Mechanics Transport Communications

ISSN 1312-3823 (print)
ISSN 2367-6620 (online)
volume 21, issue 3/1, 2023
Academic journal **http://www.mtc-aj.com** **article № 2440**

STRENGTHENING THE RESILIENCE OF CRITICAL SUBJECTS, WITH A FOCUS ON TRANSPORT AND HEALTH

Zdeněk Dvořák[1]
zdenek.dvorak@uniza.sk

University of Zilina, Faculty of Security Engineering
1.Maja 32, 010236 Zilina
SLOVAKIA

Key words: *Critical subject, critical actors, resilience, healthcare.*
Abstract: *The protection of important buildings and institutions has been going on in all parts of the world for hundreds of years. As new and new attacks have occurred, new and new ways of protecting, defending and reducing vulnerability have had to be found. The article contains a reflection on the current state of critical infrastructure protection in the context of the new European Directive 2557/2022. The aim of the article is to present the challenges for the coming years in the field of OKI, transformed in the future to increase the resilience of critical entities. The socially relevant sectors are transport and healthcare. People's lives depend on their functioning. Research in transport and healthcare is bringing new challenges. Researchers at the University of Žilina have long been working on dozens of topics on how to improve the functioning of transport and how to ensure good cooperation between transport and healthcare.*

INTRODUCTION

The opportunity to present the results of our own research activities at the international conference Transport 2023 is an excellent opportunity to present the latest trends in the field of resilience-building in transport. With the Slovak Research and Development Agency's current project focusing on healthcare facilities, we have been focusing on key challenges in recent years - presented by the terms critical actors, critical players, resilience and healthcare.

Developments in technology, local wars have been the main drivers for building protective objects in the last decades. The attack on the twin towers in New York kick-started a phase of defence and protection of critical infrastructure. Objects in the transport, energy and information and communication technology sectors were protected as a priority. The individual states of the world were developing their own concepts and legal standards for the protection of critical infrastructure. Slovakia, as a country within the European Union, prepared Act 45/2011 on critical infrastructure on the basis of EU Directive 114/2008. Expert groups met continuously to update the law to respond to current emerging threats. The

[1] Zdeněk Dvořák, prof. Ing. PhD., FBI UNIZA, 1. mája 32, 010 26 Žilina, SLOVAKIA, phone +421 41 513 6854, fax +421 41 513 6626, e-mail zdenek.dvorak@uniza.sk

security and protection of critical assets was and is the responsibility of states and state institutions. The privatisation of state-owned enterprises has resulted in some key infrastructure facilities becoming the property of private institutions. For this reason, legislators have had to lay down rules for the operation of objects that are critical infrastructure elements in particular [1] [2].

The conference's focus on transport provides an opportunity to exchange experiences and research results at international level. Research in the field of safety and security has a history of more than 50 years at our faculty. Our faculty was originally focused on the construction and reconstruction of road and rail transport and on the organisation of road and rail transport in specific conditions. We were the first institution in the former Czechoslovakia to create a software tool using the DMU200 digital terrain model. This was between 1990 and 1992. Later, the attention of researchers was focused on the creation of an integrated transport system for the event of war and martial law, tasks of this orientation were solved in the years 1995 - 2005. After 2010, our attention was directed to the protection of critical infrastructure in the transport sector. Transport as a system comprises five subsystems: transport infrastructure, transport means and equipment, control and information systems, people in transport operations and the legal-organisational framework. Each of the individual subsystems has a major impact on the overall resilience of transport. Research on resilience in the transport and energy sector has been addressed in a project of the Security Research of the Czech Republic called Resilienc2015. Within the project, the CIERA methodology was developed, tested and, after verification, certified.

Another milestone was the year 2020, since when the focus of experts and researchers has been on changing the philosophy from protecting critical infrastructure elements to strengthening the resilience of critical entities. In 2022, the European Directive 2557/2022 was published, giving a new role to all EU member states. The intention of this paper is to highlight the change of philosophy in the transport and healthcare sectors, where the impacts on the resilience of critical entities are highly socially perceived [3].

IN-DEPTH ANALYSIS OF INFORMATION SOURCES

The first part of any serious research is to find relevant sources of information, verify them and confront them with other sources. The methodological tool is an in-depth analysis of information sources. Nowadays, another challenge has emerged for researchers around the world, namely the use of artificial intelligence. However, many of the information sources used by artificial intelligence do not have the attributes of truthfulness and credibility. Therefore, any use of primary sources, not excluding artificial intelligence, must be confronted with one's own experience, with other sources and with critical thinking. A few years ago, sources from the Internet were considered relatively true and usable. The present is an era of hybrid warfare, conspiracies and lies at every turn. For this reason, it is crucial for the development of society that the academic sector is able to respond in real time to the populist pronouncements of politicians, new-age gurus and liars. Today, the most important task of scientists and researchers is to seek the truth, a truth that is objectively independent of worldview, colour or language. By analyzing scientific and institutional sources, we have come to the realization that the protection of critical infrastructure is a very topical issue, details in Table 1.

Table 1 Summary of the number of relevant publications [4] [5]

Database name	Keywords and number of records	
Web of Science	Critical infrastructure protection	4 584 x
Web of Science	Resilience of critical	17 264 x
Scopus	Critical infrastructure protection	4 923 x
Scopus	Resilience of critical	13 640 x
Scopus	Resilience of critical subject	517 x
CRZP	Kritická infraštruktúra (in Slovak)	139 x
CRPČ	Kritická infraštruktúra (in Slovak)	177 x
Google	Kritická infraštruktúra (in Slovak)	33 900 x

In the above context, it can be seen that the numbers of scientific outputs in publication databases are in the thousands to tens of thousands. In the database of final theses in the Slovak Republic there are currently 139 theses, of which 30 were bachelor's theses, 99 diploma theses and 10 dissertation theses. In the national database of publications of the Slovak Republic, out of 177 publications, there are 114 papers and chapters in books, 53 articles, 9 books and 1 book publication. A total of 150 publications were written under the authorship and co-authorship of the University of Žilina. From the above it can be concluded that the University of Žilina has a real knowledge base in the field of critical infrastructure protection in Slovakia.

THE PATH TO STRENGTHENING THE RESILIENCE OF CRITICAL ACTORS

The importance of building a resilient society is growing with the further development of science and technology and especially with the penetration of information and communication technologies into all areas of society. Modern society is more and more dependent on the functioning of ICT. Further development of society brings new challenges - security of persons, institutions, municipalities, cities, regions and states is a multi-dimensional issue built on the pillars of security, which are OSH, physical security, fire safety, information security, security of technical equipment and operational processes. The issue of critical infrastructure protection has been intensively developed since 2001. Until 2010, the challenge was to identify critical infrastructure elements at national and European level. In 2011-2018, the focus was on improving protection and creating comprehensive solutions for typological objects in order to reduce the vulnerability of critical infrastructure [6].

Since 2019, the issue of increasing the resilience not of critical objects but of critical entities has been intensively addressed at the international level (NATO, EU, H2020). This implies that the European Union, following the NATO model, has extended the scope from the protection of objects to the protection of entities - understanding by this also the personnel and other functions of the company/institution. The change from protection to resilience building is about a new understanding of priorities. The future is not about isolated measures to enhance the protection of a selected facility, but about setting the resilience of the whole system and all its subsystems. If we want to talk about transport resilience - then we need to address resilience of transport infrastructure, transport machinery and equipment, resilience of control and information systems and other transport sub-systems. With the adoption of the new Directive 2557/2002 on 14 December 2022, a new phase has been launched by the European Union, with a focus on strengthening the resilience of critical entities.

A similar approach was launched at the November 2022 NATO Defence and Foreign Ministers' meeting. Processes have now been set in motion that require changes in the legal environment of NATO and EU member states. It can be assumed that the first order of

business will be to update the lists of essential services in each member country. In parallel, a legislative process has already been started which will result in an amendment of the Critical Infrastructure Act in Slovakia and amendments to other relevant laws. It is the cooperation of academia, government, public administration, business partners and the non-profit sector that should bring all these processes to a successful conclusion. As a result, the system must be set up in such a way that all companies and institutions that will be critical entities have time to prepare relevant security plans. The question of who will develop new security plans and when, requiring a change in philosophy from protecting critical infrastructure to strengthening the resilience of critical entities, is now emerging as a major challenge.

The issue of critical entities only seemingly does not correspond to transportation. The opposite is true today, without working ICTs, we will not find a connection when we plan a trip, we will not buy a ticket, we will not have an e-ticket checked, packages will not be delivered, etc. Increasing the resilience of systems and services is just a different angle on the past and current delivery of essential services.

THE DIRECTION OF RESILIENCE RESEARCH IN TRANSPORT

As noted in Table 1, the issue of resilience enhancement is a very hot research topic. Hundreds to thousands of researchers around the world are engaged in developing theoretical foundations, improving methodologies, preparing libraries of measures, and creating appropriate information systems with the goal of having real-time expert systems set up to directly manage or support decision-making processes in enhancing the resilience of critical entities. The original focus on critical infrastructure objects/elements has been expanded to include support and development of skills and competences of personnel in critical entities. Methodologies, guidelines, standard procedures and other procedural documents are crucial for practice and can make a significant contribution to the real strengthening of transport resilience.

If before the focus was on the robustness, adaptability and recoverability of physical critical objects, now comes the time when these parts of resilience will be further addressed, but complemented by people, their selection, education, training and the organisation of the activities of companies and institutions. Educational institutions will thus have to provide in-demand forms of training (courses) for state and public institutions, for companies and other critical entities. Current students and graduates are trained in the subject Critical Infrastructure Protection in the engineering degree so that they are able to realistically develop detailed security plans for different types of objects. Close cooperation between academia and transport companies, state institutions such as the transport authority, the police and the Ministry of Transport appears to be crucial. I therefore recommend that colleagues from other countries follow our example and take up the topic of strengthening resilience comprehensively and contribute to society as a whole.

APPLICATION OF APPROPRIATE METHODOLOGIES TO HEALTH CARE SETTINGS

The issue of critical infrastructure resilience has been addressed in research projects since 2014. Several researchers of our faculty were invited to work on the RESILIENCE 2015 project, which was addressed within the framework of the Security Research of the Czech Republic. As part of a wide range of activities, we were included in the group that prepared, tested and had certified the CIERA methodology. The "Critical Infrastructure Elements Resilience Assessment (CIERA) Methodology" is 108 pages long. It has become a certified methodology in the Czech Republic and several transport and energy companies use it in real practice. Following the example of the Czech Republic, we have established a close cooperation and within the framework of the dissertations solved at our faculty we have

cooperated very well with the Railways of the Slovak Republic and with energy companies, see the dissertations of Hoterová and Chovančíková [8] [9].

The specifics of health care facilities are clear. In the case of hospitals, they are generally large areas with a rugged perimeter, accessible to vehicular traffic on several sides and to pedestrians elsewhere. When assessing the resilience of a critical entity, the first order of business is to select the facility that represents the most important asset for the hospital. It may be the headquarters, it may be the facility where operations are performed. In the next order, the relevant threats need to be identified and prioritised in the analysis of the internal and external environment and those that will be the focus of attention need to be selected. The actual application of the CIERA methodology is always linked to a specific threat, and the results of the methodology present the current state of the static threat at the time of its examination. This is an important note for hospitals because the intensity of a particular threat can change substantially in real time and can become a major concern for staff and patients.

DISCUSSION OF RESULTS

The real results of the research can be generalized as follows. Robustness and recoverability is focused on the technical part of resilience, the individual components are focused on detection capability, response capability, physical resilience, material, financial and human resources, increasing their level requires a system of continuous improvement, continuously spending money even in areas where money is "moribund".

The organisational part of resilience focuses on adaptability and is directed towards risk management, innovation, education and training of staff at all levels. In these areas, we have long experienced a lack of finance, a lack of people and a lack of innovation in Slovakia. For this reason, the tasks stemming from the new European directive aimed at increasing the resilience of critical entities will be a major challenge for hospital managements in the future and will require additional funding.

At this point, I would like to note that the support of specifically commissioned topics in security research is of significant benefit to the security of the country, to the security forces and to the national security council. Always in the run-up to parliamentary elections, we are looking for a way to convince the new incoming government that having our own security research and at the same time having a department of science and technology called Security Sciences is the minimum condition necessary for the functioning of the state in times of global, regional and local crises. External and internal threats today are changing very rapidly and only people, companies, institutions, municipalities, cities and regions that are prepared can meet these challenges.

CONCLUSIONS

The opportunity to present the results of our research teams is also an important part of the dissemination activities of the project APVV-20-0457 Monitoring and Tracking of Movement of Persons in Healthcare Facilities. The researchers aim to test the proposed technical and technological solutions in cooperation with the Ministry of Health of the Slovak Republic and selected hospitals. Our mission is to increase the resilience of the whole society.

At the time of the research project, we communicated regularly with health care facilities, regularly raising issues that health care facility management should address in the area of safety. The daily routine and stress does not allow people in the practice to realistically look for innovations, to look for new approaches and to positively change the safety culture of the company on a daily basis. The absence of 'common sense' at every step, the unconceptual work of central government bodies, the non-use of European funding, the

lack of cooperation between academia and the civil service are all strategic shortcomings of our time.

The next three years have presented us with major and unexpected challenges. The current turbulent times, hybrid threats, the ever-changing external and internal environment of the state are a certainty that new and new threats will keep coming. Faculty researchers believe that their efforts will be crowned by the continuous improvement of the theoretical foundation of Security Sciences.

ACKNOWLEDGEMENT

The publication of the article was supported by the project APVV-20-0457 Monitoring and Tracking of Movement of Persons in Healthcare Facilities.

LITERATURE

[1]. Council Directive 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection, source https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex%3A32008L0114

[2]. Act No. 45/2011 Coll. Act on Critical Infrastructure, source online https://www.zakonypreludi.sk/zz/2011-45.

[3]. Directive (EU) 2022/2557 of the European Parliament and of the Council of 14 December 2022 on the resilience of critical entities and repealing Council Directive 2008/114/EC.

[4]. Central Register of Theses and Dissertations, source online https://crzp.cvtisr.sk/

[5]. Central Register of Publications, source online https://app.crepc.sk/?fn=ResultFormChildU4APT&seo=CREP%C4%8C-Zoznam-z%C3%A1znamov

[6]. DVOŘÁK, Z. a PIALA, P.: Mathematical prediction of the spread of the covid-19 pandemic in Slovakia - available sources, p.31- 45, In: Proceedings of the 6th International Online Workshop SECULIN 2021 "Possibilities of Mathematization and Use of Modelling in the Field of Security", Zlín, Czech Republic, ISBN 978-80-7678-067-5

[7]. DVOŘÁK, Z.: Prediction of the spread of the COVID-19 pandemic in Slovakia, In. Proceedings of the RKS 2022 Conference. Zilina, Slovakia.

[8]. HOTEROVÁ, K.: Evaluation of the static resistance of infrastructure objects in the transport sector source online https://opac.crzp.sk/?fn=detailBiblioForm&sid=6BD761ABB9A8FF53EDCD0CFA5C01

[9]. CHOVANČÍKOVÁ, N.: Evaluation of static resistance of electricity infrastructure objects, source online https://www.deepl.com/translator#sk/en/Hodnotenie%20statickej%20odolnosti%20elektroenergetick%C3%BDch%20infra%C5%A1trukt%C3%BArnych%20objektov%0A