

István Mészáros<sup>1</sup>

## Comparison of the Protection of Critical Healthcare Infrastructures in Germany and Hungary

### Abstract

*In 2008, the European Union regulated the basics of the protection of critical infrastructures in a directive. The Member States therefore had to ensure that – in addition to the freedom of the method and means of implementation – the provisions of the directive were transposed into their national legal order. Accordingly, some Member States may define different detailed rules. The detailed rules related to the protection of critical infrastructures (e.g. the designation thresholds) are not public in several Member States, but in Germany and Hungary they have been recorded at the legislative level. In my study, I compare the rules related to the protection of critical healthcare infrastructures, including inpatient care institutions, primarily based on legal sources and the experiences of my study tour in Germany, from the selection criteria system to crisis planning. The good practices resulting from the differences and similarities to be discovered can help to revise and standardise the rules and practices related to the protection of critical health infrastructures.*

*Keywords: critical infrastructure, vital system, health crisis situation, operator security, hospital safety*

### Regulation of the protection of critical infrastructures in the European Union

The geopolitical and globalisation changes that took place until the 1990s resulted in extremely rapid technical development, which increased society's dependence on infrastructure systems. The proper operation of these systems is of fundamental

<sup>1</sup> PhD student, Ludovika University of Public Service Doctoral School of Military Science and Officer Training, e-mail: [meszaros.istvan.mail@gmail.com](mailto:meszaros.istvan.mail@gmail.com)

importance for the ordinary person, as well as for the economic, commercial, financial, government, and public administration sectors.

Terrorist attacks in the European Union and the United States in the 2000s prompted lawmakers to take action to protect critical system components. When the Green Paper was presented in 2007, it defined the following 11 critical infrastructure areas: energy, information and communication technologies; water supply; food safety; healthcare; financial system; public safety and justice system; public administration system; transport (road, rail and air transport, inland, ocean and sea shipping); chemical and nuclear industry; space and research.<sup>2</sup> Following the submission in 2008, the 2008/114/EC (8 December, 2008) European Council Directive formulated the concept of critical infrastructure and the criteria for classification as critical infrastructure.<sup>3</sup>

The Directive states that "primary and ultimate responsibility for the protection of critical infrastructure rests with the Member States and the owners/operators of the infrastructures".<sup>4</sup>

In addition, the Directive defines the fundamentally critical sectors and horizontal criteria (however, it refers the determination of their threshold values and the sector criteria to the competence of the Member States), as well as the basic rules of identification and designation, the obligation to prepare an Operator Security Plan and employ a Security Liaison Officer for the designated critical infrastructures.

## Regulation of the protection of critical infrastructures in Hungary and Germany

The first legislation on critical infrastructures entered into force in Hungary in 2012. This is the Act CLXVI of 2012 on the identification, designation and protection of essential systems and facilities (Act of CIP).

The Act defines the concept of a critical infrastructure element, and defines the sectors designated from the point of view of critical infrastructure protection and authorises the Government to designate the sectoral designating authority, the proposing authority, establish the general and sectoral rules for identification and designation, as well as the sectoral and the horizontal criteria.

The Government Decree 65/2013 (8.III.) on the implementation of the Act CLXVI of 2012 on the identification, designation and protection of essential systems and facilities defines the rules of designation/withdrawal, the tasks of the security liaison officer and general expectations for its employing, as well as the obligation to prepare the Operator Security Plan.

The Government Decree 246/2015 (8.IX.) on the identification, designation and protection of critical health systems and facilities entered into force in 2016 for the healthcare sector. The decree defines the sub-sectors and designation criteria, the

<sup>2</sup> COM (2005) 576 final.

<sup>3</sup> European Council Directive 2008/114/EC.

<sup>4</sup> European Council Directive 2008/114/EC.

sector-specific rules of the identification procedure and designation, as well as the sector requirements imposed on the security liaison officer.<sup>5</sup>

Sectors and sub-sectors defined for the identification and designation of critical infrastructures from the Act CLXVI of 2012 on the identification, designation and protection of essential systems and facilities:

- active inpatient care and the services necessary for its operation
- rescue management
- health reserves and blood stocks
- high security biological laboratories
- drug wholesale

In addition to all of this, Act L of 2013 on the electronic information security of state and local government bodies was also extended to cover critical infrastructures. In this law, the legislator regulates the IT security obligations of vital system elements.

In contrast, in Germany, the regulation related to critical infrastructures originates from an information security regulation, the Federal Information Security Office Act (Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, BSI), which was issued in 2009.

In this law, the legislator authorises the individual ministries to define in a decree the services that are important and are considered critical due to their importance in the given sectors, which facilities, systems or their parts are classified as critical infrastructures under this law, as well as the sectoral thresholds.

In accordance with the above, the Decree on the definition of critical infrastructures according to the BSI Act (Verordnung zur Bestimmung Kritischer Infrastrukturen nach dem BSI-Gesetz, BSI-KritisV) has been in force since 2016.

The Decree – which has undergone several additions since its publication (e.g. the addition of new sectors) – defines the critical sectors, their sub-sectors and the selection criteria system.

Based on the Decree, sub-sectors within the healthcare sector:

- inpatient care
- delivery of immediate life-sustaining medical devices that are consumables
- supply of prescription drugs and blood and plasma concentrates
- laboratory diagnostics

## **Operator safety of critical inpatient care infrastructures**

### *Criteria system for designation*

Government Decree 246/2015 (8.IX.) on the identification, designation and protection of vital health systems and facilities in Hungary defines the following threshold values:

<sup>5</sup> MÉSZÁROS 2023: 43–57.

- has at least 400 active beds
  - or the number of persons belonging to its territorial supply obligation reaches or exceeds 1.5 million people
- and
- in the event of a breakdown, the nearest hospital cannot be reached by public road within 45 minutes
  - or there is a health policy interest in the continued operation of the hospital

The operator prepares an identification report in every four years, which it submits to the Sectoral Decision Committee, where the fulfillment of the horizontal and vertical criteria is examined with the involvement of the specialised authorities. In case of fulfillment, the Sectoral Decision Committee designates the critical infrastructure in a decision.

In Germany, based on the decree on the definition of critical infrastructures according to the BSI Act, that inpatient care facility can be designated as critical infrastructure, where the number of inpatient care cases reaches or exceeds 30,000 cases per year.

Hospitals have to check each year until March 31, whether they meet or exceed this threshold. If fulfilled, the operator sends the appropriate report to the Federal Office for Information Security (BSI) and the hospital is classified as critical infrastructure from the following day (1 April).

Table 1: Selection criteria and review

	Hungary			Germany
<b>Criteria</b>	min. 400 beds	OR	min. supply district of 1.5 million people	30,000 inpatient care events/year
	AND			
	There is no other hospital within 45 minutes	OR	health policy interest	
<b>Review</b>	every 4 years			annually

Source: compiled by the author

It can be seen from the above that in Germany a simpler approach was used when determining the threshold, but with an annual review.

The peculiarity of the Hungarian inpatient care system is that within some hospitals, some medical professions have so-called levels of progressivity, which is "a peculiarity of the care system arising from the frequency distribution of diseases, according to which the more frequent – and mostly simpler – cases are organised at a lower level by the care system (according to the patient's place of residence provided in nearby) units. The rarer and mostly more complicated cases, on the other hand, are directed to centralised (territorial, county, regional, national) institutions.

In Hungary, the lowest level is the primary care, and the highest level is the national institutes and university clinics.”<sup>6</sup>

In practice, however, it happens that in some hospitals, different professions are at different progressivity levels, as a result of which they have territorial care obligations of different sizes even within certain professional groups. The following tables illustrate the identification of a university clinic (Table 2 and Table 3).

Table 2: Designation criteria and review

Name of department	Profession code	Name of profession	Number of beds	Progressivity level
Obstetrics department	405	Obstetrics	82	2–3
Perinatal Intensive Care Unit	502	PIC	23	1–3
Department of General Gynecology	406	Gynecology	20	1–3
Obstetrics and Gynecology Unit – private	400	Obstetrics Gynecology	15	1–3
Total			140	

Source: compiled by the author

Table 3: Meeting the selection criteria of the same clinic

Criteria	Value	Threshold value	Fulfillment	
A1 (number of beds)	140	400	no	
A2 (number of persons belonging to its territorial supply)	Progress 1	490 146	1 500 000	no
	Progress 2	1 132 761	1 500 000	no
	Progress 3	3 434 325	1 500 000	YES
B1 (nearest hospital)	Progress 1		It's in 45 minutes	no
	Progress 2		It's in 45 minutes	no
	Progress 3		Not in 45 minutes	YES
B2 (health policy interest)	yes: medical university, research	yes/no	YES	

Source: compiled by the author

The legislator did not specify which level of progressivity should be taken into account, and based on my practical experience, the Sectoral Decision Committee that makes the designation does not take into account the levels of progressivity, but examines the given institution as a whole.

Overall, it can be said that the German designation practice is simpler and somewhat more tangible, and uses a criteria system that adapts more linearly to the horizontal criteria. It is not known to me what kind of changes in the number of care events occur each year for some hospitals compared to the defined threshold.

<sup>6</sup> See: [https://fogalomtar.aEEK.hu/index.php/Progresszivitási\\_szintek](https://fogalomtar.aEEK.hu/index.php/Progresszivitási_szintek)

However, even if there are changes, the German practice is suitable for hospitals that lose their critical classification overnight to maintain the established operator security practice.

### *Operator Security Planning*

Both Member States have in common that the detailed requirements of the Operator Safety Plan (OSP) are contained in official recommendations, however, a significant difference is that, in accordance with European Union regulations, in Hungary, the legislation defines the obligation to prepare the OSP, and even the sectoral Regulation specifically defines mandatory content elements and that the Health Crisis Plan (HCP) is also part of the institution's Operator Security Plan (OSP). On the other hand, the legal regulations in Germany do not require any obligation to prepare an OSP, and even the official recommendations do not specifically mention OSP, but detail the planning of crisis management measures based on the risk assessment.

In Germany, the law only states that "operators of critical infrastructures are obliged to take the appropriate organisational and technical precautions to avoid disruptions in availability at the latest on the first working day after they are classified as critical infrastructure for the first time or again".<sup>7</sup>

The regulation in Germany can be said to be fundamentally information security-centric. According to the website of the Federal Office for Information Security (BSI) – on the basis of Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical organisations and the repeal of Council Directive 2008/114/EC (CER Directive) – a new legislation, which is expected to enter into force in 2024, will address general operator security issues: "This draft law identifies critical infrastructures at the federal level for the first time and sets minimum standards for physical protection for operators of critical infrastructures. Previously, such federal regulations only existed for the IT security of critical infrastructures. The regulations of the KRITIS-Umbrella law, which concern physical protection, are intended to supplement the existing IT security measures. The aim is to strengthen the resilience of critical infrastructures, the resilience against threats, in Germany as a whole."<sup>8</sup>

In addition to all this, the Federal Office for Civil- and Disaster Prevention (BBK) and the German Hospital Association (DKG) publish recommendations such as:

- Protection of critical infrastructures – Risk and crisis management Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement)
- The hospital as a critical infrastructure – Executive order of the German Hospital Association (Krankenhäuser als kritische Infrastrukturen – Umsetzungshinweise der Deutschen Krankenhausgesellschaft)

These recommendations primarily provide a framework for risk assessment and management, as well as crisis management, without specific calculation requirements,

<sup>7</sup> Gesetz über das Bundesamt für Sicherheit in der Informationstechnik, BSIG.

<sup>8</sup> See: [www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/KRITIS-DachG.html](http://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/KRITIS-DachG.html)

mainly referring to national and international standards, but using a process-based approach.

In Hungary, in addition to the fact that the law requires the preparation of the OSP with sector-specific obligations, National Directorate General for Disaster Management under the Ministry of the Interior publishes specific recommendations regarding the content and form requirements of the plans, such as:

- risk analysis
- instructions for completing the risk analysis
- OSP assistance

During the risk analysis, meteorological, geological, human, technical, communication, fire, IT risks, as well as risks related to hazardous materials and technologies, are prescribed to analyse. The risk analysis can be expanded freely, but it is not process-based. The table is equipped with formulas, and when determining the risk value, it calculates not only the probability of occurrence and the extent of its possible impact, but also the exposure of the institution. During the analysis, the possible risk reduction measures must be indicated and the given risk element must be re-evaluated accordingly.

The OSP assistance defines in detail the content and form requirements of the plan, from the detailed presentation of the infrastructure, through the risk analysis, to the risk management measures.

In summary, it can be said that while German regulation gives operators more freedom for operator security measures, it mostly uses an information security-centric approach. On the other hand, the Hungarian regulations apply a complex approach to the operator's security activities and provide operators with precise, detailed instructions for the performance of these activities.

## **Crisis planning of inpatient care institutions**

In Hungary, the Act CLIV of 1997 on healthcare defines the concept of a health crisis situation, the cooperation and planning obligation for healthcare providers.

Government Decree 521/2013 (30.XII.) on health crisis care details the rules of crisis healthcare, such as the criteria for classifying it as a health crisis situation, detailed rules for the assignment and transfer of healthcare workers, the method of providing the necessary equipment for care, and the tasks of preparation and training. In connection with the latter, the legislator determined that "the minister responsible for health, with the cooperation of the National Chief Medical Officer, can directly order healthcare providers to conduct health crisis exercises or to participate in international exercises", so individual hospitals do not have an obligation to conduct exercises in this sense. The Decree also specifies that the County Government Office must also prepare a Health Crisis Situation Plan for the performance of health crisis tasks, to which the institutional plans of the healthcare providers belonging to the county form an annex.

The Decree 43/2014 (19.VIII.) of the Ministry of Human Resources on the content requirements of the health crisis plans of health institutions and on the amendment of

certain ministerial decrees on health matters determines the rules for the preparation of Health Crisis Plans (HCP). Pursuant to the decree, the healthcare provider must review the plans every year and submit them to the County Government Office for approval. The Decree also defines the exact content and form requirements of the HCP and its sub-plans.

The HCP is actually a plan system consisting of a basic plan and fourteen sub-plans.

"To facilitate structuring, understanding and – obviously – application, plans can be grouped into four categories. These categories are:

- basic information and access to readiness
- reaction to an extraordinary event affecting the given organisation
- responding to an extraordinary event that took place elsewhere, extending the service
- operation of service processes

The implementation and application of the plans can happen separately or simultaneously in different permutations depending on the nature of the event taking place.<sup>9</sup>

It can also be concluded that domestic regulations affecting critical systems are closely related to fire prevention<sup>10</sup> and industrial safety regulations.<sup>11</sup>

In Germany, according to the provisions of the Basic Law, responsibility for the implementation of security measures rests with the individual states. Hospitals are obliged to prepare, update and implement alarm and operation plans for crisis situations. This is governed by the hospital laws or disaster management laws of that federal state.<sup>12</sup>

When creating the individual Hospital Alarm and Response Plan (Krankenhausalarm- und -einsatzplanung) (KAEP) of each hospital, the applicable legal requirements of the federal states must be taken into account. All federal states now have corresponding requirements.<sup>13</sup>

Based on the above, it is regulated at the federal state level in Germany what kind of plans each hospital must prepare and whether they have an obligation to practice these. However, the federal state legislation – as in the case of operator security planning – does not define specific content and form requirements, but generally clarifies the obligation to prepare plans and the responsibility for managing crisis situations.

Recommendations are available regarding the content and form requirements of the plans. An example is the *Handbook of Hospital Alarm and Response Planning (Handbuch Krankenhausalarm- und -einsatzplanung)*, which was published by the Federal Office for Civil and Disaster Prevention (BBK) in cooperation with the German Hospital Deployment Planning Working Group (DAKEP) and the German Traumatology Society (DGU).

Based on the manual, a KAEP must cover the following scenarios:

- operational management of the hospital during an extraordinary event

<sup>9</sup> KÁTAI-URBÁN et al. 2019: 48–83.

<sup>10</sup> ÉRCES et al. 2023: 104–128.

<sup>11</sup> CIMER et al. 2021.

<sup>12</sup> Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2020.

<sup>13</sup> Bundesamt für Bevölkerungsschutz und Katastrophenhilfe 2020.



- alarm, deployment, logistics
- crisis communication
- evacuation
- eviction
- mass casualty care
- prevention of chemical, biological and nuclear threats (including pandemics)
- appearance of aggressive persons, bomb threats, appearance of people running amok
- disturbances of the technical infrastructure

The manual also presents case studies of events that occurred in the case of the given scenarios for educational purposes.

By comparing the planning regulations and practices of the two Member States, it can be said that in both cases the planning includes a scenario-based approach, and that each extraordinary event is basically managed based on the establishment of a management structure different from the peacetime one. In Germany's plans, the management of IT incidents has a prominent role, which in Hungary does not appear according to regulations during HCP planning. Hungarian legal regulations define thorough and detailed requirements for healthcare providers, while in Germany, institutions have more freedom in this matter as well, and however, compliance with their responsibilities and obligations is checked in several federal states through mandatory practices.

## Summary

Directive (EU) 2022/2557 of the European Parliament and of the Council on the resilience of critical organisations and the repeal of Council Directive 2008/114/EC (CER Directive) needs to be transposed into the national legal systems of the Member States in 2024. The Directive takes a new type of approach to protecting vital service providers and thus critical infrastructures by focusing on building and maintaining resilience. With the above study, I would like to highlight that in the regulatory and planning practice of some Member States, there are many professional procedures based on a similar approach beyond the requirements of the Directive, and there are differences that can serve as good examples at the community level in the health sector.

In relation to the sectoral criteria used during the identification and designation of critical infrastructures, it can be said that Hungarian practice uses a more complicated approach, but is based on values that can be said to be permanent, which allow the review to take place only every four years, which provides predictability for the operator during preparation and application. However, in the German regulations, a threshold value based on practice has been defined, subject to an annual review. This practice opens up the possibility for hospitals that lose their certification in the meantime to maintain the already proven operator security practice, thereby contributing to the business continuity of the entire care system.

All in all, it can be said that the regulations in Germany apply a more IT security-oriented approach and give a lot of freedom to hospital operators both in terms of operator security and crisis planning, the implementation of which is monitored through official inspections and the implementation of exercises. On the other hand, the Hungarian regulation uses a fundamentally complex approach, placing great emphasis on physical security, and the legislator regulates in detail the duties of hospital operators, the content and form requirements of the plans, but there are no regulations regarding the maintenance of health care processes in the event of IT security incidents.

In the case of both Member States, the scenario-based approach appears in crisis planning, however, in several cases, they approach certain scenarios from a different direction. While in Hungary the plans describing the individual service processes and related additional scenarios can be applied separately to each scenario, in Germany one scenario accompanies the entire process. In the risk analysis methodology, the process-based approach prevails, as opposed to the Hungarian analysis based on the listing of risks and the examination of their general effects, but in Hungary the measurement of exposures and the evaluation of risk reduction measures appear.

Based on the above comparisons – after further professional discussions and research – in my opinion, a sectoral operator safety and crisis planning framework can be established in the health sector based on uniform guidelines at the community level, which can help beyond local emergencies, in a pandemic similar to the coronavirus pandemic, or in the effective management of the consequences of a potentially raging and escalating conflict in our neighbourhood, and in cooperation between Member States.

## References

- Bundesamt für Bevölkerungsschutz und Katastrophenhilfe (BBK) (2020): *Handbuch Krankenhausalarm- und -einsatzplanung* (KAEP). Online: [www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/Gesundheit/KAEP/handbuch-kaep.pdf?\\_\\_blob=publicationFile&v=15](http://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/Gesundheit/KAEP/handbuch-kaep.pdf?__blob=publicationFile&v=15)
- Bundesministerium des Innern (2011): *Schutz Kritischer Infrastrukturen – Risiko- und Krisenmanagement*. Online: [www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/KRITIS/bmi-schutz-kritis-risiko-und-krisenmanagement.pdf?\\_\\_blob=publicationFile&v=12](http://www.bbk.bund.de/SharedDocs/Downloads/DE/Mediathek/Publikationen/KRITIS/bmi-schutz-kritis-risiko-und-krisenmanagement.pdf?__blob=publicationFile&v=12)
- Bundesministerium des Innern und für Heimat (2023): *Entwurf eines Gesetzes zur Umsetzung der CER-Richtlinie und zur Stärkung der Resilienz kritischer Anlagen*. 28 June, 2023. Online: [www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/KRITIS-DachG.html](http://www.bmi.bund.de/SharedDocs/gesetzgebungsverfahren/DE/KRITIS-DachG.html)
- CIMER, Zsolt et al. (2021): Application of Chemical Monitoring and Public Alarm Systems to Reduce Public Vulnerability to Major Accidents Involving Dangerous Substances. *Symmetry*, 13(8), 1528. Online: <https://doi.org/10.3390/sym13081528>
- Deutschen Krankenhausgesellschaft (2017): *Krankenhäuser als kritische Infrastrukturen –Umsetzungshinweise der Deutschen Krankenhausgesellschaft*. Online: [www.dkgev.de](http://www.dkgev.de)

de/fileadmin/default/Mediapool/2\_Themen/2.1\_Digitalisierung\_Daten/2.1.4.\_IT-Sicherheit\_und\_technischer\_Datenschutz/2.1.4.1.\_IT-Sicherheit\_im\_Krankenhaus/2017\_12\_19\_483\_ITSiG\_Kritis\_Umsetzungshinweise\_BSiG\_v0.9.pdf

ÉRCES, Gergő et al. (2023): Fire Safety in Smart Cities in Hungary With Regard to Urban Planning. *IDRiM Journal*, 13(2), 104–128. Online: <https://doi.org/10.5595/001c.91474>

KÁTAI-URBÁN, Lajos – MÉSZÁROS, István – VASS, Gyula (2019): Iparbiztonság, válsághelyzeti tervezés. In MAJOR, László (ed.): *A katasztrófa-készenlét, a reagálás és a beavatkozásbiztonság egészségügyi alapjai*. Budapest: Semmelweis, 48–83.

MÉSZÁROS, István (2023). The Evolution of the Normative Regulation in Hospital Safety and Security. *Hadmérnök*, 18(1), 43–57. Online: <https://doi.org/10.32567/hm.2023.1.4>

### Legal sources

Act CLIV of 1997 on healthcare

Act CLXVI of 2012 on the identification, designation and protection of essential systems and facilities

Act L of 2013 on the electronic information security of state and local government bodies

Act on the Federal Office for Information Security – BSiG

Commission of the European Communities (2005): *Green Paper on the European Program for the Protection of European Critical Infrastructures*. COM (2005) 576 final

Decree for determining critical infrastructures according to the BSI-Act – BSI-KritisV  
European Council Directive 2008/114/EC (December 8, 2008) on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection

European Parliament and Council Directive 2022/2557 on the resilience of critical organisations and the repeal of Council Directive 2008/114/EC (CER Directive)

Government Decree 65/2013 (8.III.) on the implementation of the Act CLXVI of 2012 on the identification, designation and protection of essential systems and facilities

Government Decree 521/2013 (30.XII.) on health crisis care

Government Decree 246/2015 (8.IX.) on the identification, designation and protection of essential healthcare systems and facilities

Decree 43/2014. (19.VIII.) of the Ministry of Human Resources on the content requirements of the health crisis plans of health institutions and on the amendment of certain ministerial decrees on health matters