Unofficial translation

THE GOVERNMENT OF ROMANIA
PUBLISHED IN: OFFICIAL MONITOR nr. 555 4th of August

# DECISION no. 718 of July 13, 2011 for the approval of the National Strategy for critical infrastructures protection

## Contents



## 1. Argument/Introduction

The socio-economic development stimulated by the accelerated technological progress and the manifestation of globalization has reinforced a strong interdependence and interaction of systems that ensure the safety and welfare of human society. The interconnection system's need by eliminating the administrative barriers and access to the new emerging markets, along

with the integration of infrastructure networks, determinates developments in the security and global stability field.

With the adoption of the Government Emergency Ordinance no. 98/2010 on the identification, designation and critical infrastructure protection, approved with amendments by Law no. 18/2011, and the Government Decision no. 1.110/2010 on the composition, tasks and organization of the Inter-institutional Working Group for CIP, it was created a national legal framework for the critical infrastructure protection, but the absence of a strategic framework for the development mechanisms to protect critical infrastructure can generate duplication, inefficiency or even conflicts with implications for national interests and objectives set out in the Directive 2008/114/EC of 8 December 2008 on the identification and designation of European Critical Infrastructure and the assessment of the need to improve their protection.

In this context, it is necessary to develop the National Strategy for Critical Infrastructure Protection - a frame document for the adoption and implementation of specific measures and actions to reduce the negative effects induced by the expression of specific risk factors on critical infrastructure, at national and regional level.

The National Strategy for Critical Infrastructure Protection was developed in accordance with the Romanian National Defense Strategy, the national defense and security White Book and with the institutional conceptual boundaries in the field, both at national and international level, establishing the policies and the guide actions in the field, necessary for the development and the completion of the national regulatory framework.

# 2. International general context

The rapid developments and, sometimes, with a high degree of unpredictability, coupled with the size and complexity of vulnerabilities and risks, generate a challenge for critical infrastructure protection systems.

The transnational interconnections of infrastructures and the risk manifestation sphere, which borrowed the elements of representation and evolution set in the process of globalization, prefigures perpetuation premises by risk "resonance" to critical infrastructures and enable the

increase trough "the domino effect", in other states' areas, of the effects of aggression on some systems or processes.

The globalization, with the advantages and the positive changes that brings at international level, enables the rapid escalation, at global scale, of threats to the security of all. The globalization tendency of insecurity must be addressed through strong measures to block and eliminate present threats and future hazards, and also to establish a system of security globalization.

The risks and threats to society's vital goals and citizens' security have acquired new meanings, with high dynamic and increased intensity, which led to the need for an integrated approach to the concept of "critical infrastructure". Based on the basic characteristics of critical infrastructure, the element of criticality stability, including across borders, has acquired new connotations in terms of national/ transnational strategies.

The complexity of critical infrastructures protection and their importance for social stability, or security of the citizen and state, generated a linkage of the specific strategies initiated at organization or state level.

The connections between the functionality and viability of critical infrastructures and the fundamental elements of a state's political, military, economic and social life, alliances etc. significantly strengthen the link between the security and the role of infrastructure systems in expressing needs and promoting national interests, regardless of contextual configuration.

In recent years, with the occurrence of terrorist acts, the deliberate interruption of the supply of energy materials at the level of some states, the occurrence of technological accidents due to human error / natural disasters have highlighted the vulnerability of some national critical infrastructures and the Member States of the European Union have taken steps towards establishing a firm basis for joint action to protect their strategic value targets.

In June 2004 the European Council asked for the preparation of an overall strategy to protect critical infrastructures. In response, on 20 October 2004, the Commission adopted a Communication on critical infrastructure protection in the fight against terrorism which put

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

On 17 November 2005 the Commission adopted a Green Paper on a European programme for critical infrastructure protection which provided policy options on the establishment of the programme and the Critical Infrastructure Warning Information Network. The responses received to the Green Paper emphasized the added value of a Community framework concerning critical infrastructure protection. The need to increase the critical infrastructure protection capability in Europe and to help reduce vulnerabilities concerning critical infrastructures was acknowledged.

The importance of the key principles of subsidiarity, proportionality and complementarity, as well as of stakeholder dialogue was emphasized.

In April 2007 the Council adopted conclusions on the EPCIP in which it reiterated that it was the ultimate responsibility of the Member States to manage arrangements for the protection of critical infrastructures within their national borders.

In this context, the Directive 2008/114/EC was adopted, which constitutes a first step in a step-by-step approach to identify and designate ECIs and assess the need to improve their protection. As such, this Directive concentrates on the energy and transport sectors and should be reviewed with a view to assessing its impact and the need to include other sectors within its scope.

The European Community agrees that the scope of critical infrastructure protection, in the context of globalization, no longer takes account of national boundaries and involves joint efforts towards the identification and evaluation of any of these vulnerabilities, which can be "targets" or major hubs reflecting threats to the micro and macro security.

The climate of stability and security is dependent on the proper functioning of critical infrastructure networks, the need for their protection as being an essential element to avoid serious societal disruptions of society.

# 3. Current situation and existing regulatory framework in Romania

The evolution of global threats, coupled with current political, military and also economic status of Romania within NATO and the European Union, determines the projection of potential risk factors and onto the equivalent critical national infrastructures, especially in the context of the role of our country in ensuring regional stability and security climate, focusing on the Black Sea.

Thus, the perspective of potential threats led to strategic, institutional and functional approaches in an integrated system regarding national critical infrastructure protection issues.

Given the high dependence to critical infrastructure services, the society has become very vulnerable. This vulnerability has grown not only as a result of risks and external threats, but also because of the interdependencies between different infrastructures within the relevant systems, context in which the disruptions / interruptions can cause immense damage to the national economy.

In matters of critical infrastructure protection, the state and society effort should be directed, mainly, on two broad categories of threats: the terrorist one and the one generated by disasters / calamities that have a growing impact on infrastructure, considered as critical.

The first steps towards setting up a coherent normative legal framework to regulate critical infrastructure protection in Romania have been completed with the adoption of Government Emergency Ordinance no. 98/2010, approved with amendments by Law no. 18/2011 and other subsequent legislation. On this basis was created the Interinstitutionel Working Group on Critical Infrastructure Protection, the body that provides the necessary institutional cooperation needed for the national project development which is indispensable for the development of an integrated and fundamental approach of critical infrastructure protection.

# 4. Vulnerabilities, risk factors and threats to critical infrastructure protection

The present security environment is characterized by significant changes both in terms of the relevance of regional and global actors and the ongoing clashes environment characteristics and the optimal management objectives of the problem. The traditional reasons such as gaining vital resource or territories change their meaning and are completed with new ones, such as the conquest of markets or the environment protection. In this context, there have been changes also in the strategies that promote interests, who set up as objectives neutralizing some elements of the critical infrastructure competitors instead of effort dissipation to neutralize the competitor.

Based on data meanings - the national information security Doctrine - the concepts of "vulnerability", "risk factors", "threats", "state of danger" and "aggression", they can be defined, in terms of critical infrastructure, as follows:

Vulnerabilities represent the status quo, processes and phenomena that decrease the responsiveness of critical infrastructures to the existing or potential risks or that favor their emergence and development, with consequences in terms of functionality and utility.

The ignorance or mismanagement of the vulnerabilities can generate risk factors, threats or danger to the objectives, values, interests and to national needs subordinated to critical infrastructures.

The risk factors designate situations, circumstances, elements, internal and external conditions or circumstances, sometimes doubled by action, determining or favoring the materialization of a threat to critical infrastructure caused by vulnerability, generating effects of insecurity.

The threats are skills, strategies, intentions, plans that enhance a threat to critical infrastructure, evidenced by attitudes, gestures, acts, which often creates unbalanced states or instability and generates states of danger, with impact on national security.

The states of concern are situations, events that may put in danger or threaten the existence or the integrity of critical infrastructures.

The assaults/aggressions are attacks, including armed, endangering the existence, the balance or the integrity of critical infrastructures.

The critical infrastructure can be exposed to various types of risks and threats, according to their expression.

The risks and threats general spectrum include natural events, technical, technological and human failures, actions or intentional attacks, and other forms of expression which by their nature or scale can affect the critical infrastructure.

These events and incidents have various reasons and can cause significant damage or can destroy the infrastructure's elements that are vital to society and population in general. Due to the high level of dependence on infrastructure services, the society has become very vulnerable both because of disaster risk and in the context of major infrastructure interdependencies between different parts of the infrastructure from the relevant systems.

After September 11, 2001 the main threat on which focuses the efforts of States to acquire and maintain the protection and security is the international terrorism. With the increasing dependence of society on its basic structures and the use of modern technology by the terrorist organizations has increased the need to protect critical infrastructures against terrorist attacks. The level of this category threat remains low in Romania. In addition to risk mainly result of terrorism, particular attention should be paid to significant damage that may occur due to natural disasters.

So far, in Romania, the critical infrastructure, in different sectors has been affected, especially by extreme weather events. It is expected that in the future, the climate change adds new pressures on critical infrastructure even in the regions with temperate climates, such as those in Central Europe.

Another category of major risks arising from the technical equipment, due to insufficient / inefficient maintenance, rehabilitation and upgrading, as well as in terms of cyber size (hardware and software) to produce gaps in the functioning of computerized systems of critical infrastructure as a result of criminal acts, errors or technical/human malfunction, natural disasters or managerial deficiencies.

In this context, it is necessary to intensify the steps to protect the critical infrastructure, including:

a) the increase of the communication level and the cooperation between the state authorities and the European Union, the economic operators and the public, taking into account the sensitivity of certain information categories;

b) optimizing the cooperation between the leaders in prevention and crisis management field;

c) the operational public-private partnership in the field of critical infrastructure protection;

d) the increase of the potential for self-protection, self-guarantee of individual and institutional capacity affected by dysfunction or which may compromise the functioning of critical infrastructures;

e) acceptable level of risk prioritization based on cost-benefit ratio determined by the probability of event and its impact.

With regard to current environmental threats and security assessments, have been highlighted the main types of such events that may occur within the national territory:

a) organized crime, particularly the border one, which escalation can be enhanced by increasing Romania's role in supporting international policies to counteract this phenomenon;

b) natural hazards caused by natural phenomena;

c) technical failures, interruptions in the systems/equipment functioning, in particular due to the large length of exploitation and insufficient maintenance activities;

d) errors / human action, poor exploiting/unauthorized intrusion, etc.

# 5. Scope and strategic objectives

The strategy aim is to provide the general framework for the critical infrastructure protection in order to promote national interests and to achieve the objectives assumed in the alliance to which Romania is a party.

The strategy aims to:

a) establish the markers for national capacity continuous development of critical infrastructure protection;

b) harmonize the national legislation with the European Union and NATO's legislation in the field;

c) involve all national authorities in the field, as well as private sector partners, to formulate and implement all of the structural and procedural measures to ensure a coordinated action at national level for the identification, designation and critical infrastructures protection.

Strategic objectives:

1. Ensuring consistency of the identification, designation and protection of national and European critical infrastructures;

2. Setting up and the operationalization of a national early warning system by integrating all the networks and the existing organizational-informational capabilities;

3. Accurate the evaluation of the vulnerability level of critical infrastructure and identify the measures necessary to preventive intervention;

4. Develop the cooperation at national, regional and international level in the critical infrastructures field.

# 6. The principles for achieving the critical infrastructure protection

The strategy is based on the following principles:

The principle of legality - the activities are carried out in accordance with the law;

The principle of subsidiarity - ensure the decision making closer to the citizen, in parallel with the ongoing assessment of the need for action at the national level, coupled with the existing opportunities in the regional or local level;

The principle of complementarity - the establishment of a flexible legislative framework which enable the adoption of the specific ways and means connected to the current situation, with the recovery and, where appropriate, adaptation / development of the mechanisms and measures to ensure the critical infrastructure security already in place;

The principle of confidentiality - the dissemination of the information on critical infrastructure protection will be a framework to ensure the protection of that specific information whose disclosure could lead to security vulnerabilities at the infrastructure level. The information will be classified, and the access to them it must be made in accordance with the principle of "need to know". The management and the access to classified information are done according to law, by the persons who hold the security clearances or access authorizations, valid for their classification level;

The principle of proportionality - the protective measures will be proportionate to the acceptable risk level. By applying some appropriate risk management techniques, the attention will be focused on the areas with the greatest potential risk, taking into account the threats, the criticality, the risk probability, the cost-benefit ratio, the level of security and protection necessary and the available effective strategies. The critical infrastructures vulnerabilities are classified according to the properties and the potential effects as "acceptable" - imposing the measures to monitor the progress, or "critical" - which involves active measures to limit/remove;

The principle of cooperation between holders-all the critical infrastructure owners, operators or managers, including business and industry associations or standardization bodies play a role in critical infrastructure protection. All holders must cooperate and contribute to the development and the implementation of critical infrastructure protection in accordance with their specific roles and responsibilities. The responsible public authorities shall ensure the coordination of the development and the implementation of policies and measures for the protection of critical infrastructure in its competence areas. The critical infrastructures owners, operators and managers of will be involved at national and European level;

The principle of vital functions security - the priority in the adoption and the implementation of the protective measures will provide the services, facilities or activities that are or may be required to maintain vital functions of society, health, safety, security, economic or social well-being of individuals and whose disruption or destruction would have a significant impact at national level.

# 7. Guide actions and ways to achieve short and medium term results

To achieve its objectives, the responsible managers need to consider:

a) highlight all the existing or foreseeable risks, in parallel with the critical elements and processes identification;

b) the elimination of the dysfunctions that can affect the stability and smooth functioning of essential services with the support of critical infrastructure by applying proactive measures in an effective risk management system;

c) the increase of expertise and the update of risk analyzes, including comparative evaluations with specific situations manifested in other states, and transposing those results to national standards;

d) compliance with data privacy and information whose unauthorized dissemination can affect the critical infrastructure protection systems, according to national legislation.

The strategic objective no. 1 - Ensuring the consistency of the identification, designation and protection procedures of national and European critical infrastructures

Directions:

1.1. Establishing the criteria and the related sectoral thresholds taking account the features of the critical infrastructure individual sectors

1.2. Determining the cross-cutting criteria thresholds depending on the impact disruption severity or the destruction of a particular infrastructure

1.3. Developing common methodologies for risks and threats identification and classification and related vulnerabilities to infrastructure elements

1.4. Identifying and using the relevant indicators for the needs with greater applicability, to splitting those infrastructure categories which involve protective measures

1.5. Making assessments on legislative-institutional, organizational, functional and practical coordinates, providing a stable and dynamic frame, with high mobility potential on the identification and protection of critical infrastructure

1.6. Increasing the engagement and dynamics of the responsible persons in various levels in completing the steps / operations corresponding to the implementation of the regulatory framework for the identification and protection of critical infrastructure

1.7. Effective identification of risks, threats and vulnerabilities in specific areas based on the findings of risk assessments and foundations connected to ground realities and sustainability potential (implications, effects, resources and support capacity), enabling the clear outline of thresholds and selection criteria of the infrastructure, in view to include in the critical category

1.8. Creating an unified framework for risk assessment, establishing the real protection needs, respectively preventive intervention measures and / or reaction or to limit the effects of producing state of danger in terms of stability and security.

The strategic objective no. 2 - The setting up and the operationalization of a national early warning system by integrating all networks and existing capabilities and organizational information

Directions:

2.1. The operationalization of contact points between owners, operators and / or managers of European critical infrastructures and the competent authority of the Member State by appointing the liaison officers for security

2.2. Achieving an uniform and efficient information flow of expertise / best practices exchange, while developing the resilience capacity of critical infrastructure protection strategies in relation with the evolution developments forms of national risk factors at national and macroregional level

2.3. The implementation, at national level, of an appropriate communication mechanism between national responsible authorities and the liaison officers for security or their equivalents, in order to improve the relevant information exchange on the risks and threats identified in relation to these critical infrastructures

2.4. The initiation and the proper coordination of scientific research in public-private partnership in order to identify assess methods, risks and vulnerabilities analyze and the measures needed for the critical infrastructure protection;

2.5. The development of some modeling and simulation applications of the operation and the establishment of critical infrastructure interdependencies, in order to achieve a model of decision-making, reduce the vulnerabilities and increase the population, society and / or state institutions responsiveness, at local, regional, national and international level.

The strategic objective no. 3 - An accurate evaluation of the vulnerability level of critical infrastructures and the identification measures necessary for the preventive intervention and for its reduction

Directions:

3.1. The quality standards review, the protective adaptation mechanisms, the identification and the threats counteract, the raising of redundancy levels, the modularity increase

3.2. The streamline of the activities and actions by removing excessive bureaucracy, the interference in the normal flow of information and decision, of the information leaks, the unjustified resource consumption and the liability dissipation in case of incident

3.3. The development of the operator security plans for each designated critical infrastructure, the identification of critical infrastructure components and the existing security solutions implemented for their protection and the operationalization of an effective guidance and control system

3.4. Making of "data bank" enabling data collection and processing specific data to critical infrastructure and case studies, best practices manuals and lessons learned

3.5. The needs assessment for improving critical infrastructure protection to help protect the people, the property and the environment

The strategic objective no. 4 - Develop the cooperation at national, regional and international in the field of critical infrastructure protection

Directions:

4.1. The development of the cooperation at national and international level in order to achieve the data and information exchange on the identification and the protection of European critical infrastructures

4.2. The creation of the inter-institutional cooperation mechanisms for the critical infrastructure protection by involving the representatives designated by the responsible public authorities mentioned in the law that transpose the provisions of Directive 2008/114/EC

4.3. The achievement of institutional cooperation and the establishment of experts working groups to identify the optimal solutions to achieve the protection of the infrastructure elements and to establish the intervention modalities

4.4. The interoperability ensuring and the improvement of inter-institutional communication and with the Member States by establishing a schedules of the bilaterally meetings on specific areas or for a thematic forum

4.5. The implementation of legislative and operational measures to protection critical infrastructures, as deriving from EU and NATO Romanian membership, in terms of responsibility for its participation in ensuring the regional stability and security climate

4.6. The strength of the cooperation with the neighboring countries in order to identify those components of infrastructure that can be included in the European critical infrastructures and taking the necessary steps to ensure their protection capacity in relation to national and international security requirements

4.7. Improving and developing the dialogue between all structures with roles and responsibilities in the field by creating a partnership between critical infrastructure owners, managers and / or operators, government and society, to effective risk management and to ensure an adequate response to critical infrastructure disturbance or destruction.

The transposition in reality of these requires the dialog intensification in a partnership between the public and private field, with the responsibility of all participants on the need to setup a cohesion environment on the necessary measures to be taken and the response / application to critical infrastructure protection plan.

To achieve the proposed action directions will consider the effort conjugation on the following coordinates:

a) the effects prevention, mitigation and limitation:

1. anticipate vulnerabilities and risks;

2. continue preparation and planning;

3. ensure the control;

4. the risk factors assessment, trough comprehensive and proactive methods, with the adoption of risk management and crisis management strategy;

b) response / intervention:

1. the development of an adequate capacity to respond to all structures levels that might be affected by the design of intervention measures in emergency situations (including physical protection) and crisis management;

2. exercises and best practices that provide maximum efficiency and flexibility to any challenge;

c) sustainability:

1. risk analysis, regardless of the causal element, to provide ongoing support to adapt to the developments of the risk characteristics and critical infrastructure protection standards;

2. matching the resources with the needs for early identification and prevention / risk countermeasures.

# 8. Finance

The critical infrastructure protection activity requires a concerted and multidisciplinary effort in terms of human and material resources which will be allocated according to competences in the field by the responsible public authorities and critical infrastructures owners, managers and / or operators.

Optimizing resource management system for critical infrastructure protection could involve an increase in the share of information components, generated by their increasing relevance in all social areas and also by the diversification due to threats targeting this area.

# 9. Procedures/Mechanisms for implementation, monitoring and evaluation

In the process of adopting the procedures for implementation, monitoring and evaluation, it will consider the following coordinates:

a) legislative - the updating/completing of the specific regulatory framework in relation to the boundaries, the tasks and the competences of the institutions involved, acting in critical infrastructure protection field;

b) institutional - the development of the capacity to implement, to monitor and to coordinate the implementation of goals;

c) human - the development and training, through:

1. professionalization of human resources involved in the identification and critical infrastructure protection;

2. establish the 'niche' format in order to create opportunities for specialization at European level, which could put Romania in a training provider position in the field;

d) public and private cooperation - to ensure the harmonization of national measures, the exchange of expertise and developing the research and the innovation in the field.

In the evaluation process will be considered the national criteria and the assessment techniques established in all Member States of the European Union.

The implementation, at national level, of an appropriate communication mechanism between national responsible authorities and the security liaison officers or their equivalents, in order to exchange relevant information on risks and threats identified in the critical infrastructure field that is essential for monitoring and effectively coordinating of critical infrastructure protection in short and medium term.