Mgr. Marián Magdolen, PhD. [1]

CRITICAL INFRASTRUCTURE PROTECTION IN EUROPEAN LEGISLATION

Abstract: Critical infrastructure is an asset or system, which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may have a significant negative impact for the security of the EU and the well being of its citizens. Reducing the vulnerabilities of critical infrastructure and increasing their resilience is one of the major objectives of the EU. European Union therefore adopted various legal documents to support and implement adequate critical infrastructure protection. The European Programme for Critical Infrastructure Protection (EPCIP) sets the overall framework for activities aimed at improving the protection of critical infrastructure in Europe - across all EU States and in all relevant sectors of economic activity. A key pillar of this programme is the 2008 Directive on European Critical Infrastructure. It establishes a procedure for identifying and designating European Critical Infrastructures (ECI) and a common approach for assessing the need to improve their protection. Through these legal documents fundamental approach to critical infrastructure protection is introduced and therefore they will be described in detail in this paper.

[1] Mgr. Marián Magdolen, PhD., University of Žilina, Faculty of Security Engineering, Univerzitná 8215/1, 010 26 Žilina, Slovakia, marian.magdolen@fbi.uniza.sk

1. INTRODUCTION

Critical infrastructure is an asset or system which is essential for the maintenance of vital societal functions. The damage to a critical infrastructure, its destruction or disruption by natural disasters, terrorism, criminal activity or malicious behaviour, may have a significant negative impact for the security of the EU and the well-being of its citizens. Reducing the vulnerabilities of critical infrastructure and increasing their resilience is one of the major objectives of the EU. In the EU legislation, **critical infrastructure** (or "**CI**") is defined as "an asset, system or part thereof located in Member States which is **essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people**, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions". Because of federative aspect of European Union and interconnected spaces of economics, production, trasportation and many other areas, special category of CI was introduced in Directive 114/2008/EC. **European critical infrastructure** (or "**ECI**") is defined as "critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on **at least two Member States**. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure".

Critical infrastructure can be damaged, destroyed or disrupted by deliberate acts of terrorism, natural disasters, negligence, accidents or computer hacking, criminal activity and malicious behaviour. To save the lives and property of people at risk in the EU from terrorism, natural disasters and accidents, any disruptions or manipulations of CI should, to the extent possible, be brief, infrequent, manageable, geographically isolated and minimally detrimental to the welfare of the Member States, their citizens and the European Union.

Reducing the vulnerabilities of critical infrastructure and increasing their resilience is one of the major objectives of the EU. An adequate level of protection must be ensured and the detrimental effects of disruptions on the society and citizens must be limited as far as possible.

2. EU LEGISLATION FRAMEWORK

Requirements of generally binding legal regulations, technical standards, insurance conditions and requirements of internal company regulations for critical infrastructure protection result in adoption several framework documents.

In 2004 the European Council asked for the preparation of an overall strategy to protect critical infrastructures. In response, the Commission adopted a Communication on critical infrastructure protection in the fight against terrorism which put forward

suggestions as to what would enhance European prevention of, preparedness for and response to terrorist attacks involving critical infrastructures.

In 2005 the Commission adopted a **Green Paper on a European programme for critical infrastructure protection** which provided policy options on the establishment of the programme and the Critical Infrastructure Warning Information Network. The responses received to the Green Paper emphasised the added value of a Community framework concerning critical infrastructure protection. The need to increase the critical infrastructure protection capability in Europe and to help reduce vulnerabilities concerning critical infrastructures was acknowledged. The main objective of the Green Paper is to receive feedback concerning possible EPCIP policy options by involving a broad number of stakeholders. The effective protection of critical infrastructure requires communication, coordination, and cooperation nationally and at EU level among all interested parties - the owners and operators of infrastructure, regulators, professional bodies and industry associations in cooperation with all levels of government, and the public.

Later in the same year the Commission introduced a proposal for a **European programme for critical infrastructure protection** ('EPCIP') and decided that it should be based on an all-hazards approach while countering threats from terrorism as a priority. Under this approach, man-made, technological threats and natural disasters should be taken into account in the critical infrastructure protection process, but the threat of terrorism should be given priority.

In 2007 the Council adopted conclusions on the EPCIP in which it reiterated that it was the ultimate responsibility of the Member States to manage arrangements for the protection of critical infrastructures within their national borders while welcoming the efforts of the Commission to develop a European procedure for the identification and designation of European critical infrastructures ('ECIs') and the assessment of the need to improve their protection. EPCIP sets an overall framework for activities aimed at improving the protection of critical infrastructure in Europe - across all EU States and in all relevant sectors of economic activity. The threats to which the programme aims to respond are not only confined to terrorism, but also include criminal activities, natural disasters and other causes of accidents. In short, it seeks to provide an all-hazards cross-sectoral approach.

In 2008 the European Commission adopted **Directive 114/2008/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.** Directive constitutes a first step in a step-by-step approach to identify and designate ECIs and assess the need to improve their protection. As such, this Directive concentrates on the energy and transport sectors and

should be reviewed with a view to assessing its impact and the need to include other sectors within its scope, inter alia, the information and communication technology ('ICT') sector. Directive is a key pillar of EPCIP programme. It establishes a procedure for identifying and designating European Critical Infrastructures and a common approach for assessing the need to improve their protection.

After adoption of framework documents there are frequent reviews of critical infrastructure protection approach in order to ensure the state of the art protection as well to be uptodate with recent developments and (hybrid) threats. Such reviews were performed in 2012 and 2018.

3. EUROPEAN PROGRAMME FOR CRITICAL INFRASTRUCTURE PROTECTION (EPCIP)

The general objective of EPCIP is to improve the protection of critical infrastructures in the EU. This objective will be achieved by the creation of an EU framework concerning the protection of critical infrastructures. While recognising the threat from terrorism as a priority, the protection of critical infrastructure will be based on an all-hazards approach. If the level of protective measures in a particular CI sector is found to be adequate, stakeholders should concentrate their efforts on threats to which they are vulnerable.

Main principles of EPCIP stands on:

Subsidiarity – efforts in the CIP field will focus on infrastructure that is critical from a European, rather than a national or regional perspective.

Complementarity - the Commission will avoid duplicating existing efforts, whether at EU, national or regional level, where these have proven to be effective in protecting critical infrastructure. EPCIP will therefore complement and build on existing sectorial measures.

Confidentiality - Both at EU level and MS level, Critical Infrastructure Protection Information will be classified appropriately and access granted only on a need-to- know basis.

Stakeholder Cooperation – All relevant stakeholders will, be involved in the development and implementation of EPCIP. This will include the owners/operators of critical infrastructures designated as ECI as well as public authorities and other relevant bodies.

Proportionality – measures will only be proposed where a need has been identified following an analysis of existing security gaps and will be proportionate to the level of risk and type of threat involved.

Sector-by-sector approach – Since various sectors possess particular experience, expertise and requirements with CIP, EPCIP will be developed on a sector-by-sector basis.

EPCIP generaly provides framework where Directive 114/2008/EC is complemented by additional measures designed to facilitate the implementation of EPCIP. The Directive focus on a procedure for the identification and designation of European Critical Infrastructures (ECI), and a common approach to the assessment of the needs to improve the protection of such infrastructures. Measures supporting the implementation of EPCIP include:

- CIWIN – Critical Infrastructure Warning Information Network
- ERN-CIP – European Reference Network for Critical Infrastructure Protection
- CIP expert groups
- CIP information sharing
- Identification and analysis of interdependencies

3.1. The CIP Contact Group

An EU level mechanism is required in order to serve as the strategic coordination and cooperation platform capable of taking forward work on the general aspects of EPCIP and sector specific actions.

The CIP Contact Group bring together the CIP Contact Points from each Member State and is chaired by the Commission. Each Member State should appoint a CIP Contact Point who would coordinate CIP issues within the Member State and with other Member States, the Council and the Commission.

3.2. Critical Infrastructure Warning Information Network (CIWIN)

In CIWIN provides a platform for the exchange of best practices in a secure manner. CIWIN shall complement existing networks and could also provide an optional platform for the exchange of rapid alerts linked to the Commission's ARGUS system.

3.3. Expert Groups

Where specific expertise is needed the Commission may therefore setup CIP expert groups at EU level to address clearly defined issues and to facilitate public-private dialogue concerning critical infrastructure protection.

Expert groups will support EPCIP by facilitating exchanges of views on related CIP issues on an advisory basis. These expert groups constitute a voluntary mechanism in which public and private resources are blended to achieve a goal or set of goals judged to be of mutual benefit both to citizens and the private sector.

Specific functions of CIP expert groups may vary across CI sectors depending on the unique characteristics of each sector. These functions may include the following tasks:

- Assist in identifying vulnerabilities, interdependencies and sectorial best practices;
- Assist in the development of measures to reduce and/or eliminate significant vulnerabilities and the development of performance metrics;
- Facilitating CIP information-sharing, training and building trust;
- Develop and promote "business cases" to demonstrate to sector peers the value of participation in infrastructure protection plans and initiatives;
- Provide sector-specific expertise and advice on subjects such as research and development

3.4. CIP Information sharing process

The CIP information sharing process among relevant stakeholders requires a relationship of trust, such that the proprietary, sensitive or personal information that has been shared voluntarily will not be publicly disclosed and that that sensitive data is adequately protected. Care must be taken to respect privacy rights.

Stakeholders will take appropriate measures to protect information concerning such issues as the security of critical infrastructures and protected systems, interdependency studies and CIP related vulnerability, threat and risks assessments. Such information will not be used other than for the purpose of protecting critical infrastructure.

Any personnel handling classified information will have an appropriate level of security vetting by the Member State of which the person concerned is a national. CIP information exchange will recognize that certain CIP information, though unclassified, may still be sensitive and therefore needs to be treated with care.

CIP information exchange will facilitate the following:

- Improved and accurate information and understanding about interdependencies, threats, vulnerabilities, security incidents, countermeasures and best practices for the protection of CI;
- Increased awareness of CI issues;
- Stakeholder dialogue;
- Better-focused training, research and development.

specific expertise is needed the Commission may therefore setup CIP expert groups at EU level to address clearly defined issues and to facilitate public-private dialogue concerning critical infrastructure protection.

3.5. Identification of interdependencies

The identification and analysis of interdependencies, both geographic and sectorial in nature, will be an important element of improving critical infrastructure protection in the EU. This on-going process will feed into the assessment of vulnerabilities, threats and risks concerning critical infrastructures in the EU.

3.6. Accompanying Financial Measures

The Community programme "Prevention, Preparedness and Consequence Management of Terrorism and other Security Related Risks" for the period 2007-2013 contributed to the implementation of EPCIP.

Within the general objectives, and unless covered by other financial instruments, the programme will stimulate, promote and develop measures on prevention, preparedness and consequence management aimed at preventing or reducing all security risks, in particular risks linked with terrorism, where appropriate based on comprehensive threat and risk assessments.

Funding under the programme, by way of grants and Commission initiated actions, will be used in particular toward the development of instruments, strategies, methodologies, studies, assessments and activities/measures in the field of the effective protection of critical infrastructure (at both EU and MS levels).

With allocation of 140 million EUR this programm suported over 120 project including methodologies for risk analysis, analyses of depencencies and interdependencies, excersises and studies.

3.7. National Critical Infrastructures

With a view to improving the protection of National Critical Infrastructures each Member State is encouraged to establish a National CIP Programme. The objective of such programmes would be to set out each Member State's approach to the protection of National Critical Infrastructures located within its territory.

National CIP programmes would at a minimum address the following issues:

- The identification and designation by the Member State of National Critical Infrastructures according to predefined national criteria.
- The establishment of a dialogue with CIP owners/operators.
- Identification of geographic and sectoral interdependencies.
- Drawing-up NCI related contingency plans where deemed relevant.
- Each Member State is encouraged to base its National CIP Programme on the common list of CI sectors established for ECI.

National criteria shall taking into account as a minimum the following qualitative and quantitative effects of the disruption or destruction of a particular infrastructure:

- **Scope** - The disruption or destruction of a particular critical infrastructure will be rated by the extent of the geographic area which could be affected by its loss or unavailability.
- **Severity** - The consequences of the disruption or destruction of a particular infrastructure.

The consequences of the disruption or destruction of a particular infrastructure will be assessed on the basis of:

- Public effect (number of population affected);
- Economic effect (significance of economic loss and/or degradation of products or services);
- Environmental effect;
- Political effects;
- Psychological effects;
- Public health consequences

3.8. Contingency Planning

Contingency planning is a key element of the CIP process so as to minimize the potential effects of a disruption or destruction of a critical infrastructure.

The development of a coherent approach to the elaboration of contingency plans addressing such issues as the participation of owners/operators of critical infrastructure, cooperation with national authorities and information sharing among neighbouring countries should form an important element of the implementation of the European Programme for Critical Infrastructure Protection.

3.9. External Dimension

Terrorism, other criminal activities, natural hazards and other causes of accidents are not constrained by international borders. Threats cannot be seen in a purely national context. Consequently, the external dimension of Critical Infrastructure Protection needs to be fully taken in to account in the implementation of EPCIP. The interconnected and interdependent nature of today's economy and society means that even a disruption outside of the EU's borders may have a serious impact on the Community and its Member States. Equally true, the disruption or destruction of a critical infrastructure within the EU

may have a detrimental effect on the EU's partners. Finally, working toward the goal of increasing the protection of critical infrastructure within the EU will minimize the risk of the EU economy being disrupted and thereby contribute to the EU's global economic competitiveness.

Consequently, enhancing CIP cooperation beyond the EU through such measures as sector specific memoranda of understanding (e.g. on the development of common standards, undertaking joint CIP related studies, identification of common types of threats and exchanging best-practices on protection measures) and encouraging the raising of CIP standards outside of the EU should therefore be an important element of EPCIP. External cooperation on CIP will primarily focus on the EU's neighbours. Given however the global interconnectedness of certain sectors including ICT and financial markets, a more global approach would be warranted. Dialogue and the exchange of best practices should nevertheless involve all relevant EU partners and international organizations. The Commission will also continue promoting improvements in the protection of critical infrastructures in non-EU countries by working with G8, Euromed and European Neighbourhood Policy partners through existing structures and policies, including the "Instrument for Stability".

4. DIRECTIVE 114/2008/EC

The directive on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection constitutes a first step in a step-by-step approach to identify and designate ECIs and assess the need to improve their protection. As such, this Directive concentrates on the energy and transport sectors and should be reviewed with a view to assessing its impact and the need to include other sectors within its scope, inter alia, the information and communication technology (‘ICT’) sector.

Scope of directive focus (but is not limited to) on:

Energy sector, including:

- Electricity (Infrastructures and facilities for generation and transmission of electricity in respect of supply electricity)
- Oil (Oil production, refining, treatment, storage and transmission by pipelines)
- Gas (Gas production, refining, treatment, storage and transmission by pipelines, LNG terminals)

Transport sector, including:

- Road transport
- Rail transport
- Air transport
- Inland waterways transport
- Ocean and short-sea shipping and ports

Since various sectors have particular experience, expertise and requirements concerning critical infrastructure protection, a Community approach to critical infrastructure protection should be developed and implemented taking into account sector specificities and existing sector based measures including those already existing at Community, national or regional level, and where relevant cross-border mutual aid agreements between owners/operators of critical infrastructures already in place.

The primary and ultimate responsibility for protecting ECIs falls on the Member States and the owners/operators of such infrastructures. Owners/operators of ECIs should be given access primarily through relevant Member State authorities to best practices and methodologies concerning critical infrastructure protection.

Given the very significant private sector involvement in overseeing and managing risks, business continuity planning and post-disaster recovery, a Community approach needs to encourage full private sector involvement.

Operator security plans ('OSPs') or equivalent measures comprising an identification of important assets, a risk assessment and the identification, selection and prioritisation of counter measures and procedures should be in place in all designated ECIs. Where such plans do not exist, each Member State should take the necessary steps to make sure that appropriate measures are put in place.

Security Liaison Officers should be identified for all designated ECIs in order to facilitate cooperation and communication with relevant national critical infrastructure protection authorities. Where such a Security Liaison Officer does not exist, each Member State should take the necessary steps to make sure that appropriate measures are put in place. It is up to each Member State to decide on the most appropriate form of action with regard to the designation of Security Liaison Officers.

The efficient identification of risks, threats and vulnerabilities in the particular sectors requires communication both between owners/operators of ECIs and the Member

States, and between the Member States and the Commission. Each Member State should collect information concerning ECIs located within its territory.

The Commission should receive generic information from the Member States concerning risks, threats and vulnerabilities in sectors where ECIs were identified, including where relevant information on possible improvements in the ECIs and cross-sector dependencies.

Effective protection of ECIs requires communication, coordination, and cooperation at national and Community level. This is best achieved through the nomination of European critical infrastructure protection contact points ('ECIP contact points') in each Member State, who should coordinate European critical infrastructure protection issues internally, as well as with other Member States and the Commission.

In order to develop European critical infrastructure protection activities in areas which require a degree of confidentiality, it is appropriate to ensure a coherent and secure information exchange in the framework of this Directive. Classified information should be protected in accordance with relevant Community and Member State legislation. Each Member State and the Commission should respect the relevant security classification given by the originator of a document. The sharing of information requires a relationship of trust such that companies and organisations know that their sensitive and confidential data will be sufficiently protected.

4.1. Directive terminology

In order to avoid confusion in terms that are used in critical infrastructure protection directive established basic terminology.

'**critical infrastructure**' means an asset, system or part thereof located in Member States which is essential for the maintenance of vital societal functions, health, safety, security, economic or social well-being of people, and the disruption or destruction of which would have a significant impact in a Member State as a result of the failure to maintain those functions;

'**European critical infrastructure**' or 'ECI' means critical infrastructure located in Member States the disruption or destruction of which would have a significant impact on at least two Member States. The significance of the impact shall be assessed in terms of cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure;

'**risk analysis**' means consideration of relevant threat scenarios, in order to assess the vulnerability and the potential impact of disruption or destruction of critical infrastructure;

'**sensitive critical infrastructure protection related information**' means facts about a critical infrastructure, which if disclosed could be used to plan and act with a view to causing disruption or destruction of critical infrastructure installations;

'**protection**' means all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralise a threat, risk or vulnerability;

'**owners/operators of ECIs**' means those entities responsible for investments in, and/or day-to-day operation of, a particular asset, system or part thereof designated as an ECI under this Directive.

4.2. Identification of ECI

Member State shall identify potential ECIs which both satisfy the cross-cutting and sectoral criteria and meet the definitions set out in Directive.

The cross-cutting criteria shall comprise the following:

- **casualties criterion** (assessed in terms of the potential number of fatalities or injuries);
- **economic effects criterion** (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects);
- **public effects criterion** (assessed in terms of the impact on public confidence, physical suffering and disruption of daily life; including the loss of essential services).

The sectoral criteria shall take into account the characteristics of individual ECI sectors.

The cross-cutting criteria thresholds shall be based on the severity of the impact of the disruption or destruction of a particular infrastructure. The precise thresholds applicable to the cross-cutting criteria shall be determined on a case-by-case basis by the Member States concerned by a particular critical infrastructure. Each Member State shall inform the Commission on an annual basis of the number of infrastructures per sector for which discussions were held concerning the cross-cutting criteria thresholds.

Each Member State shall inform the other Member States which may be significantly affected by a potential ECI about its identity and the reasons for designating it as a potential ECI.

Each Member State on whose territory a potential ECI is located shall engage in bilateral and/or multilateral discussions with the other Member States which may be significantly affected by the potential ECI.

The Member State on whose territory a potential ECI is located shall designate it as an ECI following an agreement between that Member State and those Member States that may be significantly affected. The acceptance of the Member State on whose territory the infrastructure to be designated as an ECI is located, shall be required.

The Member State on whose territory a designated ECI is located shall inform the Commission on an annual basis of the number of designated ECIs per sector and of the number of Member States dependent on each designated ECI. Only those Member States that may be significantly affected by an ECI shall know its identity.

The Member States on whose territory an ECI is located shall inform the owner/operator of the infrastructure concerning its designation as an ECI. Information concerning the designation of an infrastructure as an ECI shall be classified at an appropriate level.

The process of identifying and designating ECIs shall be completed by 12 January 2011 and reviewed on a regular basis. At present appx. 100 European Critical Infrastructures is identified in total.

4.3. Operator security plans

The operator security plan (‘OSP’) procedure shall identify the critical infrastructure assets of the ECI and which security solutions exist or are being implemented for their protection. The minimum content to be addressed by an ECI OSP procedure is set out in Directive Annex II.

Each Member State shall assess whether each designated ECI located on its territory possesses an OSP or has in place equivalent measures addressing the issues. If a Member State finds that such an OSP or equivalent exists and is updated regularly, no further implementation action shall be necessary.

If a Member State finds that such an OSP or equivalent has not been prepared, it shall ensure by any measures deemed appropriate, that the OSP or equivalent is prepared addressing the issues. Each Member State shall ensure that the OSP or equivalent is in place and is reviewed regularly within one year following designation of the critical infrastructure as an ECI.

The ECI OSP procedure will cover at least:

- **identification of important assets**;

- **conducting a risk analysis** based on major threat scenarios, vulnerability of each asset, and potential impact; and
- identification, selection and prioritisation of **counter-measures and procedures**

Counter-measures and procedures shall be with a distinction between:

- **permanent security measures**, which identify indispensable security investments and means which are relevant to be employed at all times. This will include information concerning general measures such as technical measures (including installation of detection, access control, protection and prevention means); organisational measures (including procedures for alerts and crisis management); control and verification measures; communication; awareness raising and training; and security of information systems,
- **graduated security measures**, which can be activated according to varying risk and threat levels.

4.4. Security Liaison Officers

The Security Liaison Officer shall function as the point of contact for security related issues between the owner/operator of the ECI and the relevant Member State authority. Each Member State shall assess whether each designated ECI located on its territory possesses a Security Liaison Officer or equivalent.

If a Member State finds that a Security Liaison Officer or equivalent does not exist in relation to a designated ECI, it shall ensure by any measures deemed appropriate, that such a Security Liaison Officer or equivalent is designated.

Each Member State shall implement an appropriate communication mechanism between the relevant Member State authority and the Security Liaison Officer or equivalent with the objective of exchanging relevant information concerning identified risks and threats in relation to the ECI concerned.

This communication mechanism shall be without prejudice to national requirements concerning access to sensitive and classified information.

4.5. Reporting

Each Member State shall conduct a threat assessment in relation to ECI subsectors within one year following the designation of critical infrastructure on its territory as an ECI within those subsectors.

Each Member State shall report every two years to the Commission generic data on a summary basis on the types of risks, threats and vulnerabilities encountered per ECI sector in which an ECI has been designated and is located on its territory.

A common template for these reports may be developed by the Commission in cooperation with the Member States.

4.6. Commission support for ECIs

Common methodological guidelines for carrying out risk analyses in respect of ECIs may be developed by the Commission in cooperation with the Member States. The use of such guidelines shall be optional.

The Commission shall support, through the relevant Member State authority, the owners/operators of designated ECIs by providing access to available best practices and methodologies as well as support training and the exchange of information on new technical developments related to critical infrastructure protection.

4.7. ECI protection contact points

Each Member State shall appoint a European critical infrastructure protection contact point ('ECIP contact point').

ECIP contact points shall coordinate European critical infrastructure protection issues within the Member State, with other Member States and with the Commission. The appointment of an ECIP contact point does not preclude other authorities in a Member State from being involved in European critical infrastructure protection issues.

5. EPCIP REVIEW

EPCIP is reviewed in order to achieve the state of the art procedures and to reflect new threats and developments in critical infrastructure protection. Until today several reviews were performed by Commission.

In 2012 – initial review of EPCIP and Directive by Commission was performed, and based on this review in 2013 a new approach to the EPCIP was introduced. In 2018 started another review and this is scheduled to be published in first quarter of 2019.

In 2012 Review most important results were:

- EPCIP was implemented by all EU member states
- General CIP awerness has increased, particularly in the energy and transport sectors
- Less than 20 ECIs were designated

- The sector-focused approach of the Directive presents challenges
- Bilateral cooperation rather than a real European forum
- Identified need for a change from sectorial expansion towards systems and risk based approaches

Based on review new approach to critical infrastructure protection was introduced with the objective to provide a reshaped EU CIP approach, based on the practical implementation of activities.

Main features of new approach:

- Looking at interdependencies
- A step by step practical approach, based on 3 main pillars: Prevention, Preparedness, Response
- Pilot with four critical infrastructures of European dimension: Eurocontrol, Galileo, the electricity transmission grid and the gas transmission network.

6. QUESTIONS (QUIZZ)

Name:

1) European Critical Infrastructure element shall have significant impact on at least:
(a) one member state
(b) two member states
(c) three member states

2) Protection of critical infrastructure in European Union is based on:
(a) national legislation of separate member states
(b) European Programme for Critical Infrastructure Protection
(c) multilateral treaties among member states

3) The Directive 114/2008 on European Critical Infrastructures is focusing on:
(a) energy and agriculture sectors
(b) transport and mining sectors
(c) energy and transport sectors

4) Does European Union financially support critical infrastructure protection ?
(a) No. Member states are responsible for finances the protection measures.
(b) Indirectly. European Union supports projects related to European program of critical infrastructure protection in separate program.
(c) Yes. European Union pays all expenses related to critical infrastructure protection.

5) Each Member state shall identify European Critical Infrastructure based on:
(a) expert assessment
(b) cross-cutting and sectorial criteria
(c) national methodology

6) Each identified European critical infrastructure shall prepare:
(a) public description of risk and threats to the infrastructure
(b) map of affected area in case of emergency
(c) operator security plans

7. REFERENCES

[1] Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection
[2] Green Paper on a european programme for critical infrastructure protection, COM(2005) 576 final
[3] Communication from the Commission on a European Programme for Critical Infrastructure Protection, COM(2006) 786 final
[4] Commission staff working document on the review of the European Programme for Critical Infrastructure Protection (EPCIP), SWD(2012) 190 final
[5] Commission staff working document on a new approach to the European Programme for Critical Infrastructure Protection Making European Critical Infrastructures more secure, SWD(2013) 318 final
[6] Commission staff working document on Evaluation of the 2008 European Critical Infrastructure Protection Directice, 2018
[7] Národný program pre ochranu a obranu kritickej infraštruktúry v Slovenskej republike, Ministerstvo hospodárstva Slovenskej republiky, 2007
[8] Protecting Critical Infrastructure in the EU, CEPS Task Force Report, Centre for European Policy Studies, Brussels, 2010, ISBN: 978-94-6138-070-8