection" (2005). In 2008, "the Council Directive 2008/114 / EC on the identification and designation of the European Critical Infrastructures and the assessment of the need to improve their protection" came into the force. These documents and the EU's intention to address the scientific projects in the area of critical infrastructure protection, the border protection, under the Horizon 2020, influence the existing methods and results of solving teams' work at home and abroad.

Foreign R & D teams on the topic stabilized the following procedures to enable them to achieve partial results:

- *Methods and procedures for identifying the hazards and assessing the risks of major industrial and technological accidents*.

At present, the foreign teams have developed and are using the following methods, which have the potential to investigate negative impacts on human health, the environment and property:

Human Reliability Analysis (HRA)

Process Quantitative Risk Analysis (QRA) published in the "Purple Book",

IAEA: TEC-DOC-727

DOW: Fire & Explosion Index, Chemical Exposure Index.

- *Modeling impacts and effects of emergencies*

Impacts classify into the following groups:

impacts on persons,

impacts on the environment,

socio-economic impacts.

- *Specific risk analysis methodology for critical infrastructure*

From the point of view of these intentions, one of the good practices in the process of risk analysis is the use of methodology or, RAMCAP Plus All Hazards Risk and Resilience Prioritizing Critical Infrastructures Using the RAMCAP plus SM Approach, eg for the critical infrastructure elements in the energy sector.

- *Critical Infrastructure Protection Methodology* specifies the process of creating and improving the management system of the selected area of economic mobilization / critical infrastructure. The methodology developed includes standards for:

ensuring physical security,

ensuring information security in information systems,

ensuring administrative and personnel security,

ensuring the crisis management of the company's economic mobilization entity.

The innovation and originality of the selected research topics of the project team lies in the final product and it will represent:

- The comprehensive technical and information solutions for better protection of the health and life of persons (the general public and professionals, rescuers, guards, etc.) moving and working in a specific environment or near the elements of selected economic mobilization / critical infrastructure entities, in these areas.

- The resulting innovative product is also intended for a specific end-user target group such as:

The Border Police, the Ministry of Interior of the Slovak republic,

components of the Integrated Rescue System of the Slovak Republic,

the Mountain Rescue Service of the Slovak Republic,

the Forests of SR, public and private operators of critical infrastructure elements, etc.,

- the mobile information and technical equipment (product) will be used by the relevant entities within the Slovakia, within the European Union, primarily FRONTEX.

- a specific solution to the cyber-security in the civil aviation networks within the framework of The international airports forming the part of the Schengen area.

The description of the expected results in the terms of their international contribution and quality:

The main expected outcome is the innovative technical information solutions to improve the protection of a selected operator of economic mobilization / critical infrastructure subjects based on the use of spatial data obtained from the stationary and mobile terrestrial security technologies and the aircraft resources for other data digitization tools, GIS visualization, biometric research.

The new outcomes and established technology with the procedures will serve to accelerate and coordinate the response of responsible authorities to the disruptions or crisis situations in the area of the selected subject of economic mobilization and critical infrastructure. The use of project outputs have the transnational potential and application capabilities in particular in the protecting of the EU / Schengen area, the illegal migration, the cross-border organized crime with an emphasis on the trafficking in human beings, the drug crime, etc. The mobile spatial data collection solutions are also usable in the camps and reception centers for migrants, which will be the topic of the EU in the next period. The outputs can be offered to the Slovak Republic as the real technical assistance to solve this EU / FRONTEX agenda. The international airports have the unique position as the points of entry into the EU.

The part of the outputs will be the registration of intellectual property rights.

The potential for the applicability of planned outputs of the project and their possible social and economic benefits:

- the project brings its own unique solution of information and technical nature on the platform of security technologies and the mobile system solution of the transfer of dynamic image from the space of selected elements of economic mobilization /critical infrastructure entities of the Slovak Republic, with emphasis on the state borders, working in a specific environment, close to the elements of economic mobilization / critical infrastructure entities with the potential for the crisis and phenomenon of threatening persons or other protected interest in this area. The solution has a clear international potential and can be used to improve the protection of the Schengen borders of the EU and other parts of the EU internal border protection,
- the potential economic benefit of project outputs is „the measurable value" based on the number of the human lives saved in the fight against the trafficking in the human beings, the value of goods trapped freely on the EU internal market or the value of counterfeit goods that are imitations of the originals and damage trademarks and property rights. These data are by the country and statistics of border and the alien police and customs departments different. Within the EU, however, they accumulate the large values, respectively, causing the great social and economic damage.

5. CONCLUSION

Based on the security practice, we can agree with one of the EUROPOL's findings in its assessment that „the cyber threats come from both the state and non-state actors: often they are the criminal in nature, they are motivated by the profit but can also be of a political or strategic nature. The unclear boundaries between cybercrime and "traditional" crime, as criminals use the internet as a means of expanding their activities and at the same time as a resource for the finding of new methods and tools for the committing crimes "[12].

At the national level, we expect that the work of the "National Cyber Security Competence Center of the Slovak Republic" and „the Consortium for professional and legal support of the National Cyber Security Center of the Slovak Republic" will ensure the implementation of the EU cyber-security intentions and the implementation of the new cyber- Security of the Slovak Republic:

- coordination and methodological guidance of activities from the level of national authority;
- promoting a synergy effect of the potential of relevant actors at the national level (within and outside the Knowledge Alliance for Cyber Security);
- promoting the research, technology innovation, production, and the cyber security education (on a professional level, in the education of the public, participating in the national curriculum at the primary and secondary schools, the implementation of preventive programs, the university and other lifelong learning for the critical sectors / subsectors of the state infrastructure, etc.);
- developing of capacities and skills to learn forensic crime and cyber crime prevention, and the developing cyber criminology for theory and practice in critical infrastructure sectors.

The non-standard behaviors in the civil aviation network traffic may take the form of irregularities in a specific cyber space, with the criminal responsibility for damaging the protected interests. In the field of aviation safety, the expert community recognizes the 4 segments of vulnerability:

- air traffic management / civil aviation network operation,
- aviation / onboard control systems,
- airport / internal information network, passport control systems, etc.,
- Internet of Things.

The detection, tracking, and analysis of such nonstandard behavior in the civil aviation network traffic in the prevention of security incidents can act as an effective prevention tool in this cyber space for the following key purposes of forensic surveillance:

- leakage of information,
- tunneling of network traffic,
- anomalies demonstrating the long-term port scanning and other invasive activities,
- preparation for the data theft and data theft,

- unauthorized, automated data collection,
- foreign devices in the network,
- violation of the internal security rules.

Our basic concept for the implementation of the project in the Slovakia with the title "the Knowledge Alliance of Cyber Security – the Consortium for Professional and Legal Support of the National Competency Center of Cyber Security of the Slovak Republic" is based on the possibility of submitting a project at the Ministry of Education, Science, Research and Sport.

References

Journals:

[7] Adamčík, F. - Kelemen, M. Entity condition change of asymmetrical opponent. *Obrana a strategie.* Roč. 6, č. 1 (2006), p. 31.

[8] Kelemen, M. - Szabo, S. - Soušek, R. The development of the Slovak Air Force's air transport capabilities for joint logistics support operations. *Acta avionica : vedecký časopis*. Roč. 8, č. 12 (2006), p. 114.

[10] Dočkal, J. GreyCortex Mendel – bezpečnostní monitoring a analýza síťového provozu. *DSM*, č. 2/2016. s. 27-30.

Books:

[4] 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. p. 11.

[9] Szabo, S. - Němec, V. - Soušek, R. *Management bezpečnosti letiště*. 1. vyd. Brno: Akademické nakladatelství CERM, 2015. 165 s.

[11] Madarász, L. *Metodika situačného riadenia a jej aplikácie*. 1. vyd. Košice : ELFA TU Košice. 2003. s. 73.

Conference proceedings:

[6] Výrostek, J. - Kelemen, M. Synergia občianskej, národnej, medzinárodnej bezpečnosti a nové výzvy vojenskej vedy. In: *Bezpečné Slovensko a Európska únia : zborník príspevkov z 2. medzinárodnej vedeckej konferencie : 13.-14. november 2008*. Košice, 2008.

Web sides:

[1] *Spoločné oznámenie Európskemu parlamentu a Rady „Odolnosť, odrádzanie a obrana: budovanie silnej kybernetickej bezpečnosti EÚ"*, Brussels: European Commission. 2017. Available at: https://ec.europa.eu/transparency/regdoc/rep/10101/2017/SK/JOIN-2017-450-F1-SK-MAIN-PART-1.PDF

[2] *Euco-conclusions 1.* Brussels: European Commission. 2017. Available at: http://www.consilium.europa.eu/sk/press/press-releases/2017/06/23-euco-conclusions/

[3] *Euco-conclusions 2.* Brussels: European Commission. 2016. Available at: http://europa.eu/globalstrategy/

[5] *Slovak Liaison Office for Research and Development*, Brussels, internal e-mail 24. januára 2018.

[12] *Hodnotenie hrozieb závažnej a organizovanej trestnej činnosti*. Brussels: EUROPOL. 2017. Available at :https://www.europol.europa.eu/activities-services/main-reports/european-union-serious-and-organised-crime-threat-assessment-2017