

Special tasks for professional disaster management bodies related to the identification, designation and protection of critical infrastructures in Hungary

BONNYAI Tünde¹

One of the most particular priorities is to make available and operate systems and services, which guarantee the continuity of everyday life in the 21st Century. In order to ensure the efficiency of protection it is necessary to give effect to several physical, human and IT measures, which have integrated a complex framework through the legislation of critical infrastructure.

After the legal harmonization in the European Union, Hungary has begun to create its own system for critical infrastructure protection, within the first concrete step was when the Act 165th of 2012 on the identification, designation and protection of critical infrastructures and its Government Decree on the implementation came into effect. This study aims to summarize the main steps of the public proceedings related to identifying and designating critical infrastructures. In connection with the legislation I will present the function and prime assignments of the professional body for disaster management.

Keywords: *critical infrastructure protection, legislation in Hungary, sector authorities, disaster management.*

Introduction

Critical infrastructure protection is not a newly defined term, because it was always especially important to protect values and institutions which are essential to life and to maintaining an active economy. A new kind of approach was born in the first years of the 21st Century. After the terrorist attacks in 2001, 2004 and 2005 European societies were frightened of terrorism and searched for complex and common answers to the events. From 2004 there has been a comprehensive approach on critical infrastructure protection, with wide legislation on the level of the European Union by the 2008/114/EC Directive (called European Programme for Critical Infrastructure Protection — EPCIP) and many of the conclusions by the European Council, European Parliament and European Committee. Based on this Directive Hungary began to prepare for the implementation of the new obligations in 2008.

In 2012 — parallel with the review of EPCIP in the whole European Union — we built a framework for critical infrastructure protection with ten sectors and 42 subsectors, which has made it possible to assign the process of identification and designation related to critical infrastructure in details. [2] [3] The first results are the four Government Decrees — they came into effect on the 1st January 2014 — which create concrete legislation for designation in the sector of agriculture and food, energy, water, as well as public safety and security. [5–8]

¹ bonnyai.tunde@gmail.com

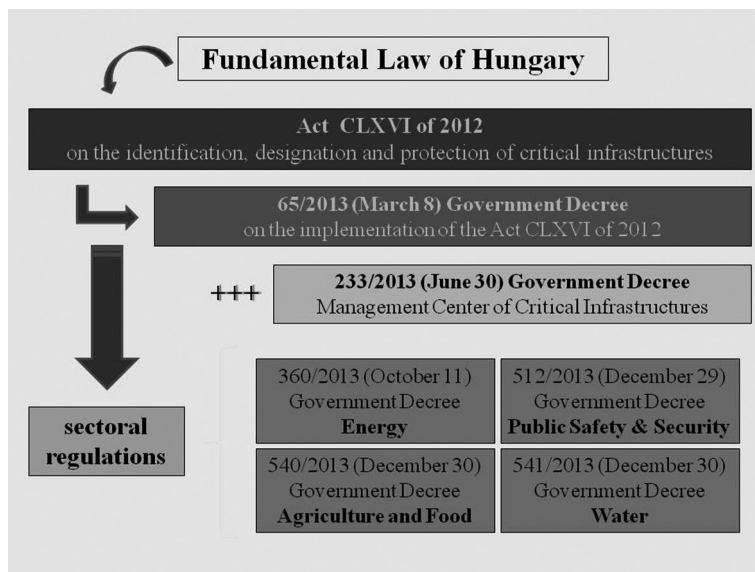


Figure 1: Legislative background of critical infrastructure protection in Hungary.²

The substance of the identification is to present the risk analysis of the examined infrastructure element. This is an obligation for every operator, according to which they must compile a so-called *identification report*,³ taking into consideration sectorial criteria. In this document will be the justified and defined designation proposal, as well as the beginning and finishing date of the examination. The deadline to render the first identification reports is the 180th day after the sector Government Decree came into force. If an operator does not meet the obligation above, but the authority stated by the law looks reasonable and makes the report, then the authority obligates the operator to make the necessary document. Submission must be accomplished to *sector-designating authority* which is defined in the related Government Decree, and which will launch public proceedings to examine the possible designation of the infrastructure.

The main aim of public proceedings is to examine sector and cross-cutting criteria, including horizontal criteria as well. During the 90 days long designation process the *sector-proposing authority* has 30 days to look over the identification report and to send its recommendations and professional opinion to the sector-designating authority. Based on the identification report and in the interest of examining the fruition of horizontal criteria, professional disaster management bodies must be involved as *consulting authority*. It has 15 days to adopt an authority statement about the fulfilling of horizontal criteria. The final *decision* taken by the sector-designating authority in the proceedings may be directed:

- designation and registration of the critical infrastructure element; or
- repeal designation and erasure of the former critical infrastructure from register; or
- rejection of the proposal for designation or cancellation; or

² Made by the author, based on [1–8].

³ Such document, which presents the activity, physical and IT security and threats to the infrastructure at the time of the examination, can confirm or confute the conditions of designation as critical infrastructure.

- making a new identification report within 90 days, marked with mistakes and deficiencies; or
- approve that the operator has no identified potential critical infrastructure element. [3]

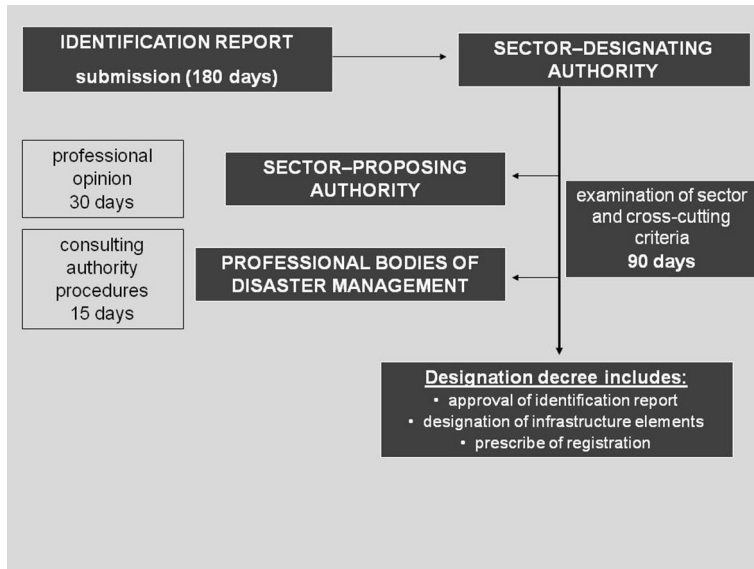


Figure 2: Identification and designation process of potential critical infrastructures.⁴

In case of designation sector–designating authorities are responsible for specifying the obligation for operators with a deadline, for making an *operational security plan (OSP)* and appointing a *security liaison officer (SLO)*. Both of them are stated in the EU Directive as obligatory elements in the system of critical infrastructure protection.

SLO — and conditions necessary for its activities — must be provided by the operator, unless such person is employed. The main task is ensuring communication and cooperation between the operator and authorities, in order to protect critical infrastructure elements. In Hungary we have special regulations for it, which are the following in general:

- certified no criminal record;
- relevant professional qualification (different by sector);
- other qualifications prescribed by government regulation (different by sector).

After 1st September 2014 qualification requirements will change. Besides the relevant professional competence it will be necessary to have some kind of special knowledge related to disaster management, like:

- higher education in law enforcement, defence management or industrial security management;
- specialization for fire protection, industrial security or civil protection;
- at least 5 years experiences in the field of industrial safety in professional disaster management bodies. [2] [3]

⁴ Made by the author, based on [2–3].

In connection with OSP the obligation must be fulfilled according to the deadline marked in the decision. It could not be less than 60 days after entry into force. There is the same exception rule as above, if the designated critical infrastructure has a security document which includes the required content elements of OSP, than it can substitute that. The mentioned content elements are defined in the 2nd Annex of the 65th Government Decree 2013 as follows:

- an exact description of critical infrastructure elements;
- organizational tool system that ensures their protection;
- provisional measures to be taken for the different risk and threat levels;
- existing or under development procedures for security solutions;
- potential extraordinary events or accidents.

The protection and continuity of the critical infrastructure element must be organized in accordance with OSP. Based on the above, OSP must be modified if activity changes and has affected protection system. [3]

Tasks of the Hungarian professional disaster management bodies [2] [3]

Duties and powers related to critical infrastructure protection are new activities in the disaster management system, which needs to create working and continuous relations with all bodies involved in the procedure. This kind of function affects all levels of the organisation; the coordination role has the central body (National Directorate General for Disaster Management — NDGDM) and the marked parts of public proceedings are carried out by directorates (county level) and offices (local level). Activities in detail will be presented according to this structure.

1) The role of the National Directorate General for Disaster Management

The subordination of the Ministry of Interior — as central authority — it carries out five categories of tasks related to critical infrastructure protection.

Registering authority, excluding European and national critical infrastructures of the defence system. Thereby all important data of operator and SLO, every OSP (as amended), as well as all decisions on critical infrastructures are available. Because of the obligation and right of Privacy NDGDM provides data for the involved bodies in the identification, designation (or withdrawal of designation) procedure:

- in order to ensure the operation of the procedure;
- to the coordination of supervisions and control;
- in order to accomplish on-site inspections; as well as
- to conduct official controls — upon written request — for authorities which has responsibilities under the law.

One year after the decision about the withdrawal of designation had become final, or after the decision about rejection of designation becomes final it must delete data from the registration and inform the operator in writing at the same time.

Supervisions and control coordinating body, excluding European and national critical infrastructures of the defence system. It prepares the annual audit plans of controls, which consist of suggestions from cooperate authorities. During the planning of supervisions — organized with more partner authorities — it pays particular attention for the critical infrastructure elements taking place every three years. After it NDGDM must draw up a summary report about the results of coordinated control. If during any kind of control it is found that

the operator fails to comply with its obligations, on the initiative of the participant authorities the sector–designating authority can:

- call the operator to fulfil the requirements;
- oblige to modify or make new OSP;
- impose a fine.

Management of emergency situations: NDGDM is entitled to request data from concerned authorities if any type of extraordinary event listed in the OSP has occurred. Giving response, organizing rescue, management, as well as informing public, assessing damage and reconstruction take place with the coordination of NDGDM. Involvement of necessary forces and tools to the efficient and successful intervention occurs on the proposal of the sector–designating authority. It is important that in treatment of events taking place, mainly forces of disaster management bodies (fire–fighter staff), and the local–level management of the situation is ensured by the professional disaster management system. There is a suitable example from Hungary March 2013, when widespread extreme weather conditions caused traffic jams on highways, prolonged blackouts and damage in buildings as well. It was necessary to handle the situation in many places, and after the weather improved to resolve the consequences of the multi–day–long power outages in Eastern Hungary.

Proposing authority: with regard to high priorities of public policy, public safety, public protection, constitutional protection, national security and counterterrorism. NDGDM has the obligation to pay special attention during public proceeding for the operating environment and specificities of potential critical infrastructure elements. If the injury, loss or destruction of the examined element can:

- have impact on the maintenance of public safety;
- influence the protection of public and property, or the functioning of the national economy;
- offend interest and principles regarding constitutional protection, national security or counterterrorism.
- NDGDM must suggest the designation of the element as national critical infrastructure toward the sector–designating authority.

Coordination of cyber security measures: contributes to maintain cyber security, analyses and evaluates events related to cyber security. It is an essential government expectation to handle challenges arising from cyber space efficiently, therefore the highest possible level of information security must be guaranteed. NDGDM operates the so–called IT Security Management Centre of Critical Infrastructure Protection (CIP), which is under accreditation, and it will soon the Hungarian CIP Computer Emergency Response Team (CERT). The main aim of the Centre is to protect services provided by national critical infrastructures from attacks arising from the internet and to ensure the coordination of preventing and eliminating interventions from global cyberspace.

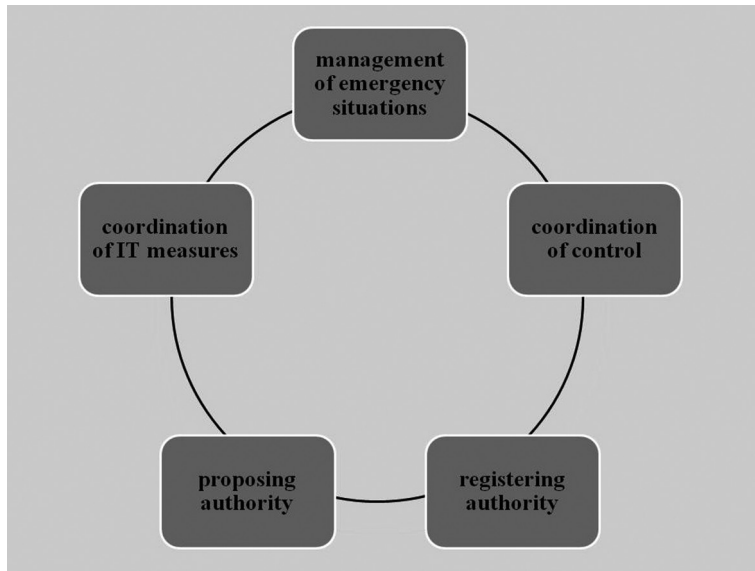


Figure 3: Integrated tasks of NDGDM.⁵

2) The role of county disaster management directorates and offices

As mentioned above, the vast majority of tasks in public proceedings are carried out by the county and local level, because the first-instance authorities are the offices, and the second-instance authorities are the directorates in the field of sectorial designation procedures, except public safety and security sector, where disaster management bodies (county level) are the first-instance.

Consulting authority: in the processes disaster management is responsible for examining horizontal criteria, and it needs to involve further bodies to compose opinions about them.

This kind of proceedings aims to adopt an authority statement — after examining scope and competence —, which is justified in detail if any horizontal criteria⁶ are met. It has an important role in the process having regard to the fact that it is enough to meet one sectoral and one horizontal criterion to designate a potential critical infrastructure element. It is an integral part of the procedure to involve the competent government office in order to examine political effect's criterion, as well as the assigned national organization for environmental protection and nature conservation management due to environmental effects criterion.

Sector-designating authority: disaster management directorates — in the field of public safety and security sector — are responsible for designating critical infrastructures of Constitution Protection Office, Hungarian Prison Service Headquarter and its bodies, National Security Special Service, National Protective Service, National Police and its bodies, Counter Terrorism Centre. In this case the request of consulting authority does not take place.

⁵ Made by the author, based on [2–3].

⁶ It is determined in the 2nd Annex of the 65th Government Decree 2013 — based on EU model: casualties criterion, economic effects criterion, public effects criterion, political effects criterion, environmental effects criterion

An important segment of the process is the obligation to make an identification report by disaster management bodies as well, taking into consideration that disaster management system elements can also be critical infrastructure in the sector of public safety and security. The sector-designating authority is the appropriate level of the national police.

Summary

Critical infrastructure protection is an extremely diverse activity, thus duties and powers delegated to disaster management bodies have particular importance. In order to ensure the legal and professional implementation it is essential to devote appropriate emphasis to training and further education, as well as follow-up headlines. Nowadays disaster management practise complex preventive activities, which has expanded by the scope of critical infrastructure protection, with public proceedings, consulting tasks, self-identification and managing emergencies. It is highly important that this kind of task can be realized in such an environment, which meets the requirements of the European Union, and national — otherwise more stringent — legislative as well.

Critical infrastructure protection is a new challenge for the EU, for Hungary and for the national disaster management system also. It is a newborn specialty with little experience. The significance of the identifying and designating procedures cannot be questioned, as they are about essential services ensuring fluency of everyday life. Taking into consideration that it is an on-going process to create legislation for the further sectors (transport, health care, finance, industry, IT, government), the expanding legislative environment will play a key role in the future. Meanwhile the deadlines of presenting the first identification reports are expiring, the number of designated critical infrastructures will rise gradually, which results in an increasing dynamism of public proceedings as well.

References

- [1] *Fundamental Law of Hungary.*
- [2] *Act CLXVI of 2012 on the identification, designation and protection of critical infrastructures.*
- [3] *65/2013 (March 8) Government Decree on the implementation of the Act CLXVI of 2012.*
- [4] *233/2013 (June 30) Government Decree on duties and function of e-government information systems management centre, sectorial event management centres, and management centre of events related to critical infrastructures .*
- [5] *360/2013 (October 11) Government Decree on identification, designation and protection of critical infrastructures in energy sector.*
- [6] *512/2013 (December 29) Government Decree on identification, designation and protection of certain critical infrastructures in public safety and security sector.*
- [7] *540/2013 (December 30) Government Decree on identification, designation and protection of critical infrastructures in agriculture and food sector.*
- [8] *541/2013 (December 30) Government Decree on identification, designation and protection of critical infrastructures in water sector.*

