

nnováció

HM Electronics, Logistics and Property Management Ltd. Volume 3, Issue 2 | 2025



Responsible publisher

Dr. László András Trembeczki

Chief Executive Officer

Editorial Board

President

Dr. László András Trembeczki (PhD)

H. Associate Professor

Members

Éva Ladányi

H. Associate Professor

Ferenc Kiss

Dr. István Kobolka (PhD)

Associate Professor

hab. Dr. János Sallai

Univ. Professor

Dr. Tibor Szilvágyni (PhD)

Dezső Kiss

László Tömböl

prof. Dr. Sándor Munk

Doctor of the Hungarian
Academy of Sciences

Dr. Zsolt Fejes (PhD)

Lajos Biró

Dr. Ákos Reményi (PhD)

Prof. Dr. habil. Sándor Szakály

Doctor of the Hungarian
Academy of Sciences

Dr. Imre Dobák (PhD)

Associate Professor

Editor-in-Chief

Dr. István Kobolka (PhD)

Associate Professor

Deputy Editor-in-Chief

Ferenc Kiss

Reading Editor

Dezső Kiss

Contacts

Postal address

1101 Budapest, Salgótarjáni street 20.

HM EI Ltd.
Competence Centre

Mobile

Dr. István Kobolka

+36 30 979 6128

E-mail

kobolka.istvan@hmei.hu

The scientific articles and studies contained in this volume do not represent the official position of HM EI Ltd. in any way. They solely reflect the authors' scientifically motivated personal opinions and are subject to copyright responsibility.

Printing: The MoD Zrínyi Geoinformation and Recruitment Support
Public Benefit Non-profit Ltd.

2025

Responsible Manager: Zoltán Pásztor Director

ISSN 2939-7677

Ferenc Dávid:¹

Ensuring Sustainability of Critical Infrastructures: The Hungarian Legal Environment

Abstract:

The sustainability of critical infrastructures (CIs) is paramount in maintaining social stability and resilience, particularly in the face of emerging challenges. The article delves into the legal framework established in Hungary to safeguard CIs, ensuring their sustainable operation and resilience. Hungary, like many other nations, recognizes the significance of CIs in supporting essential services and economic activities. In accordance with the legal guidelines set by the European Union, the Hungary has enacted comprehensive legislation and regulations to protect these infrastructures from various risks and vulnerabilities. The Hungarian legal background on the identification, designation and protection of vital systems and facilities serves as the cornerstone of this national framework, providing guidelines for the identification, designation, and protection of CIs across sectors such as energy, agriculture, healthcare, finance, information technologies, water, public security protection, defence, transportation, and social insurance.

Keywords: critical infrastructure, resilience, sustainability

One of the primary objectives of Hungarian legislation is to enhance the resilience of CIs against natural disasters, cyber-attacks, terrorist threats, and other disruptive events. The law mandates the development of risk assessment methodologies and contingency plans to mitigate potential hazards and ensure continuity of operations. Additionally, it establishes collaboration mechanisms among government agencies, private sector entities, and other stakeholders to coordinate efforts in safeguarding CIs. The importance of international cooperation and alignment with European directives and regulations regarding CI protection has to be emphasized. Cross-border collaboration enables the exchange of best practices, information sharing, and joint response mechanisms to address transnational threats effectively. Hungary actively participates in European initiatives and platforms aimed at enhancing the resilience and sustainability of CIs at the regional and global levels.

¹ Technology Transfer Institute, Research fellow, Budapest, Hungary.

Sustainability of CIs is a multifaceted challenge that requires a robust legal framework, proactive measures, and collaboration among stakeholders. Hungary's legal approach to CI protection reflects a comprehensive strategy that encompasses risk management, implicit sustainability principles, and cooperation. By adhering to these principles and continually adapting to emerging threats and technologies, Hungary aims to ensure the resilience and longevity of its CIs in the face of evolving challenges.

The identification, designation, and protection of critical infrastructure

Providing guidelines for the identification, designation, and protection of CIs across sectors like energy, agriculture, healthcare, finance, information technologies, water, public security protection, defence, transportation, and social insurance, the Hungarian legal background on the identification, designation, and protection of vital systems and facilities serves as the cornerstone of this national framework. A nationally vital system element is identified through a designation process in sectors like energy, transportation, healthcare facilities, digital infrastructure, banking services, financial market infrastructures, drinking water supply and distribution within sectors. The examination of the national system elements covers the analysis and evaluation of risk factors threatening the continuity of services, the so-called to meet sectoral and horizontal criteria, and to examine the possibility of designation as a basic service provider. Horizontal criteria are like criterion of economic-, political-, social-, environmental impact, the criteria for losses, or defence criteria. On the other hand, actors providing basic services are organizations or economic actors that provide essential services in order to ensure the performance of vital social and/or economic processes and functions, their services depend on electronic information systems and a security incident affecting their services would cause a significant disturbance in the service. These six basic services are energy, transportation, healthcare institutions, digital infrastructure, banking services, financial market information, drinking water supply and distribution. (Act, 2012)

As a result of the identification examination, a proposal is prepared for the designation of a system element as a national (or European) vital system element, which is examined by the sectoral designating authority. If at least one sectoral or horizontal criterion is met, the sectoral authority designates the vital system element or service and orders its registration, and at the same time provides for the inclusion of the operator in the list of actors providing basic services. During the procedure, a specialized authority, the Ministry of Interior National Directorate General of Disaster Prevention, the National Tax and Customs Office, the Constitution Protection Office, the Counter-Terrorism Centre, the National Information Centre (as the general Counter-Terrorism Information and Crime Analysis Centre's legal successor), the National Directorate General of Immigration, as well as the territorially competent government commissioner, the territorial environmental protection authority,

the territorial water and water protection authority, and the territorial body of the professional disaster prevention body investigate. (Bonnyai T., 2019) The register containing the designated national system elements is not static, and the central body of the disaster prevention agency – as the registration authority – checks the completion of the conditions and requirements defined in the law within the framework of a complex inspection of the designated national vital system elements every five years. (Bonnyai T., 2019)

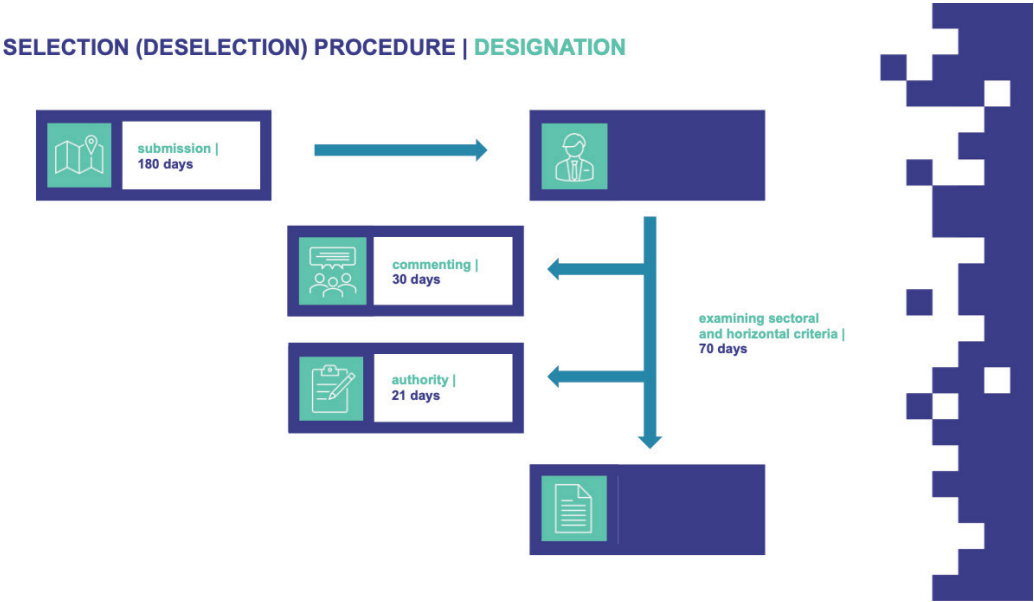


Figure 1: Process of the selection procedure

The identification of national critical (vital) infrastructures is based on risk assessment. Based on the sector criteria, the operators should evaluate and rank whether these comply with the sector criteria. The sectoral government regulations listed above determine which operators are obliged to carry out identification. The deadline for submitting identification reports is 180 days after the entry into force of the relevant sectoral government decree. The submission is made to the sectoral designating authority, which is named in the sectoral government decree for each sector. After the submission, a procedure is started to examine the designation of the given infrastructure as a national critical infrastructure. The official procedure for examining the completion of the sectoral and horizontal criteria conducted by the sectoral designating authority lasts 70 days. The sectoral proposing authority(ies) comment on the identification report, for which the law provides 30 days. The sectoral proposing authorities send their proposals related to the risk analysis to the competent appointing authority. Based on the opinion of the sectoral proposing authority, the position of the specialized authority, and the professional examination and opinion of the sectoral appointing authority, the procedure conducted according



to the above ends with a decision, during which - if at least one sectoral and one horizontal criterion is met - the CIs designated and will be registered. In other cases, according to the same procedure, the designation may be revoked and deleted from the register, the proposal for designation or revocation based on the designation documentation may be rejected, or a deadline of up to 90 days may be set, and an obligation to submit a new identification report in addition to indicating the discovered errors and deficiencies. (Bognár B., Bonnyai T., 2019). Based on the opinion of the sectoral recommending authority, the position statement of the specialized authority, and the professional examination and opinion of the sectoral designating authority, the procedure conducted as described above concludes with a decision, in which the sectoral designating authority may make the following determinations. Not only the designation and registration of critical infrastructure may take place through this procedural process, but also the withdrawal of a previous designation and removal from the register, as well as the rejection of proposals for designation or withdrawal based on the designation documentation.

Improving the resilience of vital infrastructures against terrorism, cyberattacks, natural disasters, and other disruptive occurrences is one of the main goals of Hungarian legislation. To reduce potential risks and guarantee business continuity, the legislation requires the creation of risk assessment techniques and backup plans. It also creates channels for cooperation between public and private sector organizations, as well as other interested parties, to coordinate efforts to protect vital infrastructures. (Nazarova et al., 2024) The significance of global collaboration and adherence to European rules and legislation for the safeguarding of vital infrastructure must be emphasized. To effectively address transnational risks, cross-border collaboration facilitates the sharing of information, the exchange of best practices, and coordinated response procedures. Hungary is an active participant in European platforms and projects that work to improve the sustainability and resilience of vital infrastructures on a regional and global scale. Integrating sustainability measures is a difficulty for critical infrastructure. Therefore, it would need a legally supported governance procedure that guarantees an asset, which is a component of the essential infrastructure, has been built, renovated, or is being used in a way that addresses the range of relevant environmental, social, and governance concerns. But some say that behaviour, both individual and social, is mostly influenced by cultural norms rather than legal requirements. (Stapledon, 2011) Governments are in the position of establishing the legal and environmental frameworks necessary to regulate infrastructure investments, as well as of promoting sustainability measures for important infrastructure projects. Thus, strong national regulatory frameworks and local and national resilience plans can be effective tools. (Panda et al., 2020) It has been important finding that the Hungarian legal background on CIs does not contain any reference to sustainability, but on the other hand, it is a well-functioning adaptive system ready to be reformed. Working together with the private sector is not accomplished in the usual way. To ensure that all pertinent parties are involved

in the sustainability of CI protection, specific settings are developed, such as working groups, public-private partnerships, and in some cases even through legal procedure. (ENISA 2015)

Emerging challenges and sustainable resilience

Maintaining social stability and resilience depends critically on the sustainability of key infrastructures, especially in the face of new threats. Hungary's security environment is influenced by the unique characteristics and evolving trends of European security. These days, the enforcement of dependable international security, the increasingly pervasive realities of globalization and the information age, the more equitable realization of human rights and dignity are among the causes influencing its development. Consequently, the security of humanity is determined by several interrelated global concerns, the most significant of which is the environmental sustainability issue, which is becoming more and more serious and slowly irreversible. Complex, comprehensive, and integrated security creation and maintenance are societal tasks that place distinct demands and duties on every member of society. (Amorim et al., 2022) But society's members need to be ready for this, and that readiness needs to extend to building infrastructure and the built environment's long-term resilience. (Vámosi, 2019) If neglected, CIs can undermine the intended public utility by having severe negative effects on sustainability. While much thought goes into creating a vital infrastructure with a small footprint, after a facility is up and running, little thought is given to assessing how CI interacts with the national infrastructure or its surroundings. Inadequate upkeep of sustainability performance can result in irreparable damages when the detrimental effects of infrastructures build up over time. (Tafazzoli, 2019) This is the point at which the relationship between security, resilience, and sustainability is demonstrated in relation to critical infrastructure. Resilience has been successful in introducing a fresh viewpoint to security discourses by starting from the underlying instability and the source of uncertainty rather than the traditional probabilistic worldview. (Heino et al., 2019) Due to the above, the aim and the structure of the article is twofold. On the one hand, it wants to present the robust national legal background of the Hungarian CI system. On the other hand, it is fundamental that it is necessary to strengthen the resilience against emerging challenges in order for the system itself to become sustainable, for which the article formulates recommendations.

We shall highlight that disruptive technological solutions like using digital twins simulations, artificial intelligence may support resilience of CIs against threats and challenges like cyberattacks, atmospheric phenomena, climate change, technical failures, hybrid threats, interdependence of CIs etc. Digital twins are transforming how we manage and protect CIs, making them more adaptive and robust in the face of various challenges. Virtual models that replicate physical systems, allowing for real-time monitoring and analysis. This technology can significantly enhance the

sustainability and resilience of CIs by enabling predictive maintenance, optimizing resource use, and improving response strategies to potential disruptions. (De Felice et al., 2022) (Vieira et al. 2022) Digital twins are transforming how we manage and protect CIs, making them more adaptive and robust in the face of various challenges. Providing a real-time digital replica of physical assets, allowing for continuous monitoring of CI conditions and helps in identifying issues before they become critical. By analysing data from the digital twin, predictive maintenance can be performed, which means potential failures can be anticipated and addressed proactively, reducing downtime and extending the lifespan of CI components. In the event of natural disasters or other emergencies, digital twins can simulate the impact on infrastructure and help in planning effective response strategies (see as: improves resilience and recovery times, while during the design and planning phases of CI projects, digital twins can be used to test and refine designs). This ensures that new infrastructure is built to be as sustainable and resilient as possible from the outset. The data collected and analysed through digital twins can be used to continuously improve infrastructure operations and management practices, leading to long-term sustainability and resilience. (Vieira et al., 2022) (Rathnayaka et al., 2022)

CI and legal background

The article explores the legislative framework that was put in place in Hungary to protect vital infrastructures and guarantee their resilience and long-term viability. Like many other countries, Hungary understands how important CIs are to the provision of basic services and to the support of economic activity. To safeguard these infrastructures from a range of threats and weaknesses, Hungary has passed extensive laws and regulations that conform to the legal standards established by the European Union. The complicated challenge of CI sustainability calls for proactive initiatives, strong legal frameworks, and stakeholder participation. Hungary's legal framework for safeguarding CI represents a thorough approach that includes collaboration, risk management, and implicit sustainability concepts. Hungary seeks to guarantee the resilience and durability of its vital infrastructures in the face of changing challenges by upholding these values and continuously adapting to new threats and technology.

Europe has released a program to secure its key infrastructure. The Commission issued Communication 702 of 2004 in response to the European Council's June 2004 decision, which called for the development of a plan to defend vital infrastructures within Union territory against potential terrorist attacks. The Commission's efforts resulted in the 2008 adoption of Directive 2008/114/EC, which serves as the foundation for current EU legislation pertaining to CIs. "An element, system, or part thereof located in the Member States which is essential for the maintenance of the vital functions of society, the health, safety, and economic and social well-being of citizens and whose damage or destruction would have a significant impact in a

Member State due to the impossibility of maintaining those functions” is how the directive defines a critical infrastructure. (Directive, 2008) The Directive seeks to create a procedure for the European Union to identify and classify European CI and to devise a strategy to strengthen their security. To achieve this, member states of the European Union are required to apply both sector-specific criteria unique to the kind of European CI and cross-cutting factors, such as potential losses, economic consequences, and effects on residents. Naturally, nations who are members of the European Union periodically assess the designation and identification of European CIs. (Coppolino et al., 2022) (De Felice et al., 2022)

The Directive seeks to create a procedure for the European Union to identify and classify European CI and to devise a strategy to strengthen their security. In order to achieve this, member states of the European Union are required to apply both sector-specific criteria unique to the kind of European CI and cross-cutting factors, such as potential losses, economic consequences, and effects on residents. Naturally, nations who are members of the European Union periodically assess the designation and identification of European CIs. Both directly and indirectly, infrastructure affects how well the sustainable development goals (SDGs) are achieved. Concerns about the sustainability, dependability, and safety of CIs are global in scope and call for an international response. As a result, a number of strategies and procedures have been created to guarantee CIs, considering various factors like human error, maintenance guidelines, energy, water supply, healthcare safety, and emergency transportation in the event of a disaster. (De Felice et al., 2022)

The buildings, resources, networks, and systems that support the services essential to our way of life are considered critical infrastructure. CI offers key support and essential services for economic success, national security, and the efficient functioning and inclusion of communities. These services range from the delivery of energy and water to information and communication services, from healthcare to transportation. These intricate, interrelated, and interdependent networks serve as the basis for modern sustainable development. (Popovski 2023) (Clifford, 2019) Developing a definition of essential infrastructure for Hungary was a top priority, following the EU mandate on the identification and designation of CIs. The concept’s content gradually grows as one moves from the supranational level to national independence, making the definition more and more accurate and comprehensible. Several definitions were named during the process of harmonizing nation’s laws. These were initially listed in the Hungarian Green Book, and then again in Acts CLXVI of 2012 on the identification, designation, and protection of vital systems and facilities, and CXXVIII of 2011 on the amendment of certain laws related to disaster protection. The Hungarian interpretation of CI is most accurately described by the national Green Book: “CI is defined as those networks, resources, services, products, physical or information technology systems, equipment, devices and their constituent parts, the malfunctioning or disruption of which its loss or destruction, directly or indirectly, temporarily or in the long term, may have a serious impact on

the economic and social well-being of citizens, public health, public safety, national security, the functioning of the national economy and the government”. (Green Book, 2008) (Bonnyai, 2019) (Nazarova et al., 2024)

In line with European Community-level regulations and expectations, the legal background for the protection of CI in Hungary is provided by an act on the identification, designation and protection of vital systems and facilities, a government decree on its implementation and further sectoral sub-legislation. It is a preliminary finding that the Hungarian substantive law on CI does not contain any reference to sustainability but is an integral part of a system that is flexible and sustainable in the face of challenges. The relevant legal background broadly regulates the system elements of the national CI in a hierarchical system.

Table 1: Statutory and sectoral legislative level in Hungary

European Union level	
Council Directive 2008/114/EC	on the identification and designation of European CIs and the assessment of the need to improve their protection;
Directive (EU) 2016/1148	concerning measures for a high common level of security of network and information systems across the Union;
National legislative level I.	
Act CLXVI of 2012	on the identification, designation, and protection of vital systems and facilities;
GD 65/2013. (III. 8.)	on the implementation of the Act CLXVI of 2012;
National legislative level II. – Government Decrees (GD)	
GD 374/2020. (VII. 30.)	on the identification, designation and protection of vital energy systems and facilities;
GD 540/2013. (XII. 30.)	on the identification, designation and protection of vital agricultural system elements and facilities;
GD 246/2015. (IX. 8.)	on the identification, designation and protection of vital health systems and facilities;
GD 330/2015. (XI. 10.)	on the identification, designation and protection of vital systems and facilities belonging to the financial sector;
GD 249/2017. (IX. 5.)	related to the info-communication technologies sector on the identification, designation and protection of vital systems and facilities;
GD 541/2013. (XII. 30.)	on the identification, designation and protection of vital water management system elements and water facilities and facilities;
GD 512/2013 (XII. 29.)	on the identification, designation and protection of vital systems and facilities of certain law enforcement agencies;
GD 359/2015. (XII. 2.)	on the identification, designation and protection of vital national defence system elements and facilities;
GD 161/2019. (VII. 4.)	on the identification, designation and protection of vital transport systems and facilities;

Conclusions

The sustainability of vital infrastructures is essential to preserving societal resilience and stability, particularly in the face of emerging challenges. The article explored the legislative framework that was put in place in Hungary to protect vital infrastructures and guarantee their resilience and long-term viability. Like many other countries, Hungary understands how important CIs are to the provision of basic services and to the support of economic activity. To safeguard these infrastructures from a range of threats and weaknesses, Hungary has passed extensive laws and regulations that conform to the legal standards established by the European Union. The Hungarian legal background on the identification, designation, and protection of vital systems and facilities serves as the cornerstone of this national framework, offering guidelines for the identification, designation, and protection of CIs across sectors like energy, agriculture, healthcare, finance, information technologies, water, public security protection, defence, transportation, and social insurance. One of the primary objectives of Hungarian legislation is to increase the resilience of CIs against terrorism, cyber-attacks, natural disasters, and other disruptive events. The law mandates that risk assessment methods and backup plans be developed in order to lower potential hazards and ensure company continuity. Additionally, it establishes opportunities for collaboration between entities in the public and private sectors and other relevant stakeholders to synchronize endeavours aimed at safeguarding essential infrastructures. For the protection of critical infrastructure, it is imperative that international cooperation and compliance with European regulations and laws be stressed. Cross-border collaboration enables information sharing, best practice exchange, and coordinated response procedures to effectively handle transnational hazards. In order to increase the sustainability and resilience of essential infrastructures on a regional and global level, Hungary actively participates in European platforms and projects. Proactive measures, robust legislative frameworks, and stakeholder participation are necessary to address the complex issue of CI sustainability. The comprehensive strategy that incorporates risk management, cooperation, and implicit sustainability concepts is exemplified by Hungary's legal framework for protecting vital infrastructure. By keeping these ideals and continually adjusting to new threats and technological advancements, Hungary aims to ensure the resilience and durability of its essential infrastructures in the face of rising difficulties.

Acknowledgements

1. Project no. 2022-2.1.1-NL-2022-00012 has been implemented with the support provided by the Ministry of Culture and Innovation of Hungary from the National Research, Development, and Innovation Fund, financed under the 2022-2.1.1-NL-2022-00012 funding scheme.

2. Ferenc Dávid, PhD is a Senior Advisor, Research Fellow at the Technology Transfer Institute, and Research Fellow at the National Laboratory of Cooperative Technologies.

References

1. Act, 2012, Act CLXVI of 2012 act on the identification, designation and protection of vital systems and facilities. <<https://net.jogtar.hu/jogszabaly?docid=a1200166.tv>>, accessed: 01.04.2024.
2. Amorim E. E. R., Menezes M., Fernandes K. V. G., 2022, Urban Living Labs and Critical Infrastructure Resilience: A Global Match?, MDPI Sustainability, 14(16), 9826, DOI: 10.3390/su14169826.
3. Bognár B., Bonnyai T. (ed.), 2019, Kritikus infrastruktúrák védelme I. (Protection of CIs I.) Dialóg Campus, Budapest, Hungary, ISBN 978-615-5920-36-3.
4. Bognár B., 2019, A jogszabályi környezet összefüggéseinek és részletszabályainak bemutatása. (Presentation of the connections and detailed rules of the legal environment.) Dialóg Campus, Budapest, Hungary, ISBN 978-615-5920-36-3.
5. Bonnyai T., 2019, Történeti áttekintés, a kritikus infrastruktúra. (Historical overview of critical infrastructure.) Dialóg Campus, Budapest, Hungary, ISBN 978-615-5920-36-3.
6. Coppolino L., D'Antonio S., Giuliano V., Mazzeo G., Romano L., 2022, A framework for Seveso-compliant cyber-physical security testing in sensitive industrial plants. Computers in Industry, 136, 103589, DOI: 10.1016/j.compind.2021.103589.
7. De Felice F., Baffo I., Petrillo A., 2023, CIs Overview. Past, Present and Future. MDPI Sustainability, 2022, 14, 2233, DOI: 10.3390/su14042233.
8. Directive, 2008, The Council of the European Union, Council Directive 2008/114/EC of 8 December 2008 on the Identification and Designation of European CIs and the Assessment of the Need to Improve Their Protection, Brussels, Belgium.
9. ENISA, 2015, Critical Information Infrastructures Protection approaches in EU. <<https://resilience.enisa.europa.eu/enisas-ncss-project/CIIPApproaches/NCSS.pdf>>, accessed: 01.04.2024.
10. Government Decree, 2013, GD 65/2013. (III. 8.) on the implementation of Act CLXVI of 2012. <<https://net.jogtar.hu/jogszabaly?docid=a1300065.kor>>, accessed: 01.04.2024.
11. Green Book, 2008, Government decision 2080/2008. (VI. 30.) on the National Program for CI Protection. <<https://njt.hu/jogszabaly/2008-2080-30-22>>, accessed: 01.04.2024.

12. Heino O., Takala A., Jukarainen P., Kalalahti J., Kekki T., Verho P., 2019, CIs: The Operational Environment in Cases of Severe Disruption. *MDPI Sustainability*, 11, 838, DOI: 10.3390/su11030838.
13. Panda A., Ramos N. J., Mavrodieva A., 2020, Making Critical Infrastructure Resilient. Ensuring Continuity of Service. Policy and Regulations in Europe and Central Asia. UN Office for Disaster Risk Reduction. <<https://www.undrr.org/media/48327/download?startDownload=20240527>>, accessed: 01.04.2024.
14. Popovski V., Critical Infrastructure must be resilient... it's critical, UN Development Program. <<https://www.undp.org/eurasia/blog/critical-infrastructure-must-be-resilientits-critical>>, accessed: 01.04.2024.
15. Tafazzoli M., 2019, Maintaining the Sustainability of Critical Infrastructure. DOI: 10.5772/intechopen.85915. <<https://www.intechopen.com/chapters/66727>>, accessed: 01.04.2024.
16. Vieira, J., Martins, J. P., de Almeida, N. M., Patrício, H., and Morgado J. G., 2022, Towards Resilient and Sustainable Rail and Road Networks: A Systematic Literature Review on Digital Twins. *Sustainability* 14(12), DOI: 10.3390/su14127060.
17. Nazarova, K., Hordopolov, V., Lositska, T., Nezhyva, M., & Mysiuk, V., 2024, Comparative analysis of CI and public significance enterprises. *Multidisciplinary Reviews*, 7(6), DOI: 10.31893/multirev.2024108.
18. Rathnayaka, B., Siriwardana, C., Robert, D., Amaratunga, D., Setunge, S., 2022, Improving the resilience of CIs: Evidence-based insights from a systematic literature review. *International Journal of Disaster Risk Reduction*, 78, DOI: 10.1016/j.ijdr.2022.103123.
19. Vámosi Z., 2019, Biztonságpolitikai aspektusok. Dialóg Campus, Budapest, Hungary, ISBN 978-615-5920-36-3.

Contents

Artificial Intelligence

<i>Dr. Tibor Szilvágyi:</i> The Role of Artificial Intelligence in the Defence Industry II.	3
---	---

Sustainability, Criminology, NATO

<i>Ferenc Dávid:</i> Ensuring Sustainability of Critical Infrastructures: The Hungarian Legal Environment	28
<i>Ádám Végh:</i> The Roll of DNA in Multidisciplinary Factual Science – or the Phenotyping of DNA	39
<i>Violetta Rottler:</i> Private Detectives in Hungary	57
<i>Vilmos Nosza:</i> Stronger Together! Two Years at the NATO Headquarters in Sarajevo	65

PhD Students Forum

<i>Roland Hetényi, Dániel Hanna, Péter Szabó, József L. Szentpéteri:</i> Art of the Kill: UV Inactivation in BioDefense	81
<i>Zsolt Péter Függ, Zsolt Nemeskéri, Brigitta Zsótér:</i> Kate Soper and the Notion of Sustainable Consumption	92
<i>Zuzana Križalkovičová, Péter Szabó, Kata Kumli, Miloš Štefanovský, József Szentpéteri:</i> Strategic Implications of Early Judo Training for National Defense Applications	109

