Critical infrastructures development aligned with European union procedures. Evidence from Romania

Ionut-Catalin SAVU

University Politehnica of Bucharest, Bucharest, Romania
savu_ionutcatalin@yahoo.com

Gheorghe MILITARU

University Politehnica of Bucharest, Bucharest, Romania
gheorghe.militaru@upb.ro

Abstract. *This paper aims to emphasize the significance of the Critical Infrastructures in a general European context, as well as a divided approach on the Romanian types of critical infrastructures and their specifics.*

The main topics approached in the article are analyzing the processes undergone to identify and regulate Critical Infrastructures in the field of Transportation, Energy production, Water and sanitation, Nuclear Industry in Romania, as well as to adapt and standardize the Romanian legislation to the legislation of the European Union.

Although in the international literature the Critical Infrastructures are fully covered, the Romanian literature is scarce and not unified, due to the fact the Critical Infrastructure notion is new and in ongoing development.

The source that legislates which infrastructures are considered of critical importance in Romania is the emergency ordinance 98/2010, that has been repeatedly altered and is still subjected to critique and amendment attempts.

The author, as security representative of a private infrastructure in the energy field, proposes completions of the procedures that determine the criticality of an infrastructure in the energy field through the ACIS methodology.

There was proposed a set of directions for the Romanian Critical Infrastructures alignment, with the rules introduced by the European Critical Infrastructure Protection Program, and, as well, adaptations of the requirements of the European Commission in relation to the Council Directive no. 2008/114 / EC.

We were aiming to strengthen and increase the resilience of Romanian Critical Infrastructures, making them more efficient, smart and robust.

Keywords: Critical infrastructure, EC Council Directive, Critical Infrastructure Protection, European Critical Infrastructure Protection Program, ACIS Criticality Matrix.

Introduction

Critical infrastructure is an element, system or component thereof which is essential to maintaining the vital functions of society, health, safety, security, social or economic well-being of individuals and whose disruption or destruction would have a significant impact at national level as a result of the inability to maintain those functions.

It is considered that an infrastructure is critical when it has a strategic position in the general system and has a high number of interdependencies with other components of the system or other infrastructures.

Council Directive 2008/114 / EC (The Council of the European Union, 2008), which legislates the identification and designation of European critical infrastructures and the assessment

of the need to improve their protection, adopted on December 8, 2008, gives the following definition in art. 2, paragraph. a: "Critical infrastructure refers to those objectives, networks, services, physical activities and IT resources that are so vital to nations that their decommissioning or destruction can have a serious impact on health, safety, security or economic well-being of citizens, or on the effective functioning of the governing act of the Member States ”.

There are cited a number of Critical Infrastructures of the Country, as, Infrastructures of the national energy system networks, railway networks with all related structures, command-control and traffic control systems etc.; the national air transport network, with all related infrastructures; shipping infrastructures, national communications, national alert network infrastructures; networks of national oil and gas pipelines or that are part of continental transport networks, etc. (Hopkin, P., 2018).

The source that legislates which infrastructures are considered of critical importance in Romania is the emergency ordinance 98/2010 (Guvernul României, 2010).

The responsibility for organizing the implementation of specific legislation rests with the Ministry of Internal Affairs, through the National Center for Coordination of Critical Infrastructure Protection (CNCPIC), with which public and private operators collaborate to improve the protection of Critical Infrastructures in accordance with European Commission requirements.

The author, as security representative of a private infrastructure in the energy field, proposes completions of the procedures that determine the criticality of an infrastructure through the ACIS methodology applied to Critical Infrastructures (C.I) in the energy field.

Critical Infrastructure Protection (CIP) was as well analyzed and measures that were proposed aimed at ensuring the functionality, continuity and integrity of National and European Critical Infrastructures (NCI and ECI) in order to discourage, diminish and neutralize a threat, risk or vulnerability.

The emphasis was on ensuring the protection of classified information in the CIP domain, implementing Critical Infrastructure Operators Security Plans, setting exercises, reports, re-evaluations and updates of documents drawn up on the Critical Infrastructure protection.

There were proposed as well, a set of directions of alignment for the Critical Infrastructures of Romania with the rules introduced by the European Critical Infrastructure Protection Program and, as well, adaptations of the requirements of the European Commission in relation to the Council Directive no. 2008/114 / EC.

Literature review

Although Romania is still a novice in the field of Critical Infrastructures, with the passage of time there has been a transition to the adoption of EU and NATO working methods. Thus, the evolution was gradual, at the beginning of the 2000s, Romania's national security strategy was to define the term "vulnerability" without providing details on the content of the term or the infrastructures referred to.

Given the fact Critical Infrastructures management has over time been a national priority, a number of papers have been analyzed including the National Defense Strategy Guidance – (NDS Guidance). The aim being to emphasize the importance and place of Critical Infrastructures “for the existence and the development of the society, targeting both the citizen and state institutions” (Supreme Council of National Defence no. 128, 2015).

We tried to propose way to adapt the Romanian C.I. to the so-called safety culture, which represents “the entirety of values, norms, attitudes and actions that determine the understanding

and the implementation at the society level of the concept of security and the derived concepts: national security, international security, collective security, insecurity, security policy, etc.” (Apud Ferucio Botti, 1995).

The necessity to elaborate a critical infrastructure systemic study regarding the designation, development and protection of CIs results from the operational complexity of the responsible factors and the connections that the CIs have with other CIs, governments institutions and citizens.

Thus, a Critical Infrastructure cannot exist isolated and plans for development and protection must be conceived in the right context. Defining the right context can be assimilated to describing the operational environment where the concerned infrastructure is located or where it establishes interactions with other entities.

This may be a difficult objective to achieve and it involves developing the security plan of the operator/ owner of a critical infrastructure. The security plan of the operator (PSO) has been addressed further in the paper.

In order to develop the project of adaptation and amendment of the European legislation in order to suit the specifics of the Romanian CIs, we also took into account the five supporting pillars of the protection framework developed by the European Commission (European Commission, 2009).

The five European principles from which we developed the legislation amendments are Readiness and prevention, Detection and response, Recovery after incident and mitigation, International cooperation, Criteria for the information and communications technology (ICT) (European Commission, 2020).

Defining the operational environment involves describing the circumstances, the conditions, and the factors that directly or indirectly influence the employment of the response capabilities of the infrastructure in question. (Drack, 2009) Further on, we intend to analyze the most relevant issues regarding the conceptual integration of the systemic approach to an operator identified as a critical infrastructure.

The C.S.A.T. no. 62/2006 Decision on the National Security Strategy of Romania (Consiliul de Aparare al Tarii, 2006) makes an enumeration of the risks and vulnerabilities related to C.I and mentioning the dangers that may be generated by the existence of a poorly developed and insufficiently protected infrastructure.

The interest for the Critical Infrastructure field increased over the years and we tried to deepen and define as detailed as possible the functioning of C.I, relative to the specific conditions existing in our country. At national level, this desideratum materialized through the adoption of OUG 98/2010, on the identification, designation and protection of critical infrastructures, an ordinance (Guvernul Romaniei, 2010) that was amended by the proposed Law for amending and supplementing the Government Emergency Ordinance no. 98/2010 (Parlamentul Romaniei, 2018).

In the national context, the critical infrastructure is defined in art. 3 lit. as "National Critical Infrastructure", hereinafter referred to as NCI - an element, system or component thereof, located in the national territory, which is essential for maintaining the vital functions of society, health, safety, security, social welfare or economic development of persons and whose disruption or destruction would have a significant impact at national level as a result of the inability to maintain those functions".

The field of applicability of the concept of Critical Infrastructure is established in the Law amending art. 2 paragraph 4 from OUG 98, 2010. "The provisions of this emergency ordinance apply to all legal persons of public or private law that carry out activities and provide essential

services of national interest in the sectors and subsectors provided in annex no. 1." (Guvernul Romaniei, 2010).

This strategy shall set out new strategic objectives and measures and shall contain the proposed elements:

Regarding cross-border and cross-sectoral interdependencies each member state shall set strategic objectives and priorities.

All parties involved should work together in the implementation of the strategy and should develop a governance framework to reach the strategic objectives and priorities

An analysis of the measures taken to enhance the overall resilience of critical Infrastructures including national risk assessment, the identification of critical infrastructures and the measures taken to protect and prevent.

Each Member State should complete a list of critical infrastructures that should be informed about their status as a critical infrastructure in a fixed period (European Commission, 2020).

Methodology

The authors have tried to analyze the subject of Critical Infrastructures accordingly with specialized literature in comparison with the states with tradition in Critical Infrastructures protection, such as the USA, Canada and western European countries.

A classification of critical infrastructures in Romania has been proposed based on the documents that legislate and regulate this type of infrastructure (OUG 98 and Council Directive 2008/114).

The criticality of CIs was analyzed using a matrix determined through the ACIS method, developed by BSI KRITIS (BSI, 2004) in Germany, and adapted for existing processes in an energy C.I.

The adaptation of the ACIS methodology was performed by consulting a group of specialists in the nuclear-energy field, which set the failure probability and the degree of damage of each process that affects a sector or more sectors of a critical infrastructure. Their expertise of the effects of failure of the process must be recorded and the criticality matrix developed. Once the most dangerous processes of the critical infrastructures in the field of energy have been established, they must be aligned with the 114 EU directive and with the internal policies specific to the reference country. Thus, in this paper proposals have been made to amend and supplement Council Directive 2008/114 / EC of 8 December 2008.

A comparative analysis of the legislation in force with the European one was used, and amendments to these directives were proposed. In conclusion strategic objectives were set for critical infrastructures and articles 2, 3, 5, 6, 8, 9 from Council Directive 2008/114 / EC of 8 December 2008 were modified or completed with proposals.

Results and discussions

A comparative analysis between European Union and Romanian legislation has been carried out in order to eliminate differences that can lead to vulnerabilities.

A new method for C.I. criticality determination has been elaborated. It works creating a criticality matrix that analyzes the processes that take place within the infrastructure, and their interrelationship.

Thus, the most vulnerable sectors of an infrastructure are determined, their number can be quantified and targeted measures can be taken to limit vulnerabilities and improve protection for C.I.

A plan, based on four directions of alignment of the Critical Infrastructures in Romania with the rules introduced by the European Critical Infrastructure Protection Program in order to strengthen and increase the efficiency of critical infrastructures, has been proposed. It was aimed at improving the way of preparation, response and recovery in the event of C.I. threats and attacks.

There were proposed a set of directions of alignment of the Critical Infrastructures in Romania with the rules introduced by the European Critical Infrastructure Protection Program and, as well, adaptations of the requirements of the European Commission in relation to the Council Directive no. 2008/114 / EC. We were aiming to strengthen and increase the resilience of Romanian Critical Infrastructures, making them more efficient, smart and robust.

The ACIS methodology applied in criticality determination

By definition, a Critical Infrastructure is an organization or institution that is important in the state's economy, and thus the Critical Infrastructure failure or its poor functioning will generate serious security and safety trade and logistics issues. Poor functioning will also interfere with other Critical Infrastructures, the whole system being a network, where the Critical Infrastructure is a knot.

Developed in Germany, the ACIS Methodology (BSI, 2004) proposes a different approach to critical infrastructure protection, based on the relationship between risk analysis and criticality assessment.

In the case of Critical Infrastructures, a typical risk analysis based on cataloging in objects, threats, vulnerabilities and probabilities is difficult to use because there is not enough statistical data.

This is a positive thing however, with the hope that there will not be enough catastrophes or terrorist attacks that we can have enough statistical data. That is why in practice the expert's opinions are mainly used.

That is why the ACIS method aims to assess the criticality. It is necessary to clarify the distinction between the terms "critical" and "criticality".

Figure 1. Criticality assessment

Source: Authors' own research.

In order to make a detailed analysis of a Critical Infrastructure, it is necessary to divide it into sectors as detailed and descriptive as possible and as well the sectors should be divided into processes or products. The more branches there are, the more complex the matrix of criticality. Also, the sectors and processes considered redundant for the process must be eliminated. Criticality for each process calculates a combination of effects and failure probabilities (BSI, 2004).

With the criticality of each process known, you can create a matrix, in which to set processes and sectors, in order to obtain a critical area for each of the sectors and products that make up the Critical Infrastructure.

Figure 2. The ACIS Criticality Matrix

Source: Authors' own research.

The smart development objective must be achieved with efforts of the parts involved in the field and should aim at increasing the protection of the critical infrastructure in Romania through actions aimed at:

Highlighting all existing and anticipated risks while identifying critical elements and processes;

Determination of the sectors subsectors and processes criticality;

Developing a criticality matrix for each infrastructure;

Reducing dysfunctions that can affect the stability and optimal operation of critical services with critical infrastructure support by implementing proactive measures within an effective risk management system;

Increasing the level of expertise in the field by constantly updating the risk analyzes, including through comparative evaluations with specific situations manifested in the territory of other states, transposing these results into national standards (Elky, 2006).

Knowing the criticality matrix for an CI, our mission to ensure both the informatic and the physical protection of the CI is becoming less demanding. Although it's division is only scholastic, in the following rows we have presented the main measures the Romanian governmental bodies has taken in order to insure the informatics systems protection and the physical protection of the Romanian CIs.

Measures to ensure the physical protection of Critical Infrastructures

The National System for Terrorism Prevention and Combating (SNPCT) is responsible for insuring physical protection for NCIs and is a branch Romanian Security Service-SRI (SRI, 2012). Organization responsible for the security of important establishments, their measures shall be applied gradually by security-prone services, identified on the basis of risk-specific information and assessments and may be coordinating or actionable, namely:

Counterterrorism intervention, in the event of a terrorist attack - in the strict competence of the SRI and with the support of other forces of SNPCT members;

Ensuring anti-terrorist anti-counter-terrorism control and counter-terrorism protection at civil airports - under the SRI's competence.

Preventing and combating terrorism – one of the most important threats to critical infrastructures - is carried out in accordance with the provisions of the domestic legislation, the international conventions to which Romania is a party, as well as of international regulations. The specific attributions in the field are provided in internal normative acts.

In Romania, the establishment of the CYBERINT National Center in 2008 is simultaneously the collaboration platform of the institutions within the National Security System and the cooperation interface with similar structures within NATO (Ruehle, 2009).

Measures to ensure the informatics systems protection of critical infrastructures

Accession to the European Critical Infrastructure Protection Program (PEPIC)

The European Program for Critical Infrastructure Protection mentioned at European level 11 sectors such as: Energy System, Information and Communication Technologies; Water supply; Food, Health, Financial Defense, orders, public and national security administration

The improvements in critical infrastructures were designed in conformity with 4 strategic objectives stated by the EU.

Strategic Objective 1 – Integration and Integrated Application of Procedures for Identification, Designation and Protection of National and European Critical Infrastructures (Vitorino, 2004).

Directions for action:

Establishment of sectors criteria and associated thresholds taking into account the characteristics of individual sectors of critical Infrastructures Establishment of thresholds within cross-sectors criteria depending on the severity of the impact of disruption or destruction of a particular infrastructure;

Developing common methodologies for identifying and classifying threats, threats and vulnerabilities related to infrastructure elements (Vitorino, 2004).

The strategic objective no. 2 – Set up and make operational the national early warning system by integrating all existing information, organizational capabilities and extensions.

Directions for action:

Achieving an informational flow of expertise / exchanges of good practices (uniformly and efficiently), while developing the capacity to adapt critical infrastructure protection strategies in relation to developments in national and macro-regional risk factors (Apud Dediu, 2006).

Nationally implement a proper communication mechanism between the responsible national authorities and security liaison officers or their equivalents in order to streamline the exchange of relevant information on the risks and threats identified in relation to those critical infrastructures.

Elaboration of computer applications for modeling and simulation of the functioning and establishment of interdependencies of critical infrastructures, in order to achieve a decision-making model, to reduce the vulnerabilities and to increase the resilience capacity of the population / society / state institutions *at local, regional, national and international level* (Rhee, 2005).

The strategic objective no. 3 – Decreasing the vulnerability of critical infrastructures (STS)

Directions for action:

Revision of quality standards, adapting protection mechanisms, identifying and counteracting hazards, raising redundancy levels, increasing modularity.

Efficiency of activities and actions by eliminating excessive bureaucracy, interferences in the normal flow of information and decision, information leaks, unjustified resource consumption, disparity of liability in the event of occurrence of incidents.

Creating "data banks" to collect and process critical infrastructure data as well as case studies, learned manuals (Crouhy, 2014).

Strategic Objective 4 – Development of cooperation relations at national, regional and international level

Directions for action:

Implementation of the legislative and operational measures that arise (on the protection of critical infrastructure) from the membership of the EU and the North Atlantic Alliance (Administrația Prezidențială București, 2015).

The process of identifying and designating National Critical Infrastructures (NCI) within the energy sector

The identification of NCI is relatively difficult because in our country the concept of Critical Infrastructure is relatively new and is made on the basis of the emergency ordinance OUG 98, annex 2 (Guvernul României, 2010) by the responsible public authorities. They identify potential CNIs that meet sectoral and cross-sectoral criteria.

To this pre-existing legislation is added the legislation of Council Directive 2008/114 (The Council of the European Union, 2008), to which Romania aligns and which it adapts according to the specifics of the critical infrastructures in Romania.

The sectoral criteria and the related critical thresholds, defined according to the severity of the impact of the disruption or destruction of a certain infrastructure, are established by order of the heads of the public authorities responsible, according to the areas of responsibility, for NCI.

The intersectoral criteria underlying the identification of NCI are the following:

The criterion regarding the victims, evaluated according to the possible number of deaths or injuries;

The criterion on economic effects, assessed according to the importance of economic losses and / or degradation of products or services, including possible effects on the environment;

The criterion on the effect on the population, assessed according to the impact on their confidence, physical suffering or disruption of daily life, including the loss of essential services.

To these criteria we propose to add the intrinsic criticality by the ACIS Method for energy infrastructures, developed extensively previously in this article.

Designation of NCI

Following the process of identifying NCI potentials, the responsible public authorities propose to the Ministry of Internal Affairs (M.A.I), through National Critical Infrastructure Protection Coordination Center (CNCPIC), the designation of NCI. The appointment of the NCI is approved by a decision of the Government.

The M.A.I., through CNCPIC, informs the European Commission annually on the number of CEIs designated in each sector, as well as on the number of Member States dependent on each CEI designated.

The Ministry of Interior, through CNCPIC, following the process of identifying CEI potentials, informs the member states that may be significantly influenced by a CEI presence regarding its identity and the reasons for designating the respective infrastructure as a potential CEI.

Council Directive no. 2008/114 / EC (The Council of the European Union, 2008), identifies as main parts of the necessary organizational framework the security plan of the operator and the liaison officer for security. The operator's security plan includes the identification of the main assets, the risk assessment, as well as the selection and prioritization of measures and procedures to be established in all critical infrastructures, and the role of the security liaison officer is to improve communication and cooperation with state authorities Critical Infrastructures.

Proposals to amend and supplement Council Directive 2008/114 / EC of 8 December 2008 on the identification and designation of European Critical Infrastructure and to assess the need to improve their protection of nuclear energy infrastructure

Amendment and completion of Article 2 (e): "protection" means the unitary set of processes and activities organized and conducted to ensure the functionality, continuity of services and integrity of ICN / ICE to discourage, mitigate and neutralize a threat, risk or vulnerability by identifying, implementing and the maintenance of security, organizational, technical, procedural and other measures resulting from the conduct of risk management processes.

Addition of Article 8 by the addition of a new paragraph on the CIWIN Critical Infrastructure Alert Network:

Define the critical infrastructure alert network called CIWIN and add data related to it as well as possible prevention actions, so that CIWIN can provide the necessary assistance to both the competent authorities and the critical infrastructure operators in the Member States.

Modification and completion of art. 2 by adding a new paragraph with the purpose of defining the concept of resilience.

IC / ICE resilience – its ability to absorb the initial shock, to adapt to a hazard or threat and to recover from it in order to continue to provide the essential services of society in the Member States.

Completion of art. 3 by adding a new paragraph regarding the obligation to go through the process of identification and designation of critical infrastructure.

The legal persons of public or private law that carry out activities and provide essential services in the sectors and subsectors provided in annex no. 1 have the obligation to participate, at the request of the competent national authorities, in the process of identification and designation of the CI.

Completion of Article 3 by adding a new paragraph on the need to consult potential or designated critical infrastructure operators.

The competent authorities of the Member States shall consult with potential or designated critical infrastructure operators in order to define or update the sectoral criteria, as well as to develop guidelines for the application of those criteria.

Completion of Article 6, by adding a new paragraph on OLS (security liaison officers) training / preparation.

OLS designated among the competent national authorities and CI operators participate in training programs in the field of critical infrastructure protection.

Completion of Article 5 par.1 by adding a new paragraph on the classification of the PSO (Operator Security Plan).

The confidentiality, integrity and availability of PSO information is protected by classifying the document in one of the four existing levels of secrecy at European level: Restreint UE / Confidentiel UE / Secret UE / Très Secret UE / Eu Top Secret. Member States will protect EU information classified according to national equivalents of secrecy levels.

Completion of Article 9, par.1 by adding a new paragraph on the protection of information in the field of ICN.

The dissemination of sensitive information is done according to the principle of “the need to know”: both in relation to the responsible authorities, the owners / operators / administrators of NCI/ CEI, as well as with the other member states.

Amendment and completion of Article 9 by adding a new paragraph on support for CI operators:

Each Member State shall support the efforts of critical infrastructure operators to deter, mitigate and neutralize a threat, risk or vulnerability by taking appropriate measures to deduct the investment and operational costs used to install and maintain physical security systems.

Completion of Annex 1 with new ICE sectors and completing the list by updating the ICE sectors.

Conclusion

The paper aimed to analyze the need for Romanian Critical Infrastructures to become “smarter”. Making the infrastructures “smarter” meaning making them greater in operation and use, more adaptive and high-tech.

These smart critical infrastructures should also be “smartly robust” in order to resist extreme threats, such as extreme weather disasters or terrorist attacks.

Making an existing infrastructure “smarter” is attained by making it more complex, but, as well it makes it more vulnerable, as we can easily see in the case of malicious attacks.

In this paper we tried to find practical and theoretical solutions for the problems with the increasing complexity of Critical Infrastructures, so we could improve the resilience of an CI as well as its ability to anticipate, prepare for, adapt and withstand, respond to and recover.

The legislation overview and update proposals were meant in order to select coherently and correctly the critical infrastructures, to grade their importance and to measure their criticality more accurately.

Also, the proposals for amendments to the legislation were brought, so that the country's legislation on energy based C. I. to be standardized, adapted to EU legislation and the specificity of C.I.s in Romania.

Thus, the cooperation within the European Community regarding the C.I. in the energy field is promoted, because CIs are mostly cross-border objectives, that leading to their management optimization, and a more efficient protection of the Critical Infrastructures.

References

- Administrația Prezidențială București (2015). *Strategia Nationala de aparare a tarii* 2015, p. 4.
- Apud Dediu, G. (2006). *Protecția infrastructurilor critice – o nouă provocare*, Bucharest, Editura Polirom, 22-26.
- BSI (Bundesamt für Sicherheit in der Informationstechnik) (2004). Analysis of Critical Infrastructures-, the ACIS Methodology - Analysis of Critical Infrastructural Sectors. BSI KRITIS, (4), Retrieved from https://www.bsi.bund.de/SharedDocs/Downloads/EN/BSI/Kritis/acis_paper_en_pdf.pdf?__blob=publicationFile.
- Consiliul de Aparare a Tarii (2006). Raportul Consiliului Suprem de Aparare a Tarii privind activitatea desfășurată în anul 2006, *Consiliul De Aparare a Tarii*, Retrieved January 15, 2021, from https://csat.presidency.ro/files/documente/Raport_CSAT_2006_3ro.pdf.
- Crouhy, M., Galai, D., & Mark, R. (2014). *The essentials of risk management*, New York, McGraw-Hill Education, 16-20.
- Elky, S. (2006). *An Introduction to Information System Risk Management*, 75-77.
- European Commission (Brussels, 16.12.2020). Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL on the resilience of critical entities. *EUR-Lex*. Retrieved January 15, 2021, from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2020:829:FIN>.
- Guvernul României (2010). Ordonanța de Urgență nr. 98 din 3 noiembrie 2010 privind identificarea, desemnarea și protecția infrastructurilor critice. *Monitorul Oficial* Nr. 757 Din 12 Noiembrie 2010, Retrieved January 15, 2021, from <http://legislatie.just.ro/Public/DetaliiDocument/123547>.
- Hopkin, P. (2018). *Fundamentals of risk management: Understanding, evaluating and implementing effective risk management*, Vol. 3, p. 77, London, Kogan Page.
- Parlamentul României (2018). Legea nr. 225/2018 pentru modificarea și completarea Ordonanței de urgență a Guvernului nr. 98/2010 privind identificarea, desemnarea și protecția infrastructurilor critice. *Monitorul Oficial, Partea I* Nr. 677 Din 03 August 2018. Retrieved January 15, 2021, from http://www.cdep.ro/pls/legis/legis_pck.http_act?nr=225&an=2018.
- Rhee, M.Y. (2005). *Internet security: Cryptographic principles, algorithms and protocols*. Chichester, Wiley, p. 66.
- Ruehle, M. (2009). Dimensiunea nucleară a terorismului jihadist. *Revista Nato*, p. 2.
- SRI (Serviciul Român de Informații) (2012). Protecția Infrastructurilor Critice. *Direcția Programe De Comunicare SRI*, 38, 62-63. Retrieved January 15, 2021, from <http://docplayer.net/20815324-Serviciul-roman-de-informatii-protectia-infrastructurilor-critice.html>.
- The Council of the European Union (2008). 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, *Official Journal of the European Union*, Retrieved January 15, 2021, from <https://eur-lex.europa.eu/eli/dir/2008/114/oj>.
- Vitorino, A. (2004). Communication from the Commission to the Council and the European Parliament: Critical Infrastructure Protection in the fight against terrorism. *EC (European Commission) Communication*, 2-3, Retrieved January 15, 2021, from <https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=COM:2004:0702:FIN>.
- Supreme Council of National Defence. National Defence Strategy for 2015-2019 (2015). Retrieved February 19, 2021, from <http://csat.presidency.ro/?pag=43>.
- Ferucio Botti, A. (1995). Le concept de géostratégie et son application à la nation italienne dans les théories du général Durando”, in *Stratégie*, p. 129.
- European Commission (2009). Communication of the Commission to the European Parliament, European Council, *European Economic and Social Committee and the Committee of the Regions on critical information infrastructure protection*, Brussels. Retrieved February 19, 2021, from <http://ec.europa.eu/transparency/regdoc/rep/1/2009/RO/1-2009-149-RO-F1-1.Pdf>.
- Drack, M. (2009). Early system approach. *Systems Research and Behavioral Science*, 26(5), 2-3, Retrieved February 19, 2021, from <http://journals.issn.org/index.php/proceedings52nd/article/viewFile/1032/322>.