RS Global Journals

Scholarly Publisher
RS Global Sp. z O.O.
ISNI: 0000 0004 8495 2390

Dolna 17, Warsaw, Poland 00-773
Tel: +48 226 0 227 03
Email: editorial_office@rsglobal.pl

JOURNAL	International Journal of Innovative Technologies in Economy
p-ISSN	2412-8368
e-ISSN	2414-1305
PUBLISHER	RS Global Sp. z O.O., Poland

ARTICLE TITLE	THE ESSENCE OF CRITICAL INFRASTRUCTURE IN THE EUROPEAN UNION, NATO AND G7 COUNTRIES
AUTHOR(S)	Vephkhvia Grigalashvili
ARTICLE INFO	Vephkhvia Grigalashvili. (2022) The Essence of Critical Infrastructure in the European Union, NATO and G7 Countries. International Journal of Innovative Technologies in Economy. 1(37). doi: 10.31435/rsglobal_ijite/30032022/7763
DOI	https://doi.org/10.31435/rsglobal_ijite/30032022/7763
RECEIVED	06 January 2022
ACCEPTED	23 February 2022
PUBLISHED	28 February 2022
LICENSE	This work is licensed under a **Creative Commons Attribution 4.0 International License.**

THE ESSENCE OF CRITICAL INFRASTRUCTURE IN THE EUROPEAN UNION, NATO AND G7 COUNTRIES

Vephkhvia Grigalashvili, *PhD in Public Administration, Assistant Professor, International Black Sea University, Tbilisi, Georgia*

DOI: https://doi.org/10.31435/rsglobal_ijite/30032022/7763

ARTICLE INFO

Received 06 January 2022
Accepted 23 February 2022
Published 28 February 2022

KEYWORDS

Critical Infrastructure; European Union Critical Infrastructure; NATO Critical Infrastructure; G7 Counties Critical Infrastructure.

ABSTRACT

Critical infrastructures (include the body of systems, networks, and assets that are so essential that their continued operation is required to ensure the security of a given nation, its economy, and the public's health and/or safety) are significant for the growth and development of our society, drastically affecting most of the everyday activities as the components of the critical infrastructures are increasingly vulnerable to a dangerous mix of traditional and nontraditional types of threats. Taking into account a significant role of Critical Infrastructure in national and international security maintenance, the article analyses and interprets the policy pillars of Critical Infrastructure concepts in the European Union, NATO as well as in G7 Countries. Particular attention is paid to determining the functional purpose, approaches to the classification of the main components of critical infrastructure (structural content) and characteristics of them. At the end of this article there is suggested a generalized view regarding to the essence of Critical Infrastructure, as well as attention is drawn to the fact that the adopted approaches generally take into account that Critical Infrastructure now rarely exist or function in isolation, rather, they are becoming more tightly coupled, interconnected and interacted that creates a complex multisystem - a system-of-systems.

Citation: Vephkhvia Grigalashvili. (2022) The Essence of Critical Infrastructure in the European Union, NATO and G7 Countries. *International Journal of Innovative Technologies in Economy*. 1(37). doi: 10.31435/rsglobal_ijite/30032022/7763

1. Introduction. In the past three decades the developing and modeling of Critical Infrastructure has become a growing research area as Critical Infrastructures are essential assets for the maintenance of vital societal functions and safety of which is significant because its improper functioning may result in considerable loss.

Critical Infrastructure and their effectiveness are of great importance for the quality of life, economy and functioning of other sectors as they are closely related to energy security, telecommunications, energy systems, gas and oil pipelines, transportation, water supply and etc. As a consequence of their ubiquity, disruption of normal operation of Critical Infrastructures can have severe primary (loss of life, property damage, and economic losses and etc.) as well as secondary (mass displacement of residents, widespread health consequences, and decreased quality of life) effects.

Due to threats from state- and non-state actors, as well as the increased severity and frequency of severe weather events, developing Critical Infrastructure resilience is an issue of utmost importance for ensuring security and the common good. Critical infrastructures have become a significant sector for every country - it is crucial to know which are the threats and vulnerabilities in such systems and possible attacks in order to find a way to prevent and confront them.

However, there are still ongoing debates regarding Critical Infrastructure concept and its protection, especially, how to effectively protect them given their vital positions in social and economic developments) as the concept of Critical Infrastructure has been changing over time according to the disaster situations and rapidly changeable security environment.

Necessity of strengthening and further development of Critical Infrastructure concept still is one of the main concerns. These concerns have been highlighted with the increased emphasis on improved efficiency, performance and productivity.

In such a consideration, the article reviews the existing approaches to critical infrastructure dimensions in the European Union, NATO and G7 Countries (Canada, France, Germany, Italy, Japan, the United Kingdom and the United States of America), that will facilitate further studies of Critical Infrastructure Protection Policies and their implementation strategies in above mentioned countries and international organisations.

2. The European Union.

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 of 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.

An indicative list of Critical Infrastructure sectors and services identified by the EU Member States are presented as follows:

(i) Energy: 1. Oil and gas production, refining, treatment and storage, including pipeline; 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 and Legal Order and Safety: 22. Maintaining public and 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;

(viii) Transport: 29. Road transport; 30. Rail transport; 31. Air traffic; 32. Inland waterways transport; 33. Ocean and short-sea shipping;

(ix) Chemical and nuclear industry: 34. Production and storage/processing of chemical and nuclear substances; 35. Pipelines of dangerous goods (chemical substances);

(x) Space and Research: 36. Space; 37 Research.

Challenges at the European Union level are multidimensional and under time pressure, because, as Haemmerli and Renda (2010) remarkably noticed, it is necessary to harmonize Europe at "several tracks", to coordinate 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) 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, 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 Programme (EPCIP) and a Critical Infrastructure Warning Information Network (European Commission, 2005).

The main objective of the green paper is to receive feedback concerning possible the 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 European Programme for Critical Infrastructure Protection (EPCIP): subsidiarity, complementarity, confidentiality, stakeholder cooperation and Proportionality (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 (EPCIP). 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 (EPCIP). This set out an overall policy approach and framework for Critical Infrastructure Protection activities in the EU. The Programme's four main pillars would be: (i) 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); (ii) Measures designed to facilitate the implementation of the Programme, including an Action Plan, the Critical Infrastructure Warning Information Network (CIWIN), the use of a Critical Infrastructure Protection expert group at EU level, a Critical Infrastructure Protection information-sharing process, and the identification and analysis of interdependencies; (iii) Funding for Critical Infrastructure Protection related measures and projects focusing on 'Prevention, Preparedness and Consequence Management of Terrorism and other Security-Related Risks' for the period 2007-2013; and (iv) 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 Critical Infrastructure Protection standards outside of the EU (European Commission, 2006).

Following the creation of the Programme in 2006, Critical Infrastructure Warning Information Network (CIWIN) and the Critical Infrastructure Protection expert group were established. At the same time, the Commission was developing the proposal for a mechanism that would provide a procedure for European critical infrastructure (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-sectorial 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).

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: (i) 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"; (ii) European critical infrastructure (ECI) - "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 strength 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 sectorial criteria.

The first step is that each Member State applies sectorial criteria to make the primary identification of critical infrastructure within the sector on the national territory. Sectorial 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: (i) Casualties criterion (assessed in terms of the potential number of fatalities or injuries);

(ii) Economic effects criterion (assessed in terms of the significance of economic loss and/or degradation of products or services; including potential environmental effects); (iii) 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 European critical infrastructure (ECI) process, as specified in the Directive, can be divided broadly into three distinct phases: (i) Identification of potential European critical infrastructure (ECI); (ii) Designation of European critical infrastructure (ECI); (iii) Protection of European critical infrastructure (ECI). Annex III of the Directive specifies the steps within each of these phases.

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 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 Cyberat least two Member States. 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 was adopted on 6 July 2016 with the obligation to be implemented into national legislation of all Member States until 9 May 2018.

The Directive 2016/1148 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 Directive 2016/1148 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 Directive 2016/1148 introduces regulatory elements that enable permanent monitoring of the condition of automation and digitization of the designated sectors.

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 Critical Infrastructure Protection (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 sectorial criteria: (i) Prescribe specific properties (according to its necessity for the functioning of the entire system, sector and/or organization); (ii) Identify networks of which the 'key elements' must be determined (according to the potential negative effects that may occur in the Member States); (iii) Name a specific infrastructure asset directly; (iv) Allow Member States to identify an asset directly (in the cases where no sectorial 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 perceived. As many of the critical infrastructures are in private ownership, it confirmed the view that better cooperation with the private sector and the development of publicprivate structured dialogue are needed.

Four priority areas of the European critical infrastructure protection model are additionally highlighted, which need to be further elaborated: (i) Procedures for identification and designation of European critical infrastructures and the assessment of the need to improve their protection; (ii) 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; (iii) 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; (iv) The development of the external dimension of the European Programme for Critical Infrastructure Protection (Mitrevska, Mileski, Mikac, 2019).

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).

3. NATO.

The approach and contribution of NATO in critical infrastructure protection is still a topic of scientific analyses and political debates. Despite this ongoing discussions, critical infrastructure protection has been gradually taking an active part in NATO strategies.

After the September 11, 2001 attacks, the NATO Summit in Prague initiated the "Civil Emergency Planning Action Plan" that states: "…we are committed, in cooperation with our partners, to fully implement the Civil Emergency Planning Action Plan for the improvement of civil preparedness against possible attacks against the civilian population with chemical, biological or radiological agents. We will enhance our ability to provide support, when requested, to help national authorities to deal with the consequences of terrorist attacks, including attacks with chemical, biological, radiological and nuclear weapons against critical infrastructure, as foreseen in the Civil Emergency Planning Action Plan". (Prague Summit Declaration, 2002).

In 2005, the Action Plan focused on critical infrastructure protection and victims support (in order to cover efforts during and after terrorist attacks with chemical, biological, radiological and nuclear weapons) was adopted and adjusted by the Senior Civil Emergency Planning Committee.

In NATO's Strategic Concept (adopted at the Lisbon Summit in 2010), critical infrastructure is the first and foremost clearly and unambiguously mentioned in the section on "cyber" attacks. The Concept emphasizes the commitment to develop the capacity to contribute to energy security among Allies on the basis of strategic assessments and contingency planning (Strategic Concept for the Defence and Security of the Members of the North Atlantic Treaty Organization, 2010).

In connection with the NATO critical infrastructure approach, it to be considered the definition of "Critical Infrastructure" used by Allied Command Operations (ACO) - critical Infrastructure is a general term describing a nation's infrastructure assets, facilities, systems, networks, and processes that support the military, economic, political and/or social life on which a nation and/or NATO depends. From an ACO perspective, Critical infrastructure is categorized into three different sub-categories: (i) Critical National Infrastructure; (ii) Mission-Vital Infrastructure; (iii) Key Infrastructure (Bearse, 2021).

4. G7 Counties.

In a modern variable security environment, there are growing concerns and debates regarding Critical Infrastructure concept and protection of infrastructures, especially, how to effectively protect them given their vital positions in social and economic developments. These concerns have been highlighted with the increased emphasis on improved efficiency, performance and productivity, and this implies that Critical Infrastructures now rarely exist or function in isolation. Rather, they are becoming more tightly coupled into a system of (inter)dependent infrastructures. In this case, G7 Countries is no exception regardless of their economic or military or other strength.

4.1. Canada.

The National Strategy, for Critical Infrastructure sets the direction for enhancing the resilience of Canada's critical infrastructure against current and emerging hazards, defines critical infrastructure as the processes, systems, facilities, technologies, networks, assets, and services essential to the health, safety, security or economic well-being of Canadians and the effective functioning of government (Minister of Public Safety and Emergency, 2021).

The fundamental concepts and principles outlined in this National Strategy flow from the Emergency Management Framework for Canada, which sets out a collaborative approach for federal, provincial and territorial emergency management initiatives. Therefore, the National Strategy presents a collaborative approach to strengthening the resilience of critical infrastructure, by ensuring that federal, provincial and territorial critical infrastructure activities are complementary and respect the laws of each jurisdiction, outlines mechanisms for enhanced information sharing and information protection, and identifies the importance of a risk management approach to strengthen the resilience of critical infrastructure in Canada and identifies three main objectives to strengthen critical infrastructure resilience: building partnerships, sharing and protecting information, and practicing an all-hazards risk approach (Government of Canada, 2021).

The National Strategy is based on the recognition that enhancing the resiliency of critical infrastructure can be achieved through the appropriate combination of security measures to address intentional and accidental incidents, business continuity practices to deal with disruptions and ensure the continuation of essential services, and emergency management planning to ensure adequate response procedures are in place to deal with unforeseen disruptions and natural disasters. Following this pillar, the goal of the National Strategy for Critical Infrastructure is to build a safer, more secure and more resilient Canada. To this end, the National Strategy advances more coherent and complementary actions among federal, provincial and territorial initiatives and among the ten critical infrastructure sectors listed below: (i) Energy and utilities; (ii) Finance; (iii) Food; (iv) Transportation; (v) Government; (vi) Information and communication technology; (vii) Health; (viii) Water; (ix) Safety; (x) Manufacturing (Government of Canada, 2021).

4.2. France.

Critical infrastructure protection policy, established by the 2013 White Paper on Defence and National Security, provides a framework in which public or private critical operators can assist in implementing the national security strategy in terms of protection against malicious acts and natural, technological and health risks (The French White Paper on Defence and National Security (2013).

Critical infrastructures are institutions, structures or facilities that provide the essential goods and services forming the backbone of French society and its way of life. Based on that approach, there are separated twelve sectors of critical importance across four key areas of responsibility: (i) Basic human need: Food Water management Health; (ii) Sovereign: Civilian activities Legal activities Military activities; (iii) Economic: Energy Finance Transport; (iv) Technological: Communication, technologies and broadcasting Industry Space and research (SGDCN, 2017).

4.3. Germany.

The German National Strategy for Critical Infrastructure Protection summarizes the Federal Administration's aims and objectives and its political-strategic approach to actively address matters of critical infrastructure protection. The strategy is guided by the principle of joint action by the state, society, and business and industry. The state co-operates with other public and private actors in developing analyses and protection concepts.

The Strategy first defines critical infrastructure, as organizational and physical structures and facilities of such vital importance to a nation's society and economy that their failure or degradation would result in sustained supply shortages, significant disruption of public safety and security, or other dramatic consequences. This strategy, with reference to their technical, structural and functional specifics, classifies critical infrastructures as vital (absolutely essential) technical basic infrastructure, on the one hand, and vital (absolutely essential) socio-economic services infrastructure, on the other hand. In Germany, these include: (i) Technical basic infrastructure: Power supply; Information and communications technology; Transport(ation); (Drinking-) water supply and sewage disposal; (ii) Socio-economic services infrastructure: Public health; food; Emergency and rescue services; disaster control and management; Parliament; government; public administration; law enforcement agencies; Finance; insurance business; Media; and cultural objects (cultural heritage items). It seems significant interdependencies exist between these two infrastructure sectors since nearly all of the socio-economic services infrastructures largely rely on the unrestricted availability of the technical basic infrastructure. However, technical basic infrastructures, in their turn, depend on socio-economic services infrastructure, such as a stable legal service or functioning first response, emergency medical and rescue services in the event of a crisis (Federal Ministry of the Interior,2009).

This approach shoes that the main focus is clearly on the disruption of supplies and services. Infrastructures, in which dangerous substances are handled such as chemical industry factories or nuclear waste sites, are, for example, not addressed in the definition. The infrastructures under consideration are those, whose failure can lead to an effect on the population or on other infrastructures (EISMANN, 2009).

According to Critical Infrastructure Regulation"/BSI-KritisV critical infrastructures are organizations or facilities of major importance to the state community, the failure or impairment of which would result in lasting supply bottlenecks, significant disruptions to public safety or other dramatic consequences (Bundesamt für Bevölkerungsschutz und Katastrophenhilfe, 2021).

On 1 January 2022, the second amendment to the German Regulation for Critical Infrastructure ("Critical Infrastructure Regulation"/BSI-KritisV) entered into force. It broads the definition of Critical

Infrastructures, particularly in the IT services and energy sectors. The definition of Critical Infrastructure in the pertinent German legislation has two limbs:

(i) The infrastructure in question must fall within certain categories of the energy, water, food, IT and telecommunication, health, finance and insurance, or transportation and traffic sectors;

(ii) The infrastructure in question must reach certain thresholds as to the size and importance of the respective infrastructure. The most relevant changes to the Critical Infrastructure Regulation include: Software and IT services; Energy sector; IT and telecommunication sector; Health sector; Finance and insurance sector; Transportation and traffic sector; Joint infrastructure (Petersen and etc., 2002).

4.4. Italy.

The DPCM Asset of National Interest identifies the "assets of National interests" within the sectors indicated in the European Regulation no. 452/2019 (*i.e.*, financial, credit and insurance sectors, critical infrastructures and technologies including energy, transport, water and healthcare, food safety, access to sensitive information, including personal data, artificial intelligence, robotics, semiconductors, cybersecurity, as well as nanotechnology and biotechnology, media freedom and pluralism"):

(i) "Critical infrastructure" means the critical infrastructure for maintaining the vital functions of society, health, safety and the economic and social well-being of the Italian population;

(ii) "Critical technology" means the critical technologies for maintaining the vital functions of society, health, safety, economic and social well-being of the Italian population, as well as for technological progress;

(iii) "Critical production factors" means the assets and interests critical for maintaining the vital functions of society, health, safety and the economic and social well-being of the Italian population;

(iv) "Critical information" means the information critical for maintaining the vital functions of society, health, safety and the economic and social well-being of the Italian population; (v) "Strategic economic activities" means the economic activities critical for maintaining the vital functions of society, health, safety, economic and social well-being of the Italian population, as well as technological progress (Decrees, 2020).

4.5. Japan.

In the "Action Plan on Information Security Measures for Critical Infrastructure" promulgated by the Information Security Policy Council (ISPC) in 2005, critical infrastructure is defined as: Critical infrastructure which offers the highly irreplaceable service in a commercial way is necessary for people's normal lives and economic activities, and if the service is discontinued or the supply is deficient or not available, it will seriously influence people's lives and economic activities. Based on the definition of the action plan, the critical infrastructure contains: (i) Telecommunication systems; (ii) Administration services of the government; (iii) Finance; (iv) Civil aviation; (v) Railway; (vi) Logistics; (vii) Power, gas, water; (viii) Medical services (Information Security Policy Council, 2009).

Since 2005, the "Cybersecurity Policy for Critical Infrastructure Protection" (the 4th edition was published in 2017) has been set as a common action plan shared by the government (which bears a responsibility for protection of critical infrastructure) and by critical infrastructure operators (which independently carry out relevant protective measures), identifies the critical infrastructure sectors and expects stakeholders to undertake the five measures as below: development and penetration of safety principles; enhancement of information sharing system; reinforcement of incident response capacity; risk management and preparation of incident readiness; building up of basis of critical infrastructure protection (NISC,2021).

4.6. The United Kingdom.

The UK`s Critical National Infrastructure is increasingly interconnected and interdependent. It includes both public (The Defence, Emergency Services, Government and Health sectors are predominantly considered as public sector (CPNI, 2021) sector and private (Much of the UK's CNI is owned by the private sector, rather than the UK government. The NCSC has a team dedicated to supporting cyber security within each CNI sector in order to help protect their essential services (CPNI, 2021) sector organisations.

The UK's Critical Infrastructure is defined by the UK government as Those critical elements of infrastructure (namely assets, facilities, systems, networks or processes and the essential workers

that operate and facilitate them), the loss or compromise of which could result in: (a) Major detrimental impact on the availability, integrity or delivery of essential services – including those services whose integrity, if compromised, could result in significant loss of life or casualties – taking into account significant economic or social impacts; and/or (b) Significant impact on national security, national defence, or the functioning of the state (NCSC, 2021).

Based on these pillars, UK Critical National Infrastructure incorporates 13 sectors: (i) Chemicals; (ii) Civil Nuclear; (iii) Communications; (iv) Defence; (v) Emergency Services; (vi) Energy; (vii) Finance; (viii) Food; (ix) Government; (x) Health; (xi) Space; (xii) Transport; (xiii) Water. (UK Parliament, 2021)

Several sectors have defined 'sub-sectors'; Emergency Services for example can be split into Police, Ambulance, Fire Services and Coast Guard. However, not everything within a national infrastructure sector is judged to be critical (CPNI, 2021).

4.7. The United States of America.

Since mid-1990s, by issuing the Executive Order (EO) 13010 Critical Infrastructure Protection, the US government has begun to formalise efforts to develop a comprehensive national policy for Critical Infrastructure. Mentioned order stated that "certain national infrastructures so vital that their incapacity or destruction would have a debilitating impact on the defense or economic security of the United States (EO 13010).

Through 2007 the focus was on the identification and cataloging of the nation's Critical Infrastructure assets. From 2007 to 2013 the focus turned to the identification and prioritisation of lifeline sectors and the overall interdependency of the critical infrastructure system as a whole.

Today Presidential Policy Directive 21 (PPD-21), which supersedes Homeland Security Presidential Directive 7, establishes national policy on Critical Infrastructure security and resilience. The directive declares that: a) "The Nation's Critical Infrastructure is diverse and complex. It includes distributed networks, varied organisational structures and operating models (including multinational ownership), interdependent functions and systems in both the physical space and cyberspace, and governance constructs that involve multi-level authorities, responsibilities, and regulations. Critical Infrastructure owners and operators are uniquely positioned to manage risks to their individual operations and assets, and to determine effective strategies to make them more secure and resilient"; b) Critical Infrastructure must be secure and able to withstand and rapidly recover from all hazards. Achieving this will require integration with the national preparedness system across prevention, protection, mitigation, response, and recovery" Presidential Policy Directive (2013).

The term "critical infrastructure" has the definition given to that term in section 1016(e) of the USA PATRIOT Act of 2001 (42 U.S.C. 5195c (e)) - the term ''critical infrastructure'' means systems and assets, whether physical or virtual, so vital to the United States that the incapacity or destruction of such systems and assets would have a debilitating impact on security, national economic security, national public health or safety, or any combination of those matters".

The National Infrastructure Protection Plan (NIPP) provides the coordinated approach that is used to establish national priorities, goals, and requirements for protecting and ensuring the continuity of Critical Infrastructure and key resources (CIKR) protection so that federal resources are applied in the most effective and efficient manner to reduce vulnerability, deter threats, and minimize the consequences of attacks and other incidents. It establishes the overarching concepts relevant to all CIKR sectors identified under the authority of Homeland Security Presidential Directive 7, and addresses the physical, cyber, and human considerations required for effective implementation of protective programs and resiliency strategies.

The National Infrastructure Protection Plan (NIPP) specifies the key initiatives, milestones, and metrics required to achieve the Nation's Critical Infrastructure and Key Resources (CIKR) protection mission. It sets forth a comprehensive risk management framework and clearly defined roles and responsibilities for the Department of Homeland Security, Federal Sector-Specific Agencies (SSAs), and other Federal, State, local, tribal, territorial, and private sector partners. The cornerstone of the National Infrastructure Protection Plan (NIPP) is its risk management framework establishing the processes for combining consequence, vulnerability, and threat information to produce a comprehensive, systematic, and rational assessment of national or sector risk.

There are 16 critical infrastructure sectors (Cybersecurity and Infrastructure Security Agency. (2022) whose assets, systems, and networks, whether physical or virtual, are considered so vital to the United States:

(i) Chemical Sector. This sector is an integral component of the U.S. economy that manufactures, stores, uses, and transports potentially dangerous chemicals upon which a wide range of other critical infrastructure sectors rely. Securing these chemicals against growing and evolving threats requires vigilance from both the private and public sector;

(ii) Commercial Facilities Sector. This sector includes a diverse range of sites that draw large crowds of people for shopping, business, entertainment, or lodging. Facilities within the sector operate on the principle of open public access, meaning that the general public can move freely without the deterrent of highly visible security barriers. The majority of these facilities are privately owned and operated, with minimal interaction with the federal government and other regulatory entities;

(iii) Communications Sector. This sector is an integral component of the U.S. economy, underlying the operations of all businesses, public safety organizations, and government. Presidential Policy Directive 21 identifies the Communications Sector as critical because it provides an "enabling function" across all critical infrastructure sectors;

(iv) Critical Manufacturing Sector. This sector is crucial to the economic prosperity and continuity of the United States. A direct attack on or disruption of certain elements of the manufacturing industry could disrupt essential functions at the national level and across multiple critical infrastructure sectors;

(v) Dams Sector. This sector delivers critical water retention and control services in the United States, including hydroelectric power generation, municipal and industrial water supplies, agricultural irrigation, sediment and flood control, river navigation for inland bulk shipping, industrial waste management, and recreation. Its key services support multiple critical infrastructure sectors and industries. Dams Sector assets irrigate at least 10 percent of U.S. cropland, help protect more than 43 percent of the U.S. population from flooding, and generate about 60 percent of electricity in the Pacific Northwest.

(vi) Defense Industrial Base Sector. This sector is the worldwide industrial complex that enables research and development, as well as design, production, delivery, and maintenance of military weapons systems, subsystems, and components or parts, to meet U.S. military requirements. The Defense Industrial Base partnership consists of Department of Defense components, more than 100,000 Defense Industrial Base companies and their subcontractors who perform under contract to the Department of Defense, companies providing incidental materials and services to the Department of Defense, and government-owned/contractor-operated and government-owned/government-operated facilities. Defense Industrial Base companies include domestic and foreign entities, with production assets located in many countries. The sector provides products and services that are essential to mobilize, deploy, and sustain military operations. The Defense Industrial Base Sector does not include the commercial infrastructure of providers of services such as power, communications, transportation, or utilities that the Department of Defense uses to meet military operational requirements. These commercial infrastructure assets are addressed by other Sector Risk Management Agencies;

(vii) Emergency Services Sector (ESS). This sector is a community of millions of highly-skilled, trained personnel, along with the physical and cyber resources, that provide a wide range of prevention, preparedness, response, and recovery services during both day-to-day operations and incident response. The ESS includes geographically distributed facilities and equipment in both paid and volunteer capacities organized primarily at the federal, state, local, tribal, and territorial levels of government, such as city police departments and fire stations, county sheriff's offices, Department of Defense police and fire departments, and town public works departments. The ESS also includes private sector resources, such as industrial fire departments, private security organizations, and private emergency medical services providers;

(viii) Energy Sector. This sector as uniquely critical because it provides an "enabling function" across all critical infrastructure sectors. The energy infrastructure is divided into three interrelated segments: electricity, oil, and natural gas;

(ix) Financial Services Sector. This sector includes thousands of depository institutions, providers of investment products, insurance companies, other credit and financing organizations, and the providers of the critical financial utilities and services that support these functions;

(x) The Food and Agriculture Sector. This sector is almost entirely under private ownership and is composed of an estimated 2.1 million farms, 935,000 restaurants, and more than 200,000 registered food manufacturing, processing, and storage facilities. This sector accounts for roughly one-fifth of the nation's economic activity;

(xi) The Government Facilities Sector. This sector includes a wide variety of buildings, located in the United States and overseas, that are owned or leased by federal, state, local, and tribal governments;

(xii) The Healthcare and Public Health Sector. This sector protects all sectors of the economy from hazards such as terrorism, infectious disease outbreaks, and natural disasters;

(xiii) The Information Technology Sector. This sector is central to the nation's security, economy, and public health and safety as businesses, governments, academia, and private citizens are increasingly dependent upon Information Technology Sector functions;

(xiv) The Nuclear Reactors, Materials, and Waste Sector. This sector includes: 99 Active and 18 Decommissioning Power Reactors in 30 states that generate nearly 20 percent of the nation's electricity;

(xv) The Transportation Systems Sector. This sector consists of seven key subsectors, or modes: Aviation; Highway and Motor Carrier; Maritime Transportation System; Mass Transit and Passenger Rail; Pipeline Systems; Freight Rail; Postal and Shipping;

(xvi) The Water and Wastewater Systems Sector.

5. Conclusions.

Although the term "Critical Infrastructure" is relatively new, in today's turbulent security environment and dynamic development of technologies and artificial intelligence, as well as in existing hybrid threats nature, understanding of Critical Infrastructure concept moves within the framework, according to which Critical Infrastructure might be considered as a set of all objects, systems, networks and functions (whether physical or virtual, private or public) effectiveness of which is of great importance for maintaining the development of every society and the general functioning of the state.

Critical Infrastructure now rarely exist or function in isolation, rather, they are becoming more tightly coupled, interconnected and interacted that creates a complex multisystem - a system-of-systems which generally includes sectors related to chemicals, communications, defence, emergency services, energy, finance, food and water, government, health, space, transport and any other sectors that might be vital for state security.

REFERENCES

1. Agrafiotis, I., Nurse, J. R. C., Goldsmith, M., Creese, S., and Upton. D. (2018). "A taxonomy of cyber-harms: Defining the impacts of cyber-attacks and understanding how they propagate," J. Cybersecurity, vol. 0, no. 0, pp. 1–15, 2018.
2. Alcaraz, C. and Zeadally, S. (2015). "Critical infrastructure protection: Requirements and challenges for the 21st century," Int. J. Crit. Infrastruct. Prot., vol. 8, pp. 53–66, 2015.
3. Alsubaie. A., Alutaibi. K, and Marti. J. (2016). "Resilience Assessment of Interdependent Critical Infrastructure," Crit. Inf. Infrastructures Secur. CRITIS 2015. Lect. Notes Comput. Sci., vol. 9578. 2016.
4. Bearse. R.S. (2021). An Overview of Critical Infrastructure, its Importance, and Key Policy Terms. For 2021 NATO COEDAT TEC. https://www.tmmm.tsk.tr/TEC2021/presentation/Ronald%20BEARSE.pdf
5. Bloomfield, R. E., Popov, P., Salako, K., Stankovic, V., and Wright, D. (2017). "Preliminary interdependency analysis: An approach to support critical-infrastructure risk-assessment," Reliab. Eng. Syst. Saf., vol. 167, no. March, 2017.
6. Bundesamt für Bevölkerungsschutz und Katastrophenhilfe. (2021). Was sind Kritische Infrastrukturen und warum sind sie so wichtig? https://www.bbk.bund.de/DE/Themen/Kritische-Infrastrukturen/kritische-infrastrukturen_node.html
7. Commission Staff Working Document on the Review of the European Programme for Critical Infrastructure Protection (EPCIP). Brussels, 22.6.2012 SWD (2012) 190 final.
8. 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.
9. Cook, A., Janicke, H., Smith, R., and Maglaras, L. (2017). "The industrial control system cyber defence triage process," Comput. Secur., vol. 70, pp. 467–481, 2017.
10. CPNI. (2021), Critical National Infrastructure, https://www.cpni.gov.uk/critical-national-infrastructure-0NCSC. (2021), What is Critical National Infrastructure (CNI)? https://www.ncsc.gov.uk/section/private-sector-cni/cni#section_1
11. Cybersecurity and Infrastructure Security Agency. (2022). Critical Infrastructure Sectors. https://www.cisa.gov/critical-infrastructure-sectors
12. Decrees No. 179 and 180 of 18 and 23 December 2020: the new "Golden Power" Regulation, Ashurst Milan | Private Equity Update 18 JAN 2021.
13. Eismann, C. (2009), Trends in Critical Infrastructure Protection in Germany, DOI: 10.2478/tvsbses-2014-0008
14. Engdahl, E-M. (2016), The European Programme for Critical Infrastructure Protection, Gas Infrastructure Europe.

15. EO 13010: Critical Infrastructure Protection. Homeland Security Digital Library. https://www.hsdl.org/?abstract&did=1613
16. European Commission. (2004), Communication on Critical Infrastructure Protection in the fight against terrorism
17. European Commission. (2005), Green Paper on a European Programme for Critical Infrastructure Protection.
18. European Commission. (2006), European Programme for Critical Infrastructure Protection.
19. 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.
20. 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.
21. European Commission. (2014), ECHO Factsheet – Disaster Risk Management – 2014
22. European Commission. (2014). The post 2015 Hyogo Framework for Action: Managing risks to achieve resilience
23. European Commission. (2017), Commission staff working document on assessment of the EU 2013 Cybersecurity Strategy
24. 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
25. European Environment Agency. (2011), Mapping the impacts of natural hazards and technological accidents in Europe (Technical report No 13/2010),
26. 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
27. Federal Ministry of the Interior. (2009), National Strategy for Critical Infrastructure Protection (CIP Strategy). https://www.bmi.bund.de/SharedDocs/downloads/EN/publikationen/2009/kritis_englisch.pdf?__blob=publicationFile&v=1
28. Government of Canada. (2021), National Strategy for Critical Infrastructure, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx
29. Government of Canada. (2021), National Strategy for Critical Infrastructure, https://www.publicsafety.gc.ca/cnt/rsrcs/pblctns/srtg-crtcl-nfrstrctr/index-en.aspx
30. Grigalashvili, V. (2021). Conceptual Review of the United States Critical Infrastructure Architecture: Policy, Law and Administration. DOI: https://doi.org/10.31435/rsglobal_conf/25042021/7522
31. Grigalashvili, V. (2021). Conceptual Review of the European Union Critical Infrastructure Architecture: Policy, Law and Administration. DOI: https://doi.org/10.31435/rsglobal_conf/25052021/7562
32. Homeland Security Presidential Directive 7: Critical Infrastructure Identification, Prioritisation, and Protection https://www.cisa.gov/homeland-securitypresidential-directive-7
33. Haemmerli, B. and Renda, A. (2010). Protecting Critical Infrastructure in the EU, Brussels: Centre for European Policy Studies
34. Information Security Policy Council, (2009). The Second Action Plan on Information Security Measures for Critical Infrastructures, Japan National Security Information Center, at 10 (Feb. 3 2009)
35. 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
36. Joint Research Centre of the European Commission. (2017). The ERNCIP Project Platform
37. Kudrjashov, V. (2021). Critical infrastructure and its functions. DOI: 10.33763/npndfi2021.02.005
38. Lazari, A. (2014), European Critical Infrastructure Protection, Springer International Publishing Switzerland
39. 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
40. Laugé, A., Hernantes, J., and Sarriegi, J. M. (2015). "Critical infrastructure dependencies: A holistic, dynamic and quantitative approach," Int. J. Crit. Infrastruct. Prot., vol. 8, pp. 16–23, 2015
41. Maple, C. (2017). "Security and privacy in the internet of things," J. Cyber Policy, vol. 2, no. 2, pp. 155–184, 2017
42. 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
43. Minister of Public Safety and Emergency. (2021), National Cross Sector Forum 2021-2023 Action Plan for Critical Infrastructure
44. Mitrevska M., Mileski T., Mikac R., (2019) Critical Infrastructure Concept and Security Challenges
45. National Infrastructure Protection Plan https://www.dhs.gov/xlibrary/assets/nipp_consolidated_snapshot.pdf
46. NISC. (2021). Commitment to a Free, Fair and Secure Cyberspace. https://www.nisc.go.jp/eng/index.html#sec4
47. Oliva, G., Panzieri, S., and Setola, R. (2012). "Modeling and simulation of critical infrastructures," WIT Trans. State Art Sci. Eng., vol. 54, pp. 39–56, 2012

48. Pescaroli, G. and Alexander, D. (2016). "Critical infrastructure, panarchies and the vulnerability paths of cascading disasters," Nat. Hazards, vol. 82, no. 1, pp. 175–192, 2016
49. Petersen, L, Tilman, Kuhn T., Arhold. C., Wienke, T. (2002), Broadened scope of Critical Infrastructure Regulation will increase FDI screening in Germany
50. Presidential Policy Directive. (2013). Presidential Policy Directive - Critical Infrastructure Security and Resilience. https://obamawhitehouse.archives.gov/the-press-office/2013/02/12/presidential-policy-directive-criticalinfrastructure-security-and-resil 42 U.S. Code § 5195c - Critical infrastructures protection
51. Pursiainen, C. (2018). "Critical infrastructure resilience: A Nordic model in the making?" Int. J. Disaster Risk Reduct., vol. 27, no. 653390, pp. 632–641, 2018
52. Rehak, D., Senovsky, P., and Slivkova, S. (2018). "Resilience of Critical Infrastructure Elements and Its Main Factors," Systems, vol. 6, no. 2, p. 21, 2018
53. Setola, R., Luiijf, E., and Theocharidou, M. (2016). "Critical Infrastructures, Protection and Resilience," Springer Cham, 2016
54. SGDCN. (2017), The Critical Infrastructure Protection in France. http://www.sgdsn.gouv.fr/uploads/2017/03/plaquette-saiv-anglais.pdf
55. Stergiopoulos, G., Vasilellis, E., Lykou, G., Kotzanikolaou, P., and Gritzalis. D. (2016). "Critical Infrastructure Protection Tools: Classification and Comparison," in Critical Infrastructure Protection X. ICCIP 2016. IFIP Advances in Information and Communication Technology, Vol 485., M. Rice and S. Shenoi, Eds. Springer Cham, 2016
56. The French White Paper on Defence and National Security. (2013), https://koziej.pl/wp-content/uploads/2015/07/France_White_Paper_English2008.pdf
57. UK Parliament. (2021), Critical National Infrastructure, https://committees.parliament.uk/committee/111/national-security-strategy- joint-committee/news/159219/critical-national-infrastructure/