A kritikus szervezetek ellenálló képességéről szóló Irányelv végrehajtása Magyarországon

Implement regulation on the resilience of critical entities in Hungary

Ronyecz Lilla
doktorandusz
Nemzeti Közszolgálati Egyetem
Email: lillaronyecz@gmail.com
ORCID: 0000-0001-5062-5488

Dr. Bognár Balázs tű. dandártábornok
adjunktus
Nemzeti Közszolgálati Egyetem
Email: balazs.bognar@katved.gov.hu
ORCID: 0000-0002-6029-1917

Bevezetés

A cikk a kritikus szervezetek rezilienciájáról szóló Európai Uniós irányelv magyarországi jogszabályi átültetését veszi át, felvázolja a nemzet kritikus szervezetei és infrastruktúrái ellenálló képességének és kapacitásának javítását célzó legfontosabb jogalkotási és szabályozási intézkedéseket. A nemzeti prioritásokhoz és az uniós irányelvekhez egyaránt igazodó szakpolitikák a kiberbiztonság, a kockázatkezelés és a működési készenlét fokozására összpontosítanak, miközben elősegítik a kormányzati és gazdasági ágazatok közötti együttműködést. A megközelítés fejlett módszereket és keretrendszereket integrál, biztosítva az európai szabványokkal, például a NIS 2 és a CER irányelvekkel való összhangot. Ezek az intézkedések a kritikus ágazatok, például az energia, a közlekedés és a kommunikáció sebezhetőségével foglalkoznak, miközben hangsúlyt fektetnek a szereplők közötti együttműködésre, az ellenálló képesség tervezésére és az egyszerűsített adminisztratív folyamatokra. Az új jogszabályok jelentős fejlődést jelentenek, és fokozott hangsúlyt fektetnek az átfogó kockázatkezelésre, a határokon átnyúló együttműködésre és a digitális ellenálló képességre.

Introduction

The article takes a Hungarian transposition of the EU Directive on the Resilience of Critical Organizations, outlining the key legislative and regulatory measures to improve the resilience and capacity of the nation's critical organizations and infrastructures. Aligned with both national priorities and EU directives, the policies focus on enhancing cybersecurity, risk management and operational readiness, while fostering cooperation between government and industry sectors. The approach integrates advanced methodologies and frameworks, ensuring consistency with European standards such as NIS 2 and CER directives. These measures address vulnerabilities in critical sectors such as energy, transport and communications, while emphasizing cooperation between actors, resilience planning and simplified administrative processes. The new legislation represents a significant improvement with an increased focus on comprehensive risk management, cross-border cooperation and digital resilience.

Kulcsszavak: kritikus szervezetek, jogszabályi implementáció

Keywords: critical organisation, legislative implementation

Brief Overview and Literature Review

The emergence of new regulation on critical infrastructure on the resilience of critical organizations and Council Directive 2008/114/EC of the European Parliament and of the Council (EU) 2022/2557 Directive of the European Parliament and of the Council of 2022/2006 of the European Parliament and of the Council of 2022/2006 on Critical Infrastructure (hereinafter referred to as the CER Directive). The public consultation on draft legislation, such as the law on the resilience of critical organisms or the draft government decree on the resilience of critical organisms, was closed on 23 October 2024.

The draft legislation contains provisions that are in line with the need to improve the resilience of Hungary's critical organizations and infrastructures and with national and EU directives. These elements include: the establishment of risk management methodologies, the designation of authorities responsible for the supervision and support of critical processes, and requirements for cybersecurity and business continuity. It stresses the need for the nation's government authorities and organizations to work together to ensure national security and to secure critical economic sectors such as energy, transport, communications services and networks.

There is a significant Hungarian literature on the protection of vital systems and facilities, which has been formulated as part of industrial safety and environmental safety [1,2]. The identification of critical infrastructure is carried out in most areas of industry, energy and transport by applying disaster risk management and analysis techniques [3,4]. In addition, we consider the resilience of hospital infrastructure, among other things, due to the Covid 19 epidemic, among today's challenges [5]. There is also a significant body of literature discussing issues related to terrorist acts [6], although in recent years the emphasis of regulation has shifted to the resilience of individual entities of economic sectors.

The Critical Organism Resilience Act

The document provides a clear structure for the protection of critical infrastructure without compromising the national security approach and the EU integration perspective.

It aims to protect against all threats by improving the quality of active measures to manage essential services.

The Critical Organizations Act is briefly presented as follows:

1. Integration with EU standards: the Act is quite closely aligned with the EU NIS 2 Directive, which places more emphasis on high level cybersecurity features and inter-jurisdictional cooperation.
2. Comprehensive risk management: companies should have in place developed risk mitigation structures and resilience action plans that consider internal and external aspects.
3. Restructuring of vulnerable sectors: the energy and health sectors, among others, are partly targeted with measures to cushion the provision of critical services.
4. 4 Resilience planning: the law requires plans to build resilience and regular updates of risk matrices to avoid stagnation.
5. 5 Authority and oversight: Supervisors should be empowered to ensure that all measures are followed and complied with. [7]

Comparison with Law CLXVI of 2012 on the identification, designation and protection of critical systems and installations

The similarities between the two laws start with the central role of critical infrastructure protection in supporting national security and public safety continuity, followed by the mandate for risk assessment and the designation of authorities responsible for overseeing the resilience of critical systems.

In addition, the Critical Organizations Act further strengthens cybersecurity measures and cross-border interdependency considerations through updated EU standards.

The new legislation also foresees more extensive resilience planning mechanisms, such as the use of resilience matrices, as well as more stringent monitoring mechanisms.

The new law represents a significant improvement compared to Act CLXVI of 2012, in terms of integrating EU cybersecurity standards and a comprehensive approach to risk and resilience. The Regulation reflects a more holistic understanding of threats, recognizing the importance of physical and cyber elements in protecting critical infrastructures. [8]

Government Decree on the Resilience of Critical Importance Organizations

The Regulation contains provisions for the development of resilience measures for critical organizations and multiple infrastructures in line with the EU CER Directive. Key elements include the identification and designation of critical organizations, in-depth resilience and risk management requirements, optimized administrative procedures and cooperation frameworks at national and EU level. The Government Regulation sets out guidelines on what the competencies of the Security Liaison Officers should look like, emphasizing the importance of the individual, emphasizing cyber security and infrastructure continuity in the design.

The Government Decree is briefly presented as follows:

1. Harmonization with EU Directives: this Regulation will, inter alia, facilitate compliance with EU legislation, in particular the CER and NIS 2 Directives, which require high safety standards and a thorough approach to risk management.
2. Simplification of administrative procedures: A simplified and clear procedure should be introduced to reduce red tape by shortening the timing of flexibility assessments and designation processes.
3. targeting key sectors: the regulation introduces a focus on ensuring that sectors deemed vital by the country, including energy, health and digital services, have a specific resilience plan.
4. Inter-agency cooperation: the Regulation clearly outlines the roles and responsibilities of the different government and regulatory bodies, emphasizing cooperation within national authorities as well as with the EU institutions.
5. Training and capacity building: the Regulation calls for the continuous training of designated resilience officers to ensure that they are best prepared to respond and react to risks.

The regulation also addresses the need to enhance national resilience to a wide range of threats. It aims to better protect critical infrastructure by aligning with EU standards and reducing administrative burdens. However, the effective implementation of the Regulation depends on the cooperation of stakeholders and the continuous updating of risk assessments [9].

Comparison with the Government Decree 65/2013 (8.III.) on the implementation of Act CLXVI of 2012 on the Identification, Designation and Protection of Critical Systems and Facilities

The similarities are that both regulations emphasize the need to protect critical infrastructure and maintain services, provide for steps to identify critical infrastructure and create a way for authorities and operators to work together.

There are a number of differences between the two Regulations, including:

- Scope and integration: the new regulation covers more sectors and includes stricter cybersecurity rules, aligned with new EU legislation (such as the CER and NIS 2 directives).
- Simplification of administration: the new Regulation simplifies administrative tasks compared to the 2013 Regulation, reducing bureaucracy and setting faster deadlines for important actions.
- Flexibility and training: the new Regulation requires training for resilience officers and focuses on continuous capacity building, which was not previously emphasized as much.
- Emphasis on cybersecurity: The updated Regulation puts more emphasis on cybersecurity, recognizing the growing need for digital resilience, whereas the 2013 Regulation only addressed this issue in a limited way.
- Addressing interdependencies: The current Regulation addresses interdependencies between sectors more effectively, taking into account both physical and digital aspects. [10]

The latest government regulation is a significant update compared to the 2013 framework, incorporating new EU rules and addressing topical issues such as cybersecurity. It offers a more comprehensive and proactive way to enhance resilience, helping Hungary's critical infrastructures to be prepared for different threats.

Conclusions

The new law and the government regulations reflect the pervasive change in the way Hungary wants to protect its critical infrastructure. These legal frameworks are closely aligned with contemporary EU instruments such as NIS 2 and the CER Directive, with a particular focus on enhancing cybersecurity and resilience planning and simplifying procedures for the highest-level authorities. Sectoral coverage and cooperation between authorities will contribute to ensuring comprehensive protection against threats now and in the future. Together, these measures will bring Hungary's critical infrastructures in line with European standards and facilitate cooperation at national and cross-border level to strengthen such infrastructures. Furthermore, these measures will ensure risk assessment and cooperation between stakeholders.

Literature

[1] Bognár, Balázs et. al. Iparbiztonságtan I.: Kézikönyv az iparbiztonsági üzemeltetői és hatósági feladatok ellátásához. Budapest: Nemzeti Közszolgálati és Tankönyv Kiadó Zrt. (2013) , 564 p.

[2] Sibalin, Iván és Kátai-Urbán, Lajos és Vass, Gyula (2019) Environmental and Industrial Safety Aspects of International Regulations Relating to the Operation of Energetic Systems = Az energetikai rendszerek működésével kapcsolatos nemzetközi szabályozás környezet- és iparbiztonsági aspektusai. *Műszaki Katonai Közlöny*, 29 (3). pp. 153-161. http://doi.org/10.32562/mkk.2019.3.11

[3] Kátai-Urbán, Lajos ; Érces, Gergő ; Sibalin, Iván ; Vass, Gyula: Risk assessment in the field of disaster management in Hungary. In: Savic, Branko (szerk.) *13. Међународно Саветовање Ризик И Безбедносни И Инжењеринг Зборник Радова.* Novi Sad, Szerbia : Visoka tehnička škola strukovnih studija u Novom Sadu (2018) pp. 340-345. [Online]. Available: http://www.rizik.vtsns.edu.rs/wp-content/uploads/2018/01/Zbornik-RIZIK-januar-2018.pdf#page=340 (15.12.2024.)

[4] Kátai-Urbán, Lajos ; Vass, Gyula ; Sibalinné, Fekete Katalin: Establishment and Implementation of Hungarian system for critical infrastructure protection. In: Andrea, Peterkova (szerk.) *Riešenie krízových situácií v špecifickom prostredí: 19. medzinárodná vedecká konferencia*, 21.-22.máj 2014, Žilina: zborník. 1. část. Zilina, Szlovákia: Žilinská univerzita v Žiline (2014) 264 p. pp. 353-360. [Online]. Available: https://www.fbi.uniza.sk/uploads/Dokumenty/weby/rks-archiv/2014/articles/KataiUrban_Vass_SibalinneFefete.pdf (15.12.2024.)

[5] Kátai-Urbán, Lajos ; Mészáros, István ; Vass, Gyula: Egészségügyi kritikus infrastruktúrák biztonsága a koronavírus árnyékában. In: Gaál, Gyula; Hautzinger, Zoltán (szerk.) *Rendészet a rendkívüli helyzetekben: húsz éves a Szent László napi konferencia.* Pécs: Magyar Hadtudományi Társaság Határőr Szakosztály Pécsi Szakcsoport (2021) 433 p. pp. 87-97. [Online]. Available: https://pecshor.hu/periodika/XXIII/katai_meszaros_vass.pdf (15.12.2024.)

[6] Almási, Csaba; Cimer, Zsolt ; Kátai-Urbán, Lajos ; Vass, Gyula: Prevention of Terrorist Attacks during the Transport of Dangerous Goods by Road in Hungary. *American Journal of Research Education and Development* 2022 (2) 2-10. (2022) [Online]. Available: https://www.red.devlart.hu/issues/2022_2.pdf#page=4 (15.12.2024.)

[7] Draft Critical Organism Resilience Act [Online]. Available: https://cdn.kormany.hu/uploads/document/b/bf/bfc/bfc1dfcacb8a49c51e64364bbd58d4939929e68e.pdf (15.12.2024.)

[8] Act CLXVI of 2012 on the Identification, Designation and Protection of Critical Systems and Facilities. [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=a1200166.tv (15.12.2024.)

[9] Draft government decree on the resilience of organisations of importance for the defence and security of the country [Online]. Available: https://torvenyfigyelo.hu/te/dokumentumtar-azorszagvedesbiztszempjelszervellenallokepessegerolszkormrend-belugyminiszterium-20241206/downloaded.zip (15.12.2024.)

[10] Government Decree No. 65/2013 (8.III.) on the implementation of Act CLXVI of 2012 onthe Identification, Designation and Protection of Critical Systems and Facilities. [Online]. Available: https://net.jogtar.hu/jogszabaly?docid=a1300065.kor (15.12.2024.)