Acta Universitatis Danubius

JURIDICA

# Concerns at the Level of the European Union for the Protection of Critical Infrastructures

**Oana Elena Iacob**[1]

**Abstract:** Critical infrastructures are of particular importance for the smooth running and global evolution of the entire human society, at the level of all the states that make up the international community. For this reason, it is imperative that they are protected from the risks to which they are exposed and that all measures are taken to prevent and combat them as quickly as possible. This study presents some of the existing concerns in the international context at the level of the European Union in order to identify the benefits that these infrastructures bring to society and the most appropriate ways to protect them, to prevent those major risks to which critical infrastructures are exposed and to combat them, in order to ensure, by doing so, of the smooth running of the Union.

**Keywords:** critical infrastructures; threats; protection; Union and international level

[1] Associate Professor, PhD, Faculty of Law and Administrative Sciences, "Dunărea de Jos" University of Galati, member of the Research Centre of Juridical, Administrative, Social and Political Sciences of "Dunărea de Jos" University of Galati, Romania, Address: 111 Domneasca Str. Galati 800201, Romania, Corresponding author: oana.galateanu@ugal.ro.

## 1. Aspects Concerning Critical Infrastructures

At present, information and communication technology is the pillar of the economic development of all states and is an opportunity of utmost importance that is the foundation of all sectors of the economy. It is the basis of all systems that allow the proper functioning of national economies in areas of major importance such as health, transport, finance[1].

Within this computerized society, the classical borders (in their classical sense) have disappeared and new types of dangers and insecurities have appeared, namely the cyber ones, to which all infrastructures are exposed, that is, according to the definitions of specialists, all those systems made up of material, organizational and informational elements, which belong to a social microsystem and through which the resistance and natural evolution of society can be guaranteed.

Specialists have made a classification of the infrastructures into:

1. ordinary – with which the smooth running of a certain system is ensured;

2. special – with a greater role in the functioning of the systems, which gives them greater effectiveness;

3. critical – those on which the safety and continuity of systems depend.

The terminology "critical infrastructure" is used to highlight any economic institution that functions and provides products of public interest and necessity, which are fundamental to the whole society and whose wear and tear or deterioration would have a decisive effect on the population and the national and international economy (Vivera, 2017, pp. 7-9).

The assessment of an infrastructure or set of infrastructures as *critical* is due to the following aspects[2]:

a) the unique condition, but also the complementarity within the infrastructures of a system or process;

b) the important role they play in the stability, reliability, safety, functionality and in particular in the security of systems;

[1] See http://eur-lex.europa.eu/legal-content/Ro/Txt/, *Joint Communication of the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, EU Cybersecurity Strategy: An Open, Safe and Secure Cyberspace.*

[2] SRI (Romanian Intelligence Service), *Protecția infrastructurilor critice / Protection of Critical Infrastructure*, p. 9.

c) increased vulnerability to direct threats, as well as to those aimed at the processes of which they are part;

d) the sensitivity to the variation of conditions and, in particular, to sudden changes in the situation (Rizea, 2008, p. 7).

At the level of the European Union, Council Directive no. 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of needs to improve their protection, defines critical infrastructures as "*an asset, system or part thereof located in the Member States, which is essential for the maintenance of vital social functions, health, safety, security, social or economic 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 inability to maintain those functions*". [1]

The same Directive defines European critical infrastructure as a "*critical infrastructure located in EU Member States, the disruption or destruction of which would have a significant impact on at least two Member States*" [2], and the protection of critical infrastructures as "*all activities aimed at ensuring the functionality, continuity and integrity of critical infrastructures in order to deter, mitigate and neutralize a threat, risk or vulnerability*". [3]

Operators or owners of critical infrastructures are defined by the same Union normative act as those entities responsible for investments in a certain element, system or component thereof, designated as European critical infrastructure by the Directive to which we refer and/or for their current operation.[4]

## 2. The Risks that the Critical Infrastructures Face

The dangers for these infrastructures are quite numerous, including human errors and omissions that can generate harmful effects in several of their components, technical

[1] Article 2, letter a) of Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.
[2] Article 2, letter b) of Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.
[3] Article 2, letter e) of Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.
[4] Article 2, letter f) of Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

accidents and natural events that can cause great material, human and ecological damage, and aggressions on them.

The features of cyberspace threats are asymmetry, very high dynamics and global nature. They make it difficult to detect and prevent by measures correlative to the effect of the manifestation of risks.

The threats targeting cyberspace critical infrastructures include: the increase in the number of unconventional and disruptive IT networks, the increasing activity of hackers and cyberterrorism (Vivera, 2017, p. 53).

Critical infrastructures are not safe from cyber-attacks, in fact, these attacks are one of the dangers to which these infrastructures are subjected. Specifically, cyber-attacks have as their preferred direction the information systems through which most of the critical infrastructures operate. Attacks involving the IT systems of State institutions or the private sector assimilated to these infrastructures are more difficult to prevent and, for this reason, more serious. They can belong to organized crime groups or they can be started by such groups that aim, in most cases, to acquire pecuniary benefits. However, it is not only such groups that initiate them, but also states can do so as a way of achieving their own political objectives.

Specifically, ensuring a safe and stable environment is necessary for the smooth running of critical infrastructure networks, and protecting them is fundamental to prevent any serious disturbances that could be brought to the normal existence of society.

Certainly, we believe, this awareness is also the reason why in March 2024 an *Act of Cyber Solidarity* was concluded, whereby the Council and the European Parliament reached a provisional agreement to strengthen Europe's security capacity, by adopting a Union Regulation in this regard. The purpose is represented by: consolidating the cooperation, solidarity and capacity of the Union and its member states; detecting cybersecurity threats and incidents; preparing for these incidents and threats; increasing the EU's cyber power; making amendments to the normative acts regarding cybersecurity; creating a high standard of cybersecurity services at common level of the entire EU, by enabling managed security services to be qualified and thereby facilitating their transnational distribution in the interest of citizens and enterprises.

It is desired through adopting this Regulation:

- to support the actions to identify and raise awareness on important or extensively manifested cybersecurity dangers and events;

- to intensify the preparation and protection of critical bodies and basic services such as: public utility services, hospitals;

- to support the creation of a secure digital framework for citizens, and

- to introduce an IT security alert procedure for the purpose of quickly and effectively detecting cyber threats.

The Cybersecurity Alert System is seen as a Europe-wide infrastructure made up of national and transnational cyber hubs across the EU. These hubs are units that have the task of exchanging information, identifying cyber threats and acting as such. It is intended that they will improve the current European context in this field and support the authorities and bodies with relevance in the field to have a more beneficial reaction to essential events. It follows that the official Union's document will be approved by the Council and European Parliament in order to be officially adopted at EU level.

We believe that the drafting of the final texts should also be carried out considering the concerns that currently exist at EU level regarding:

1) The creation of the European Health Data Space, so that all Member States can set up national health data access services based on the My health@EU platform, platform that gives the possibility to securely access databases of public interest. On the creation of this space, a provisional agreement was reached between the European Parliament and the Council of the EU on 15.03.2024.[1]

2) The EU policy programme for the Digital Decade, which aims to be concretely achieved by 2030, which is why strategic investments in critical technologies (including semiconductors and cloud infrastructure) are underway. Collective action by Member States is sought to speed up the digital transformation to achieve the objectives of the Program and it is also sought, at the same time, to find a common direction of the national strategies, beneficial investments in the digital infrastructure and development of innovations.

3) Adopting a new EU legislative framework – a Regulation – whereby to be decided upon a governance on interoperability for the possibility of forming a system of

[1] https://www.caleaeuropeana.ro/ - *The EC report on the Single market and Competitiveness. The digitalization of the EU enterprises and services.*

interoperability remedies targeting the EU public sector, in particular through the creation of regulatory sandboxes.

These achievements aim: to enable public administrations in the EU to modernize together; to establish a new system of collaboration for national public administrations in the EU, with a view to achieve the uninterrupted provision of transnational public services and to find support measures for supporting the modernization and strengthening the exchange of skills and knowledge; to form an interconnected digital public administration system and speed up the digitalization of the European public sector.

The key aspects of the EU Regulation include: consistency with the legal provisions on artificial intelligence and the General Data Protection Regulation (GDPR) on the creation of and participation in interoperability standardization sandboxes.

On 21st February 2024, the European Commission published a package of actions aimed at supporting innovation and the power of digital infrastructures in Europe[1]. The extremely important role that the Commission attaches to actions to ensure a fast, safe and widespread way of connectivity that is fundamental for the integration of technologies such as automated driving, telemedicine, predictive maintenance of buildings, precision agriculture is underlined[2].

In this package, a key initiative is the White Paper entitled "*How to master Europe's digital infrastructure needs*", which addresses today's challenges and highlights possible ways to secure investment, encourage innovation and build a digitalized single market at EU level.

The European Commission also makes a recommendation on the safety and soundness of submarine cable infrastructures by using funding and planning at national and European level. It also underlines the need to support a community of European innovators that is active through a collaborative and connected cyber network, the "*3C network*", which could support the development of integrated infrastructures and collaborative platforms for *cloud* and *edg telco*, and thus promote innovation in various fields.

The European Commission also comes up with proposals regarding the defense of Europe's network and cyber infrastructure, recommending the encouragement of the development and improvement of the protection of fundamental submarine cable

[1] Press release, https://www.caleaeuropeana.ro/, 21.02.2014.
[2] Press release, https://www.caleaeuropeana.ro/, 21.02.2014.

infrastructures, including by creating at EU level a common system for the administration and development of private analytics through appropriate means.

To support all these proposed actions, the European Commission has set up the Expert Group on Submarine Cable Infrastructure, comprising authorities from EU Member States, and has also opened a public consultation on the possibilities set out in the White Paper, with a deadline on 30th June 2024, to find support from stakeholders who will inspire the next policy activities in this area.

## 3. Conclusions

The protection of critical infrastructures has represented, especially since the end of the 20th century, a concern and an action under the responsibility of all actors involved at international level (states and international organizations), because the risks to which they are exposed are increasingly connected to each other. They are not enclosed by national borders and, for this reason, require the concern of the entire international society, the detection and estimation of the unsafe aspects of these infrastructures being necessary to maintain a climate of safety and constancy. That is why it is very important to resort to harmonized policies in this area, at international, regional and national level, capable of making it possible to find and prevent dangers as early as possible, at the same time with taking those intervention measures for the purpose of preventing and encumbering their occurrence.

At the national level, the competence for carrying out all these steps and actions lies with the intelligence services, their effectiveness in this regard being also conditioned by the ability of the other state institutions to guarantee national security. In Romania, the SRI (the Romanian Intelligence Service) is competent in the field.

As proof of the existing concerns at the level of the international community regarding the protection of critical infrastructures, by identifying as quickly as possible and resorting to suitable methods to combat the identified dangers, there are also the actions of NATO and the EU[1]. Thus:

- At the level of the NATO alliance, within the Higher Committee for the Planning of Civilian Activities for Emergency Situations, measures have been taken to outline

[1] Romanian Intelligence Service, *Protecţia infrastructurilor critice/Protection of critical infrastructures*, 2010, p. 7, www.sri.ro.

and put into practice a series of common procedures for detecting and analyzing dangers and defending infrastructures considered by the organization as critical.[1]

➢ Within the EU, some measures have been initiated to guarantee the creation of the legal and operational framework for detecting and improving the protection of critical infrastructures, being able to highlight for example:

- the beginning of the European Programme for Critical Infrastructure Protection (EPCIC) on 12th December, 2006, which included 11 areas and 32 services considered indispensable and closely related to those areas at European level;

- the adoption of the Council Directive 2008/114/EC of 8th December 2008 on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection.

To protect critical infrastructures from cyber-attacks, an extremely important aspect due to the consequences that the dangers to them could generate for people, states, national economies and unions of states, it is necessary to find and adopt rapid measures at national level, mainly aimed at[2]:

- creating the national legal framework whereby to establish which infrastructures are qualified as critical, taking into account the relevant international and regional-EU norms;

- the establishment of the institutional system to effectively implement the adopted legal norms and the measures to protect critical infrastructures;

- involvement in the adoption of legal norms in the fields and of the critical infrastructure operators/administrators and in the process of their implementation;

- creating the appropriate and necessary environment to achieve early prevention and to intervene on threats that may affect the functioning of infrastructure's structures and its assembly;

- continuous improvement of the expertise in this area;

- intensification of the collaborations between national, European and macro regional institutions.

[1] Romanian Intelligence Service, *Protecţia infrastructurilor critice/Protection of critical infrastructures*, 2010, p. 7, www.sri.ro.
[2] Romanian Intelligence Service, *Protecţia infrastructurilor critice/Protection of critical infrastructures*, 2010, p. 22, www.sri.ro.

## Bibliography

Rizea, Marian, et al. (2008). *Protecţia infrastructurilor critice în spaţiul euroatlantic/Protection of critical infrastructures in the Euro-Atlantic Space*. Bucharest: Ed. Ani.

Vivera, Victor (2017). *Securitate şi putere în spaţiul cibernetic/Security and power in the cyberspace*. Bucharest: Ed. Militară.

***Online*** Sources

http://eur-lex.europa.eu/legal-content/Ro/Txt/, *Comunicare comună a Parlamentului European, Consiliului, Comitetului Economic şi Social şi Comitetul Regiunilor, Strategia de Securitate cibernetică a UE: un spaţiu cibernetic deschis, sigur şi securizat/Joint Communication of the European Parliament, the Council, the Economic and Social Committee and the Committee of the Regions, EU Cybersecurity Strategy: an open, safe and secure cyberspace*.

Romanian Intelligence Service (2010). *Protecţia infrastructurilor critice/Protection of critical infrastructures*, www.sri.ro.

http://www.sri.ro/.

https://www.caleaeuropeana.ro/.