American Journal of Research, Education and Development

RED

ISSN 2471-9986

American Journal of Research, Education and Development

IMPRESSUM

American Journal of Research, Education and Development
ISSN 2471-9986

Publisher: DEVLART LLC
250 Camelback Ridge Ave. Henderson, NV 89012
devlart@devlart.hu

Editor in Chief:
prof. Gyula KÓRÓDI MD. PhD

Managing Editor:
dr. Zsolt FEJES MD. PhD
Dr. János RIKK

Editorial Secretary:
Dr. Dia SZŰCS

Business Development Manager:
Benami STERN

Table of Content

Changes in cybersecurity strategy over the last fifteen years

Dr. Megyeri Lajos: megyeri.lajos@uni-nke.hu, ORCID: 0000-0002-3743-1520, Assistant professor, Ludovika University of Publik Service, Faculty of Military Sciences and Officer Training.

Szűcs Attila: szucs.attila@uni-nke.hu, ORCID: 0009-0003-7971-3088, PhD student, Óbuda University, Doctoral School of Security Sciences

Training overview of the disaster management duty service

Mónika Balogh, University of Public Service, Doctoral School of Military Engineering Hungary, balogh.monika@matrixcbs.com, ORCID ID: 0009-0005-7701-3277

Potential Applications of Artificial Intelligence in Healthcare Surveillance I.

Current State, Benefits, and Limitations

K. Filyo; NUPS Doctoral School of Military Engineering

I. Negyesi; NUPS negyesi.imre@uni-nke.hu

Potential Applications of Artificial Intelligence in Healthcare Surveillance II.

Data Requirements and Practical Applications

K. Filyo; NUPS Doctoral School of Military Engineering

I. Negyesi; NUPS negyesi.imre@uni-nke.hu

ANALYSIS AND ASSESSMENT OF FISCAL AND MONETARY POLICY RESPONSES TO THE EFFECTS OF THE RUSSIAN-UKRAINIAN CONFLICT

László Teknős, Ludovika University of Public Service teknos.laszlo@uni-nke.hu *ORCID: 0000-0003-0759-5871*

Evolution and Practical Application of Critical Infrastructure Protection Planning Requirements for Healthcare

Gábor Mongel, University of Public Service, Faculty of Law Enforcement, Institute of Disaster Management, Department of Industrial Safety, mongelgabor@gmail.com *ORCID: 0009-0001-9024-5233*

THE EFFECTS OF CLIMATE CHANGE IN HUNGARY – AN EXAMINATION OF NATURAL DISASTERS AND RESPONSES

Regő Levente Kovács, Komárom-Esztergom County Disaster Management Directorate, fire sergeant, kov.rego.levente@gmail.com orcid: 0009-0001-1995-7561

Changes in cybersecurity strategy over the last fifteen years.

Dr. Megyeri Lajos: megyeri.lajos@uni-nke.hu, ORCID: 0000-0002-3743-1520, Assistant professor, Ludovika University of Publik Service, Faculty of Military Sciences and Officer Training.

Szűcs Attila: szucs.attila@uni-nke.hu, ORCID: 0009-0003-7971-3088, PhD student, Óbuda University, Doctoral School of Security Sciences

Abstract

The evolution of technology is constantly creating new opportunities and new challenges. This is particularly true in a dynamic area such as the world of infocommunications networks, where the emergence of Artificial Intelligence has brought an avalanche of change. At the same time, there is a growing societal need to ensure that technology and those who possess it do not gain a disproportionate advantage. To this end, governments are enacting laws and developing an international legal framework. The objectives of this paper are to examine how, since the 2010s, changes in ICT have been accompanied by changes in its regulation and to assess the adequacy of the change. It concludes with suggestions for more effective regulation.

Keywords: cybersecurity, Artificial Intelligence, cyberspace regulation

Introduction

Laws and international treaties are always developed in response to an existing problem. The process of reaching these agreements, especially between several actors with different interests, is time-consuming and often takes years. When a new technological trend emerges, there is not always enough time. In such cases, the rule-maker either tries to counteract the harmful effects on the basis of an existing analogy or tries to apply a general principle. However, if a completely new phenomenon is encountered, there is a chance of a rapid and effective assessment and proposal if there is a body of experts with competence in the matter. At international level, the subsequent decision making process is still a lengthy one of back-and-forth negotiations.

Cyberspace itself has been variously defined as follows:

The National Cyber Security Strategy defines cyberspace as “a set of globally interconnected, decentralized, and growing electronic information systems and the social and economic processes that take the form of data and information that are expressed through these systems.”[1]

According to Kovács, "There are different positions and views on the definition and interpretation of cyberspace, all experts in the field agree that cyberspace is the domain of networks, including the Internet, and the devices that connect to them, either wired or wirelessly.“[2]

Haig interprets cyberspace as ”Networked infocommunications technology offers great potential for the application of various tools and methods to produce cognitive effects. And the Internet, including social media, significantly expands the possibilities for cognitive influence and manipulation." [3]

In any case, it is clear that cyberspace is an area that cannot be controlled by national jurisdictions, where international consensus is needed on who can and cannot do what.

The situation was further complicated by the fact that NATO recognised cyberspace as an operational area in the official final declaration of its 2016 summit.[4] International cooperation on cybersecurity had already faced challenges. In the case of a cyber fraud, it was not easy, and still is not, to credibly identify the perpetrators in the complex network of cyberspace. The declaration of cyberspace as a theatre of operations has raised further serious problems that remain unresolved. Under the defence treaty, NATO member states collectively defend each other in the event of an attack by any member state. The exception is when the attacking and defending parties are both NATO members (e.g. Turkey-Greece). In the case of conventional warfare, there is a declaration of war, but in the absence of a declaration of war, land operations can clearly identify the attacking and attacked parties. In cyberspace, identification is not at all easy. It is therefore very important to establish with credibility whether or not a country has been cyber-attacked, and equally important to establish with clarity and credibility which state launched the attack. Without this, collective defence may not work or may have unforeseen consequences based on misinformation.

---

[1] Magyarország Nemzeti Kiberbiztonsági Stratégiája, 2013
[2] Kovács László: A kibertér védelme, Dialóg Campus 2018, Budapest
[3] Haig Zsolt: Információs műveletek a kibertérben Dialóg Campus 2018 Budapest
[4] Warsaw Summit Key Decisions (https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170206_1702-factsheet-warsaw-summit-key-en.pdf)

When planning military cyber operations, the country is preparing for passive (defensive), active (offensive) or proactive (preventive) activities in cyberspace, depending on its defence doctrine. Therefore, it is very important that the organisations carrying out these tasks operate under continuous state direction and control.

The emergence of Artificial Intelligence (AI) and its spread at a speed beyond any previous technology has further clarified the picture and requires a rapid and dynamic response from legislators.

Hungarian cybersecurity strategies of the 2010s

In Hungary, Government Resolution 1139/2013. (III. 21.) on the National Cybersecurity Strategy of Hungary[5] first regulated this area in detail. It also established the order of international cooperation. Hungary "strives to guarantee the free and secure use of global cyberspace through its system of federal and international relations, in particular through its membership in the EU and NATO, as well as the Organization for Security and Cooperation in Europe (OSCE), the UN, the Council of Europe and other international organizations." As its name suggests, this is a strategic directive, which is transformed into tangible rules in practice by the laws and regulations adopted in accordance with it.

Such was Act L. of 2013 on the electronic information security[6] of state and local government bodies, which regulated access to and data processing on IT systems operated by state actors. The legislation standardized the rules of protection procedures applicable during electronic data processing. This was greatly needed, because previously, various state and local government bodies had developed their own protection procedures within their own competences and depending on their resources. It was expected that systems operating to perform similar tasks, generally processing data of public interest, would operate on the basis of a uniform procedure. This was also an expectation of the European Union and NATO.

The competences were clarified by the Government Decree No.187/2015 (VII. 13.) on the duties and competences of the authorities responsible for the security supervision of electronic information systems and the information security supervisor, and the Decree on the definition of

[5] https://2010-2014.kormany.hu/download/b/b6/21000/Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf

[6] https://njt.hu/jogszabaly/2013-50-00-00

closed electronic information systems.[7] The Decree clearly defined the information security requirements for information communication systems, the responsibilities and the supervisory authority. The supervisory body has been given official powers, including the power to impose penalties.

The planning and operation of the infocommunication networks of vital system elements have been separately regulated: Annex 3 of Act CLXVI of 2012 on the identification and protection of vital system elements and facilities includes infocommunication technologies[8] as critical infrastructure to be protected, but this is not yet an independent regulation of this area. This only appears in Government Decree 249/2017. (IX. 5.) on the identification, designation and protection of vital systems and facilities related to the infocommunication technologies sector.[9]

Measures taken at the international level to protect cyberspace in the 2010s

In the European Union, the Directive (EU) 2016/1148 - cybersecurity of network and information systems[10], known only as NIS, proposes to delegate cybersecurity tasks to designated organisations. It also provides for the establishment of cyber incident response teams CSIRTs. It establishes a CSIRT network for the cooperation of national CSIRTs[11], which will facilitate the response to cross-border incidents

In the UK, The UK Cyber Security Strategy[12], published in November 2011, not only preceded the above-mentioned documents, but also allocated a budget to implement them. The seriousness with which cyber security is taken in the UK is demonstrated by the fact that, in 2016, an updated version of the National Cyber Security Strategy 2016 to 2021 was published, following the constant changes.

NATO, reacting firstly to the tensions caused by the armed conflict between Russia and Ukraine, and secondly to counteract the military policy of the People's Republic of China, which NATO considers dangerous, has taken strategic decisions: "Effective deterrence and protection are key to the safe use of and unrestricted access to space and cyberspace. We will enhance our ability to operate effectively in space and cyberspace to prevent, detect, counter and respond to threats across

[7] https://njt.hu/jogszabaly/2015-187-20-22
[8] https://mkogy.jogtar.hu/jogszabaly?docid=a1200166.TV
[9] https://njt.hu/jogszabaly/2017-249-20-22
[10] https://eur-lex.europa.eu/legal-content/HU/LSU/?uri=CELEX:32016L1148
[11] computer-security incident response teams
[12] https://assets.publishing.service.gov.uk/media/5a78a991ed915d04220645e2/uk-cyber-security-strategy-final.pdf

the full spectrum of threats, using all available tools. Malicious cyber threats are one-off or escalating, cumulative activity; or hostile operations to, from or within space; can rise to the level of an armed attack, and may prompt the North Atlantic Council to invoke Article 5 of the North Atlantic Treaty. We recognise the applicability of international law and will support responsible behaviour in cyberspace and outer space. We will also enhance the resilience of the space and cyber capabilities on which our collective defence and security rely."[13]

Evolution of cybersecurity strategies in Hungary from 2020 onwards

In Hungary, Act LXIX of 2024 on the cybersecurity of Hungary will be published six times from January 2025. This not only sets out the general requirements for electronic information systems and their operators, but also provides for forward-looking provisions for their development.[14]

In March 2025, the new Government Resolution 1089/2025 (31.III.) on the Cybersecurity Strategy of Hungary[15] was issued. The issue of digital dependency and the increased vulnerabilities resulting from these dependencies is a completely new element in point 3.3. Furthermore, our country supports the adoption of a new international agreement against cybercrime under the auspices of the UN.

Unfortunately, one of the cornerstones of this legislation is funding. While in the Cybersecurity Act of Hungary it appears in one place in point 69. Even there, it only refers to the various financial funds of the Eropian Union. The Cybersecurity Strategy devotes an entire sub-chapter 10.1 to this issue, but this too contains little specificity.

Changing strategy for the 2020s in the international aren

As a result of the revision and rewording of the directives, Directive 2022/2555 NIS2[16] entered into force on 18 October 2024 in the European Union, listing 18 critical sectors, of which Digital Infrastructure is already included in 9 subsectors. As part of this, EU Member States are not only required to draw up a list of operators of essential services, but also to update it regularly. The review of the NIS Directive has also revealed a wide divergence in the transposition of the NIS Directive into national legislation in the Member States. Key issues such as which establishments and operators

[13] forrás: https://www.nato.int/cps/en/natohq/opinions_214382.htm?selectedLocale=en
[14] https://njt.hu/jogszabaly/2024-69-00-00
[15] https://njt.hu/jogszabaly/2025-1089-30-22
[16] https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

should be covered by the Directive have also been left to individual competence. Similarly, Member States had a great deal of freedom as regards the obligation to report security incidents. This has been much tightened under the new directives, reducing the scope for wide discretion. As regards funding, it is only an option that "Member States may introduce a funding mechanism at national level to cover the necessary expenditure related to the performance of the tasks of public bodies responsible for cybersecurity in the Member State under this Directive."[17]

The new US National Cybersecurity Strategy 2023 will focus on proactive action, with an emphasis on developing offensive capabilities.[18]

During the COVID-19 outbreak, many businesses were forced to work over the internet under homeofice, for which security conditions were initially unavailable or only partially available. Companies were forced to devote more resources to creating a secure cyber environment and to develop their own internal policies.

Changes in strategies in the light of their causes

As can be seen above, the changes in policies and strategies follow the evolution of technology, but the dynamics lag behind. Artificial Intelligence, which is now invading every aspect of life[19], is only mentioned in NIS2. For example, in a context such as point 51 of the introduction, where the strategy's authors state that "the use of AI must also comply with EU regulations." A similar situation is described in point 89, where it is written in relation to critical organisations that "these organisations should assess their own cybersecurity capabilities and, where appropriate, seek to integrate cybersecurity-enhancing technologies such as artificial intelligence or machine learning systems to enhance their capabilities and the security of their network and information systems." These are now too general even at directive level.

[17] NIS2 46. pont https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=CELEX:32022L2555
[18] Molnár, D., & Nagy, G. (2023)
[19] Tilesh, Atamleh,: Mesterség és Intelligencia.

Comparison of Hungary and international regulatory developments:

Aspect	International trend	Hungarian practice
Institutional frameworks	Early design (e.g. USA, NATO)	Gradual development from 2013
Legal regulation	Detailed, mandatory (EU, USA)	EU compliance, but gaps
Offensive capabilities	USA, China: proactive action	Hungary: defensive approach
Critical infrastructure protection	Featured role	Under continuous development
International cooperation	NATO, EU, bilateral agreements	EU legal harmonisation, Active NATO participation

The above comparison shows the similarities and differences in development trends. NATO already had a coherent information security strategy (Policy) in place in the early 2000s, in particular for the management of its classified information. In Hungary, after joining NATO, only alliance data was handled with the required priority. After joining the European Union, it became an urgent task to create and harmonise our national legislation with EU legislation.

Hungary prioritises a defensive approach to military cyber operations in line with the National Security Strategy. For the planning and execution of tasks, for cooperation with national and international organisations (e.g. NATO), the Cyber and Information Operations Group Headquarters of the Defence Forces was established on 01.01.2025.

New challenges are constantly emerging: deepfake, AI-based attacks, supply chain security, etc. In Négyesi's opinion, “in addition to the controversial issues, it is also necessary to examine whether AI can commit crimes (e.g. smuggling, say using unmanned vehicles, harassment, torture, sexual offences, theft, fraud, assault, etc.).” Therefore, keeping a continuous review of strategies on the agenda is essential to maintain cyber security at least at an acceptable level. Continuity need not necessarily mean that a new strategy needs to be developed every few months, but it should be complemented by a response to the emerging problem.

Summary

The conclusion to be drawn from the above is that activities in cyberspace are becoming increasingly diverse and interconnected. In this system, where not only national players are now dominant, but often cross-border international companies and businesses are more important, international regulation is important. There are two areas in which improvements are definitely needed. Firstly, since regulation is slow to keep pace with technological developments, it would be advisable to set up an international research institute to draw up uniform guidelines, bringing together at least the leading players in the field of technological development. This should follow in real time the constant threats and the rapid development of artificial intelligence. The ability of this technology to produce and imitate voice, video and images can have a significant impact by deceiving and impersonating key individuals (state leaders, military leaders, politicians, businessmen, celebrities). This method can cause significant financial and moral damage to an unethical user.

Secondly, given the international nature of cyber-attacks, a uniform set of rules and public authority action is necessary to establish a system of sanctions with a real deterrent effect.

Hungary's progress in cybersecurity is positive, but critical infrastructure protection, public awareness and private sector involvement need to be further strengthened.

References

1089/2025. (III. 31.) Korm. határozatot Magyarország Kiberbiztonsági Stratégiájáról https://njt.hu/jogszabaly/2025-1089-30-22

187/2015. (VII. 13.) Kormány rendelet az elektronikus információs rendszerek biztonsági felügyeletét ellátó hatóságok, valamint az információbiztonsági felügyelő feladat- és hatásköréről, továbbá a zárt célú elektronikus információs rendszerek meghatározásáról https://njt.hu/jogszabaly/2015-187-20-22

2012. évi CLXVI. törvény – a létfontosságú rendszerelemek és létesítmények azonosításáról és védelméről https://mkogy.jogtar.hu/jogszabaly?docid=a1200166.TV

2013. évi L. törvény – az állami és önkormányzati szervek elektronikus információbiztonságáról https://njt.hu/jogszabaly/2013-50-00-00

249/2017. (IX. 5.) Korm. rendelet az infokommunikációs technológiák ágazathoz kapcsolódó létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről https://njt.hu/jogszabaly/2017-249-20-22

2024. évi LXIX. törvény Magyarország kiberbiztonságáról https://njt.hu/jogszabaly/2024-69-00-00

Beláz Annamária: The Changing Role of the EU in Cybersecurity: Az Európai Unió változó kiberbiztonság koncepciója, Biztonságtudományi Szemle 1: 1-2 pp. 17-30., 14 p. (2019)

Directive (EU) 2016/1148 — cybersecurity of network and information systems https://eur-lex.europa.eu/legal-content/HU/LSU/?uri=CELEX:32016L1148

The UK Cyber Security Strategy https://assets.publishing.service.gov.uk/media/5a78a991ed915d04220645e2/uk-cyber-security-strategy-final.pdf

Haig Zsolt: Információs műveletek a kibertérben Budapest: Dialóg Campus 2018

Molnár, D., & Nagy, G. (2023). A 2023-as amerikai kiberbiztonsági stratégia áttekintése és értékelése. *Hadtudomány*, *33*(E-szám), 88-100.

Kovács László: A Kibertér védelme,Budapest: Dialóg Campus 2018

Imre Négyesi: The Future of Information Gathering, The Future of Information Gathering, Military Science Review (2676-9816 2060-0437): 1 (3) pp. 95-100. (2008)

Magyarország Nemzeti Kiberbiztonsági Stratégiája https://2010-2014.kormany.hu/download/b/b6/21000/Magyarorszag_Nemzeti_Kiberbiztonsagi_Strategiaja.pdf

Négyesi, I. (2023). A mesterséges intelligencia társadalmi és etikai kérdései. Honvédségi Szemle–Hungarian Defence Review, 151(4), 6-18. https://tudasportal.uni-nke.hu/xmlui/bitstream/handle/20.500.12944/20955/A%20mesters%c3%a9ges%20intelligencia%20t%c3%a1rsadalmi%20%c3%a9s%20etikai%20k%c3%a9rd%c3%a9sei.pdf?sequence=1&isAllowed=y

NIS2 Directive: new rules on cybersecurity of network and information systems https://digital-strategy.ec.europa.eu/en/policies/nis2-directive

Tilesh, György – H-Atamleh, Omar: Mesterség és Intelligencia. Budapest: Libri 2021

ISBN: 9789634338291

Imre Négyesi: Social issues surrounding the military use of artificial intelligence Armed Forces Review: The central journal of the Hungarian Armed Forces (2060-1506 2732-3226): 149 (1) pp. 133-144. (2021)

Warsaw Summit Key Decisions – NATO varsói csúcsértekeztethttps://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170206_1702-factsheet-warsaw-summit-key-en.pdf

Training overview of the disaster management duty service

Mónika Balogh, University of Public Service, Doctoral School of Military Engineering Hungary, balogh.monika@matrixcbs.com*, ORCID ID: 0009-0005-7701-3277*

Abstract

This study reviews the training of the on-duty staff of the disaster management service, presenting the themes and structure of the training. The Operations Control Course and the Operations Control Reference Training prepare participants in different number of hours to perform the tasks awaiting them at a high level, in which the acquisition of the use of various decision-support IT systems is also expected in the training. In connection with the topic, the relevant partial results of the empirical research conducted in the second half of 2024 are presented, one of the question blocks of which assessed the digital and IT knowledge of the on-duty staff.

Keywords: disaster management duty service, operations management course, operations management officer training, digital competence

Corresponding author:

Mónika Balogh, University of Public Service, Doctoral School of Military Engineering Hungary, balogh.monika@matrixcbs.com*, ORCID ID: 0009-0005-7701-3277*

Introduction

Within the organisational structure of the National Disaster Management Directorate, the on-call staff of the operational control are on duty at national level, in the capital and in all the counties, and they perform important coordination tasks in emergencies and along the declared measures to avoid disasters. Their activities are carried out in accordance with legal provisions, which are supplemented by a number of internal regulations and measures of the organisation (in relation to the subject under examination, the BM OKF Director-General's Instruction No. 6/2023 on the operational procedures of the on-call and stand-by services of professional disaster management bodies), clearly declaring

their responsibilities and boundaries. It is essential that the members of the staff on duty have adequate professional training, and the expectations and requirements in this respect have been laid down in training and educational documents. With regard to the legal background of the training programmes, two measures should be highlighted in this article, namely BM OKF Director-General Measure No 1/2024 on the operational management of professional disaster management bodies and the professional rules of alerting, and BM OKF Director-General Measure No 6/2023 on the operational management of on-call and stand-by services of professional disaster management bodies. The aim of the study is to provide insight into the training aspect of this key speciality, which is not covered by domestic publications, although all on-call personnel play a crucial role in disaster management. A further aim of the study is to present the partial results of a comprehensive survey on the relevance of the present topic, which was conducted in the second half of 2024 on a national scale, analysing the response rate of the on-call staff, which is about 84%.

Operations management course

The emergency and standby services of the professional disaster management services manage a number of alarm and information systems that are essential for the proper management of disaster situations and incidents. The use of these systems ensures, among other things, the rapid dissemination of information, the understanding of tasks, the rapid cooperation of different units and partner services, as well as the basis for various reports, data services and database management. The basic tasks of the on-call and standby services include, in addition to providing day-to-day tasks, the management of incidents, the operation of reporting and defined data systems, and the execution of tasks related to the enhancement of preparedness (Muhoray Á., 2016).

The Operations Manager course is intended for staff members who are planning to take up the position of Operations Manager within the disaster management service and are coming to the training for professional preparation. An additional requirement for enrolment in the training is that the trainee must also have a Unified Digital Radio Telecommunication System Dispatcher Workstation Operator qualification. The total number of hours of training is 36 hours, taking into account prior studies and professional experience already acquired. The course content comprises four units of study:

1. Knowledge of decision support and data applications.
2. Fire-fighting, technical rescue rules and organisation.
3. Industrial safety and civil protection knowledge.

4. Fundamentals of official work and fire investigation.

Part of the lessons will be delivered in the form of theory, as described in the training programme, through classroom lectures using the frontal classroom method. In addition to the theoretical lessons, participants will be able to learn the practical aspects of each subject in the form of practical lessons in a computer classroom. The maximum number of participants is 20.

The training programme presents each curriculum unit by further curricular elements, broken down into the number of hours required to learn each curricular element, their types, the methods required to teach them and the levels of requirement expected of trainees, defined at the level of recognition, definition, proficiency, skill, order. In the first unit, participants will be introduced in depth to the Call Interceptor System (CIR), its components and the relationships between them. Skills will also be acquired in the various applications for decision support and data provision, such as PAJZS, KAP-Online, DÖMI and Marathon Terra 3 communication system. Following this block, the next focus topic is firefighting and related tasks from an on-call approach. By completing this unit, the participants will be informed about the rules for the organisation of firefighting and technical rescue and will also learn the rules of operations management and on-call reporting obligations through an understanding of the rights and obligations of participants in firefighting and technical rescue (Mihály et. al., 2025). Industrial safety is one of the disaster management disciplines and is naturally included in the training programme for operations controllers. After the training, the participant will learn about the tasks of Industrial Safety and Civil Protection, its place in the Civil Protection system and its role, its practical aspects and the management of protection software, as well as the role of civil society organisations, which can be involved in the rescue process under certain rules. In the last unit, the basics of official work and fire investigation will be introduced, and participants will learn about the main types of cases that arise in the course of their duty of duty and their responsibilities in the management of incidents. The training will end with a final examination, after which the trainee will receive a certificate.

Operations management officer training

The qualification of Operations Management Officer is an intermediate vocational qualification, which can be completed in 274 hours of training. In addition to secondary education, the training requires the candidate to be in the professional service of a professional disaster management organisation, to have passed at least the basic firefighter's examination and to have at least 2 years' professional experience. As regards the professional experience, it is important to note that only time

spent in firefighting and technical rescue or as an operations manager can count, i.e. the candidate must provide evidence of relevant professional experience.

The training programme of the Operations Officer training course, similar to the Operations Officer course, contains details of the units of the training, their curricular elements, and the number of hours, the expected knowledge, skills and training methods. The 274-hour training course is delivered over 8 weeks, with a maximum group size of 15-20 people. The overall objective of the training is to prepare participants to deal with fire and damage incidents in accordance with the appropriate tactical rules and to equip them with the knowledge to manage the intervention of the emergency services and other intervention bodies. These objectives will be achieved through six modules. During the training, the participants will learn in theoretical and practical classes, with additional hours of consultation to deepen the learning. The curricular units of the training are:

1. Organisation and management of fire-fighting and technical rescue.
2. Applied firefighting and technical rescue.
3. System of training, further training and exercises.
4. Fire prevention, fire investigation and fire safety systems, training and management systems.
5. Technical knowledge.
6. Protection against disasters.

The knowledge to be acquired in the curriculum units is set out in detail in the curriculum elements, with objectives, teaching methods and levels of requirements. In the first major unit, the organisation and management of firefighting and technical rescue, participants will learn about the regulation of these activities and the feedback and reporting obligations. A significant number of lessons are devoted to fire fighting and applied technical rescue, with particular emphasis on the possibilities of fire occurrence, such as fires in industrial premises, in various installations, in agriculture or in road, rail, air and waterborne transport (Kátai-Urbán et. al., 2023). A separate block of material will cover the training system for disaster management and the basic knowledge of the authorities required for the job. Of the total number of hours, a significant amount of time is devoted to the acquisition of technical knowledge during the training. The knowledge acquired in this unit will enable them to apply the decision support and management support software and hardware used in disaster management to their future work at a high level of proficiency. In addition to the basics of on-scene communications management, they will learn the tactical use of individual vehicles, the tasks of DWS3 (Digital Wireless System Dispatcher) workstation operators, cartography, the structure of the VPN (Virtual Private Network) measure, mass incident management and geo-

information technology. In the integrated interpretation of disaster management, as a compulsory part of the training, participants will acquire the knowledge and tasks required for their job in civil protection and industrial safety. The training will culminate in a final examination, which will consist of three examination activities. The knowledge and skills acquired by the participant are assessed in the form of a written questionnaire and an oral task, which is supplemented by a practical task. A pre-prepared situation has to be solved by the Operations Officer candidate on the basis of the information given in the specifications, in an Operations or IT classroom.

In the chapter above, when I described the content of the training courses, I already referred to the IT software used by the staff on duty in their daily work. The following is a summary of the purpose and main features of the use of each software.

- *PAJZS software*: a decision support system with geographic information support, which supports the work of the general and operational management of the county/metropolitan disaster management directorate, providing online data at local, regional and national level. The system has four main elements, which serve the management of incidents, alerts and emergency situations, complemented by a map function.
- *DÖMI software*: the Decision Support Map is directly accessible from the PAJZS application, which supports day-to-day work with an information map. The software supports the management work by providing visual and textual information, documenting each decision taken.
- *KAP Online system*: the Disaster Management Data Service Programme allows data to be recorded and is designed to provide up-to-date information to the disaster management departments. (Lakatos, Vass, Teknős, 2023) One of its segments is the Fire and Technical Rescue Report, the Fire Survey, the Fire Investigation, the Forest and Vegetation Fire Survey, etc., which can be used to generate statistical reports from the data by setting various filters (Kersák, 2021).
- *Marathon Terra 3 system*: developed and operated to support disaster management and security management tasks. The primary purpose of the system is to provide emergency and general communications during large-scale incidents, coordinated protection operations and cooperation between organisations involved in disaster management. It also provides a means for the secure storage, access and transmission of related data and information.

These infocommunication systems are included in the training curriculum of the course in the field of emergency management in the form of a stand-alone 19-hour course, predominantly in the form of practical training (7 hours of theory and 12 hours of practical training). The main focus of the training will be on the user interface and the services available in the application through practical

implementation and individual task solving. "One of the important areas of support from the human side of defence activities is the related professional training and knowledge sharing, which provides the basis for the ICT support." (Farkas, 2020) Following the training, once the users have mastered the use of the systems at a skill level, the creation of opportunities for continuous knowledge enhancement and feedback, which can be achieved through pre-planned, structured training courses based on pedagogical methods, should not be overlooked. During the training, it is also necessary to address issues of firefighters' health protection, which has become a key safety issue during firefighting interventions and technical rescue operations (Kanyó, 2011).

Partial results of empirical research relevant to the present study

The on-call staff of the disaster management service are a segment of law enforcement who have not been the focus of surveys and studies so far. In my own research, I will primarily examine the staff from the perspective of training and general competence development, with a special focus on IT and digital competences, which are an integral part of their training. In this paper, I present the partial results of a national survey on IT and digital skills conducted in the second semester of 2024, which also provide some feedback on the current content of training, reflecting staff satisfaction.

Research problem, hypothesis, objective

My assumption is that the emergency services' on-call staff have the digital/technical competence (using telecommunication and IT tools) to perform their tasks, but that there is a significant difference in skills and knowledge between generations. The aim of my research was to find out respondents' perceptions of their own digital and IT skills and where they acquired them. On the other hand, I wanted to find out how many hours of training they had received to learn how to use the IT software and programs they use at work, and how often they had the opportunity to improve their knowledge at work. Thirdly, I wanted to know their perception of their knowledge of the use of software.

Research methodology and context

I chose the written questionnaire method and the questionnaire instrument to conduct the research, given that they work on a national scale and this research method made it possible to interview people in this field at the same time. The complete questionnaire consisted of 37 questions, all of which were

closed questions except one. After the introductory and demographic questions, validated questionnaires to reject or confirm hypotheses and a series of questions formulated by myself were asked to the respondents, anonymously and voluntarily. The questionnaire was completed online using Google form. A link to the questionnaire was sent to all the directorates in the county, inviting the staff on duty to complete the questionnaire. The questionnaire was completed by survey respondents between 15 September 2024 and 05 December 2024.

Presentation of samples

The number of on-call staff of the disaster management service according to the staffing table was 415 in the period under review. The questionnaire was filled in by 347 people, 84% of the total staff, which indicates that the results are representative. Several counties had a 100% response rate, with several counties having a response rate of over 90%. For the other counties, 65-90% of the staff in the period under study helped me by completing the questionnaire.

Presentation of results

The questionnaire was a separate block of questions on the digital and IT skills of on-call staff and satisfaction with the training they received. As a first question, I wanted to find out how they rated their digital skills on a scale of one to ten. The results are shown in Figure 1.

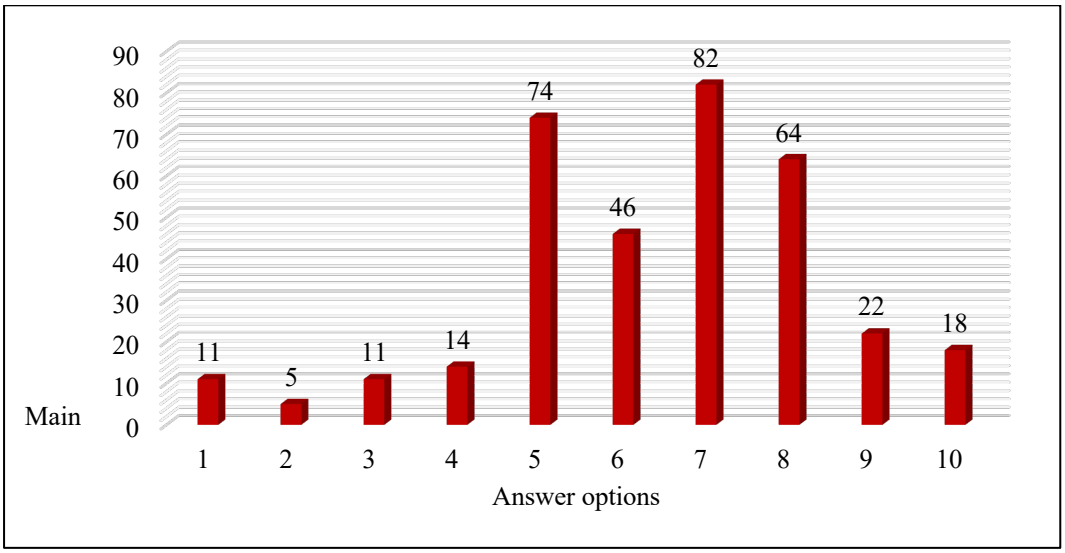


Figure 1: Assessment of the on-call staff's own digital/IT knowledge (N=347)

(Source: own editing)

The largest proportion of respondents described their own IT skills as a seven, with around 82 (23.6%) choosing this value. This was followed by those who answered a five, with 74 (21.3%), and then by those who answered an eight, with 64 (18.4%). Of the sample, 41 (11.8%) thought their level of digital knowledge was below a five on a scale of ten, and a total of 40 (11.5%) rated their knowledge as a nine or ten. 46 (at the time of taking the questionnaire) said they would rate their IT knowledge as a six. Summarising the responses, emergency response staff rate their own digital and IT skills as an average of 6.4, with scores ranging from one to ten.

Respondents had multiple choices when asked where they had learned to use a computer. The aggregated responses of the respondents to the questionnaire are shown in Figure 2.

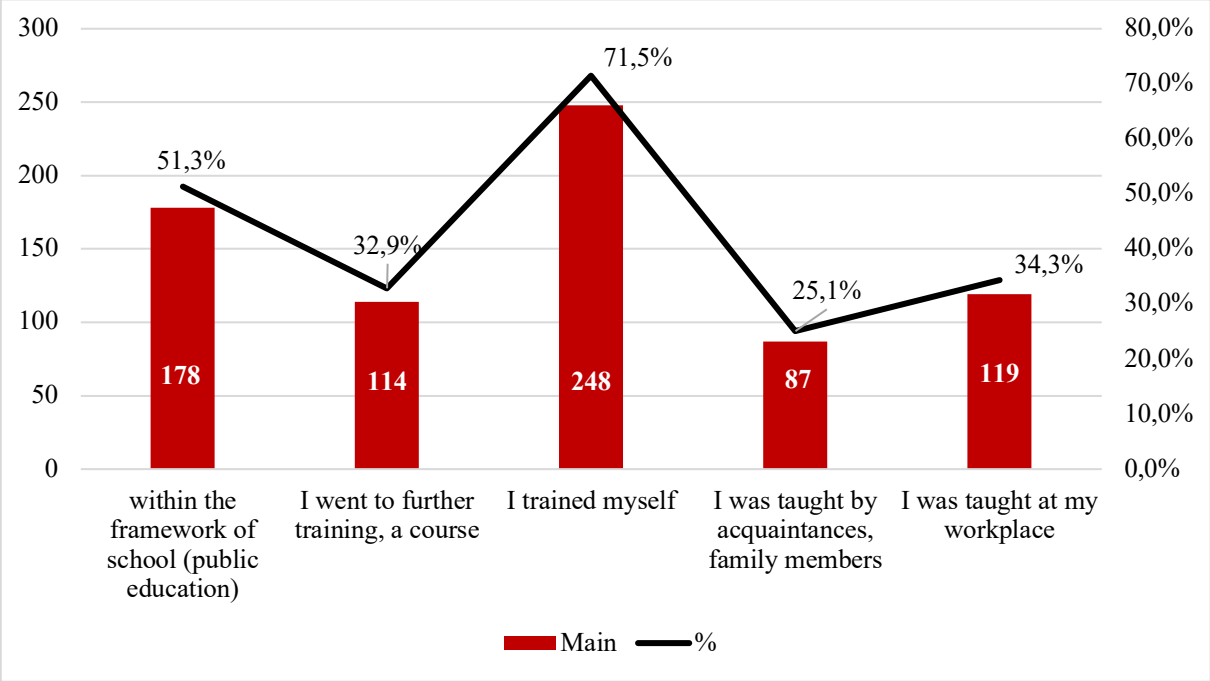


Figure 2: Self-reported method of learning to use a computer (N=347)

(Source: own editing)

The highest proportion of employees who learned to use the computer as a result of self-improvement was 71.5% (248) of the employees who selected "self-trained" as one of the answers. Almost half of the sample, 178 persons, 51.3% of the sample, had also learned how to use a computer in a school setting, in public education. Almost the same proportion of respondents indicated further education or training (32.9%) and learning at work (34.3%). Some people also had help from friends and family members to learn, with 25.1% of respondents, 87 people, indicating this response option.

In their daily work, the members of the emergency services on duty use a number of IT programs, ranging from general programs such as Word or Excel spreadsheet management to specific programs for their work, such as PAJZS, DÖMI software, KAP-Online and Marathon Terra 3. Given that their work is done on a computer, they typically type data and information into the various systems, so the questions included hours of training in shorthand. The results are shown in Figure 3.

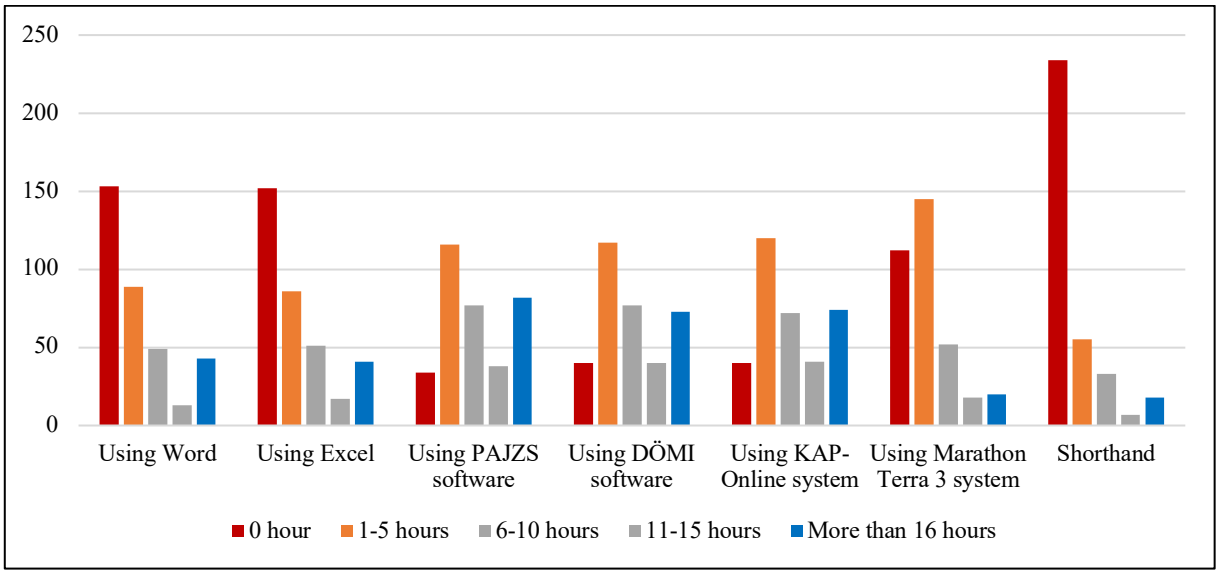


Figure 3: How many hours did you spend preparing yourself to use the following software and programs when you started working in this position? (N=347)

(Source: own editing)

The majority of respondents said that they had not received adequate training in the use of common programs (e.g. Word, Excel), with most indicating "0 hours" or "1-5 hours" at most. Shorthand training was almost absent, with 70% of respondents saying it was not included in the curriculum. For specialised software (PAJZS, DÖMI, KAP-Online), most respondents recalled "1-5 hours" of instruction, while two thirds of respondents recalled no or minimal hours of instruction on the Marathon Terra 3 system. Of the 347 respondents who completed the questionnaire, 10% indicated that they had spent zero hours on PAJZS, 12% on DÖMI and 12% on KAP-Online. The adequacy of the responses in this case raises doubts, as they are basic applications for operations management. Looking further at the results obtained, according to the length of time in the job, it can be seen that the primary candidates who indicated 0 hours (40) were those who had been working in the organisation for between 0 and 1 year (6).

Following the questions regarding the number of training hours for each program and software, the next question in the questionnaire aimed to assess how frequently respondents have the opportunity to participate in further training during their daily work, and whether they are able to improve their existing knowledge within the system. (Figure 4)

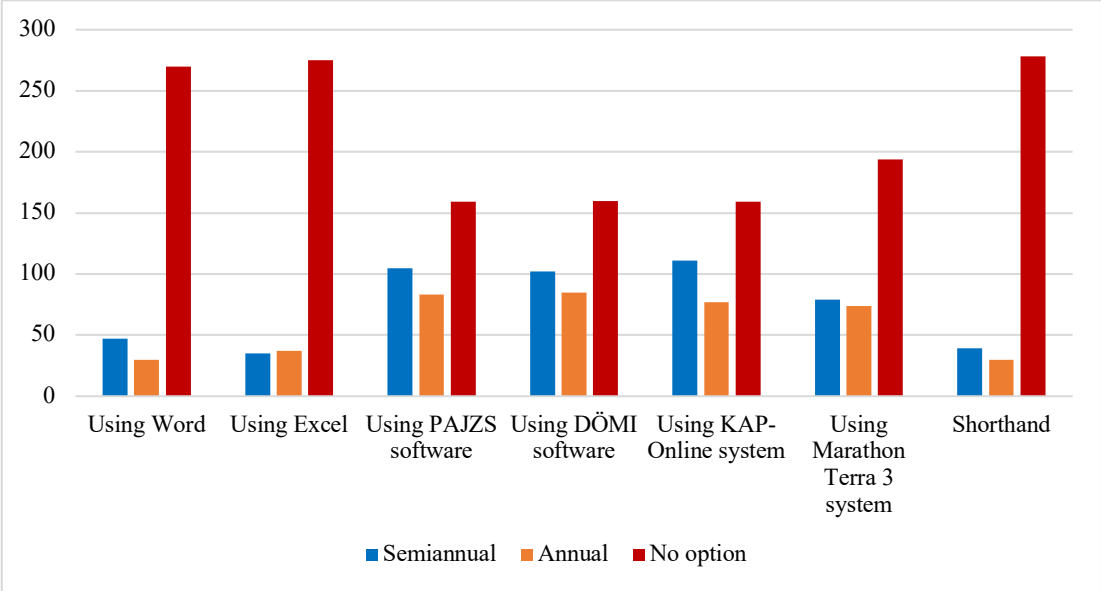


Figure 4: How often do you have the opportunity to participate in further training to improve the use of programs and software used in your work? (N=347)

(Source: own editing)

Based on the results of the above graph, it can be clearly stated that the development of general programs such as word, excel and shorthand is not considered as an area for improvement for this job. The picture is more positive for job-specific software, with 20 to 30% of respondents considering that the possibility of providing training every six months or every year is guaranteed. However, a higher proportion of respondents consider that there is no possibility of such training, with 46% of respondents indicating this option for PAJZS, DÖMI, KAP-online systems. 56% of the respondents indicated that the possibility of attending training on the management of the Marathon Terra 3 system does not exist in their work.

Respondents described their own digital, IT skills with a mean score of 6.46 on a scale of 10, with a standard deviation of 1.85. Only 11.15% of the sample feel that they have this kind of knowledge at the 9-10 level. For each software-specific outcome, the mean score is 7.5 (standard deviation 1.9), except for Marathon Terra 3, where the mean is 5.77 and the standard deviation 2.66.

Summary

Disaster management staff on duty and on standby are crucial to the life of the organisation, but little is known about them. Their training is key to the effective functioning of the organisation, ensuring a rapid and coordinated response to emergencies. The training structure is based on two main pillars, the 36-hour Operations Control course and the 274-hour Operations Control Officer training. Both programmes are based on a strict set of requirements, aiming to equip participants to confidently deal with the situations they are called upon to deal with, using state-of-the-art decision support and IT systems such as PAJZS, DÖMI, KAP-Online or Marathon Terra 3.

Based on the data from my empirical research relevant to this study, the staff rated their own digital literacy at an average level of 6.4 on a scale of 10. However, for some systems, such as Marathon Terra 3, this average is as low as 5.77, suggesting that the current form of training does not always ensure that practical knowledge is acquired in sufficient depth. Self-learning and on-the-job experience were identified as the primary sources of digital knowledge acquisition in a high proportion - over 70%. However, it was also clear that the system of hours devoted to software use and subsequent training opportunities is not satisfactory, with a third of respondents saying, for example, that there is no opportunity for regular further development. This result deserves particular attention, given that the confident and skilled use of digital tools can be seen as a basic infrastructure requirement for service delivery.

In my view, the current training courses provide an adequate basis for preparedness, but in order to ensure the continuous high quality of complex service tasks, it would be essential to incorporate the development of non-professional competences. I think it is important to point out that, depending on their experience, the professional training of staff is either 36 or 274 hours, which is exclusively devoted to the transfer of professional knowledge and practical skills. In the two types of training, the teaching of IT software used in everyday work is not equally represented, and the higher number of hours does not include the teaching of this software as a separate curriculum unit, which in my opinion requires a revision of the curriculum. None of the training programmes includes, beyond the professional subjects, subjects aimed at developing skills such as communication, conflict management, stress management, digital literacy or even burnout prevention, promoting intergenerational cooperation, which would enable the daily performance of tasks to be more effective and would open up new perspectives for the organisation's human resources planning, while preserving staff. I believe that the training programmes described in this article could provide a basis for the development of non-professional competences with a basic number of hours, on which a

complex training matrix could be drawn up, didactically, for years ahead, for the development of individual skills, taking into account individual development needs.

Bibliography

BM OKF Informatics Department (2021): user's guide for the PAJZS application supporting mission control. Version 2021/1.

Árpád Muhoray: Disaster Prevention I. University notes. National University of Public Service, Institute of Disaster Prevention, NKE Szolgáltató Nonprofit Kft., Budapest, 2016. ISBN 978-615-5527-85-2

Tibor Farkas: Defence infocommunications networks and systems - professional training. Hadtudományi Szemle Vol.13, No 1 (2020) pp. 37-48. DOI: 10.32563/hsz.2020.1.3.

József Zsolt Kersák: Analysis and evaluation of disaster management operations based on the closed firefighting and technical rescue data sheets. Hadtudomány, Vol. 31, E-szám, (2021) pp. 84-98. https://doi.org/10.17047/Hadtud.2021.31.E.84

Bence Lakatos, Gyula Vass, László Teknős: Application possibilities of systems supporting disaster management authority tasks. Belügyi Szemle Vol. 71, No. 4, (2023) pp. 669-690.
https:doi.org/10.381146/BSZ.2023.4.7.

Kátai-Urbán, Maxim, Tibor Bíró, Lajos Kátai-Urbán, Ferenc Varga, and Zsolt Cimer. 2023. "Identification Methodology for Chemical Warehouses Dealing with Flammable Substances Capable of Causing Firewater Pollution" *Fire* 6, no. 9: 345. https://doi.org/10.3390/fire6090345

Kanyó, Ferenc: Telemetriai rendszer alkalmazási lehetősége a tűzoltók egészségvédelmének érdekében. Védelem - Katasztrófa- Tűz- és Polgári Védelmi Szemle 19 : 1 pp. 1-5. (2011)

Mihály, István, László Bérczi, Balázs Bognár, Maxim Kátai-Urbán, Levente Tóth, Lajos Kátai-Urbán, Gyula Vass, and Ferenc Varga. 2025. "Experimental Study to Determine the Leakage

Area of Single-Leaf Smoke Control Doors in the Design of Pressure Differential Systems" Fire 8, no. 1: 5. https://doi.org/10.3390/fire8010005

BM OKF Director General's Measure No. 6/2023 on the procedure for the operational management of professional disaster protection bodies and the professional rules for the alert

BM OKF Director General's Measure No. 1/2024 on the procedure for the operational management of professional disaster protection bodies and the professional rules for the alert

30/2023. (XI. 30.) BM Instruction on the operation of the Marathon Terra information and communication application for defense administration

2/2013. (I. 30.) BM Decree on the system of further training and leadership training of professional staff members of bodies under the control of the Minister of the Interior, and on the law enforcement recruitment and leadership data bank legal act

Potential Applications of Artificial Intelligence in Healthcare Surveillance I.

Current State, Benefits, and Limitations

K. Filyo, I. Negyesi

Abstract

This article provides an in-depth overview of the current state of artificial intelligence (AI) in healthcare surveillance. It outlines the core technologies—machine learning, natural language processing, and computer vision—and their role in detecting disease patterns and improving data analysis. The study emphasizes the key advantages of AI, including enhanced accuracy, predictive capabilities, scalability, and cost efficiency. It also critically examines the challenges related to data privacy, algorithmic bias, infrastructure, and regulation, concluding that successful implementation depends on addressing these limitations.

Keywords: artificial intelligence, healthcare surveillance, machine learning, data privacy

Introduction

Artificial intelligence (AI) is rapidly revolutionizing various industries, with healthcare emerging as one of its most significant beneficiaries. The ability to process vast amounts of healthcare data, identify subtle patterns, and generate actionable insights has positioned AI as a cornerstone of modern healthcare strategies. Among its many applications, AI's role in healthcare surveillance stands out for its potential to transform how diseases are monitored, outbreaks are predicted, and interventions are implemented. This article delves deeply into the current state of artificial intelligence, outlining why its use in healthcare surveillance is essential, and examining both its advantages and the challenges it faces in this domain.

The Current State of Artificial Intelligence in Healthcare

The adoption of AI in healthcare has grown exponentially over the past decade, fueled by advancements in computational power, access to vast datasets, and the development of sophisticated algorithms. AI technologies, including machine learning (ML), natural language processing (NLP), and computer vision, are being integrated into healthcare systems worldwide. These tools are reshaping how data is analyzed, enabling faster, more accurate insights that would be impossible for human analysts to achieve alone.

Machine Learning in Healthcare

Machine learning algorithms are at the heart of AI innovations in healthcare. These systems are trained on large datasets to recognize patterns and make predictions. For example, neural networks are employed to analyze medical imaging data, such as X-rays and MRIs, to detect early signs of diseases like cancer. Additionally, ML models are used in predictive analytics to identify patients at risk for certain conditions, such as cardiovascular diseases, based on historical health data.

Natural Language Processing

NLP plays a critical role in extracting meaningful information from unstructured clinical data. By analyzing electronic health records (EHRs), physician notes, and patient feedback, NLP algorithms can identify emerging health trends and potential public health threats. This capability is particularly valuable for monitoring diseases in real-time and informing policy decisions.

Computer Vision

Computer vision is another AI technology transforming healthcare. It enables the analysis of visual data, such as images and videos, to identify abnormalities. For instance, AI-driven imaging systems are now used in dermatology to detect skin cancers and in ophthalmology to diagnose diabetic retinopathy. These tools not only improve diagnostic accuracy but also make screenings more accessible in resource-limited settings.

Benefits of AI in Healthcare Surveillance

The integration of AI into healthcare surveillance offers numerous benefits that enhance the efficiency and effectiveness of public health initiatives:

- Enhanced Accuracy: AI algorithms process complex datasets with unmatched precision, reducing the likelihood of errors in identifying health trends. This is particularly crucial during outbreaks when timely and accurate insights can save lives.
- Predictive Capabilities: AI excels in forecasting potential health crises. For example, machine learning models can analyze environmental, demographic, and clinical data to predict the spread of infectious diseases.
- Scalability: AI's ability to handle large-scale data analysis makes it indispensable for global health surveillance efforts. Whether monitoring a local outbreak or a pandemic, AI tools can manage the vast amounts of data involved.
- Cost Efficiency: Automating tasks such as data processing and pattern recognition reduces operational costs significantly compared to traditional methods relying on human labor.

Limitations and Challenges

Despite its numerous advantages, the implementation of AI in healthcare surveillance is not without challenges. Addressing these limitations is essential for realizing AI's full potential:

- Data Privacy and Security: The use of AI in healthcare involves handling sensitive personal data, raising concerns about privacy and security. Ensuring compliance with regulations such as GDPR and HIPAA is critical.
- Algorithmic Bias: Biases in training datasets can lead to skewed results, disproportionately affecting certain populations. This issue underscores the need for diverse and representative data.
- Infrastructure Requirements: Implementing AI solutions requires robust infrastructure, including high-quality hardware and reliable internet

connectivity. These requirements can be challenging to meet in low-resource settings.

- Regulatory Hurdles: Strict regulations governing the use of AI in healthcare can delay its adoption. Establishing clear guidelines that balance innovation with safety is essential.

Conclusion

Artificial intelligence has the potential to revolutionize healthcare surveillance by providing unparalleled analytical capabilities, predictive insights, and scalability. However, addressing challenges related to data privacy, bias, and infrastructure is crucial for its successful implementation. As AI technologies continue to evolve, their integration into healthcare surveillance systems promises to make public health efforts more proactive, efficient, and impactful.

Bibliography

- Kovács, J. (2020). Az MI alkalmazása a magyar egészségügyben. Egészségügyi Innovációk, 12(3), 45-60.
- Smith, A., & Brown, P. (2018). Machine Learning in Healthcare Surveillance. Journal of AI Research, 25(6), 112-130.
- WHO. (2021). Artificial Intelligence in Global Health. [URL]
- Rab, Á. (2021). *Mesterséges intelligencia és egészségügy*. Medicina Kiadó.
- Földes, Á., & Tóth, B. (2020). *Egészségügyi adatvédelem és mesterséges intelligencia*. Egészségügyi Szemle, 59(3), 122-135.
- Bánkuti, G. (2023). *Katonai egészségügyi rendszerek és a digitális transzformáció*. Honvédorvos, 175(1), 45-56.
- Kovács, L. (2022). *Egészségbiztonság és hírszerzés*. Nemzetbiztonsági Szemle, 10(2), 87-98.
- Magyar Kormány (2023). *Digitális Egészségügyi Stratégia 2030*.
- Topol, E. (2019). *Deep Medicine: How Artificial Intelligence Can Make Healthcare Human Again*. Basic Books.

- Jiang, F., Jiang, Y., Zhi, H., et al. (2017). *Artificial intelligence in healthcare: Past, present and future*. Stroke and Vascular Neurology, 2(4), 230–243.
- European Commission (2021). *White Paper on Artificial Intelligence – A European approach to excellence and trust*.
- Obermeyer, Z., & Emanuel, E. (2016). *Predicting the Future — Big Data, Machine Learning, and Clinical Medicine*. NEJM, 375, 1216–1219.
- Chui, M., Harryson, M., Manyika, J., et al. (2018). *Notes from the AI frontier: Applications and value of deep learning*. McKinsey & Company.

Figures

- Figure 1: Diagram depicting AI's impact on disease prediction.
- Figure 2: Graph showing adoption rates of AI technologies in hospitals worldwide.

Potential Applications of Artificial Intelligence in Healthcare Surveillance II.
Data Requirements and Practical Applications

K. Filyo, I. Negyesi

Abstract

This article focuses on the data requirements of healthcare surveillance systems and explores how AI technologies can address them. It discusses the importance of demographic, epidemiological, clinical, and environmental data in public health, and illustrates how AI supports the collection, analysis, and application of these data types. Through real-world examples such as COVID-19 tracking and malaria control, the article demonstrates the practical utility of AI in outbreak detection, resource allocation, real-time monitoring, and personalized healthcare. It concludes that AI significantly enhances the responsiveness and precision of surveillance systems in managing global health challenges.

Keywords: data-driven surveillance, outbreak detection, resource allocation, personalized medicine, real-time monitoring

Introduction

Effective healthcare surveillance depends on the availability and analysis of accurate, comprehensive data. Artificial intelligence (AI) offers powerful tools to meet the complex data requirements of surveillance systems. By integrating AI into data collection and analysis processes, healthcare systems can gain deeper insights into disease patterns and improve response strategies. This article examines the specific data needs of healthcare surveillance and explores practical applications of AI in addressing these requirements.

Data Requirements for Healthcare Surveillance

Healthcare surveillance systems rely on diverse data sources to provide a holistic view of public health. Key data requirements include:

- Demographic Data: Information such as age, gender, and geographic location is vital for identifying at-risk populations and tailoring interventions.
- Epidemiological Data: Tracking disease incidence, prevalence, and transmission patterns is essential for understanding the spread of infectious diseases and planning containment measures.
- Clinical Data: Patient symptoms, diagnostic results, and treatment outcomes provide valuable insights into disease progression and the effectiveness of interventions.
- Environmental Data: Factors such as temperature, humidity, and pollution levels can influence the spread of certain diseases, making environmental data a critical component of surveillance systems.

Practical Applications of AI

AI technologies have numerous practical applications in healthcare surveillance, enabling more efficient and accurate data analysis:

Outbreak Detection

AI systems can analyze data from multiple sources, such as social media, news reports, and hospital records, to identify early signs of disease outbreaks. For example, during the COVID-19 pandemic, AI tools were used to detect spikes in infection rates and predict the virus's spread, allowing for timely interventions.

Resource Allocation

Predictive algorithms can optimize the distribution of medical resources, such as vaccines and hospital beds, during health crises. By analyzing data on disease prevalence and healthcare capacity, AI systems can guide decision-makers in allocating resources where they are needed most.

Real-Time Monitoring

AI-powered dashboards provide real-time updates on global health trends, enabling healthcare providers and policymakers to respond quickly to emerging threats. These systems consolidate data from various sources, presenting actionable insights in a user-friendly format.

Personalized Medicine

AI can tailor healthcare interventions to individual patients based on their risk profiles. For example, predictive models can identify patients at high risk for complications from a particular disease, enabling targeted preventive measures.

Case Studies

Real-world examples demonstrate the transformative impact of AI in healthcare surveillance:

- COVID-19 Surveillance: AI tools played a crucial role in monitoring infection rates, guiding vaccine distribution, and predicting the pandemic's progression. These technologies provided insights that informed public health policies worldwide.
- Malaria Control: In regions prone to malaria outbreaks, AI models have been used to predict seasonal transmission patterns, enabling targeted interventions such as insecticide spraying and bed net distribution.

Conclusion

AI's integration into healthcare surveillance systems offers a transformative approach to data analysis and decision-making. By addressing the specific data requirements of surveillance efforts, AI can enhance the accuracy, efficiency, and impact of public health initiatives. As these technologies continue to evolve, their role in healthcare surveillance is poised to grow, paving the way for a more proactive and data-driven approach to global health challenges.

Bibliography

- Nagy, L. (2021). MI alapú felderítés az epidemiológiában. Magyar Epidemiológiai Folyóirat, 15(1), 23-35.
- Chen, Y., & Wang, L. (2019). Data-Driven Healthcare Surveillance. International Journal of Health Informatics, 32(4), 78-95.
- CDC. (2020). AI in Healthcare Surveillance. [URL]
- Ghosh, A., Gupta, R., & Sharma, R. (2021). Machine learning for COVID-19 detection and prognosis: a review. *IEEE Reviews in Biomedical Engineering, 14*, 61–73.
- Choi, E., Bahadori, M. T., Schuetz, A., Stewart, W. F., & Sun, J. (2016). Doctor AI: Predicting Clinical Events via Recurrent Neural Networks. *Machine Learning for Healthcare Conference*.
- Salathé, M., Bengtsson, L., Bodnar, T. J., Brewer, D. D., Brownstein, J. S., Buckee, C., ... & Vespignani, A. (2012). Digital Epidemiology. *PLOS Computational Biology, 8*(7), e1002616.
- Brownstein, J. S., Freifeld, C. C., & Madoff, L. C. (2009). Digital disease detection — harnessing the Web for public health surveillance. *New England Journal of Medicine, 360*, 2153–2157.
- Chan, M. S., et al. (2021). Real-time monitoring of influenza-like illness in Hungary using IoT and AI. *Hungarian Epidemiology Journal, 45*, 235–245.

Figures

- Figure 1: Diagram showing AI's role in outbreak detection.
- Figure 2: Graph comparing traditional and AI-based surveillance accuracy.

ANALYSIS AND ASSESSMENT OF FISCAL AND MONETARY POLICY RESPONSES TO THE EFFECTS OF THE RUSSIAN-UKRAINIAN CONFLICT

László Teknős

Ludovika University of Public Service

teknos.laszlo@uni-nke.hu

ORCID: 0000-0003-0759-5871

ABSTRACT

The outbreak of the Russian-Ukrainian conflict on 24 February 2022 has caused global economic and geopolitical instability, especially in the regions directly affected.

This paper aims to provide a comprehensive overview of the economic impact of the conflict, with a particular focus on the market consequences of the sanctions mechanisms, as well as the impact on unemployment, tourism, agriculture, energy security (energy prices, markets, supply chains), and changes in fiscal (budgetary) and monetary policy. The paper provides a detailed analysis of the economic policy responses to the crisis, highlighting the stabilisation measures implemented through monetary and fiscal instruments, the factors affecting economic growth and the practical applicability of various economic protection measures. New theoretical and practical approaches in economics are also presented.

The study pays particular attention to exploring the economic consequences for Hungary. It examines in detail the trade and financial effects, the development of country risk (e.g. changes in the forint exchange rate and yields), and the challenges affecting the production and supply chains of individual sectors. It

assesses the Hungarian fiscal and monetary policy responses, the economic implications of solidarity measures, and the economic aspects of the humanitarian aid and support programmes provided by the government. The analysis covers the measures taken by the Central Bank of Hungary, the professional discourse of Hungarian economists and the administrative, economic and social aspects of the packages of measures they propose.

Keywords: Russian–Ukrainian conflict; economic policy responses; fiscal policy; monetary policy; inflation; Hungarian economy

INTRODUCTION

The outbreak of the Russian-Ukrainian conflict on 24 February 2022 has had not only military and humanitarian consequences, [1] but also serious economic repercussions – globally, but particularly in Europe and Central and Eastern Europe. The disruption of energy markets, accelerating inflation, supply chain disruptions and an uncertain investment environment have posed new challenges for economic policy. The rapid deployment of traditional fiscal and monetary instruments has become necessary to enable policymakers to cope with soaring energy costs, falling real incomes and stalling economic growth. These effects were particularly acute in Hungary, which, with its open economy, high energy import dependency and limited fiscal space, was more sensitive to external shocks. The aim of this study is to explore and assess the fiscal and monetary responses, with a particular focus on the adjustment possibilities of the Hungarian economy.

ON THE ECONOMIC IMPACT OF THE RUSSIAN-UKRAINIAN CONFLICT

The escalation of the Russian-Ukrainian war in 2022 triggered radical changes in the global economic system, with effects extending to both macroeconomic indicators and structural relationships. The conflict affected energy prices, inflation

dynamics, international trade processes and supply chains, while sanctions brought new dimensions to the economic space.

At the global level, the war has primarily resulted in dramatic increases in the prices of energy carriers (oil, natural gas) and agricultural commodities (e.g. wheat, corn, sunflower oil). As both Russia and Ukraine were key players in global grain exports, the closure of export channels and the decline in production hit African and Middle Eastern countries particularly hard, as they are heavily dependent on agricultural exports from these countries. Fluctuations in world market prices for gas and crude oil have become a major source of inflationary pressure, which has hit low- and middle-income countries particularly hard.

In order to secure their supply chains, companies and governments are increasingly favouring "friendshoring" or "nearshoring" solutions, i.e. cooperation with politically reliable partners or production closer to home. In addition, geopolitical risks have played a greater role in international capital market movements, and investors have become more risk-averse, resulting in a volatile market environment.

Since the start of the war, the EU has clearly stood by Ukraine, recognising the country's right to self-defence and strongly condemning Russia's aggression, which it considers a violation of the UN Charter [2]. It has imposed sanctions for this reason [3].

Sanctions regimes and their market consequences: Sanctions imposed by the EU, the US and the G7 countries[20] affected the following areas: [4]

- Financial sector (e.g. exclusion of Russian banks from the SWIFT system[21]). Financial restrictions reduce investment, slowing economic growth. In March

[20] G7 countries: Group of Seven, an informal international forum comprising the seven most developed industrial democracies in the world. Canada, France, Germany, Italy, Japan, United Kingdom, United States. The European Union also participates in the work of the G7, although not as a full member, but as a permanent invitee. Russia was a member of the group between 1997 and 2014, when it operated under the name G8. However, in 2014, following the annexation of the Crimean peninsula, Russia's membership was suspended.

[21] The SWIFT system (full name: Society for Worldwide Interbank Financial Telecommunication) is a global financial messaging network used by banks and other financial institutions worldwide to conduct international

2022, seven Russian banks were excluded from the system, including VTB Bank and Bank Rossiya [5]. By december 2022, the number of excluded Russian banks had risen to 23, and Belarusian banks to 4.

- Energy market (restrictions on oil and gas imports).[22] Energy and commodity markets were particularly sensitive to the conflict. According to an OECD report [6], the Russian invasion caused further price increases in the European gas, nickel and wheat markets, which were already on an upward trend before the war. Russian foreign trade shifted towards China and India. By 2023, Russia had successfully redirected 60 % of its crude oil exports to Asia, mainly to India and China, while EU energy imports from Russia fell by 80 %.[7] However, this shift came at the cost of comparative advantages, lower prices had to be charged on Asian markets and transport costs rose by 40 % due to the distances involved.
- Technology transfers,
- Export restrictions (microchips, components),
- Personal sanctions against oligarchs and politicians. [8]

Sanctions against Russia [9] [23] were introduced in several stages by the EU and other Western countries starting in 2014, [4] primarily due to Russia's aggression against Ukraine and the annexation of Crimea. These sanctions are intended to weaken Russia's economic base, restrict access to critical technologies and markets, and reduce its military capabilities. [4] The main objective of the sanctions introduced in 2022 was to isolate Russia economically. [10] Lingen (2023) analysed the effectiveness of the sanctions through four channels. One of these was the military channel, where there was a visible decline in Russian military production, but

transactions. SWIFT does not move money or financial instruments, but securely transmits financial messages (e.g. transfer orders, account information) between financial institutions.

[22] On 5 december 2022, the European Union imposed an embargo on Russian crude oil as part of a package of sanctions against Russia in response to its invasion of Ukraine. Under the decision, EU Member States may no longer purchase Russian crude oil transported by sea. This ban does not apply to crude oil transported by pipeline (which affects Hungary, Slovakia and the Czech Republic, for example), but these are subject to specific exemptions and restrictions. The aim of the sanctions is to weaken the Russian economy by reducing its energy export revenues.

[23] First stage: 20 February 2014. Second stage: 24 February 2022.

this was partially offset by the procurement of components from third countries (e.g. Iran and North Korea). Budget channel: the Russian government deficit reached 4.2 % of GDP in 2023. The fourth channel is smart sanctions, which initially destabilised the Russian financial system, but the effects were mitigated by government support and the emergence of a shadow banking system. The social channel, according to which 40 % of the population has seen their standard of living decline. [11].

By June 2025, the EU had already adopted 17 sanction packages, including export bans, banking restrictions, suspension of broadcasting licences and freezing of assets of individuals and organisations. The sanctions affect not only Russia but also countries (Belarus, Iran, North Korea) that provide military support to Russia. The latest, 16th round of sanctions covers trade and import bans, such as a ban on imports of primary aluminium, whereby the EU has banned imports of primary aluminium originating in Russia. [12] Furthermore, the export of dual-use products, such as chemical precursors (e.g. substances that can be used to manufacture chemical weapons), software for CNC (computer numerical control) machines, and video game controllers (which can be used to control drones) has been banned. [13] Energy measures included a ban on support for Russian LNG projects and a temporary ban on the storage of Russian crude oil and petroleum products.

Restrictions on Russian ownership of road transport companies, aviation and port bans (e.g. two Moscow airports, Novorossiysk port), and action against the 'Shadow Fleet'. In addition, 13 more financial institutions were excluded from the SWIFT system. 48 individuals and 35 organisations were added to the sanctions list and their assets were frozen. Overall, the 16th package of sanctions targets Russia's sources of revenue, its military industry, transport and energy sectors, and the methods used to circumvent sanctions, while also tightening financial, media and personal sanctions.

Although the sanctions had a significant impact initially, Russia adapted to the situation, for example by redirecting energy exports to China and India. At the same time, however, it should be noted that the sanctions will limit the Russian economy's

growth potential and technological development in the long term. Restrictions on technology imports limit access to advanced technologies such as semiconductors, industrial equipment, aerospace and energy technologies, which hinders innovation and industrial modernisation. The forecast for the *2025 budget deficit* has tripled to 1.7% of GDP, mainly due to a 24% decline in revenues from energy exports. This suggests that sanctions will undermine the stability of the state budget in the long term. If money from energy exports dries up and there are no other sources of revenue (e.g. from technology or manufacturing), this will undermine the financial foundations of the economy and long-term economic stability could be at risk.

In terms of market consequences, *Russia became isolated***.** The initial collapse of the rouble was followed by artificial stabilisation, but foreign capital left the country. Commodity markets,[24] i.e. the world market prices of oil, natural gas, grain and metals, rose significantly. The price of natural gas rose by nearly 500% in Europe in 2022. The price of oil also jumped above USD 120 per barrel, then gradually stabilised. The price of Brent crude oil is currently around USD 62.14 per barrel, while the price of WTI (West Texas Intermediate) is USD 59.11 per barrel. Gas price fluctuations peaked at EUR 340/MWh in August 2022, a sixfold increase compared to the pre-war level of EUR 50/MWh. Although prices have partially stabilised by 2023, infrastructure changes (e.g. the development of LNG terminals in Germany) and the rapid introduction of renewable energy sources have permanently altered the structure of European energy supply. Among the countries of Central and Eastern Europe, Hungary and Slovakia proved to be more sensitive to price fluctuations, as their energy imports accounted for 8-10% of GDP. [15] The conflict is also accompanied by geopolitical realignments that affect global markets, investment confidence and economic performance. [16] One of the typical consequences of this has been the restructuring of the energy export market. Before the outbreak of

[24] The degree of price fluctuation, most commonly measured using standard deviation. It refers to the extent and speed at which the price of a financial instrument (e.g. a share, currency or index) changes over a given period of time. The greater and more frequent these price fluctuations, the higher the volatility. [14]

the war, Russia had the world's 11th largest nominal GDP[25], while ranking first in natural gas exports and third in crude oil exports. This position allowed it to use its energy exports as a geopolitical tool, particularly against the European Union, which sourced 40% of its gas imports from Russia in 2021.

The EU aims to become independent from Russian energy (REPowerEU programme). LNG investments have increased (USA, Qatar). Europe has lost its former price advantage over Far Eastern markets and now has to compete for the same LNG supplies, which further increases prices and market volatility. The shift towards renewable energy sources has accelerated. Europe's natural gas supply has now diversified significantly,[26] but in the short term there have been supply shocks and cost increases. The share of Russian gas imports in the EU was still 29.3% in 2019, falling to 5.4% by 2023. This shortfall has been mainly offset by increased imports of LNG (liquefied natural gas), particularly from the United States and Norway. [17] Russia has redirected its exports to eastern markets (the 'Power of Siberia' gas pipeline).[27] Also worth mentioning is the planned expansion of 'Power of Siberia 2', which would be a 2,600 km long gas pipeline transporting 50 billion cubic metres of gas per year from Russia to China via Mongolia. [19] The project is of strategic importance for Russia to compensate for the loss of European markets, but negotiations with China are progressing slowly, mainly due to pricing and the development of Chinese gas demand. [20] This would alleviate the loss of market

[25] Nominal GDP (gross domestic product) is an indicator of a country's economic performance, calculated at current market prices for a given period (e.g. one year). Nominal GDP includes the effect of inflation, i.e. if prices rise, nominal GDP may increase even if the quantity produced has not changed. It shows the total value of all goods and services produced at the prices of the given year. If in 2024 Russia produced 1 million (10^6) 1-litre bottles of Kalashnikov Red Army premium vodka at 10,000 (10^4) roubles per bottle, the nominal GDP would be: $10^6 \times 10^4 =$ 10 billion rubles ($10^6 \times 10^4 = 10^{10}$, i.e. 10 billion). If 1 million bottles are produced in 2025, but their price rises to 12,000 rubles due to inflation, then the nominal GDP will be: 1 million × 12,000 = 12 billion rubles.

This shows that GDP has grown, but only because of price increases, not because more was produced.

[26] The volume of gas imported from Russia will decrease from 150 billion cubic metres in 2021 to 52 billion cubic metres in 2024, and the share of Russian gas imports will fall from 45% to 19%. Russian coal imports have been banned by sanctions.

[27] The 'Power of Siberia' gas pipeline began operating in December 2019 and was completed in its entirety by the end of 2024. The pipeline is over 3,000 km long and capable of transporting 38 billion cubic metres of natural gas to China annually. [18]

share, but would not solve the problem, as 180 billion cubic metres of gas were previously supplied to Europe each year.

On 6 May 2025, the European Commission announced that it would completely end the EU's dependence on Russian energy. This includes stopping imports of Russian gas and oil and phasing out Russian nuclear energy.[28] The decision aims to increase energy security, accelerate the transition to renewable energy sources and strengthen the EU's strategic autonomy. [21] The Commission also proposed specific measures, such as improving energy efficiency, developing infrastructure and encouraging investment in renewable energy sources. The EU's goal is to become completely independent of Russian energy by 2027.

According to the European Central Bank (ECB), the war in Ukraine has increased uncertainty about the economic and inflation outlook for the euro area. As a result of the conflict, the ECB was forced to adjust its monetary policy, which affected the yield curve. As a result of the war, yields on European government bonds rose as investors demanded higher risk premiums due to increased uncertainty. According to the OECD report, long-term government bond yields rose overall, while the stock of negative-yielding debt declined significantly globally. [22]

War-induced inflation spread through two main channels: indirectly through higher energy and food prices, and directly through supply shocks resulting from disruptions in production chains. [23] In Russia, a 14% nominal increase in wages in 2022 served to sustain household consumption, but annual inflation of 9% resulted in a real decline in purchasing power. [24] According to an analysis by the Hungarian National Bank, indirect tax increases (e.g. special taxes) added a further 2-3 percentage points to inflationary pressures in the region.

[28] The EU is expected to replace up to 100 billion cubic metres of natural gas by 2030, reducing demand by 40-50 billion cubic metres by 2027. At the same time, LNG capacities are expected to increase by around 200 billion cubic metres by 2028, which is five times the EU's current gas imports from Russia.

The economic consequences of the shortage of critical raw materials include a 70% decline in neon production in Ukraine (a raw material for microchip manufacturing), which led to a global chip shortage, causing a loss of USD 200 billion in the automotive industry in 2022. [25] Cost increases in the metalworking industries (e.g. steel, aluminium) have led to price increases of 15-20% in end products. In Central Europe, Polish and Hungarian automotive suppliers reported a 30% drop in capacity utilisation due to component shortages. As part of its 'RePowerEU' initiative, the EU has supported the internal extraction of critical raw materials (e.g. rare earths) with investments of EUR 15 billion, reducing external dependence.

In terms of unemployment, the official Russian unemployment rate has not risen dramatically, but hidden unemployment and underemployment have increased significantly. In Ukraine, due to active fighting and the destruction of infrastructure, unemployment rose above 30% in 2022. In March 2025, Ukraine's unemployment rate was 12.1%, the lowest since the start of the full-scale war. [26] However, according to the IMF's April World Economic Outlook, the annual unemployment rate is expected to be around 11.6% in 2025. [27]

In summary, the Russian-Ukrainian war has had serious economic consequences for both countries and has also had a significant impact on the global economy. The conflict has highlighted the importance of managing economic dependencies and geopolitical risks.

THE ECONOMIC IMPACT OF THE RUSSIAN-UKRAINIAN CONFLICT ON HUNGARY

The effects of the war were particularly acute in Hungary, as the country was heavily exposed to Russian energy sources and also suffered direct impacts due to its geographical proximity. The Hungarian economy declined in real terms. GDP growth stalled and inflation reached 20% in 2023, one of the highest rates in the European Union.

The Russian-Ukrainian war had a significant economic impact on Hungary, particularly due to its open economic[29] structure [28], which is heavily dependent on foreign trade [29] and energy imports. [30] In terms of energy prices and energy import dependency, Hungary is a major energy importer, particularly of natural gas and crude oil, most of which previously came from Russia. The war and sanctions have led to a sharp rise in energy prices, which has had a severe impact on the Hungarian economy and budget. The increase in gas imports alone caused an additional expenditure of HUF 6,386 billion for the Hungarian economy.

Hungary is considered one of the most open economies in the world.[30] The combined value of foreign trade (exports and imports) is close to, and sometimes exceeds, GDP, indicating extreme openness. This indicator is also exceptionally high in international comparison; in 2015, for example, only nine countries were more open than Hungary.

- High export/GDP ratio: Hungary's economy is extremely export-oriented. Exports can reach more than 80% of GDP in some years, which is one of the highest ratios in the EU.
- Presence of multinational companies: Many large global companies operate in Hungary (e.g. Audi, Mercedes-Benz, Bosch, Samsung, Huawei, etc.), and these companies are predominantly exporters.

The war has had a negative impact on 75 % of Hungarian businesses, particularly in energy-intensive sectors such as chemicals, construction and manufacturing. There has been a significant decline in investment among small and medium-sized enterprises, while export-oriented companies have been hit by the loss of Eastern markets. Although the share of Hungarian exports to Russia and Ukraine is relatively low (around 3.6 %), Hungarian companies sold HUF 695.8 billion less on the Russian market due to the war. [32] The number of companies and

[29] Export-oriented: exports account for a large share of GDP (e.g. automotive industry, electronics). Import-dependent: mainly energy (gas, oil), raw materials, components. Small open economy: external influences have a rapid impact.

[30] Hungary is one of the most open economies in the world. [31]

employees affected is significant, with manufacturing and trade being particularly sensitive to the changes. The income situation of households also deteriorated: consumption fell due to a sharp rise in food prices and cuts in utility subsidies.

The embargo and rising energy prices contributed to inflation in Hungary. In 2023, inflation exceeded 25 %, one of the highest rates in the EU. This high inflation weakened household purchasing power and increased economic uncertainty. The government sought alternative routes to secure energy supplies, such as Russian gas imports via Turkey. In addition, Hungary maintained its economic ties with Russia, particularly in the energy sector, including nuclear energy.

External financing exposure. The exchange rate of the forint is highly volatile, which increases the cost of external financing in times of crisis. The value of the forint changes rapidly and frequently in relation to other currencies (e.g. the euro or the dollar) – often fluctuating significantly within a short period of time. What causes volatility? On the one hand, external shocks such as war, energy crises and inflationary concerns. Rising energy prices fuel inflation on the import side and push up prices. Investor sentiment: if investors turn away from the forint, this can cause significant movements. On the other hand, central bank decisions can also play a role if monetary policy is not credible or consistent enough. Furthermore, high external debt and a weak balance of payments can also be factors. The forint may weaken due to rising import costs and a balance of payments deficit. However, a weaker forint could boost exports, which would partially offset the shock. The departure of foreign-owned companies and foreign investors (e.g. during times of risk aversion) makes the financial system vulnerable. [33]

Structural problems and one-sided economic dependence. Strong dependence on the automotive industry (especially German multinationals) means that a global decline in demand (e.g. COVID, chip shortages, technological change) quickly spreads. Innovation and productivity indicators are weak in regional comparison, which limits the internal economy's ability to defend itself. Overall effect: output declines, inflation rises – stagflationary pressures. Under a fixed exchange rate

regime, the central bank defends the forint exchange rate and does not allow it to depreciate. The central bank burns foreign exchange reserves to maintain the exchange rate. Monetary policy is not free – it cannot regulate interest rates independently. Monetary policy is only effective with a flexible exchange rate.

Real economic shocks, such as disruptions in production chains, influence the functioning of the economy through expectations in neoclassical models. As a result of the Russian-Ukrainian war, the structure of Hungarian industrial and agricultural exports has also changed, while global uncertainty has reduced the appetite for investment. [34]

Geopolitical risks caused Hungarian government bond yields to rise significantly, increasing the cost of new financing by HUF 1968.9 billion.31 The budget deficit increased, but the government sought to manage the crisis without resorting to external borrowing. [35]

IMF32 forecasts real GDP growth of 1.4 % for 2025. [36] In terms of challenges, the Hungarian economy contracted by 0.2 % on a quarterly basis in the first quarter of 2025, the fourth decline in the last six quarters. Inflation remains high at around 4.9 %. The 2026 budget anticipates 4.1 % growth, which the Fiscal Council considers overly optimistic, as the IMF forecasts only 2.6 %. Global trade tensions, particularly US tariff measures, could negatively affect the export-oriented Hungarian economy. Budget reserves are low, limiting the government's room for manoeuvre in the event of unexpected economic shocks.

FISCAL AND MONETARY MEASURES

Fiscal policy (also known as budgetary policy) is a tool of economic policy used by the state to influence the functioning of the economy by regulating public

[31] According to research by Századvég, Hungary incurred costs of approximately HUF 9,100 billion in the first three years of the war, which represents more than 2% of GDP. These costs were incurred in three main areas: the ‘war surcharge’ on gas imports (HUF 6,386.3 billion), additional financing costs due to the rise in government bond yields (HUF 1,968.9 billion), and the decline in exports to the Russian market (HUF 695.8 billion).

[32] International Monetary Fund. An international financial institution whose purpose is to promote global financial stability, support cooperation between currencies, stimulate economic growth and reduce poverty worldwide.

revenues (e.g. taxes) and expenditures (e.g. public services, subsidies, investments). Its main objectives include stimulating economic growth (e.g. through public investment); increasing employment; keeping inflation under control; making income distribution fairer; and ensuring the balance of public finances (managing deficits and debt). Its tools include tax policy (tax rates, changes in types of taxes, e.g. personal income tax, VAT) and expenditure policy (level and direction of public spending, e.g. education, health, military spending). Types Expansionary fiscal policy: increasing public spending or reducing taxes → stimulating the economy, and restrictive fiscal policy: reducing spending or raising taxes → curbing inflation, reducing deficits. If necessary, fiscal policy is used in conjunction with monetary policy (central bank interest rate and money supply regulation) to maintain economic balance.

In terms of fiscal measures

In the EU: Government spending has skyrocketed due to household and corporate support (e.g. energy price compensation), and public debt has increased (e.g. Germany's €100 billion energy crisis fund). Total defence spending by EU Member States[33] increased by more than 30 % between 2021 and 2024, reaching an estimated €326 billion in 2024.[34] [38]

Reducing budget deficits: According to the European Commission's forecast for 2024, the EU's general government deficit is expected to fall by 0.4 percentage points to 3.1% of GDP, driven by revenue surpluses and fiscal consolidation efforts. Growth prospects: However, fiscal tightening has raised concerns about its impact on economic growth. According to the IMF and other economic analysts, fiscal consolidation could reduce euro area growth by around 0.35 percentage points per year between 2025 and 2027. The EU's fiscal policy between 2022 and 2024 has

[33] Revenues are also worth mentioning. The European defence industry generated €158.8 billion in revenue in 2023, which is 16.9% higher than in 2022 and 28.5% higher than in 2021.

[34] During Russia's aggression in Crimea in 2014, EU military spending was EUR 147 billion (as in 2012-2013), rising to EUR 240 billion in 2022 and EUR 336 billion in 2024. This represents an increase of 228% compared to 2014. [37]

gradually shifted from crisis management to fiscal sustainability and structural reforms. The introduction of a new fiscal framework and efforts to reduce budget deficits aim to ensure economic stability and long-term growth.

With regard to Russia: According to the model developed by Ghironi et al. (2024) [39], sanctions resulted in a 30% decline in Russian GDP in the first year after the war, but the economy's ability to adapt (e.g. import substitution) mitigated the effects. [40]

Increased military spending (approx. USD 149 billion in 2024).[35]

Revenue losses due to Western sanctions and the departure of Western companies. Lower oil and gas prices, declining export revenues. Fiscal responses such as increasing military spending to more than 7 % of GDP. Corporate and income tax increases to replace revenue. Creation of funds: e.g. use of the National Welfare Fund to cover the budget deficit. This is also an expansionary policy, but due to revenue difficulties, it is accompanied by higher tax increases, which makes it risky. Due to falling oil prices, the budget deficit is expected to rise to 1.5 % of GDP, three times the previous target. Due to slowing economic growth and rising inflation (7 %), the central bank kept its base rate at 21%. Despite war spending and sanctions, Russia's economy grew by 4.3 % in 2024, but growth is expected to slow significantly in 2025.

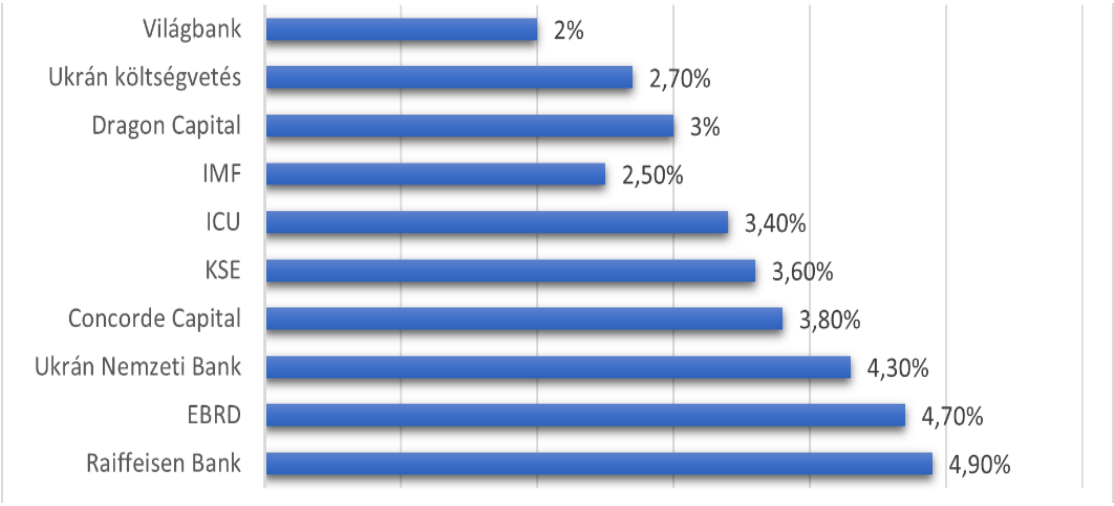
Looking at Ukraine: The country's revenues fell (tax revenues decreased due to the war). Expenditures increased dramatically (maintaining the army, supporting refugees, public services). The budget has basically switched to a war economy,[36]

[35] USD 65.9 billion in 2021; USD 86.4 billion in 2022; USD 109 billion in 2023; USD 149 billion in 2024. This represents a 226% increase compared to 2021. [41]

[36] Since 2022, the EU has provided €50.3 billion in support to the Ukrainian armed forces. As a result of the adoption of the third package of sanctions against Russia on 28 February 2022, approximately €210 billion worth of Russian central bank assets have been frozen in the EU. [42]

with international aid (IMF, World Bank, EU) keeping things going. Increased spending: nearly 50 % of the budget has been spent on defence and internal security. Reliance on international aid: the IMF, World Bank, EU and US financial aid cover the deficit. The budget deficit has increased but is acceptable given the extraordinary circumstances. This is a typical expansionary fiscal policy[37] in a war environment. Due to the war, significant amounts are being spent on defence, social support, infrastructure reconstruction and economic stimulus programmes. [43]

The IMF has forecast GDP growth of 2-3 % for 2025. As a result of the war, labour shortages and damage to energy infrastructure pose significant obstacles to economic growth. Inflation is high, reaching 12.9 % in January, mainly due to rising food and wage costs. The IMF and Ukraine have agreed on a new financing package of approximately $1.1 billion to address the economic challenges of the war.



1. figure. Forecasted GDP Growth in Ukraine for 2025 by Various Organizations and Companies (expressed in percentage)

[37] It refers to a package of government economic policy measures aimed at stimulating economic growth, particularly during times of economic downturn or recession. The essence of expansionary fiscal policy is that the government injects money into the economy in various ways, thereby increasing aggregate demand, real income and employment.

(Prepared by: Oeconomus Economic Research Foundation) [44]

If the war continues with the same intensity in 2025 – i.e. there are no larger or more serious attacks than before, and the conflict does not spread further – then most analyses suggest that the Ukrainian economy will perform similarly to last year, 2024. The International Monetary Fund (IMF) forecast real GDP growth of 3 % for last year, which is expected to be achieved, and the rate of growth in gross domestic product is likely to be similar in 2025. The Ukrainian central budget is more pessimistic, forecasting economic growth of 2.7 % for this year, while independent analysts expect higher growth of 3.7 %. The National Bank of Ukraine has also published its expectations on the subject: according to their forecast, which is the most optimistic to date, GDP could grow by 4.3 % in 2025. [44]

The consequences of fiscal expansion include rising inflation and increased tax burdens, but these are specific to a war economy and are necessary for survival and maintaining the functioning of the economy. Ukraine is currently pursuing an expansionary fiscal policy, the main objectives of which are to sustain the economy, ensure basic state functions and mitigate the damage caused by the war, all with significant external financial support.

Both countries are pursuing expansionary fiscal policies, but from different sources. Ukraine is relying on international aid, while Russia is drawing on its own reserves and tax increases.

The Hungarian economy has not been left untouched, requiring complex fiscal, monetary and administrative responses. Keynesian economic policy favours state demand stimulation in crisis situations, primarily through budgetary (fiscal) instruments. According to Keynesian theory, in times of crisis, the state must actively intervene in the economy (e.g. price regulation, subsidies, price freezes, direct budget transfers). Due to the supply shock and decline in demand caused by the

war, temporary price freezes, utility price protection measures and targeted transfers were also implemented in Hungary. [45] Measures introduced as part of fiscal adjustment (e.g. price caps, direct subsidies, sectoral surcharges) are economic instruments frequently used in times of crisis to share the risk between the population and the state. [46]

According to the monetarist approach, inflation is primarily a monetary[38] phenomenon. The rise in energy prices triggered by the Russian-Ukrainian conflict generated significant inflation in Hungary, to which the Magyar Nemzeti Bank (MNB) responded with a strict interest rate hike policy. [47]

Multifactor crisis management models (e.g. frameworks used by the OECD and IMF) recommend a combination of fiscal, monetary and structural measures. In line with EU regulations, Hungary introduced 'extra profit taxes' and a utility protection fund aimed at protecting the population while also ensuring budgetary balance. [48]

Centralised decision-making was strengthened in the period 2022–2023, including through the Economic Protection Operational Staff and various action plans. The practice of rapid response and strata intervention fits well into the top-down crisis management model. [49] The V4 countries and other Central and Eastern European states faced similar challenges. Common features include inflation management through monetary tightening (Poland, Czech Republic) and targeted forms of budgetary support (e.g. energy subsidies for households in Slovakia). Hungary's economic crisis management measures draw on a variety of economic approaches and have been implemented in a very active and centralised manner.

[38] According to monetarist theory, however, the primary means of controlling inflation are interest rate policy and the regulation of the money supply.

Measure	Characteristic	Remark
Food and fuel price cap	State-regulated prices	In 2022, it was one of the strictest price regulation systems in the EU
Introduction of windfall taxes	Sector-specific extra taxes in 8 sectors	E.g., banks, energy providers, telecommunications
Transformation and maintenance of utility cost reduction	Strongly focused on protecting households	The most extensive energy price compensation system
Export restrictions on certain products	E.g., grain, timber	State market regulation aimed at supply security
Economic Protection Operational Task Force	Centralized crisis management	Decision-making was centralized with fast mechanisms

Figure 2. Measures and interventions taken by Hungary

Poland's measures included energy price compensation subsidies, VAT reductions on food and energy, and an interest rate hike cycle by the central bank. [50] Anti-inflationary measures (VAT reduction) eased prices. The budget is more controlled than in Hungary, but there were populist elements (e.g. large transfers before the elections).

In Slovakia, sectoral taxes are not typical, there is state compensation for energy prices and inflationary effects are mitigated. [51] Sustainable fiscal response. Energy subsidies were financed from EU funds. Lower social outreach, fewer household benefits, narrower target group. Inflation rose moderately, with the aim of maintaining economic stability.

Czech Republic: targeted social and energy policy measures. Energy price compensation package, no direct price regulation to combat inflation; monetary

policy: interest rate hike. [52-54] Inflation remained relatively low – through targeted energy subsidies, not through official price controls. Budget deficit kept under control – no price caps or extra profit taxes introduced. Social support targeted at those in need. No spectacular populist measures, but effective in terms of stability. [52]

Inflation in Hungary [55] will be the highest in the EU between 2022 and 2023, and price caps have distorted the market. The budget balance has been disrupted, particularly due to the costs of price caps and utility subsidies. Social protection is visible and extensive, but often untargeted (e.g. everyone received price caps). Some elements are unsustainable in the long term (extra profit taxes are holding back investment). [56; 57]

Country	Price Regulation	Windfall Taxes	Energy Subsidies	Crisis Management Approach
Hungary	Yes, wide-ranging	Yes, for many sectors	Strongly supported	Centralized, direct
Poland	Partial (VAT reduction)	Not typical	Targeted	Moderate, targeted
Slovakia	Not typical	Not typical	Temporary support	EU-compliant, moderate
Czech Republic	No price regulation	Not typical	Targeted, market-oriented	Decentralized, market-friendly

Figure 3. Comparative table of measures taken by the V4 countries

Hungary's crisis management is unique in the region in its direct, centralised and highly interventionist nature, which can be considered extremely active from both a Keynesian and crisis management perspective. In contrast, the other V4 countries have used more targeted and less regulatory instruments.

The Czech Republic's fiscal response can be considered the most balanced and effective in the long term, as it did not distort the market, protected those most in need and did not destroy the fiscal balance. According to the IMF, Czech fiscal policy remained prudent, avoiding excessive spending while providing adequate support to the economy.

In terms of monetary policy measures

The Russian-Ukrainian conflict (since February 2022) has caused a serious *economic shock* in Central Europe, particularly through inflation, rising energy prices and supply chain disruptions. The *monetary policy responses* of Poland, the Czech Republic, Slovakia and Hungary were similar in many respects, but not identical.

Poland raised its base rate. Due to the war and inflation, the NBP began aggressive interest rate hikes (between the end of 2021 and mid-2022), peaking at 6.75 % in September 2022. Due to high food and energy prices, the central bank's main objective was to curb inflation. Stabilisation of the zloty: War risks weakened the zloty; the NBP also defended the exchange rate through market interventions (foreign exchange market intervention).

Czech Republic – Česká národní banka (ČNB). Strong interest rate hikes. Tightening had already begun before the war, but the process was accelerated in 2022: base rate 7 % (June 2022). Inflation in the Czech Republic exceeded 18% in 2022, and the ČNB, as a strong and independent institution, responded with tough measures. Defence of the koruna: The central bank also used foreign exchange reserves to stabilise the koruna's exchange rate fluctuations.

Slovakia – Národná banka Slovenska (NBS). Limited room for manoeuvre, as Slovakia is a member of the eurozone, meaning that monetary policy is determined

not by its own central bank but by the European Central Bank (ECB). The ECB reacted more slowly to the crisis, but began raising interest rates in mid-2022, to around 4.5 % by 2023. Inflation in Europe ranged between 8% and 12 % in 2022, mainly due to rising energy and food prices (which put upward pressure on inflation). To curb inflation, the ECB began aggressive interest rate hikes. The Russian central bank raised its base rate to 20% in 2022 to defend the rouble, then gradually lowered it. The NBS was more involved in crisis management through financial stability analyses and recommendations.

Hungary – Magyar Nemzeti Bank (MNB). Radical interest rate hikes. Continuous interest rate hikes from June 2021 to October 2022, with the base rate rising to 13 %, the highest in the region. Stabilisation of the forint: The war, energy crisis and domestic political uncertainty combined to weaken the forint significantly. The MNB also used foreign exchange reserves and verbal intervention. Special note: Amid conflicts with fiscal policy, the MNB tried to act independently to combat inflation.

After the outbreak of the war, the Magyar Nemzeti Bank continued the cycle of monetary tightening that it had begun in 2021. In the first half of 2022, the central bank tightened monetary conditions at all of its interest rate-setting meetings. The MNB's Financial Stability Report of May 2022 highlighted that 'domestic banks are well prepared for the rising risks in the wake of the Russian-Ukrainian war: capital and liquidity buffers make institutions resilient, even in the event of prolonged geopolitical tensions'. The central bank decided to tighten monetary policy in order to achieve its inflation target, which was one of the strictest in Europe.

After the outbreak of the war, banking system liquidity peaked in February 2022 at its highest level ever, close to HUF 11,550 billion. At the end of the quarters – in March and June – the MNB's tenders temporarily reduced excess liquidity. The central bank also announced swap tenders providing euro liquidity at the end of the quarters. [58]

By July 2022, the base rate was only 7.75 %, while inflation was already above 10 %. HUF: 430 HUF/EUR – began to raise interest rates, up to 13 % (in October 2022,

1240 basis points) – The forint strengthened, but inflation was 25%. Related measures: increase in the reserve requirement ratio; regularisation of discount bond auctions; introduction of longer-term deposit instruments, etc.

Liquidity management measures: The MNB used several tools to restrict liquidity in the banking system, including raising the reserve requirement ratio to 5 % and introducing long-term deposit instruments.

*Money market stability***:** keeping the base rate high.

In 2022, the MNB pursued one of the tightest monetary policies in Europe. Between June and August, it raised the base rate by 635 basis points to 11.75 % in order to curb inflation and stabilise the forint exchange rate. On 14 October 2022, it implemented an extraordinary 500 basis point increase in the policy rate in response to unprecedented pressure on financial markets and a wave of forint depreciation. The aim of the interest rate hike cycle was to anchor inflation expectations, restore price stability and maintain financial stability.

*Interest rate caps***.** Measure: maximum interest rates on retail and corporate loans (e.g. on personal loans from October 2022). Objective: to reduce borrowing costs and maintain solvency. Impact: reduced instalments in the short term. Distorted the lending market and weakened interest rate transmission in the long term. Reduced banks' profitability. Even after the end of the interest rate hike cycle, the MNB emphasised that it was ready to take further extraordinary measures to maintain market stability.

As a result of these measures, the forint exchange rate strengthened significantly and there was a spectacular fall in yields on the government securities market, which contributed to calming the financial markets.

*Mandatory reserve requirements in 2023***:** maximum optional reserve ratio of 10 % from April.

*Base rate cut in 2024***.** The base rate was reduced every month by a total of 375 basis points, falling from 10.75 % to 7.75 % at the end of June, and then to 6.5%.

Simplification of the toolkit. At the end of January, variable-rate deposit instruments with a maximum maturity of six months were phased out.

Green financing programmes: from January 2025: support for sustainable investments and projects (green lending – capital requirement waivers – for households, small businesses and local governments).

The central bank's primary objectives were to reduce inflationary pressures, maintain financial stability and protect the forint exchange rate, which it achieved mainly through significant interest rate hikes and liquidity management tools. [59-62]

SUMMARY

The Russian-Ukrainian war broke out in February 2022 and has since had a profound impact not only on the two countries involved, but on the entire world, especially from an economic perspective. Following the outbreak of the war, rapid and significant changes took place on the world market, with energy and raw material prices skyrocketing, supply chains disrupted, new geopolitical blocs emerging and inflation remaining persistently high at the global level.

The *European Union* was particularly sensitive to the economic impact of the war, as it was heavily dependent on Russian energy supplies. In the wake of the conflict, the EU was forced to make rapid changes to its energy policy, as part of which Member States began to gradually reduce their dependence on Russian gas and oil imports. One striking example of this is the REPowerEU programme, which aims to promote the expansion of renewable energy sources and the rapid introduction of energy-saving measures. However, in the short term, these measures have led to higher energy prices and a decline in industrial production.

Inflationary effects became increasingly apparent in the EU economy between 2022 and 2023, with consumer price indices reaching historic highs in several member states and economic growth slowing significantly. The

consequences of the Russian-Ukrainian war thus also led to a weakening of economic confidence and budgetary constraints. In addition, countries neighbouring Ukraine, such as Poland, Slovakia and Hungary, were directly affected by the refugee crisis, which placed an additional burden on national budgets.

The EU stands united and consistent in its support for Ukraine against Russia's aggression, imposing unprecedented sanctions against Russia and its allies, while providing significant political, economic, military and humanitarian support to Ukraine.

The war has accelerated the EU's dual trade strategy: on the one hand, it has reduced its dependence on Russian energy sources and, on the other, it has deepened trade relations with alternative partners (e.g. Azerbaijan and Norway). Among the V4 countries (Poland, the Czech Republic, Slovakia and Hungary), Poland's exports increased by 12 % by 2023, partly due to growing global demand for military products.

The economic impact of the conflict reveals a complex network of relationships, with sanctions causing short-term damage but structural changes having long-term consequences. Strengthening regional cooperation to ensure the flexibility of supply chains is recommended.

The economic impact of the Russian-Ukrainian war will continue to be felt in Hungary and Europe in the long term.

Hungary's vulnerability is structural in nature. It is a small, open, energy-import-dependent economy with limited fiscal room for manoeuvre and strong external exposure. Therefore, in the event of a *global shock* (pandemic, war, energy price surge, interest rate hike, supply chain disruptions), the Hungarian economy is affected to a *greater extent than average*. The transformation of the global energy market, the vulnerability of supply chains and the reactions of financial markets have presented decision-makers with new challenges. Hungary is a good example

of how small, open economies are particularly sensitive to this type of geopolitical crisis.

The Hungarian response – including interest rate policy, price controls, windfall taxes and the system of state intervention – reflects a mixture of Keynesian and monetarist approaches in theory, and an extremely centralised crisis management model in practice. Compared to other countries in the region, Hungary has been among the most active in terms of intervention, but the long-term fiscal impact of these measures is still being assessed.

The scope for fiscal and monetary policy was limited, but government measures were essential to ensure a rapid response and maintain social stability.

Due to the openness of the Hungarian economy and its dependence on energy imports, the effects of the war have been particularly severe, taking the form of energy price shocks, inflation, loss of export markets, slower growth and budgetary burdens.

In the future, it will be crucial to increase energy independence, diversify supply chains and develop crisis-proof economic structures. Economic thinking must also adapt to new types of challenges, which are not only economic but also political and social in nature.

REFERENCES

[1] Csáki, Gy. A 2022. évi orosz–ukrán háború gazdasági következményei. Nemzet és Biztonság folyóirat (2021/3. szám)

[2] Council of the European Union. (n.d.-b). Russia's war against Ukraine. *Consilium Europa*. https://www.consilium.europa.eu/hu/topics/russia-s-war-against-ukraine/

[3] Európai Unió Tanácsa. (2023). Az Oroszország Ukrajna elleni agresszív háborúja: az EU elfogadta a gazdasági és egyéni szankciók 11. csomagját [Sajtóközlemény]. EU Tanács.

[4] Csehes, L., & Tóth, Á. (2023). Hogyan hatnak a szankciók Oroszországra, és hogyan védekezik Moszkva? Külügyi Szemle, 22(2), 46-65.

[5] Perez, C. (2022). What does Russia's removal from SWIFT mean for the future of global commerce? *Foreign Policy*. https://foreignpolicy.com/2022/03/08/swift-sanctions-ukraine-russia-nato-putin-war-global-finance/

[6] Organisation for Economic Co-operation and Development (OECD). (2022). *Impacts of the Russian invasion of Ukraine on financial market conditions and resilience: Assessment of global financial markets* (OECD Publishing). https://doi.org/10.1787/879c9322-en

[7] Kim, D. (2024). *Economic sanctions: Lessons from the Russia–Ukraine conflict*. Poole College of Management, NC State University. https://poole.ncsu.edu/thought-leadership/article/economic-sanctions-lessons-from-the-russia-ukraine-conflict/

[8] Európai Unió Tanácsa. (2024). Uniós szankciók Oroszország ellen. Consilium.europa.eu.

[9] Council of the European Union. (2024). *Uniós szankciók Oroszország ellen*. Consilium.europa.eu. https://www.consilium.europa.eu/hu/topics/russia-s-war-against-ukraine/

[10] Council of the European Union. (n.d.). *Sanctions against Russia*. Consilium.europa.eu. https://www.consilium.europa.eu/hu/policies/sanctions-against-russia/

[11] Bod, P. Á. (n.d.). *Orosz–ukrán háború és gazdaság – makroadatok tükrében*. Privatbankár. https://privatbankar.hu/cikkek/benchmark/bod-peter-akos-orosz-ukran-gazdasag-makroadatok.html

[12] Kneppelhout. (2024). *The European Union adopts 16th sanctions package against Russia*. https://kneppelhout.com/news/the-european-union-adopts-16th-sanctions-package-against-russia/

[13] DS Avocats. (2024). *16th sanctions package*. https://www.dsavocats.com/en/16th-sanctions-package/

[14] Capital.com. (n.d.). *Volatility – Definition*. https://capital.com/hu-hu/learn/glossary/volatility-definition

[15] Daianu, Daniel and Grosu, Tudor and Neacsu, Andrei and Tanase, Andrei and Vranceanu, Radu, Macroeconomic Consequences of the War in Ukraine on Central and Eastern European Economies: A SVAR Analysis (2024). ESSEC Business School Research Paper No. 2407, Available at SSRN: https://ssrn.com/abstract=5064007

[16] Caldara, D., & Iacoviello, M. (2022). *Measuring Geopolitical Risk*. American Economic Review, 112(4), 1194–1225. DOI: 10.1257/aer.20190332

[17] Deák András György: Az orosz energia után - Az európai ellátás új térképe

[18] Gazprom. (n.d.). *Power of Siberia*. https://www.gazprom.com/projects/power-of-siberia/

[19] Világgazdaság. (2023). *Jövőre kezdik építeni a következő orosz gázvezetéket Kína felé*. https://www.vg.hu/nemzetkozi-gazdasag/2023/10/jovore-kezdik-epiteni-a-kovetkezo-orosz-gazvezeteket-kina-fele

[20] Walsh, B. (2023, március 29). *Russia is doubling down on fossil fuels in China*. Time. https://time.com/6265109/russia-china-fossil-fuels-siberia-2/

[21] European Commission. (2025, április 24). *Ukraine: EU continues support with €1.5 billion under Macro-Financial Assistance+*. https://ec.europa.eu/commission/presscorner/detail/en/ip_25_1131

[22] OECD (2022), *Impacts of the Russian invasion of Ukraine on financial market conditions and resilience: Assessment of global financial markets*, OECD Publishing, Paris, https://doi.org/10.1787/879c9322-en.

[23] Daianu, Daniel and Grosu, Tudor and Neacsu, Andrei and Tanase, Andrei and Vranceanu, Radu, Macroeconomic Consequences of the War in Ukraine on Central and Eastern European Economies: A SVAR Analysis (December 16, 2024). ESSEC Business School Research Paper No. 2407, Available at SSRN: https://ssrn.com/abstract=5064007

[24] Bod, P. Á. (n.d.). *Orosz–ukrán háború és gazdaság – makroadatok tükrében*. Privatbankár. https://privatbankar.hu/cikkek/benchmark/bod-peter-akos-orosz-ukran-gazdasag-makroadatok.html

[25] Economx.hu. (2022). *Neonhiány és chiphiány: az orosz–ukrán háború hatása az ellátásra*. https://www.economx.hu/tech/neonhiany-orosz-ukran-haboru-chiphiany-gyartas-ellatas.749012.html

[26] Centre for Economic Strategy. (2024). *Tracker: Ukrainian economy during the war*. https://ces.org.ua/en/tracker-economy-during-the-war/

[27] International Monetary Fund (IMF). (2024). *World Economic Outlook: Real GDP growth*.https://www.imf.org/external/datamapper/NGDP_RPCH@WEO/OEMDC/ADVEC/WEOWORLD

[28] Palócz Éva – Kopint-Tárki tanulmányok: A külkereskedelmi szerkezet és a nyitottság vizsgálata;

[29] Éltető Andrea (MTA KRTK): *A magyar gazdaság integrációja a globális értékláncokba. MTA KRTK.*

[30] Csath, M. (2022). Versenyképesség és gazdasági növekedés az EU-ban és Magyarországon. Budapest: Akadémiai Kiadó.

[31] Osszkép Magazin. (2017). *Magyarország a világ egyik legnyitottabb országa*. https://osszkep.hu/2017/03/magyarorszag-a-vilag-egyik-legnyitottabb-orszaga/

[32] Századvég. (2022). *Az orosz–ukrán háború és Ukrajna gyorsított EU-csatlakozásának költségei Magyarország szempontjából*. https://szazadveg.hu/cikkek/az-orosz-ukran-haboru-es-ukrajna-gyorsitott-eu-csatlakozasanak-koltsegei-magyarorszag-szempontjabol/

[33] Financial Times. (2023, december 5). Hungary embraces Chinese EV investment in push to be-come manufacturing hub. Financial Times. https://www.ft.com/content/ca5f5ce6-46ad-4a34-80b1-b0f7d4b17d58

[34] Lucas, R. E. (1972). Expectations and the Neutrality of Money. *Journal of Economic Theory*, 4(2), 103–124.

[35] Index.hu. (2024). *Háború, szankciók, évforduló – Gazdasági mérleg az orosz–ukrán konfliktusról*. https://index.hu/gazdasag/2024/02/24/haboru-oroszorszag-ukrajna-evfordulo-szankciok/

[36] International Monetary Fund (IMF). (n.d.). *Hungary – Country information*. https://www.imf.org/en/Countries/HUN?utm

[37] Council of the European Union. (n.d.). *Defence in numbers*. https://www.consilium.europa.eu/hu/policies/defence-numbers/

[38] European Commission. (2024). *Autumn 2024 economic forecast: Gradual rebound in adverse environment*. https://economy-finance.ec.europa.eu/economic-forecast-and-surveys/economic-forecasts/autumn-2024-economic-forecast-gradual-rebound-adverse-environment_en

[39] Ghironi, F., Kim, D. & Ozhan, G.K. International Economic Sanctions and Third-Country Effects. *IMF Econ Rev* **72**, 611–652 (2024). https://doi.org/10.1057/s41308-023-00232-9

[40] Kim, D. (2024, február 26). *Economic sanctions: Lessons from the Russia–Ukraine conflict*. Poole College of Management, NC State University. https://poole.ncsu.edu/thought-leadership/article/economic-sanctions-lessons-from-the-russia-ukraine-conflict/

[41] Trading Economics. (n.d.). *Russia - Military expenditure*. https://hu.tradingeconomics.com/russia/military-expenditure

[42] Council of the European Union. (n.d.). *Military support for Ukraine*. https://www.consilium.europa.eu/hu/policies/military-support-ukraine/

[43] Economic.karpat.in.ua. (2024). *Az ukrán gazdaság 2025-ben – Erre számíthat az ország a háború harmadik évében*. https://economic.karpat.in.ua/?p=56206&lang=hu

[44] Oeconomus Gazdaságkutató Alapítvány. (2024). *Az ukrán gazdaság 2025-ben – Erre számíthat az ország a háború harmadik évében*. https://www.oeconomus.hu/oecoglobus/az-ukran-gazdasag-2025-ben-erre-szamithat-az-orszag-a-haboru-harmadik-eveben/

[45] Keynes, J. M. (1936). *The General Theory of Employment, Interest and Money*. London: Macmillan.

[46] Stiglitz, J. E. (2010). *Freefall: America, Free Markets, and the Sinking of the World Economy*. New York: W. W. Norton & Company.

[47] Friedman, M. (1968). The Role of Monetary Policy. *American Economic Review*, 58(1), 1–17.

[48] OECD (2022). *Economic Outlook No. 111 - Preliminary version*. Paris: OECD Publishing.; European Commission (2022). *Economic forecast for Hungary*. Brussels.

[49] Hajnal, G., & Kákai, L. (2023). Crisis Management and the Administrative State in Hungary. *NISPAcee Journal of Public Administration and Policy*, 16(2), 25–47.

[50] European Commission (2023). Poland Country Report; OECD (2023). Economic Survey of Poland; IMF (2023). Poland: Selected Issues

[51] World Bank (2023). Slovakia Economic Update; OECD (2022). Slovakia Country Note

[52] IMF (2023). Czech Republic Country Report. Online: https://www.imf.org/en/Countries/CZE

[53] European Central Bank (ECB). (2023). *Czech monetary policy responses*.

[54] Euractiv.cz (2022). Czech responses to inflation and war impact. https://vlada.gov.cz/assets/evropske-zalezitosti/aktualne/2022-european-semester-country-report-czechia_en_2.pdf

[55] BTI Project. (2024). *Hungary Country Report*. https://bti-project.org/en/reports/country-report/HUN?utm

[56] International Monetary Fund. European Dept. "Hungary: 2024 Article IV Consultation-Press Release; and Staff Report", *IMF Staff Country Reports* 2024, 268 (2024), accessed July 5, 2025, https://doi.org/10.5089/9798400283703.002

[57] OECD Economic Outlook (2023), EC Hungary Report. Online? https://www.oecd.org/en/topics/sub-issues/economic-surveys/hungary-economic-snapshot.html

[58] Magyar Nemzeti Bank (MNB). (2022). *Inflációs jelentés – 2022. szeptember*. https://www.mnb.hu/letoltes/fe-leves-jelente-s-2022-hun-0928.pdf

[59] Magyar Nemzeti Bank (MNB). (2022, 2023). Inflációs jelentés és Pénzügyi stabilitási jelentés. https://www.mnb.hu

[60] Központi Statisztikai Hivatal (KSH). (2023). Statisztikai Tükör – Gazdasági teljesítmények. https://www.ksh.hu

[61] Portfolio.hu. (2022–2023). Makrogazdasági elemzések. https://www.portfolio.hu

[62] Magyar Nemzeti Bank (MNB). (2023). *Közlemények a kamatdöntésekről*. https://www.mnb.hu

„SUPPORTED BY THE EKÖP-24-2-165 UNIVERSITY RESEARCH SCHOLARSHIP PROGRAM OF THE MINISTRY FOR CULTURE AND INNOVATION FROM THE SOURCE OF THE NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION FUND."

KULTURÁLIS ÉS INNOVÁCIÓS MINISZTÉRIUM

EKÖP Egyetemi Kutatói Ösztöndíj Program

SUPPORTED BY THE EKÖP-24-2-165 UNIVERSITY RESEARCH SCHOLARSHIP PROGRAM OF THE MINISTRY FOR CULTURE AND INNOVATION FROM THE SOURCE OF THE NATIONAL RESEARCH, DEVELOPMENT AND INNOVATION FUND.

Evolution and Practical Application of Critical Infrastructure Protection Planning Requirements for Healthcare

Gábor Mongel, University of Public Service, Faculty of Law Enforcement, Institute of Disaster Management, Department of Industrial Safety, mongelgabor@gmail.com ORCID: 0009-0001-9024-5233

Abstract

The operational safety of critical healthcare infrastructure is of paramount importance for the continuity of care for the population and for social stability. Crisis planning has evolved significantly over the past decades, with the former disaster-based approach gradually being replaced by a resilience-based approach. The aim of this paper is to provide a comprehensive picture of the protection planning system and its evolutionary curve for inpatient care facilities as critical infrastructures, with a particular focus on the domestic regulatory environment and recent legislative changes. The historical and content structure of health emergency, operator safety, national defence and emergency response plans will be presented. The introduction of the Resilience Capability Plan, which represents a new approach to moving from protection to resilience and integrates business continuity and risk management practices of healthcare providers, will be analysed. The study is based on the example of an academic-research-patient care institution in Budapest, illustrating the theoretical and practical planning processes, including stakeholder analysis and the operation of the crisis management team and the expectations for the implementation of resilience practices. The paper highlights that the future of planning in the health sector is moving towards process-based, dynamic approaches.

Keywords: health critical infrastructure, emergency planning, resilience, health emergency plan, dangerous substance, hazardous waste

Corresponding author:

Gábor Mongel, University of Public Service, Faculty of Law Enforcement, Institute of Disaster Management, Department of Industrial Safety, mongelgabor@gmail.com ORCID: 0009-0001-9024-5233

1. Introduction

There are countless plans in an organisation's operations, such as the Fire Safety Plan, External Protection Plan, Internal Protection Plan, Business Continuity Plan, Pandemic Plan, Food Safety Plan, Health Emergency Plan, Hazard Analysis and Critical Control Point Plan, Rescue Plan - these are just a fraction of the total number of plans that occur in organisations. [1]

In Hungary, the security planning system of an inpatient care facility designated as a critical infrastructure includes the Operator Security Plan (OSP), the Health Emergency Contingency Plan and the Defence Action Plan, which are approximately 1000 pages long. [2]

As providers of essential services, critical organisations play an indispensable role in maintaining essential social functions or economic activities in the internal market of the European Union. Recognising this fundamental importance, an EU framework - Directive 2022/2557 of the European Parliament and of the Council (CER Directive) - has been developed to both enhance the resilience of critical organisations operating in the internal market by setting harmonised minimum standards and to assist them through coherent and targeted support and supervision measures.

The healthcare sector, including inter alia healthcare providers, should have the capacity to prevent, effectively protect against, respond to, and resist events caused by natural disasters or man-made threats (e.g. terrorism, sabotage), and to take appropriate and effective measures to mitigate, mitigate, adapt to and recover from damage caused - i.e. to be resilient. [3]

In this study, the related plans - their antecedents and the foundations of the Resilience Plan that is being prepared - are presented, alongside the legal requirements, by examining the plans of an inpatient care facility with a teaching-research-patient care profile in Budapest.

2. Historical overview of the legal environment

The detailed regulation of the operation of hospitals and medical institutions in Hungary appeared as early as 1876, which, among other things, provided for the establishment of a statute adapted to local conditions and the minimum conditions necessary for the operation of medical institutions (sufficient staff, instruments, fire extinguishers, etc.). The Decree of the Minister of National Welfare and Labour No. 1.300 of 1932 on hospitals and medical institutions, in addition to regulating their operation in greater detail, also defined the types of institutions (public hospital, private hospital-medical institution, medical clinic-institution).

The independent Ministry of Health was established in 1950 with the amendment of Act XX of 1949 - the Constitution of the Hungarian People's Republic. For the first time, Article 2 of Act II of 1972 on Health defined among the tasks of the Ministry of Health the preparation of health bodies and ensuring their operation in the event of extraordinary circumstances (epidemics, floods, etc.). On the basis of this provision, the Order of the Ministry of Health No 11/1982 (EÜ. K. 8.) on the preparation of disaster plans for preventive health care institutions was the first to prescribe the preparation of plans with a disaster prevention aspect and the mandatory content of such plans. Such a plan had to be prepared by the independent national institutes under the direct supervision of the Ministry of Health, the universities of medicine and the Institute of Postgraduate Medical Education, as

well as by the health institutes providing preventive medical care maintained by the metropolitan, county, county town and town councils, pursuant to Article 2(1) of the Instruction.

With the promulgation of Act CLIV of 1997 on health, the pre-transition regulations were repealed and, from that time onwards, a separate chapter on disaster health care was made law, providing for the preparation of disaster plans by health institutions designated by the Minister of Health - hospitals, other inpatient health care providers, outpatient specialised care, nursing homes. The content requirements for the plans of health care institutions were laid down in Decree 29/2000 (X. 30.) of the Ministry of Health, which now also provides for the preparation of various sub-plans.

Hungary has been a member of the European Union since 1 May 2004, and as such, 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 is a mandatory objective for Hungary. The relevant laws have been developed by the individual member states themselves - in Hungary, Act CLXVI of 2012 on the Identification, Designation and Protection of Critical Systems and Facilities and its implementing regulation, Government Decree 65/2013 (8.III.) entered into force on 1 March 2013. Pursuant to Government Decree 246/2015 (IX. 8.) on the identification, designation and protection of critical health systems and facilities, the tasks of the sectoral designating authority were performed by the Minister of Health. Instead of the provision of Act CLIV of 1997 on Health requiring a disaster plan, health care providers designated by the Minister are required to prepare a health emergency plan as part of their preparedness as of 01.01.2014.

In January 2025, Act LXXXIV of 2024 on the Resilience of Critical Organisms and its implementing decree, Government Decree 474/2024 (31.XII.) - based on the CER Directive - entered into force, thus repealing Act CLXVI of 2012 and related government decrees, and in addition to the structure set out therein, several previous definitions and concepts were amended and supplemented.

3. Healthcare Crisis Planning

In accordance with the provisions of the EüM Instruction 11/1982 (EüK 8.) on the development of disaster plans for preventive medical institutions, the disaster plan prepared by the metropolitan health care institution (medical university) in 1982 was intended to help implement the regulations that need to be applied in the event of mass disasters in order to provide professional care for a large number of injured persons in accordance with the principles of compromise medicine. The plan provided that in the event of a disaster, the institution would be responsible for receiving the injured from the designated traction areas, in accordance with the territorial principle agreed with the Metropolitan Council's Health Department, taking into account the leading injuries and profiles, classifying them, providing them with first aid and specialist care if necessary, and administering the necessary medication and follow-up care until the injured had fully recovered. In addition to these tasks, it was necessary to provide outpatient and inpatient care for the population in accordance with the territorial coverage principle and, as instructed by the authorities, the specialist staff needed to set up medical emergency posts.

In order to ensure the full implementation of the tasks, it was necessary to make use (with certain redeployments) of the various theoretical institutes in addition to the Clinics under the authority of the institution, to free up beds and place extra beds in order to increase the supply and diagnostic capacity, to install new electromedical and therapeutic machines, and to apply rapid diagnostic methodology.

In the event of a disaster, the head of the institution could, on the initiative of the authorities, order the transfer of part or all of the institutions to take care of the mass casualties at the site of the disaster. For the operational organisation and management of medical activities, a so-called University Directorate General and a subordinate Regional Hospital Directorate General were to be created from the existing staff, with the subdivision shown in Figure 1. Operational committees (teams) were to be appointed in the institutions under the responsibility of the DGs in order

to ensure the smooth and continuous provision of care. A three-stage system of periodic distribution of care and the staffing required to start it within the required 16 hours was also laid down in the plan - this is also shown in Figure 1.

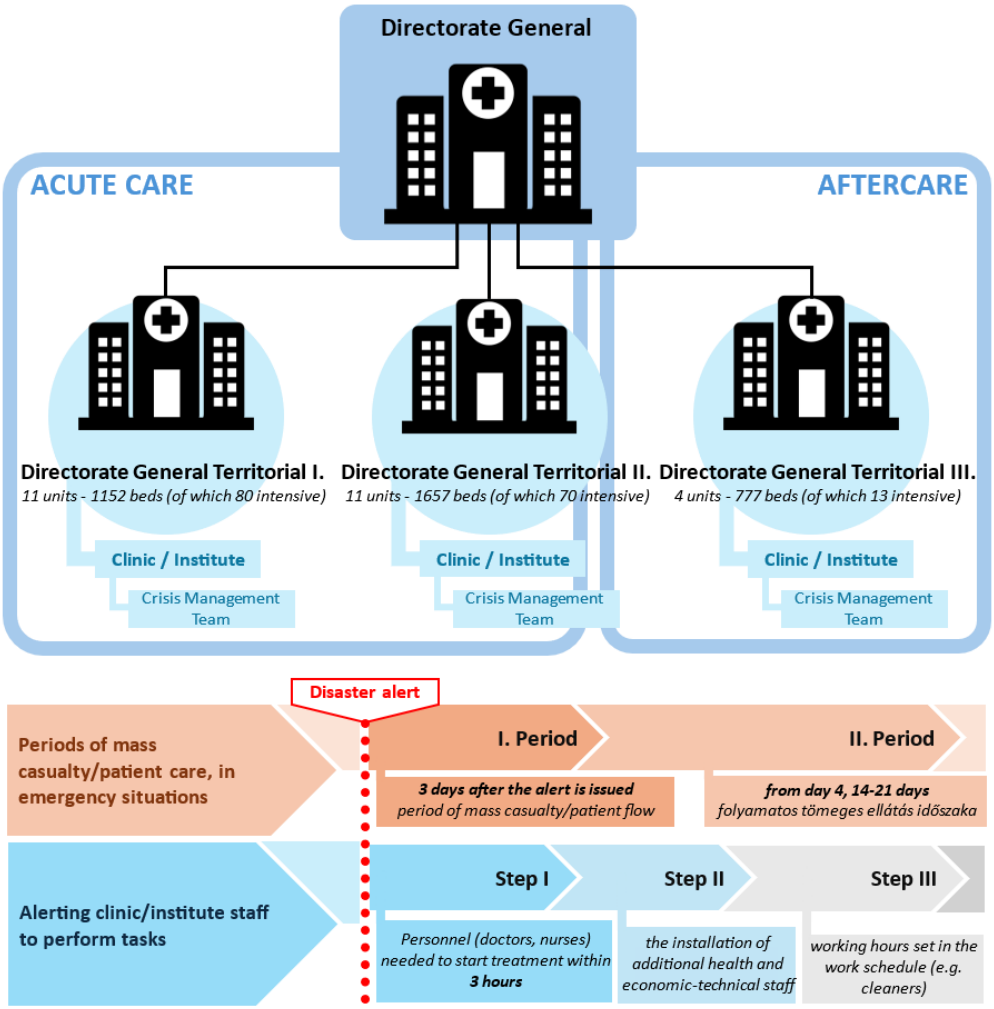


Figure 1 The operational organisation and management of care, the disaster organisation of the metropolitan health institution in 1982, the planned periods of patient care in the event of a disaster, the stages of the equipment

(Plan of the institution of the study 1982 / author's diagram)

With the promulgation of the Health Care Act in 1997, the pre-transition regulations were repealed, but the preparation of disaster management plans remained a requirement, as stipulated in Decree 29/2000 (X. 30.) of the Ministry of Health.

On the basis of Government Decree 158/1999 (XI. 19.) on disaster health care, Decree 29/2000 (X. 30.) of the Ministry of Health and the measures of the State Public Health and Veterinary Service (ÁNTSZ), the preparation of disaster prevention plans for health care institutions included the planning of the establishment and operation of so-called emergency hospitals - supplementary and independent emergency hospitals and medical emergency centres - as a separate planning task for the designated hospitals.

The definition of a health emergency and the criteria for its application are defined in Act CLIV of 1997 on Health Care and Government Decree 521/2013 (XII. 30.) on Health Emergency Care. Health care institutions are required to prepare Health Emergency Contingency Plan, the content and form of which are specified in EMMI Decree No. 43/2014 (VIII. 19.). [2]

In the examined health care institution (medical university) of the capital city, the Health Emergency Contingency Plans are prepared for vital system elements, institution by institution. Based on the plans, the replacement of the lost health professional, technical and supply services, the restructuring of the institution's human and technical resources, the internal reorganisation of the work schedule during a crisis situation is carried out under the direction of the institution's Crisis Management Team (hereinafter: CMT).

The CMT is the operational body formed by the management of the health care provider for outpatient and inpatient care, which is responsible for preparing for health emergencies and for directing and controlling the necessary activities, and which operates under the leadership and direct supervision of the Director at a workplace (e.g. secretariat) at the headquarters of the institution. [4]

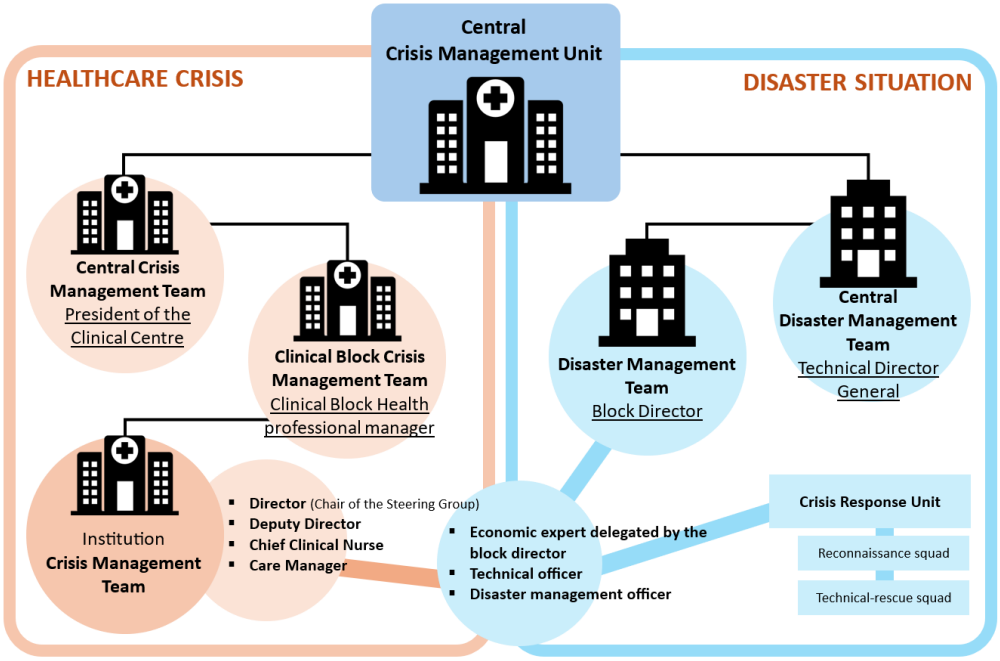


Figure 2 Operation of the CMT recorded in the Health Emergency Contingency Plan at the test facility (2024)

(author's image)

The rules for the preparation of the Health Emergency Contingency Plan and the precise content and format of its sub-plans are laid down in the Decree of the Minister responsible for health, under which the health care provider must review the plans annually and submit them to the county government office for approval. The Health Emergency Contingency Plan is essentially a system of plans consisting of a basic plan and 14 sub-plans. The plans are grouped into four categories:

- Baseline Information, Readiness of Contingency (CMT),

- Response of the organisation covered by the plan - to an internal incident,

- response of the organisation covered by the plan - external incident, extension of service,

- operation of service processes.

The (sub)plans can be used separately, but also in different combinations, depending on the type of event taking place. [5] These plans were not used during the coronavirus outbreak, one reason being that the situation was so specific that

the plans did not provide adequate guidance and a different internal crisis management structure was developed.

During the epidemic, adaptive measures were needed in a specific VUCA (Volatile, Uncertain, Complex, Ambiguous) environment. [2] The structure of care is illustrated in Figure 3.

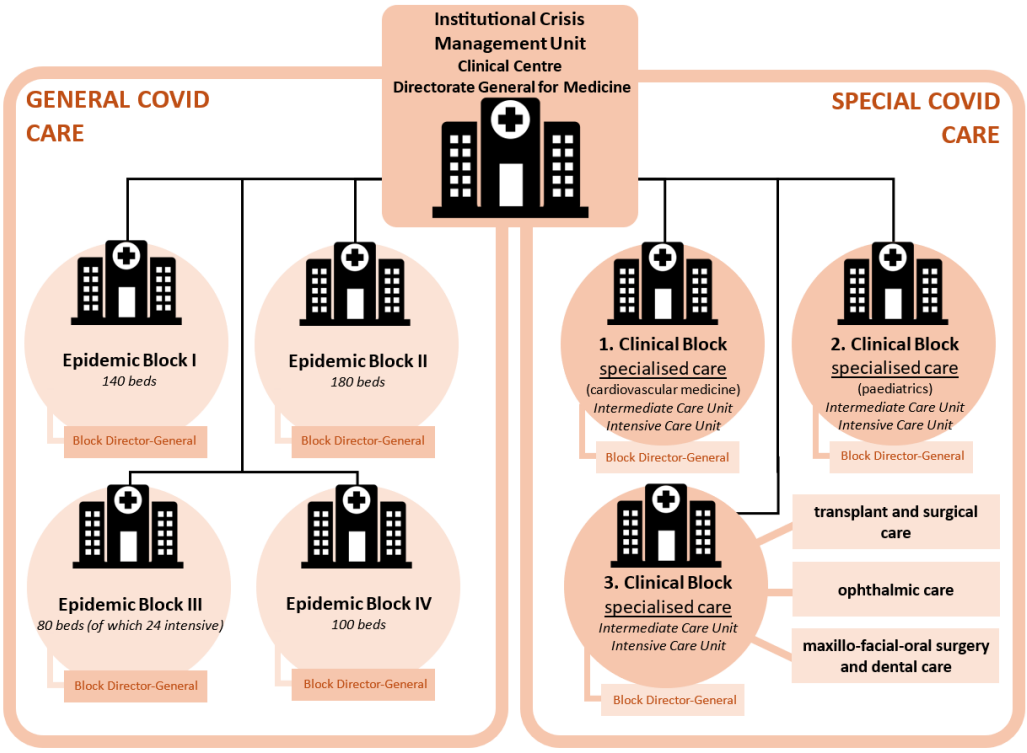


Figure 3 Operational organization and management of care during wave II of the COVID-19 epidemic in the institution under study (2020) (author's image)

4. Emergency Planning - Municipal Emergency Plan

Since some of the healthcare facilities that can be linked to the institution under investigation are considered critical system elements, a contingency plan is justified. The hazard management planning includes the definition of disaster risk management responses, their conditions, implementation rules and how they will be monitored, as well as measures to help enhance national resilience to different risks. The purpose of emergency planning is to identify the risks related to natural, civil and

other hazards and, on the basis of their analysis and assessment, to establish a coherent system of disaster management tasks and measures, the arrangements for their implementation and the allocation of the human, material and technical resources required to ensure them. The relevant level of emergency response planning is the workplace emergency response plan. The evacuation and accommodation of patients in the territory of the institution under consideration from the endangered area or object must be planned in accordance with the emergency plan of the local defence administration, in accordance with the guidelines of the emergency services and the provisions of the health emergency activity, and must be carried out in coordination with and on the basis of the instructions of the central and block-level operational bodies of the institution, with the involvement of the competent territorial patient transport and care services, ensuring the conditions for the safe accommodation and further treatment of patients.

No specific Facility-Level Emergency Plan has been prepared in the institution under review, as the content of the available related plans (Operator Safety Plan, Health Emergency Contingency Plan, Defence Action Plan) covers this. The plans were not drawn up for the institution as a whole, but for specific departments, which are classified as critical infrastructure elements.

5. The Defence Action Plan

According to Act CX of 1993 on Defence, the Minister of Defence was obliged to cooperate with the competent ministers in the professional management of the relevant activities in the location of civil defence and military installations and, among other things, in ensuring the functioning of the health system. The Law on National Defence, which came into force in 2011, already empowered the competent ministers, acting within their remit and in agreement with the Minister of National Defence, to define the national defence tasks of the sector by decree.

Accordingly, in 2016, the Ministry of Human Resources issued a decree regulating the defence tasks of the health sector and stipulated the preparation of the Defence Action Plan, a document setting out the tasks to be performed in the special legal period and the related units of care. The following comparative table shows the main content requirements of the Defence Action Plan contained in the two regulations and the scope of the organisations within the health sector that are obliged to prepare a plan.

6. Operator Security Plan (OSP) – evolving into Resilience Plan

In November 2005, the European Council published a Green Paper on Critical Infrastructure Protection. In 2008, the Council enacted the principles for the identification and designation of European Critical Infrastructures, Directive 2008/114/EC, and required the preparation of an Operator Security Plan (OSP) for critical infrastructures and the appointment of a Security Liaison Officer (SLO). In 2012, the Act on the Identification, Designation and Protection of Critical Systems and Facilities and its implementing decree entered into force in Hungary. The basic principles for identification and designation in the healthcare sector were laid down in 2015 in the relevant government decree, on the basis of which designations in inpatient care started in 2016 and were reviewed in 2020.

The operator's safety responsibilities include preparing for incidents, planning crisis responses in advance, maintaining operations and recovery. In the event of a disproportionate shift in health care needs and capacity due to an emergency event, patient care activities will be carried out according to the rules of emergency health care. [2]

The definition of the critical system elements, the relevant services and the organisational and instrumental arrangements that will ensure their protection are included in the Operator Security Plan. The Operator Security Plan shall identify the security measures, taking into account risk analysis and risk management, the design and operation of which will ensure the protection, continuity and restoration of the operation of the European Critical Control Element or the national critical control

element, and the interim measures to be taken in accordance with the different risk and threat levels.

In our country, the legislation specifies the mandatory content of the OSP, names the mandatory risks to be assessed, provides that the OSP shall include a Health Emergency Contingency Plan, which shall include a plan for the replacement and alternative operation of utilities, a sub-plan for the provision of essential services, food, medicines, medical consumables, blood and blood products, and a communication sub-plan. [5]

The Operator Security Plan differs from the plans presented before - and after. In some respects, it is a summary document, and in the future, it will be expanded and made even more complex, as its approach - and now its name: Resilience Plan - will now also focus on resilience, not just protection. If an organisation already has relevant documents that serve the same purpose as the OSP, or specific points in the Resilience Plan, or a specific set of risk analysis and their content fully incorporates all mandatory requirements, they will form part of a comprehensive, complex plan. The first step in preparing any plan is to identify the objective and the risks that will affect the achievement of that objective.

The protection of critical infrastructure elements is part of the renewed, complex system of disaster management under the leadership of the industrial safety department. The operator safety planning for inpatient healthcare critical infrastructure elements in the domestic inpatient care sector is not taking into account sector specificities and current planning practice is static and not process based. The operator safety planning practice for healthcare critical infrastructure elements should be based on the healthcare emergency planning approach. [6]

In addition to direct health care and the provision of care, there are other service units in health care facilities: warehouses, medical gas storage, various dangerous substances and waste, catering, sterilisation, and other technical areas for staff and property maintenance. The infrastructure in the health sector is varied. In addition to the classical operational areas (utilities, heating, lighting, lifts), the IT

area also plays a major role in ensuring continuity of operations. In addition to the 24-hour operation of existing buildings and equipment, it is also necessary to be prepared to prevent expected breakdowns (planned maintenance) and to deal quickly and efficiently with unexpected breakdowns. [7]

A Dangerous substances Management Plan may also be part of the Resilience Plan. The model Resilience Plan published by the Authority addresses the management of hazardous waste generated at several points, and the Resilience Matrix, which is a mandatory annex to the plan, also addresses the risk of release of dangerous substances and other hazards associated with dangerous substances (fire, overpressure, poisoning, transport). This area is also reflected in the health sector, with 21 designated critical health care facilities with critical health care systems, which, based on the experience of internal audits in recent years, use a significant amount of dangerous substances, both in the provision of patient care and in related research and educational activities. Some of the substances used are classified as hazardous due to their chemical properties, such as carcinogenic, mutagenic and reprotoxic substances (CMR substances - formaldehyde, xylene), which exceed 3000 litres/year for the whole organisation. [8] It also includes gaseous substances stored in pressure vessels - about 1000-1500 gas cylinders are in use in the whole body every day - which (oxygen, carbon dioxide, nitrous oxide) can lead to fire and explosion hazards if not properly stored and handled. [9]

For health care providers, in addition to the large amount of specialised health care (infectious) hazardous waste (more than 1 million kg/year - in the organisation under study), there is also the management of hazardous waste (more than 45 thousand kg/year - in the organisation under study), which is hazardous due to its chemical and physical composition. These are typically transported by road to the place of discharge. The delivery and collection of dangerous substances is usually carried out by external partners, but it is common for the delivery to be made to a central unit and then further distribution to internal and external areas - i.e. also by road - to be carried out by the healthcare provider under its own responsibility, which is thus subject to Act LXXXIX of 2015 on the promulgation of Annexes A and B

to the European Agreement concerning the International Carriage of Dangerous Goods by Road and on certain aspects of its domestic application.

7. The Resilience Simulation Exercise

Plans play an important role in the development of practices - they allow for the precise definition of objectives, the identification and management of risks, the involvement of stakeholders (internal and external), the clarification of responsibilities and the setting of deadlines. Under the regulation in force from 01.01.2025, in addition to the complex resilience exercise, a resilience exercise and a stress test will be introduced (involving other partners, in other locations). The complex resilience exercise will continue to be conducted at critical organisations and infrastructures designated by the National Directorate General for Disaster Management of the Ministry of Interior (BM OKF), at least once a year, under the coordination of the Resilience Manager, followed by a mandatory evaluation of the experience, the evaluation of the exercise will be carried out by the General Designating Authority.

The authority shall formally notify the head of the critical organisation of the obligation to conduct the exercise. The exercise shall be preceded by contact and joint planning with all relevant partners (e.g. critical suppliers, utility providers) - the date of the exercise shall be set accordingly and in accordance with the annual cycle of the organisation or infrastructure.

The planning of the exercise should be based on and tested in practice:

- approved and currently valid plans,
- sector specificities (in-patient care, risk of infection, people with reduced mobility, visitors in the "work area", research laboratories, etc.),
- exposures, dependencies - interdependencies (energy, transport, water, social security, ICT),
- main risks, risk factors (hazards, sources of failure) - and their management,

- alert chain (follow up of member notifications, EDR device use compliance, activation of specific management modes, management of emergency, notification of relevant bodies),
- asset systems, back-up equipment (e.g. commissioning of aggregators),
- organisation and critical infrastructure, essential service characteristics,
- range of people involved (e.g. critical workers, external workers),
- relevant protective equipment (status, practical use).

The exercise should be carried out on the basis of an exercise plan, and the events should be sequenced from the very beginning of the exercise, so that the current ability of the organisation or infrastructure to respond to the situation can be perceived.

Criteria for the evaluation of the exercise:

1. Check the adequacy of the Resilience Plan and the Resilience (Risk) Matrix,
   - supplementation, modification in case of non-compliance,
   - In case of serious discrepancies, restore the documentation and repeat the exercise,
2. testing for addictions: confirmation/rejection,
3. introducing identified new risks into the matrix, developing relevant measures,
4. compliance determination/modification of notification protocols (alert chain),
5. determination/action of the operability of back-up and protection equipment.

The purpose of the substantive evaluation of planning, practice and practice is to identify any weaknesses, errors or potential for error in the system and to develop a proposal for improvement in response to these, taking into account the priority of the factor in question. [1]

In the competitive sector, the preparation of Operator Security Plans is already based on the Business Continuity Planning (BCP) planning practice, i.e. the business continuity approach, which is essentially a process-based approach - the

plans prepared are dynamic, i.e. they are essentially continuously updated.[10] In contrast to the plans prepared in the healthcare sector, which have been prepared in a static manner, taking into account local risks, and are tailored to the facility and not to the processes within it. Business continuity planning principles can bring a new approach to the design practice of critical infrastructure for inpatient care. First of all, it is necessary to identify the basic processes, starting with the identification of the value holders, i.e. the stakeholders (stakeholder analysis), and then involving them in the further planning process. [5]

Accordingly, the audited institution, under the guidance of the Resilience Manager, started to conduct stakeholder analyses within the organisation.

This analysis is followed by an impact analysis of patient care as a core process to be protected in the healthcare institution, and of its core sub-processes and the processes that serve them. The potential risks to these processes are then identified and assessed to determine whether the planning process requires the risk to be reduced, eliminated or, due to its trivial nature, requires no action other than continuous monitoring. [11]

8. Other plans related to hospital safety

In addition to the above, plans for other areas of protection are also relevant to the operation of critical infrastructures.

The Rescue Plan, not to be confused with the Escape Plan (fire safety), should be prepared in the event of abnormal conditions, where safety standards for the proper operation of the establishment cannot be met. From 2023, the preparation of the plan will be considered as an occupational safety and health activity. The planning must take into account the nature, location and extent of the workplace, the impact of the hazards and the occupants within the scope of the work. These plans may be interpreted in industrial areas (e.g. chemical industry), but the

legislator has not made any distinction, so they must be drawn up for essentially all workplaces. In the institution under review, such plans have been prepared since 2023 with the change in legislation, which primarily address the affected areas at clinical block level, referring to other relevant plans (Health Emergency Contingency Plan, Fire Safety Plan, etc.), provide a general procedure for responding to the different hazard factors in terms of content, and include relevant information on the affected areas (e.g. on-call contact details, dispatching partners, utility shut-offs). Since the relevant provision allows for the Rescue Plan to be included in a plan required by specific legislation, such as a safety, security, response or similar plan, it is recommended that it should be part of the Resilience Plan.

In the event of a fire in an establishment, the Fire Safety Plan is the emergency management scenario that contains the data, tasks, organisational solutions, technical and personnel options that can be planned. [12] The aim of the plan is to ensure that, in the event of a fire in a facility, it is possible to effectively implement fire detection, escape, extinguish the fire as quickly as possible, rescue potentially endangered persons and high-value property - i.e. to minimise damage. [13] Annexed are the escape plans. The escape plan is a drawing displayed to the occupants of the building to help them find their way to escape. [14] The health care institutions in our country show a varied picture in terms of their building design, but a common point is that in the event of a fire, the possibility of smoke-free escape is generally not resolved. Typically, these facilities have a large, continuous air space and fire compartment, with a central corridor system with wards opening onto the building. Fires can be caused by a number of factors: smoking and the use of open flames, failure of electrical equipment and appliances. [15]

Physical protection is defined as the combination of technical means, force protection and internal regulations aimed at deterring, delaying, detecting and countering unlawful theft and sabotage of nuclear facilities and nuclear and other radioactive materials as part of nuclear security. The Physical Protection Plan is a plan describing the operation of the physical protection system and the specific

implementation of the protection functions. Physical protection also includes the protection of programmable systems (also known as cyber protection), and to develop this area, the Hungarian Atomic Energy Authority (HAEA) and the US National Nuclear Security Administration (NISA) organised a two-day workshop for relevant organisations from 10-14 July 2023. Presentations by invited US experts focused on cyber security of nuclear and radiological facilities, especially in the context of healthcare institutions. In addition, relevant information on other cyber security factors (ransomware, phishing emails) was presented, with illustrative examples (waterworks, hospital cyber attack).

The storage of flammable dangerous substances poses significant risks not only in chemical storage facilities but also in healthcare facilities [16]. Of course, even in small quantities, the storage of flammable dangerous substances can lead to similar major accident consequences as in case of establishments involving dangerous substances [17]. Similar dangers also exist in the event of major fires occurring in university sports facilities [18]. In addition to discussing fire safety issues, there are also significant public safety aspects of hospital safety that can be examined from a police science perspective [19]. Incidents involving hazardous materials and the treatment of mass casualties in human epidemics also pose a significant challenge for hospital safety professionals [20].

9. Summary

Ensuring continuity of care is one of the most important safety and security tasks in healthcare institutions. In this area, the number of services used by the critical organisation from third parties is already pronounced, and this dependency can also affect the service provided by the operator (patient care - availability of medicines, dressings, etc.) and can also affect business continuity. Of course, this dependency may arise not only from the interdependence of contracted partners, but also from the interdependence of the organisation's own internal processes.

It can be concluded that the protection planning system in inpatient healthcare institutions has evolved significantly over the past decades. The

Operational Security Plan (OSP), the Health Emergency Contingency Plan and the Defence Action Plan have been a set of interrelated but fragmented documents. The Resilience Plan introduced under Act LXXXIV of 2024 and Government Decree 474/2024 (31.12.2024) has brought a new approach, shifting the static, event-based approach to a process-based, dynamic planning practice based on business continuity principles.

The case study of the in-patient care facility in the capital city under investigation highlights the need for special attention to be paid to the dangerous substances used and the hazardous waste generated in the design practice. The safe management of these materials can have a direct impact on maintaining the resilience of the institution.

In the course of resilience planning, it is also necessary to identify and assess the risks related to dangerous substances when developing the sector-specific risk matrix. Regular practice of internal protocols (e.g. training, training, alerting) is also necessary in this area.

References:

[1] Baloghné Pruha M. A. (2024). Tervek és gyakorlatok szerepe a kritikus szervezetek ellenálló képességének fejlesztésében. Védelem Tudomány, 9(ksz.), 9-13.

[2] Mészáros István: A kórház – mint kritikus infrastruktúra – biztonságának aktuális kérdései, Belügyi Szemle (2010-) 71: 6 pp. 1059-1072., 14 p. (2023)

[3] EUR-Lex. A kritikus szervezetek rezilienciájának fokozása. Online: **https://eur-lex.europa.eu/HU/legal-content/summary/making-critical-entities-more-resilient.html** (letöltve: 2025.06.28.)

[4] [Internal document] Based on the Health Emergency Plan of the institution under study (2024).

[5] Mészáros István: A fekvőbeteg-ellátással foglalkozó egészségügyi létfontosságú rendszerelemek komplex üzemeltetői biztonságának kutatása és fejlesztése, különös tekintettel az egészségügyi válsághelyzet-tervezési feladatok ellátására. Nemzeti Közszolgálati Egyetem, Budapest, 2024, 305 p.

[6] Mészáros, István ; Cimer, Zsolt ; Kátai-Urbán, Lajos: A fekvőbeteg-ellátással foglalkozó egészségügyi létfontosságú rendszerelemek komplex üzemeltetői biztonságának kutatása és fejlesztése, különös tekintettel az egészségügyi válsághelyzet-tervezési feladatok ellátására. In: Gőcze, István; Padányi, József (szerk.) Szemelvények a katonai műszaki tudományok eredményeiből V.: Hallgatói és oktatói kötet. Budapest, Ludovika Egyetemi Kiadó (2025) pp. 233-249.

[7] Veresné Rauscher, Judit; Berek, Lajos: Kórházak biztonsága és védelme I.: Kockázati tényezők és lehetséges következmények Hadmérnök 16: 4. 13-24. (2021)

[8] [Internal document] Summary report of the internal occupational and fire safety audit related to CMR substances, 2024.

[9] Simon, Mátyás; Daruka, Norbert; Szabó, Gyula: Az orvosi gázok veszélyei az egészségügyi kritikus infrastruktúrák tekintetében. In: Horváth, Richárd; Lukács, Judit; Stadler, Róbert; Pinke, Péter (szerk.) Mérnöki Szimpózium a Bánkin Előadásai : Proceedings of the Engineering Symposium at Bánki (ESB 2023) Budapest, Óbudai Egyetem (2024) 367 p. pp. 355-360. , 6 p.

[10] Kátai-Urbán, Lajos ; Mészáros, István ; Vass, Gyula: Iparbiztonság, válsághelyzeti tervezés. In: Major, L; Liptay, L; Orgován, Gy (szerk.) A katasztrófa-készenlét, a reagálás és a beavatkozásbiztonság egészségügyi alapjai. Budapest, Semmelweis Kiadó (2019) pp. 48-83.

[11] Mészáros, István; Bognár, Balázs: Üzletmenet-folytonossági tervezés kórházi környezetben II.: Kockázatértékelés és hatékonyságmérés, Hadmérnök 17: 3 pp. 153-168., 16 p. (2022)

[12] Duruc József: A tűzriadó terv lényege és készítése OMKT 2011.

[13] Cziva Oszkár, Duruc József: Tűzvédelmi Igazgatás, Belügyminisztérium Vezetőképzési és Továbbképzési Főosztály 2016.

[14] Tűzvédelmi Műszaki Irányelv TvMI 2.3:2020.01.22.

[15] Cziva Oszkár: Kórházakban keletkezett tüzek veszélyei, Védelem - Katasztrófa- Tűz- és Polgári Védelmi Szemle online: Tanulmányok pp. 1-4., 4 p. (2010)

[16] Kátai-Urbán, Maxim, Tibor Bíró, Lajos Kátai-Urbán, Ferenc Varga, and Zsolt Cimer. 2023. "Identification Methodology for Chemical Warehouses Dealing with Flammable Substances Capable of Causing Firewater Pollution" Fire 6, no. 9: 345. https://doi.org/10.3390/fire6090345

[17] Mihály, István, László Bérczi, Balázs Bognár, Maxim Kátai-Urbán, Levente Tóth, Lajos Kátai-Urbán, Gyula Vass, and Ferenc Varga. 2025. "Experimental Study to Determine the Leakage Area of Single-Leaf Smoke Control Doors in the Design of Pressure Differential Systems" Fire 8, no. 1: 5. https://doi.org/10.3390/fire8010005

[18] Kanyó, Ferenc ; Varga, Ferenc: Sportcsarnoktűz a Testnevelési Egyetemen. Védelem Katasztrófavédelmi Szemle 23 : 1 pp. 47-49. (2016)

[19] Bakai, Kristóf Péter (2012): Bizalom és biztonság. In: Gaál, Gyula; Hautzinger, Zoltán (szerk.) Tanulmányok "A biztonság rendészettudományi dimenziói - változások és hatások" című tudományos konferenciáról: Változások és hatások. Pécs, Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport pp. 459-462.

[20] Zsitnyányi, Attila. Increasing the safety of persons affected by CBRN incidents, with particular regard to developing a procedure and methodology determining the application of mass decontamination capabilities in Hungary. American Journal of Research Education and Development 2024 : 4 pp. 56-85. , 30 p. (2024)

[21] Fejes, Zsolt Dezső; Pitlik, László; Rikk, János; Szűcs, Diána; Túri, Péter; Budaházy, Péter,E-volution a védelem-egészségügyben: A virtuális oktatási és képzési lehetőségek áttekintése, HONVÉDORVOS 76: 1-2pp. 61-69., 9 p.(2024)

Relevant legal regulations:

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

Magyarországi rendeletek tára 1876. 133. Szabályrendelet a kórházakra és gyógyintézetekre nézve *(Decree No. 133/1876 on Hospitals and Medical Institutions)*

1950. évi IV. törvény a Magyar Népköztársaság Alkotmányának módosításáról *(Act IV of 1950 on the Amendment of the Constitution of the Hungarian People's Republic)*

1997. évi CLIV. törvény az egészségügyről *(Act CLIV of 1997 on Healthcare)*

234/2011. (XI. 10.) Korm. rendelet a katasztrófavédelemről és a hozzá kapcsolódó egyes törvények módosításáról szóló 2011. évi CXXVIII. törvény végrehajtásáról *(Government Decree 234/2011 (XI.10.) on Disaster Management and the Implementation of Act CXXVIII of 2011)*

49/2016. (XII. 28.) EMMI rendelet - az emberi erőforrások miniszterének feladatkörét érintő ágazati honvédelmi feladatokról *(EMMI Decree 49/2016 (XII.28.) on Sectoral Defence Tasks within the Scope of the Ministry of Human Capacities)*

2012. évi CLXVI. törvény a létfontosságú rendszerek és létesítmények azonosításáról, kijelöléséről és védelméről *(Act CLXVI of 2012 on the Identification, Designation and Protection of Critical Systems and Facilities)*

1993. évi XCIII. törvény a munkavédelemről *(Act XCIII of 1993 on Occupational Safety and Health)*

190/2011. (IX. 19.) Korm. rendelet az atomenergia alkalmazása körében a fizikai védelemről és a kapcsolódó engedélyezési, jelentési és ellenőrzési rendszerről 4. melléklet alapján *(Government Decree 190/2011 (IX.19.) on Physical Protection in the Application of Atomic Energy)*

1996. évi CXVI. törvény az atomenergiáról *(Act CXVI of 1996 on Atomic Energy)*

THE EFFECTS OF CLIMATE CHANGE IN HUNGARY – AN EXAMINATION OF NATURAL DISASTERS AND RESPONSES

Regő Levente Kovács

Komárom-Esztergom County Disaster Management Directorate, fire sergeant

kov.rego.levente@gmail.com

orcid: 0009-0001-1995-7561

ABSTRACT

Climate change poses increasingly severe challenges worldwide, including in Hungary, where its consequences are becoming more frequent and destructive. This paper examines the connection between climate change and natural disasters, focusing on key phenomena such as drought, water scarcity, and wildfires. The study highlights the dramatic effects of the exceptionally dry year 2022, analyzing its consequences on agriculture, water supply, and environmental security. The paper explores how prolonged drought and rising temperatures contribute to a chain reaction of threats that impact human health, biodiversity, and infrastructure. In addition to assessing the national risk environment, the study evaluates Hungary's institutional and disaster management responses, and draws attention to the importance of community awareness and preparedness. Emphasis is placed on both human-induced and natural factors driving climate change, as well as the significance of long-term planning and mitigation.

The paper concludes that managing climate-related risks requires interdisciplinary coordination and strong policy support. Proactive adaptation and resilience-building efforts are critical to protecting human lives and natural resources. The findings of this research aim to support national disaster risk reduction methods in a time of accelerating environmental transformation.

Keywords: climate change, Hungary, natural disasters, drought, water management, disaster preparedness

INTRODUCTION

Disasters can be considered as old as the Earth itself, since ever since our planet formed, it has been continually afflicted by disasters. Even the first humans on Earth experienced these catastrophic phenomena and, albeit primitively at first, began to defend themselves against their harmful effects. It is enough to consider that prehistoric people would retreat into caves to escape an oncoming windstorm or hailstorm, or, upon recognizing the destructive power of fire, would flee along with the surrounding animals. Over time, this defensive behavior continuously improved and became more effective. However, it is important to mention that with the development of humanity and the advent of modern technology, not only have our defensive capabilities improved, but our world itself has become more dangerous and unpredictable. We can state that as time passes, humanity has to face more and greater threats. For example, just in the last 20 years, the number of natural disasters on Earth has doubled, and these disasters have claimed the lives of nearly 1.5 million people . It is also important to highlight that human society is in a constantly changing environment, and new kinds of dangers and threats have emerged up to the present day. Moreover, not only the number but also the nature of disasters has changed over time. [1]

"A disaster can strike anywhere, anytime nowadays, causing loss of human lives, destruction of property, and the annihilation of priceless assets." [2]

Disasters continue to afflict the world today, meaning that essentially a tragedy could occur anywhere at any time. Furthermore, [3] I would add that with the overpopulation and overexpansion of humanity (in terms of territory, e.g. pushing the boundaries of residential areas, increasing the population density of settlements), this danger becomes greater and greater. It is much easier for what was originally a “smaller” trouble to cobble itself together into a large-scale disaster. As is well known, our world is constantly changing and evolving, and these changes do not always move in a positive or favorable direction for humanity. These changes can stem from natural processes, human activities, or even a combination of the two. In my view, today’s world is filled with challenges and threats, which present numerous — even novel — trials for the inhabitants of the Earth, and along with them for our country and the disaster management organization as well . Most of these threats, by their nature (natural disasters), have a long history, and consequently the evolution of defenses against them has accompanied this process. Therefore, we can say that the process of defense and damage elimination in these areas has become more effective. At the same time, it is essential to recognize new types of dangers, to learn about them in more detail, and to prepare effectively — yet

optimally — for possible events and for eliminating their consequences. In my view, this is indispensable for creating a level of safety that can be deemed critical, since according to the literature the word “safety” itself means the absence of threat or the ability to avert a threat.

"Safety plays more than a fundamental role in a person’s life. If we examine the topic a bit more thoroughly, we can notice that the pursuit of safety is inherent to every living organism. The key to survival is adapting to one’s environment, taking every source of danger into account, and reacting to every change." [4]

CATEGORIZATION OF RISKS

“Secure Hungary in a changing world” [5]

Hungary’s 2024 National Disaster Risk Assessment report (the so-called ex ante report) provides for the identification and mapping of those risks that could significantly endanger the population, territory, natural environment and/or economic stability of our country . At the same time, it offers an opportunity for effective preparation, defense planning, and overall for increasing and improving disaster resilience. The report divides the risks into three main categories, which are as follows: [6]

- intentionally induced events,
- serious accidents,
- natural events.

Furthermore, the 2024 ex-ante report – in line with previous reviews – also identifies 12 areas within these 3 main categories, which are the following.

Risk Areas	
Intentional Events (Human-Inudec.)	Terrorism
	Security Policy Crisis
	Energy Supply Crisis
	Cyberattack, Information and Communications
Serious Accidents	Transport Accident
	Nuclear Accident
	Hazardous Materials–Related Events
Natural Events	Extreme Weather
	Space Weather
	Adverse Effects of Waters
	Geological Hazards
	Health Crisis

Figure 1. The 12 risk areas defined by ex ante report 2024 [6]

"According to the Report, among the identified hazard types in Hungary, those of natural origin exert their effects most intensively, and they are occurring with increasing frequency. In connection with climate change, due to increasingly extreme weather, we must reckon with events that are becoming more frequent and carry more severe consequences." [7]

THE PHENOMENON OF CLIMATE CHANGE

"It is an indisputable fact that the Earth's near-surface air layer is warming, and the concentration of numerous greenhouse gases has increased in the past one or two centuries. The magnitude of these changes is much greater than what natural processes could justify, and nothing of this scale has ever occurred during the span of geologic history we are able to comprehend." [8]

Climate change is a complex process that is fundamentally natural, observable across the entire world — that is, at a global level. The signs of climate change are primarily to be sought in the changes occurring in the Earth's atmosphere and sea level, since the temperature of both the air and the oceans/seas is rising year by year. As a consequence of the resulting melting processes, a rise in sea level can be observed. [9]

Additionally, it can be stated that the presence of humans and certain types of human activities are significant accelerating factors in this process. [10] Consequently, it can be determined that climate change itself has two main sources/causes.

Anthropogenic (human-derived) factors: These are human activities that involve the emission of greenhouse gases. [11] Such gases include carbon dioxide (CO_2), methane, and ozone. Emitting these gases negatively affects the Earth's atmosphere by preventing sunlight from being reflected off the Earth's surface, thereby promoting the warming of the atmosphere.

Natural factors: This category includes volcanic activities and eruptions, as well as changes in solar activity.

Human-induced, anthropogenic factors	Natural factors
Industrial processess, activities (emissions arising industrial production and energy supply)	Change in solar activity (cyclical solar activity, warming trends)
Use and combustion of fossil fuels	Volcanic activity (volcanic eruption → large amounts of ash and a gas may reach the atmosphere cause short-term cooling)
Deforestation	
Transportation emissions (e.g. motor-vehicles, aircraft)	Temperature changes in oceans/seas (for example, natural climatic phenomena El Niño and La Niña)
Agricultural practices (livestock farming and arable farming activities)	
Wildfires, forest fires (large amounts of carbon dioxide and other greenhouse gases released into the atmosphere	Natural greenhouse effect (carbon dioxide, water vapor present in the atmosphere naturally)

Figure 2. Presentation of the most common examples of the two factors

Climate change has numerous negative aspects and impacts, including extreme weather events, the rearrangement of ecosystems and the consequences of these changes. [12] The early signs and symptoms of this process can already be noticeable to the average person — and for the most part they are — since these increasingly frequent factors influence people's everyday lives and health status. [13]

Overall, we can conclude that climate change brings numerous challenges for humanity; the process is perhaps one of the greatest, if not the greatest, problems in today's world. In order to cope with the negative effects and consequences of climate change, it is important to recognize and understand the potential dangers, analyze them, prepare and train for them, eliminate or reduce them, and if feasible, to prevent them. [14]

CONSEQUENCES AND CHALLENGES OF THE EXCEPTIONALLY DRY, DROUGHT-STRICKEN PERIOD

The year 2022 brought a drought period of a severity not seen in a long time. As the drought intensified, it posed increasingly large challenges for the country, the population, and the disaster management authorities as well. From a disaster management perspective, I would like to highlight three interlinked negative phenomena in which severe changes occurred as a result of the extremely dry weather.

Drought

The phenomenon of drought can be classified among disaster types. "Drought is a prolonged lack of precipitation coupled with great heat. It directly affects primarily agriculture, but it makes its impact felt in every other sector of the economy as well." [15]

Fundamentally, we are dealing with a random phenomenon whose cause is a lack of precipitation. In addition, we must mention that its onset and severity are also influenced by human factors and interventions.

The severity of drought can be measured with a "drought index." Hungary is extremely threatened by drought periods, since nearly 80% of the country can be classified as an area at risk of drought, and only the western part of the country can be considered drought-free. According to statistics and experience, in Hungary 40% of the last 10 years can be recorded as drought years.

Over the years, several methods have been developed to defend against droughts, but these have never — and to this day do not — represent a complete solution. Among these we can include

water transfer installations built on multiple occasions between regions or settlements (e.g. water transfer canals, the construction of river barrages and reservoirs), as well as the complex activity of soil improvement for reducing damage. These interventions provide partial solutions with which the productive capacity of soils can be preserved. In addition, the rational use of water — which requires social and individual conscientiousness — can be mentioned as a kind of solution to mitigate the harmful effects of drought periods.

"At present, drought is a weather event causing very serious problems; there are degrees of such events that can even claim human lives, and in the last 50 years the number of natural calamities related to water and climate/weather is estimated to be 11,000." [16]

Water Scarcity

In connection with the drought period, the phenomenon of water scarcity also reared its head in 2022. Owing to the extreme dryness, the Minister of the Interior declared a prolonged water scarcity period as of March 21, 2022, and as a result special rules and measures related to water resource fees were put into effect.

"To manage the drought situation, the National Water Management Directorate General (OVF), in addition to technical interventions, established a scheduled irrigation plan, and in order to eliminate illegal water extractions, it requested the involvement of disaster management." [17]

With this, they strove to satisfy the increased water demand of agriculture, since the prolonged rainless, hot period meant that crops required continuous irrigation. At the same time, everyone attempted to secure their water needs on their own land, so there were areas that received less water for irrigation, or none at all. It can be stated that this period caused enormous damage in agriculture, and complex problems arose in a domino effect — one problem gave birth to the next.

It is important to mention that the water scarcity problem arising from the worsening drought affected the adequate drinking water supply of the population, and in some settlements it outright endangered it. One such example was Solymár, where the higher-lying areas did not receive water because the pumps did not get a sufficient supply. In addition to Solymár, several other settlements in Pest County — Pilisborosjenő, Budakalász, Pomáz — struggled with similar issues. In this matter, multiple discussions took place among the local operative task force, the disaster management authorities, and the experts of Danube Regional Waterworks Ltd.; the waterworks company asked the population to reduce their water consumption in order to improve the situation.

The drought also affected the country's natural bodies of water: heightened attention was paid to Lake Balaton, the Danube, the Tisza, Lake Velence, and Lake Fertő, as a drastic decrease in average water levels was observed. This threatened and damaged not only the water supply but also the wildlife that had developed there; in several places, mass fish die-offs were observed as well.

HIDROLÓGIAI ADATOK HYDROLOGICAL DATA

Észlelés: 2022. augusztus 01. **EXLEIS**

LAKE NAME	WATER LEVEL [cm]			Change in 24 h (cm)	(°C) Morning water temperature	
	yesterday		today			
	morning	evening	morning			
Fertő-tó	2	//	0	-2	21,0	
Velencei-tó	61	62	61	0	20,5	
Balaton	84	82	83	-1	22,5	
Balaton	81	80	81	0	24,2	
Balaton	85	83	84	-1	//	
Balaton	83	//	82	-1	//	

Figure 3. Water levels in Hungary's major lakes in August 2022. (According to statistics, the water level of Lake Velence reached a negative record — such a low level has never been measured here before).[39]

Wildfires

In general it can be said that almost 100% of outdoor fires (wildfires) are caused by human negligence. These incidents can cause great trouble if unfavorable, impeding factors hinder firefighting — for example, strong winds, extreme dryness and heat, drought periods, or the presence of a large amount of flammable material in the environment. Such incidents and tragedies can be prevented in the simplest way if the population is prepared for the basic safety rules of outdoor fire use and fire prevention, and applies those rules correctly. [18]

Overall, in 2022 we can state that we encountered far more wildfires than in previous years. These incidents affected virtually the entire country without exception, causing serious damage to the population, agriculture, and industry alike. The agricultural sector was particularly impacted — nearly 60% of these outdoor fires struck this sector.

[39] Data used: www.hydroinfo.hu

	2021	2022	Change
Standing grain	70,77 h	650,51 h	9,19 x
Stubble fire	139,4 ha	595,58 h	4,27 x
Agricultural equipment	8 pieces	10 pieces	1,25 x

Figure 4. The relationship between outdoor fires and agriculture, supplements with the number of changes [19]

To fully explore the topic, we must also clarify that in 2022 — in view of the drought and the increased fire risk arising from it — on several occasions fire bans were imposed covering either the counties of Hungary or even the entire country. These bans were ordered by the National Food Chain Safety Office (abbreviated as Nébih), with the agreement of the Ministry of the Interior's National Directorate General for Disaster Management.

Solution Ideas and Possibilities

In addition to presenting the identified problems and phenomena, I consider it important to brainstorm further and search for possible solutions. Therefore, in the following section I would like to outline, in a few points, my views related to the topic, which I have based on what I have learned, my readings, and my own experiences.

Alternative/renewable energy sources: as is known, climate change cannot be completely stopped – since it is a natural process – but slowing its course in various ways is indispensable. From the perspective of slowing climate change, the promotion and use of alternative energy sources is of paramount importance. Even a partial transition to renewable energy sources helps reduce greenhouse gas emissions; this in turn assists in curbing the pace of global warming and in preserving the Earth's climate balance. For our country as well, the use of alternative energy sources is of key importance (I would note that the country has relatively good conditions in this respect), since the transition plays a major role not only in the fight against climate change, but also in the protection of the environment and in establishing the nation's energy independence.

Multipurpose reservoirs: it is well-known that as a result of climate change, the frequency and intensity of extreme weather events — including the flooding of waterways — may continue to increase in the future. Multipurpose reservoirs make it possible to regulate water levels and channel water away during critical flood situations, thereby significantly reducing the harmful impacts caused

by floods – conversely increasing the safety of life and property. It is also worth mentioning the supply role of reservoirs, since with climate change we see increasingly prolonged dry periods. During these dry periods, the reservoirs in question – thanks to their storage function – are capable of ensuring continuity of water resources and the supply of the population. Furthermore, with proper planning and operation, multipurpose reservoirs can help maintain ecosystems, preserve the natural biological diversity of waters, and last but not least, provide an opportunity for energy storage and regulation.

Proper water management: [20] The efficiency of water management can be improved and optimized through numerous methods (for example, in the agricultural sector by promoting/ supporting/applying sustainable farming practices). According to my readings, the nowemerging and largely refined intelligent irrigation systems can greatly help optimize water use in agriculture, and they can play an important role even in household gardens. The top-tier models of these systems are not only capable of regulating water dispensing sufficient for the given area, but also have timer functions. Moreover, they take into account the amount of precipitation that has fallen, evaporation, evapotranspiration, and absorption into the root zone. Using and aggregating these data, the system in question determines the necessary irrigation for the given area day by day. As a result, water wastage can be significantly reduced.

CONCLUSION

In summary, we can say that the entire world – including our country – faces numerous challenges and threats. [21-25] Some of these risks existed at the very beginning of human history; however, as time has passed and humanity has developed and expanded, the risks themselves have evolved and transformed, and new, often more formidable challenges have also appeared. Just as every era has its own most relevant issues and greatest challenges, so does the 21st century. It is essential that we recognize and understand these factors and — with regard to a given country, taking into account the characteristics of the region — analyze and evaluate them in detail in order to achieve an appropriate level of preparedness.

In today's modern world, everything is interconnected. Based on my readings and personal opinion, one of the most burning problems of our age is climate change and its harmful concomitant phenomena, such as drought, water scarcity, and the surge in the number of wildfires. In addition, we can include the issue of mass migration as a significant security challenge, as well as environmental migration resulting from the connection between these factors. Furthermore, in the case of our country — in relation to climate change — we must also take floods into account, since this is the greatest water-related risk. [26; 27] Preparing for, defending against, and restoring damages from these phenomena (drought caused by climate change, water scarcity, wildfires, environmental migration, as well as floods) has proven to be an enormous task – this is very well illustrated by the Danube flood of 2013 that struck our country and the extraordinary drought of 2022, which moreover highlight the danger of a domino effect.

Precisely because of these factors, it is necessary to develop, consider, and as soon as possible implement solution options and appropriate methods. Fortunately, in our time more and more people recognize these dangers, and thus several countries and international organizations — often in a coordinated manner — are working on this. As a result, it is to be hoped that proven and enduringly effective solutions will be applied as soon as possible, so that humanity can enjoy the delights our planet provides for a long time to come, and so that we can achieve a better understanding and more effective preparation against the future effects of climate change.

BIBLIOGRAPHY

[1] László Teknős: Analysis and Evaluation of Trends in Natural Disasters. Belügyi Szemle / Academic Journal of Internal Affairs: (2010-) 72:2 pp. 309-328. (2024)

[2] Muhoray Árpád: A katasztrófavédelem területi irányítási modelljének vizsgálata. PhD-értekezés. ZMNE, Budapest, 2002., 74. p.

[3] Bodnár László; Teknős, László: A globális éghajlatváltozás hatásai az erdőtüzekre Védelem Tudomány: 8: különszám pp. 177-184. (2023)

[4] Szabó Lajos: Mi a biztonság? - Pécsi Határtudományi Tudományos Közlemények XIII., Pécs, 2012, 73. p.

[5] 1163/2020. (IV. 21.) Korm. határozat Magyarország Nemzeti Biztonsági Stratégiájáról. Online. https://net.jogtar.hu/jogszabaly?docid=A20H1163.KOR&txtreferer=00000001.txt

[6] Magyarország nemzeti katasztrófakockázat-értékeléséről szóló jelentése. 2024. Online. https://www.katasztrofavedelem.hu/application/uploads/documents/2025-06/86142.pdf

[7] Teknős László; Muhoray Árpád: A területi védelmi bizottság tagjai, a helyi védelmi bizottságok elnökei, valamint a területi szintű védelmi igazgatási és katasztrófavédelmi feladatok ellátásában közreműködők felkészítésének feladatai: (II. fejezet). In: Szabó, Csaba; Ambrusz, József (szerk.) A katasztrófavédelem lakosságfelkészítési feladatai: Lakosság és ifjúság katasztrófavédelmi felkészítési komplex tanulmány. Budapest, Magyarország: Pytheas (2023) 725 p. pp. 128-286.

[8] Barcza Zoltán; Bartholy Judit; Bihari Zita; Lakatos Mónika; Mészáros Róbert; Pieczka Ildikó; Pongrácz Rita; Práger Tamás; Radics Kornélia: Klímaváltozás. Eötvös Loránd Tudományegyetem, 2013, 5. p.

[9] Padányi József: The Effects of Climate Change on the Military: Risks, Challenges and Answers. Budapest, Magyarország: Ludovika Egyetemi Kiadó (2024), 260 p.

[10] Padányi József: Éghajlatváltozás, természeti katasztrófák, környezeti hatások, katonai képességek. HADTUDOMÁNY: A Magyar Hadtudományi Társaság Folyóirata 33: E-szám pp. 101-119. (2023)

[11] IPCC, 2023: *Climate Change 2023: Synthesis Report.* Contribution of Working Groups I, II and III to the Sixth Assessment Report of the Intergovernmental Panel on Climate Change [Core Writing Team, H. Lee and J. Romero (eds.)]. IPCC, Geneva, Switzerland, pp. 35-115, doi: 10.59327/IPCC/AR6-9789291691647.

[12] Horváth Zoltán; Teknős, László: Climate change impacts on energy infrastructure - analysis of impacts on energy security. In: Lestyán, Mária; Bodnár, László; Érces, Gergő; Varga, Ferenc (szerk.) International Disaster Management Scientific Conference - Focus on Changes in the Fire Safety Situation. Budapest, Magyarország: Magyar Tűzvédelmi Szövetség (2024) 154 p. pp. 137-145.

[13] Antal Z. László (szerk.); Ferencz, Zoltán (szerk.) ; Páldy, Anna (szerk.): Éghajlatváltozás és egészség. Budapest, Magyarország: Társadalomtudományi Kutatóközpont (2020) ISBN: 9789634180401

[14] László Teknős; Krisztina A. Debreceni: Disaster Management Aspects of Global Climate Change. In: Molnár, András; Wenczel, Dóra (szerk.) Third International Conference on Effective Response: Conference Proceedings. Budapest, Magyarország: Magyar Vöröskereszt (2022) 125 p. pp. 45-55.

[15] A 2022-es rendkívüli szárazság fizikai meteorológiai háttere. Online. https://www.met.hu/ismerettar/erdekessegek_tanulmanyok/index.php?id=3200&hir=A_2022-es_rendkivuli_szarazsag_fizikai-meteorologiai_hattere

[16] Kornélia Radics, former president of OMSZ (HungaroMet), speaking on InfoRádió

[17] Fenyegető a vízhiány, már a katasztrófavédelem segítségét kérték. Online. https://infostart.hu/belfold/2022/07/22/fenyegeto-a-vizhiany-mar-a-katasztrofavedelem-segitseget-kertek

[18] Bodnár László; Teknős, László: Természeti katasztrófák és az éghajlatváltozás kapcsolatának elemzése - kiemelten az erdőtüzek hatásaira, bekövetkezési gyakoriságára. In: Huszár, András; Pálvölgyi, Tamás; Schaffhauser, Tibor; Tálas, Péter (szerk.) Klímaváltozás és biztonság Magyarországon: Összefoglaló jelentés. Budapest, Magyarország: Green Policy Center (2024) 152 p. pp. 115-133.

[19] Data used in the table: https://promenad24.hu/2022/06/29/ez-valami-brutalis-iden-33-szorannyi-gabonatabla-egett-le-mint-tavaly/, https://www.agrotrend.hu/hireink/iden-mar-ketszer-annyi-szabadterituz-keletkezett-mint-tavaly

[20] Jánosi Imre; Bíró Tibor; Lakatos Boglárka; Jason Alfredo Carlson Gallas; Szöllosi-Nagy András: Changing Water Cycle under a Warming Climate: Tendencies in the Carpathian Basin. *Climate* 11:6 pp. 1-21. (2023)

[21] Teknős László: A katasztrófatudomány terminológiai vizsgálata, tudománymetriai elemzése. Budapest, Magyarország: Ludovika Egyetemi Kiadó (2023), 176 p.

[22] Vass Gyula; Ambrusz József; Restás Ágoston; Varga Ferenc; Kátai-Urbán, Lajos: Results and Future of Disaster Management Research in the System of Law Enforcement Sciences. Belügyi Szemle / Academic Journal Of Internal Affairs 72:5 pp. 909-927. (2024)

[23] Teknős László: Interpreting Disaster Science, Defining Its Objectives and Range. Studia Universitatis Babes-Bolyai Studia Ambientum 67:1-2 pp. 75-95. (2023)

[24] Teknős László: Az éghajlatváltozás és a rendkívüli időjárás hatásaiból adódó katasztrófavédelmi feladatok kockázatalapú megközelítése, Nemzeti Közszolgálati Egyetem, Budapest, 2018.

[25] Papp Bendegúz: Veszélyes helyen élünk? – Közép-Európa katasztrófaveszélyeztetettségi vizsgálata, Védelem Tudomány VII. évfolyam, 2. szám, 2022.

[26] Fejes, Zsolt Dezső; Pitlik, László; Rikk, János; Szűcs, Diána; Túri, Péter; Budaházy, Péter,E-volution a védelem-egészségügyben: A virtuális oktatási és képzési lehetőségek áttekintése, HONVÉDORVOS 76: 1-2pp. 61-69., 9 p.(2024)

[27] Sea Level Rise and Coastal Flooding (recent) - https://www.science.smith.edu/climatelit/sea-level-rise-and-coastal-flooding-recent/

[28] Teknős László; Kóródi Gyula: A globális éghajlatváltozás biológiai kockázatainak elemzése, hatásainak vizsgálata a katasztrófavédelemre I. Bolyai Szemle 2016:1 pp. 115-130. (2016)

[29] Sandra Banholzer; James Kossin; Simon Donner (2014). The Impact of Climate Change on Natural Disasters. In: Ashbindu Singh; Zinta Zommers (eds) Reducing Disaster: Early Warning Systems For Climate Change. Springer, Dordrecht. https://doi.org/10.1007/978-94-017-8598-3_2

ISSN 7234561-6