LEGAL AND POLITICAL SCIENCE

CONCEPTUAL REVIEW OF THE EUROPEAN UNION CRITICAL INFRASTRUCTURE ARCHITECTURE: POLICY, LAW AND ADMINISTRATION

Vephkhvia Grigalashvili, *PhD, Assistant-professor, International Black Sea University, Tbilisi, Georgia*
Khatuna Abiashvili, *PhD Candidate, Georgian Technical University, Tbilisi, Georgia*

DOI: https://doi.org/10.31435/rsglobal_conf/25052021/7562

Abstract*. Critical infrastructure protection represents an essential part of the European Union security concept whose dynamic development has been actively taking place since 2004. Based on a systematic review approach (methodology), this paper aims to provide an assessment of the evolution and contribution since mentioned period of the European Union infrastructure protection policies. The first part discusses the EU's critical infrastructure policy for 2004-2008 that laid the groundwork for the adoption of the Council Directive 2008/114/EC of 8 December 2008. The second section explains the main political and legal features of the Council Directive 2008/114/EC of 8 December 2008 as well as requirements to be implemented by EU member states in order to comply their national systems with the standards of the Directive 2008/114/EC. The third section presents the results of a study on EU policy developed in 2008-2020 parallel with Directive 2008/114/EC. Final sector introduces recent Past and present cooperation activities within the European Union for further development of the critical infrastructure protection system at the EU and Member States national levels.*
Keywords*: EU Critical Infrastructure; Critical Infrastructure Architecture; Critical Infrastructure Policy; Critical Infrastructure Protection.*

Introduction. Over the past 20 years, the attention of policymakers and industry players towards the protection of critical infrastructure has grown remarkably at European level.

The EU Internal Security Strategy highlights that critical infrastructure must be better protected from criminals who take advantage of modern technologies and that the EU should continue to designate critical infrastructure and put in place plans to protect such assets, as they are essential for the functioning of society and the economy.

The critical infrastructure protection in the European Union is a complex and dynamic process that takes place on a daily basis at a multitude of different levels and perspectives. The Union has worked as strong as the Member States have required and have looked for new and better solutions. Without wanting to be critical, a lot has been done, there are missed opportunities, but this is a dynamic and extremely interactive area that will get more and more space and time in all spheres of political, social and security activity, because every day countries depend more and more on the effective functioning of critical infrastructures.

Despite on what has already done at the EU level, "the European Union is still seeking its place and role in this area. From the European Union institutions, the European Commission is most active and seeks to promote the importance of this topic, to ensure cooperation between Member States, to accelerate the exchange of knowledge and experience and to guide the Member States in their efforts to develop the area of strengthening resilience and critical infrastructure protection. Challenges at the European Union level are multidimensional and are under time pressure, because as Haemmerli and Renda (2010) remarkably noticed, it is necessary to harmonize Europe at "several tracks", to harmonize various policies and in all of that to find and create own identity in this area. Therefore, the Union is trying at an accelerated pace to develop its own recognisability and set standards to be followed by all Member'' Nations (Mitrevska, Mileski, Mikac, 2019).

I. Historical Glancing Before the Council Directive 2008/114/EC of 8 December 2008

Terrorist attacks that took place in the United States in 2001 and in Europe (2004 in Madrid, 2005 in London) essentially led to the development of critical infrastructure protection policies at the EU level.

In June 2004 the European Council asked the European Commission to prepare an overall strategy in the area of critical infrastructures in the European Union and to establish a normative

framework for its protection. Based on the aforementioned requirement, in October 2004, the European Commission adopted first document in this area entitled Communication on Critical Infrastructure Protection in the fight against terrorism, which presented the proposals what Europe should do to prevent terrorist attacks on critical infrastructures, to enhance the level of preparedness for emergency situations, to raise their resilience and to develop the ability to respond to attacks (European Commission, 2004).

In December 2004, the Council endorsed the intention of the Commission to propose a European Programme for Critical Infrastructure Protection (European Commission, 2004).

One year later, the Commission created a Green Paper on a European Programme for Critical Infrastructure Protection, which provided policy options on how the Commission could establish a critical infrastructure protection program and a Critical Infrastructure Warning Information Network (CIWIN) (European Commission, 2005).

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 (European Commission, 2005).

The following key principles are suggested to form the basis of EPCIP*:*

• "Subsidiarity - Subsidiarity would be at the heart of EPCIP, with the protection of critical infrastructure being first and foremost a national responsibility. The prime responsibility for protecting critical infrastructure would fall on the MS and owners/operators acting under a common framework. The Commission would in turn concentrate on aspects related to the protection of critical infrastructures having an EU cross border effect. The responsibility and accountability of owners and operators to make their own decisions and plans for protecting their own assets should not change;

• Complementarity - The common EPCIP framework would be complementary to existing measures. Where community mechanisms are already in place, they should continue to be used and will help guarantee the overall implementation of EPCIP;

• Confidentiality - Information sharing regarding critical infrastructure protection would take place in an environment of trust and confidentiality. This is a necessity bearing in mind that specific facts about a critical infrastructure asset can be used to cause failure or unacceptable consequences for critical infrastructure installations. Both at EU level and MS level CIP information would be classified and access granted only on a need-to-know basis.

• Stakeholder Cooperation – All stakeholders including MS, Commission, industry/business associations, standardisation bodies and owners, operators and users ('users' being defined as organizations that exploit and use the infrastructure for business and service provision purposes) have a role to play in protecting CI. All stakeholders should cooperate and contribute to the development and implementation of EPCIP according to their specific roles and responsibilities. MS authorities would provide leadership and coordination in developing and implementing a nationally consistent approach to the protection of critical infrastructure within their jurisdictions. The owners, operators and users would be actively involved at both the national and EU level. Where sectoral standards do not exist or where international norms have not yet been established, standardisation organisations could adopt common standards where appropriate.

• Proportionality - Protection strategies and measures would be proportionate to the level of risk involved as not all infrastructures can be protected from all threats (for example, electricity transmission networks are too large to fence or guard). By applying appropriate risk management techniques, attention would be focused on areas of greatest risk, taking into account the threat, relative criticality, cost-benefit ratio, the level of protective security and the effectiveness of available mitigation strategies." (European Commission, 2005).

The next input came from the Justice and Home Affairs Council, which in December 2005 called upon the Commission to make a proposal for a European Programme for Critical Infrastructure Protection. The drafting guidelines emphasize that the Programme should take into account all dangers, where priority should be given to countering terrorist threats. Such approach in process of critical infrastructure protection takes into account the technological threats caused by human activity and natural disasters, but priority should be given to the threats from terrorism (European Commission, 2005).

As a result, in December 2006, the Commission issued a Communication on a European Programme for Critical Infrastructure Protection. This set out an overall policy approach and framework for CIP activities in the EU. The Programme's four main pillars would be: (a) A procedure for the identification and designation of European critical infrastructure (ECI) and for the assessment of the need to improve their protection (provided for in the ECI Directive adopted in 2008); (b) Measures designed to facilitate the implementation of the Programme, including an Action Plan, the Critical Infrastructure Warning Information Network (CIWIN), the use of a CIP expert group at EU level, a CIP information-sharing process, and the identification and analysis of interdependencies; (c) Funding for CIP-related measures and projects focusing on 'Prevention, Preparedness and Consequence Management of Terrorism and other Security-Related Risks' for the period 2007-2013; and (d) The development of an external dimension in recognition of the interconnected and interdependent nature of societies both within and beyond the EU. The external dimension would entail cooperation with third countries outside the EU through measures such as sector-specific memoranda of understanding and encouraging the raising of CIP standards outside of the EU (European Commission, 2006).

Following the creation of the Programme in 2006, CIWIN and the CIP expert group were established. The CIPS funding also came available and the Programme's external dimension was activated. At the same time, the Commission was developing the proposal for a mechanism that would provide a procedure for ECI identification and designation. In December 2006, the Commission published a Proposal for a Directive of the Council on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection (European Commission, 2006).

In April 2007, the Council of the European Union considered the European Programme for Critical Infrastructure and issued conclusions stating that the ultimate responsibility for managing critical infrastructure protection solutions lies on Member States, within their national borders. In addition to this, it is directed to the Commission to develop a European procedure for identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Mentioned is an important determinant of the development of this area, as it is recognized that there are a number of critical infrastructures in the Union which disruption of work or destruction could have significant cross-border effects. Work disruptions may include cross-border cross-sectoral effects resulting from the interdependence of mutually connected infrastructures (European Commission, 2007).

In parallel with the work of the Commission, the Council of the European Union adopted in 2007 a special program the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks. This program identifies a number of security-related risks, with the focus on supporting Member States' efforts to prevent terrorist attacks and to carry out preparations for the protection of people and critical infrastructure from risks related to terrorist attacks (European Commission, 2007).

II. Council Directive 2008/114/EC of 8 December 2008 and Critical Infrastructure Sectors

Directive 2008/114/EC should be observed in the scope and time when it was adopted. Certainly it was a huge step forward, but clearly, it could not respond to all requirements of complete regulation of the area for identification, designation, and protection of European critical infrastructures. At the same time, it had to partially level the already developed national policies of individual Union's Member States with those who did not pay enough attention to this area or started just now, under its impact, to regulate this area. Directive 2008/114/EC was originally used to guide Member States in their mutual cooperation and as an example of how they can directly establish and organize the national framework for identification and designation of critical infrastructures and indirectly for their protection. It was further on Member States to develop this area with the help of the Commission and not for it to have a main role (European Commission, 2008).

The Council of the European Union, taking into account the proposal of the Commission, has brought immediately a key document for the area of critical infrastructures in the European Union, 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 (further Directive 2008/114/ EC), which is no longer primarily focused on the threat of terrorism, but seeks to establish a comprehensive process of critical infrastructure protection both at the level of the Member States and the Union as a whole (European Commission, 2008).

The mentioned directive suggests two significant definitions: a) Critical infrastructure - "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"; b) European critical infrastructure - "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 crosscutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure".

In the introductory provisions of Directive 2008/114/EC, the Council of the European Union has taken steps to highlight the essential guidelines for all those concerned. It was emphasized that the first step in the multiphase approach is aimed at identification and designation of European critical infrastructures and the assessment of the need to improve their protection. Then, that focus is primarily on the energy and transport sectors, but other significant sectors such as information and communication technology sectors need to be considered. As well, and what is especially important, that the Member States and the owners or operators of the above mentioned have the primary and ultimate responsibility for the critical infrastructure protection in Europe. The next important aspect of Directive 2008/114/EC is that it has become a common platform for the cooperation of all relevant stakeholders of the critical infrastructure protection system at Union level. Prior to its adoption, the obligation of official cooperation among various stakeholders, as well as the forum for achieving this cooperation, did not exist. Its strenght is in mandatory application, and each Member State chooses the way how it will be transposed into national legislation (Mitrevska, Mileski, Mikac, 2019).

The central part of Directive 2008/114/EC is the procedure for identification and designation of European critical infrastructures. The identification procedure was adopted in Article 3 and the accompanying attachment. It consists of several steps involving the terminology equivalence of the observed infrastructure according to the set definition and the fulfilment of the cross-cutting and sectoral criteria. The first step is that each Member State applies sectoral criteria to make the primary identification of critical infrastructure within the sector on the national territory. Sectoral criteria are the first selection of potential critical infrastructures. The second step is to apply definitions to the considered infrastructure in order to see if it meets the "critical infrastructure" requirements/conditions as well as "European critical infrastructure". The third step is to look at the cross-border impact of the definition of "European critical infrastructure" and to determine whether a certain infrastructure is mutually significant for two Member States, whether the both determined it as a significant or that one of the member finds that there is infrastructure on the territory of the other Member State that is significant to her alone. The fourth step is the application of cross-cutting criteria that include the observation of three criteria: (a) Casualties criterion (assessed in terms of the potential number of fatalities or injuries); (b) Economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects); (c) 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) (Mitrevska, Mileski, Mikac, 2019).

The ECI process, as specified in the Directive, can be divided broadly into three distinct phases: identification of potential ECI, designation of ECI, and protection of ECI. Annex III of the Directive specifies the steps within each of these phases (Fig. 1).

The suggestion that members of the European Union, following the adoption of Directive 2008/114/EC, are obliged to incorporate its provisions into national legislation has become a multiple challenge because the "older" EU Member States have begun the process of critical infrastructure protection prior to the adoption of Directive 2008/114/EC so this is potentially an obstacle in the implementation of their own policies, but they are required to harmonize national policy with the Union's policy in this area. The new Member States found themselves in the need for quick adaptation or opening up the process for the first time although some of them were not yet fully organizationally ready for that purpose. But Directive 2008/114/EC left no room for them to be postponed and did accelerate their adjustment (Mitrevska, Mileski, Mikac, 2019).

Based on EC 2008/114 of the European Council as a European critical infrastructure (ECI), we can define critical infrastructure located in Member States that the disruption or destruction of which would have a significant impact on at least two Member States. Table 1 presents an indicative list of CIs sectors and services identified by the EU Member States.

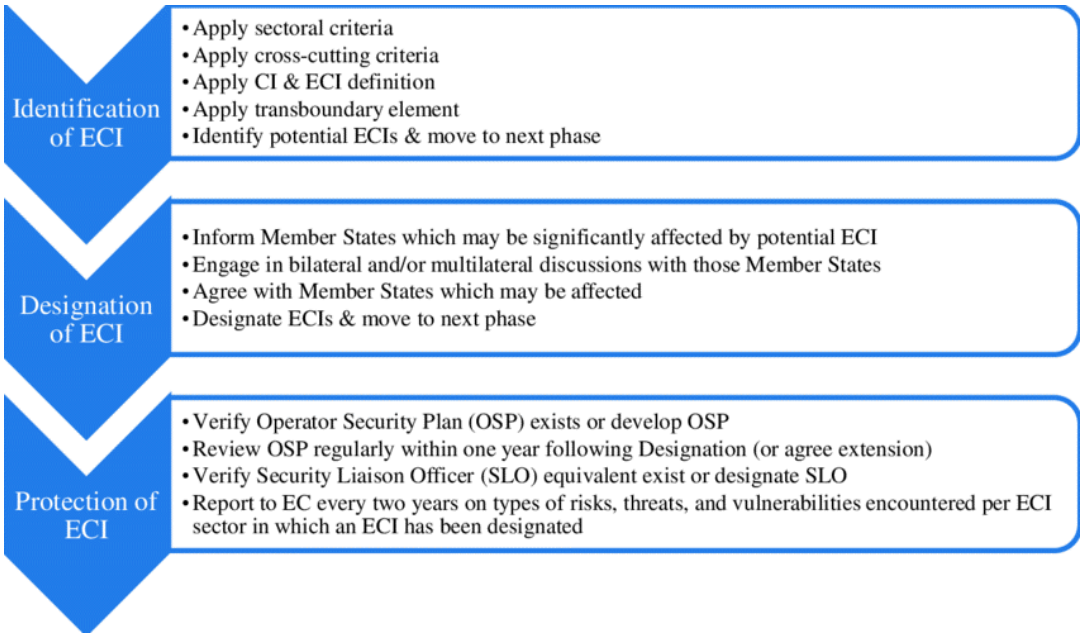

Fig. 1. Implementing the ECI process (COMMISSION STAFF WORKING DOCUMENT, 2012)

Table 1: Indicative list of ECI sectors (*European Commission 2005)*

Sector	Product or service
I Energy	1 Oil and gas production, refining, treatment and storage, including pipelines; 2 Electricity generation; 3 Transmission of electricity, gas and oil; 4 Distribution of electricity, gas and oil;
II Information, Communication Technologies, ICT	5 Information system and network protection; 6 Instrumentation automation and control systems (SCADA etc.); 7 Internet; 8 Provision of fixed telecommunications; 9 Provision of mobile telecommunications; 10 Radio communication and navigation; 11 Satellite communication; 12 Broadcasting;
III Water	13 Provision of drinking water; 14 Control of water quality; 15 Stemming and control of water quantity;
IV Food	16 Provision of food and safeguarding food safety and security;
V Health	17 Medical and hospital care; 18 Medicines, serums, vaccines and pharmaceuticals; 19 Bio-laboratories and bio-agents
VI Financial	20 Payment services/payment structures (private); 21 Government financial assignment;
VII Public & Legal Order and Safety	22 Maintaining public & legal order, safety and security; 23 Administration of justice and detention VIII Civil administration; 24 Government functions; 25 Armed forces; 26 Civil administration services; 27 Emergency services; 28 Postal and courier services;
IX Transport	29 Road transport; 30 Rail transport; 31 Air traffic; 32 Inland waterways transport; 33 Ocean and short-sea shipping;
X Chemical and nuclear industry	34 Production and storage/processing of chemical and nuclear substances; 35 Pipelines of dangerous goods (chemical substances);
XI Space and Research	36 Space; 37 Research.

III. Following to Council Directive 2008/114/EC of 8 December 2008

As critical infrastructures are connected and increasingly dependent on the Internet and processes in the cyberspace.

In 2013, the European Commission, together with the High Representative of the European Union for Foreign Affairs and Security Policy, put forward a Cybersecurity Strategy of the European Union that articulates the EU's vision of cyber security through five priorities: 1. Achieving Cyber

Resilience; 2. Drastically reducing cybercrime; 3. Developing cyber-defence policy and capabilities related to the Common Security and Defence Policy (CSDP); 4. Developing the industrial and technological resources for cyber security; and 5. Establishing a coherent international cyberspace policy for the European Union and promote core EU values (Mitrevska, Mileski, Mikac, 2019).

Based on a Cybersecurity Strategy of the European Union, the Directive 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union (further NIS Directive) was adopted on 6 July 2016 with the obligation to be implemented into national legislation of all Member States until 9 May 2018.

The NIS Directive covers two groups of actors: Operators of Essential Services (The criteria for the identification of the operators of essential services are defined as follows: (a) an entity provides a service which is essential for the maintenance of critical societal and/or economic activities; (b) the provision of that service depends on network and information systems; and (c) an incident would have significant disruptive effects on the provision of that service) and Digital Service Providers. The main objective of the NIS Directive is to provide a common level of security of network and information systems in all Member States, whose malfunctions due to security incidents may have strong consequences on society or the national economy. In doing so, the NIS Directive introduces regulatory elements that enable permanent monitoring of the condition of automation and digitization of the designated sectors.

IV. Co-operation activities within the European Union

Albeit the Commission has embraced various arrangement drives around here, various extraordinary issues remains. “First, Member States are at varying degrees of maturity with respect to the development of a comprehensive and effective CIP policy. Second, there are islands of cooperation across the EU Member States but no overall concept of operations at the EU level. Third, partnerships and relationships are scattered across countries (each individual country has and will maintain unique relationships with private sector owner operators and global companies that enable them). Fourth, critical EU infrastructure is also scattered across many different countries”, (Mitrevska, Mileski, Mikac, 2019), (Haemmerli and Renda, 2010).

To help Member States, the Commission has also engaged its own Joint Research Centre, which in 2008 produced a document entitled Non-Binding Guidelines for application of the Council Directive on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection. The document aims to assist Member States in the proper application of technical provisions for the determination of European critical infrastructures (Lazari, 2014). It is proposed to use following criteria or conditions for cumulative observation of the sectoral criteria: 1. Prescribe specific properties (according to its necessity for the functioning of the entire system, sector and/or organization); 2. Identify networks of which the ‘key elements’ must be determined (according to the potential negative effects that may occur in the Member States); 3. Name a specific infrastructure asset directly; 4. Allow Member States to identify an asset directly (in the cases where no sectoral criteria exist) (The Joint Research Centre, 2008), (Mitrevska, Mileski, Mikac, 2019).

The significant opportunity, that the European Commission provides to all interested actors in the area of critical infrastructure protection are projects. Through the program the Prevention, Preparedness and Consequence Management of Terrorism and other Security-related Risks, during the period 2007-2012, 111 projects were co-financed (70 – directly related to critical infrastructure protection, 32 – related to crisis management, 9 – mixed) with a total of 45 million Euros allocated. The Commission continued to invest in projects that enable to all interested co-financing the projects costs to the greatest extent and most importantly the transfer of the required knowledge and technology (Mitrevska, Mileski, Mikac, 2019), (Engdahl, 2016),

The next important step in establishing cooperation and exchange of knowledge and experience at the European level was designing and launching of Critical Infrastructure Warning Information Network (CIWIN). This was already announced in the Green Paper on a European Programme for Critical Infrastructure Protection in 2005, and has been gradually created by a modular approach and has become operational in January 2013. The purpose of the network is to exchange information on strategies and measures to reduce risk in critical infrastructure protection (Mitrevska, Mileski, Mikac, 2019).

Also, the Commission has recognized the standstill in the normative area of the developing process of the area for identification and designation of European critical infrastructures as well as in cooperation between Member States, and in 2012 it has started to carry out a revision of the previous

activities and the development of a working document dedicated to a new approach in critical infrastructure protection. In mid-2013, it presented the Commission Staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructures more secure. The above is an updated version of the European Programme, originally adopted in 2006. The solutions proposed so far have been reviewed, a new look at ways and models on how to continue to develop this area is presented, including some data such as: how less than 20 European critical infrastructures are designated, and among them aren't for example the main energy distribution network (European Commission, 2013). By 2016, in total 89 European critical infrastructures (Engdahl, 2016) were designated (Mitrevska, Mileski, Mikac, 2019).

The Working Document presents a new look at the more practical implementation of the European Programme for Critical Infrastructure Protection, provides an analysis of the elements of the current program and proposes a transformation of the approach of European critical infrastructure protection, based on the practical implementation of activities within the area of prevention, readiness and response. Part of the new approach is to look at the interdependence between critical infrastructure, industry and state entities, as it has been noted that the interdependence so far has not been sufficiently percieved. As many of the critical infrastructures are in private ownership, it confirmed the view that better co-operation with the private sector and the development of public-private structured dialogue are needed. Four priority areas of the European critical infrastructure protection model are additionally highlighted, which need to be further elaborated: 1. Procedures for identification and designation of European critical infrastructures and the assessment of the need to improve their protection; 2. Measures designed to assist the implementation of the European Programme for Critical Infrastructure Protection, including the Action Plan, the establishment of a Critical Infrastructure Warning Information Network (CIWIN), the use of expert groups for critical infrastructure protection at Union level, exchange of information, identification and interdependency analysis; 3. Financing of measures related to the critical infrastructure protection and projects associated with a special program Prevention Preparedness and Consequence Management of Terrorism and other Security-related Risks; 4. The development of the external dimension of the European Programme for Critical Infrastructure Protection (Mitrevska, Mileski, Mikac, 2019).

At present, the key activity carried out over the last few years, at the Commission's initiative, is the revision of Directive 2008/114/EC. So far, its evaluation has been carried out by the Commission. As a final product, the evaluation has brought identified challenges in implementation, the best practices of individual Member States, conclusions and recommendations what is presented in the final, very comprehensive document. Based on this evaluation it will be determined in the next step what will happen with Directive 2008/114/EC. Will it change or create a whole new document (about which format will be afterwards decided) that will completely replace it (Mitrevska, Mileski, Mikac, 2019), (Cesarec, 2019).

REFERENCES

1. Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP). (Brussels, 22.6.2012 SWD (2012) 190 final
2. Commission staff working document. Evaluation of council directive 2008/114 on the identification and designation of european critical infrastructures and the assessment of the need to improve their protection {SWD(2019) 310 final} Brussels, 23.7.2019 SWD(2019) 308 final
3. Engdahl, E-M. (2016), The European Programme for Critical Infrastructure Protection, Gas Infrastructure Europe
4. European Commission (2004), Communication on Critical Infrastructure Protection in the fight against terrorism
5. European Commission (2005), Green Paper on a European Programme for Critical Infrastructure Protection
6. European Commission (2006), European Programme for Critical Infrastructure Protection
7. European Union Council Directive 2008, On the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection, Official Journal of the European Union, 23/12/2008;
8. European Commission (2013), Commission staff Working Document on a new approach to the European Programme for Critical Infrastructure Protection: Making European Critical Infrastructures more secure
9. European Commission (2014) ECHO Factsheet – Disaster Risk Management – 2014
10. European Commission (2014) The post 2015 Hyogo Framework for Action: Managing risks to achieve resilience

11. European Commission (2017), Commission staff working document on assessment of the EU 2013 Cybersecurity Strategy
12. European Commission (2019), Cybersecurity European Commission and High Representative of the European Union for Foreign Affairs and Security Policy (2013), Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace
13. European Environment Agency (2011) Mapping the impacts of natural hazards and technological accidents in Europe (Technical report No 13/2010),
14. European Parliament and of the Council of the European Union (2016), Directive 2016/1148 of the European Parliament and of the Council concerning measures for a high common level of security of network and information systems across the Union
15. Joint Research Centre of the European Commission (2008), Non-Binding Guidelines for application of the Council Directive on the identification and designation of European Critical Infrastructures and the assessment of the need to improve their protection
16. Joint Research Centre of the European Commission (2017), The ERNCIP Project Platform
17. Haemmerli, B. and Renda, A. (2010), Protecting Critical Infrastructure in the EU, Brussels: Centre for European Policy Studies
18. Lazari, A. (2014), European Critical Infrastructure Protection, Springer International Publishing Switzerland
19. Lazari, A. and Simoncini, M. (2014), Beyond compliance: An analysis of the experiences that maximise the implementation of the Directive 114/08/EC on European Critical Infrastructures, International Journal of Critical Infrastructure
20. Mikac, R. and Cesarec, I. (2019), Current state of play of the Republic of Croatia regarding Critical infrastructure security and resilience, accepted publication work as a chapter in a book to be published by Springer International
21. Mitrevska M., Mileski T., Mikac R., (2019) Critical Infrastructure Concept and Security Challenges