DOI: https://doi.org/10.55843/ivisum2116009p

THE LEGAL FRAMEWORK OF THE EUROPEAN UNION TOWARDS CRITICAL INFRASTRUCTURE

Vesna Poposka, Hasan Oktay , page 9-19

ABSTRACT

Critical infrastructure protection is crucial to enrich and develop the four main freedoms of movement that settle the single European market. Besides, due to the recent developments related to the pandemic and energy crisis, the critical infrastructure development and protection gets different dimension. The EU has followed a sectoral approach in this area, with activities scattered across spheres of action led by a variety of institutional actors. In principle, this provides an adapted approach to different integrity needs and different legal competencies within the policy spectrum, but as will be discussed later in this paper , this also has important implications for a coherent and holistic European response. Although there are several sectoral legal bases for the protection of critical infrastructure at EU level (for example, in the transport and energy sectors), the founding agreements do not directly address critical infrastructure protection issues directly. Although the milestones of the protection of critical infrastructure were settled more than a decade ago, the basic framework has not changed much a cornerstone of action that generates and allocates funding through different programs and projects. The paper aims to provide overall framework and general vision over the framework of activities in the area that is pretty diverse.

Key words: critical infrastructure, acquis communautaire, harmonization, subsidiarity, funding

Ass. Prof. Vesna Poposka, PhD

İnternational Vision University, Gostivar-North Macedonia

e-mail: vesna.poposka @vizyon.edu.mk

Assoc. Prof. Hasan Oktay, PhD

İnternational Vision University, Gostivar-North Macedonia

e-mail: hasan.oktay @vizyon.edu.mk

UDK:
351.86:341.24(4-672ЕУ)
351.78:341.24(4-672ЕУ)

Date of received:
January 03, 2021

Date of acceptance:
February 12, 2021

Declaration of interest:
The authors reported no conflict of interest related to this article.

INTRODUCTION

As the European society becomes more interconnected and advanced, its dependence on critical infrastructure is inevitably delicate. Despite its increasing importance, many European businesses and citizens still seem to underestimate the risks to which critical infrastructures are exposed.
The indicative list of EU sectors of critical infrastructure includes 11 sectors :

1. Energy (Oil and gas production, refining, treatment and storage, including pipelines, Electricity generation, Transmission of electricity, gas and oil, Distribution of electricity, gas and oil)
2. Information, Communication Technologies, ICT (Information system and network protection, Instrumentation automation and control systems, Internet, Provision of fixed telecommunications, Provision of mobile telecommunications, Radio communication and navigation, Satellite communication, Broadcasting)
3. Water (Provision of drinking water, Control of water quality, Stemming and control of water quantity)
4. Food (Provision of food and safeguarding food safety and security)
5. Health (Medical and hospital care, Medicines, serums, vaccines and pharmaceuticals, Bio-laboratories and bio-agents)
6. Financial (Payment services/payment structures (private) Government financial assignment)
7. Public & Legal Order and Safety (Maintaining public & legal order, safety and security, Administration of justice and detention)
8. Civil administration (Government functions, Armed forces, Civil administration services, Emergency services, Postal and courier services)
9. Transport (Road transport, Rail transport, Air traffic, Inland waterways transport, Ocean and short-sea shipping)
10. Chemical and nuclear industry (Production and storage/processing of chemical and nuclear substances, Pipelines of dangerous goods /chemical substances)
11. Space and Research(A Review of Critical Infrastructure Domains in Europe - SPEAR Project, 2021)

The European Critical Infrastructure Protection Program (EPCIP) sets out the overall framework for activities aimed at improving the protection of

critical infrastructure in Europe - across all EU countries and in all relevant sectors of economic activity (Critical infrastructure protection - EU Science Hub - European Commission, 2021). The threats that the program aims to address are not limited to terrorism, but also include criminal activity, natural disasters, and other causes of accidents. A key pillar of this program is the 2008 European Critical Infrastructure Directive (COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection). Historically, the initiative began after the London and Madrid bombings, after which the Council called for a comprehensive strategy to protect critical infrastructure. The European Commission has adopted the Communication on the Protection of Critical Infrastructure in the Fight against Terrorism, which proposes initiatives that will improve European prevention, preparedness and response to terrorist attacks involving critical infrastructure. The Council Conclusions on "Prevention, Preparedness and Response to Terrorist Attacks" and the "EU Solidarity Program on the Consequences of Terrorist Threats and Attacks", adopted by the Council in December 2004, supported the Commission's intention to propose a European program to protect Critical Infrastructure (EPCIP) and the establishment of the Critical Infrastructure Warning Information Network (CIWIN). Following this call, several initiatives have been launched at EU level to contribute to a more integrated critical infrastructure protection policy.

KEY DOCUMENTS

The European Critical Infrastructure Protection Program focuses on four main pillars (European critical infrastructure Revision of Directive 2008/114/EC):

- creating a procedure for identifying and assessing Europe's critical infrastructure and learning how to better protect it. This procedure is established for the energy and transport sectors in the Directive on the identification and designation of European critical infrastructure
- measures to assist in the protection of infrastructure, including EU-designated expert groups and the establishment of the Critical Infrastructure Warning Information Network (CIWIN) - an Internet-based communication system for the exchange of information, studies and best practices.

- financing of over 100 projects for critical infrastructure protection from 2007 onwards. These projects focused on a variety of issues, including national and European information exchange and alert systems, the development of ways to assess the interdependence between electronic and electricity transmission networks, and the creation of a "good practice" handbook for policy makers.

- international cooperation with the countries of the European Economic Area (EEA) and the countries of the European Free Trade Area (EFTA), as well as expert meetings between the EU, the United States and Canada.

The measures taken through this proposal cannot be achieved by any EU member state alone, and must therefore be considered at EU level. Although each Member State is responsible for protecting critical infrastructure in its jurisdiction, no Member State can provide pan-European data exchange and sufficient protection in the area on its own. Therefore, a joint initiative and a consultation period were taken. Then followed the preparation of the so-called "Green Paper on the European Critical Infrastructure Protection Program " (Commission, 2005).

The Green Paper was adopted on November 17, 2005 (GREEN PAPER ON A EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION). Numerous informal meetings were held with representatives of private businesses as well as industry associations. Although a "policy document", it is the Green Paper of the European Critical Infrastructure Protection Program, providing an indicative list for identifying critical infrastructure by sectors, as well as a proposed list of framework definitions of key terms.

The EU has followed a sectoral approach in this area, with activities scattered across spheres of action led by a variety of institutional actors. In principle, this provides an adapted approach to different integrity needs and different legal competencies within the policy spectrum, but as will be discussed later, this also has important implications for a coherent and holistic European response.

The key document is council directive 2008/114/EC (COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection) that settles common methodology for

designation of national critical infrastructure and criteria for establishing European critical infrastructure.

All Member States have implemented the Directive by establishing a process for identifying and designating critical European infrastructure in the energy and transport sectors. In the Directive itself, critical infrastructure is defined as: "an asset, system or part thereof located in the Member States which is essential for the maintenance of the vital social functions, health, safety, economic or social well-being of the people and whose disruption or destruction would "had a significant impact in a Member State as a result of the failure to maintain those functions."

The Directive specifically recognizes the "European Critical Infrastructure" (ECI) as critical infrastructure whose disruption or destruction would have transboundary effects in the Member States, and which should be referred to as such in a joint procedure. The evaluation of security needs in such a case should be performed with the least common approach, through bilateral cooperation schemes. Information regarding such critical infrastructure should be (safely) classified in accordance with the requirements of common and national legislation.

As different sectors have specific experience, expertise and requirements in relation to the protection of critical infrastructure, the Community approach to critical infrastructure should be developed and implemented taking into account sectoral specifics and existing measures, including those already in place at Community level, national or regional level, and where relevant mutual assistance agreements between owners / operators of critical infrastructure are already in force. Given the significant involvement of the private sector in monitoring and risk management, business continuity planning and disaster recovery, community access should encourage full private sector involvement. In accordance with the Directive, the primary and ultimate responsibility for the protection of ECI falls on the Member States and the owners / operators of such infrastructures. Operator Security Plan – OSP or equivalent measures covering the identification of significant assets, risks, assessment and identification, selection and prioritization of countermeasures and procedures should be in force in all designated ECIs. In order to avoid unnecessary work and duplication, each Member State should first assess

whether the owners / operators of the designated ECIs have relevant operational security plans or similar measures. Where such plans do not exist, each Member State should take the necessary steps to ensure that appropriate measures are taken. Each Member State shall decide on the most appropriate form of action to be taken in connection with this activity. The directive also provides for a special procedure for the determination and identification of critical infrastructure. Article 3 of the Directive lays down the conditions to be taken into account.

In accordance with the procedure set out in Annex III, each Member State shall identify potential ECUs (European Critical Infrastructures) that meet the cross-sectoral and sectoral criteria and meet the definitions set out in Article 2 (a) and (b). The Commission can assist Member States at their request to identify potential ECIs.

The Commission may draw the attention of the Member States concerned to the existence of potential critical infrastructures which may be considered to meet the requirements for designation as ECI. Each Member State and the Commission shall continue the process of identifying potential ECIs.

The cross-sectoral criteria contain the following elements:
(a) criterion for casualties (estimated in relation to the potential number of casualties or injuries);
(b) an economic impact criterion (assessed in relation to the significance of the economic loss and / or degradation of products or services, including potential effects on the environment);
(c) public effects criterion (assessed in relation to the impact on public confidence, physical suffering and disruption of daily life, including the loss of basic services).

The threshold for cross-sectoral criteria will be based on the severity of the impact of the disruption or destruction of a particular infrastructure. The precise thresholds applied to the cross-sectoral criteria are determined on a case-by-case basis by the Member States affected by a particular critical infrastructure. Each Member State shall report annually to the Commission on the number of infrastructures by sector discussed in relation to the thresholds for cross-sectoral criteria.
While helping to strengthen European cooperation in the area of critical infrastructure, the Directive mainly encourages bilateral engagement by member states rather than producing a genuine European forum for

cooperation. On the other hand, the majority position of the community is that the general awareness of the protection of critical infrastructure and the level of cooperation in the EU has increased through various activities and forums organized under the Directive, especially in the energy and transport sectors.

Although the Directive is generally welcomed, some actors have criticized it for being counterproductive to the EU's overall efforts. In general, and due to the fact that some critical infrastructures are related to defense, the EU work in this area will have to find a way to overcome the reluctance of member states to provide information, especially if here Member States refrain from exchanging sensitive information due to suspicions. for the obligations of others. Lack of trust is an important notion as the Directive gives national governments a great deal of freedom to evade their responsibilities by simply creating a minimal list of designated critical infrastructures or failing to enforce rules for private operators (Argomaniz, 2013).

RIGHT TO ACT

Although there are several sectoral legal bases for the protection of critical infrastructure at EU level (for example, in the transport and energy sectors), the founding agreements do not directly address critical infrastructure protection issues directly. Initial initiatives in the area can be made under the Treaty on European Community (Treaty establishing the European Community) from 2002 which in Article 2 identifies a number of objectives, the achievement of which can be facilitated by strengthening the protection of critical infrastructure in Europe:

• to promote harmonious, balanced and sustainable development of economic activities;
• to promote a high degree of competitiveness;
• to promote a high degree of protection and improvement of the quality of the environment;
• to promote raising the standard of living and quality of life;
• to promote solidarity among member states.

The Lisabon Treaty (TREATY OF LISBON, 2007) has largely introduced the solidarity clause in Article 222, which calls on member states to act together and to assist one another in the event of a terrorist attack or a natural or man-made disaster. In addition, Lisbon introduced

the formula for additional EU competence in Article 196 to foster cooperation between Member States in order to improve the effectiveness of protection and rescue systems against natural or man-made disasters (Even before the Lisbon Treaty entered into force in 2001, the Commission began coordination to establish the Civil Protection Mechanism and assistance provided by Member States to another Member State which has suffered a disaster (Boin, Rhinard and Ekengren, 2014). The Emergency Coordination Center (ERCC) was set up within the European Directorate for Humanitarian Aid and Civil Protection to facilitate coordination and respond more quickly to disasters both inside and outside the EU.

In addition, the competence for the internal market referred to in Article 114 of the TFEU enables the adoption of sectoral measures for security and protection. Importantly, this did not prevent, or perhaps better yet, prompted the Commission to set up various informal networks and centers within the Directorate-General, including networks of national contact and early warning points. The Commission has further developed a knowledge-building approach on how to better protect critical infrastructure by seeking a common approach to basic scientific methodologies and assessments of seemingly less political issues.

To reach this goal, it funds various projects to provide expert knowledge and a deeper understanding of protection at all levels. Examples of this are risk assessment studies and management methodologies. Furthermore, Article 308 of the Treaty provides that if, during the functioning of the common market, Community action is necessary to achieve one of the objectives of the Community and the agreement does not provide the necessary powers, the Council shall act unanimously on a proposal from the Commission and after consultation. with the European Parliament, will take appropriate measures.

The EU's right to act has been recognized by the Council, which in this case has asked the Commission to develop a program to improve the protection of critical infrastructure in the EU. The legal analysis in the context proved that the principles of subsidiarity and proportionality are satisfied.

CONCLUSION

Despite the fact that there are differing opinions on the effective improvement of security, the Directive is a striking example of how the existence of a legal instrument has encouraged policies to protect national critical infrastructure. This has resulted in concrete actions, such as the creation of specific national policy bodies. In the energy sector, there is progress in risk management and protection measures in cooperation with operators

Given the fact that in recent years the security environment of the European Union has changed dramatically, the Union is also trying to provide more coherent responses to security threats, which directly or indirectly include the protection of critical infrastructure. Key challenges to peace and stability in the EU's eastern and southern neighborhoods continue to underscore the need for the Union to adapt and increase its capacity, with a strong focus on the close link between external and internal security. Many of the current challenges to peace, security and prosperity stem from instability in the EU's immediate neighborhood and changing forms of threats.

Within the EU, member states have defined their critical infrastructure differently according to their own needs, so that, for example, some countries do not have an official list at all, some are indicative and some are tactical. With regard to the central authority, the practice is also very fragmented. European critical infrastructure does not enjoy special protection and no central coordinating body for monitoring activities or implementation monitoring mechanism and therefore relevant data is difficult to obtain even for academic purposes.

The European Union has recognized the need to integrate critical infrastructure protection into overall risk management. Risk management in the protection of critical infrastructure has a number of specifics. Risk assessment should be recognized as one of the elements of regulatory decisions in addition to "other legitimate factors" such as social, ethical and political issues at national and EU level. How risks are assessed is not just a technical matter that it can be left to the institutions, but it is a political issue whereas risk management can be fueled by risk assessment and expert advice, but political responsibility cannot be hidden or delegated to scientific experts (van Asselt, Vos and Wildhaber, 2015).

In addition, there is a wide range of horizontal activities aimed at enhancing security and directly related to the protection of critical infrastructure. However, some experts are of the opinion that horizontal activities lack consistency. Horizontally consistent policy response means that it will ensure that its various components follow the common goals set out in the joint programming documents.

Hence, as the resistance of national governments to moving processes rapidly in some areas is unlikely to soften in the near future, a potential aspect for EU institutions to increase their contribution may be to work on better coordination of institutional actors in critical infrastructure protection, transport, critical information infrastructure protection and security as research fields.

BILBIOGRAPHY

1. Argomaniz, J., 2013. The European Union Policies on the Protection of Infrastructure from Terrorist Attacks: A Critical Assessment. Intelligence and National Security, 30(2-3), pp.259-280.
2. Boin, A., Rhinard, M. and Ekengren, M., 2014. Managing Transboundary Crises: The Emergence of European Union Capacity. Journal of Contingencies and Crisis Management, p.n/a-n/a.
3. Comission of the Europen Communities, 2005, Green Paper on a European programme for critical infrastructure protection /* COM/2005/0576 final */
4. COUNCIL DIRECTIVE 2008/114/EC of 8 December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.
5. EU Science Hub - European Commission. 2021. Critical infrastructure protection - EU Science Hub - European Commission. [online] Available at: <https://ec.europa.eu/jrc/en/research-topic/critical-infrastructure-protection> [Accessed 14 October 2021].
6. European critical infrastructure Revision of Directive 2008/114/EC.
7. European Union, Treaty Establishing the European Community (Consolidated Version), Rome Treaty, 25 March 1957, available

at: https://www.refworld.org/docid/3ae6b39c0.html [accessed 16 October 2021]

8. European Union, Treaty of Lisbon Amending the Treaty on European Union and the Treaty Establishing the European Community, 13 December 2007, 2007/C 306/01, available at: https://www.refworld.org/docid/476258d32.html [accessed 18 October 2021]
9. Spear2020.eu. 2021. A Review of Critical Infrastructure Domains in Europe - SPEAR Project. [online] Available at: <https://www.spear2020.eu/News/Details?id=120> [Accessed 14 October 2021].
10. van Asselt, M., Vos, E. and Wildhaber, I., 2015. Some Reflections on EU Governance of Critical Infrastructure Risks. European Journal of Risk Regulation, 6(2), pp.185-190.