ROMANIAN INTELLIGENCE SERVICE

CRITICAL INFRASTRUCTURES PROTECTION
CRITICAL INFRASTRUCTURES PROTECTION
Without a sufficient knowledge of the new threats to security, we will not be able to build a climate of stability for us and the next generations.
Table of contents

Preamble .......................................................................................................................... 4
Introduction .................................................................................................................... 5
I. Critical Infrastructure Role and Importance for Security and Stability .................................................. 6
   International Context........................................................................................................ 6
   Defining and Identifying Infrastructures........................................................................ 7
   Types of Risk Factors against Critical Infrastructures................................................... 11
   National Infrastructure System...................................................................................... 14
II. Romanian Intelligence Service Competences in Ensuring Critical National Infrastructure Protection .......................................................... 16
   SRI Activity Coordinates on Critical Infrastructure Protection ................................... 16
      A. Intelligence Measures .............................................................................................. 16
      B. Measures Ensuring Physical Protection of Critical Infrastructures........................ 18
      C. Measures Deriving from SRI’s Role as National Cyber-Intelligence (CYBERINT) Authority .......................................................... 19
      D. Physical, Judicial and Procedural Protection Measures for Classified Information on Critical Infrastructures .......................................................... 19
   Romanian Intelligence Service’s Public Communication on Critical Infrastructure Protection .......................................................... 21
Conclusions .................................................................................................................... 22
Appendix: European Programme for Critical Infrastructure Protection .......................................................... 23
Notes: ............................................................................................................................... 24
Preamble

The Romanian Intelligence Service (SRI), an integral part of the national security community, has included, in its institutional transformation agenda, steps aimed at involving citizens in achieving national security, developing relations with civil society main actors. The Service elaborates and develops communication programs and projects, whose purpose is tributary to the national security goals.

The expertise accumulated by the Service – after consultations with prominent civil society figures, Romanian and foreign experts, representatives of partner intelligence services – has highlighted the need to create, within the current legal system, an efficient framework to debate security-related topics, offering the possibility to strengthen ties with dialogue partners and establish work patterns compatible both at the European and the Euro-Atlantic levels.

The Centre for Information on Security Culture (CICS), established on September 30, 2003 within the Romanian Intelligence Service, is an interactive and multidisciplinary information system, unique at the regional level, meant to draw the civil society’s attention to national security issues. Its main goal is to adopt a correct attitude towards the participation of specialized institutions and citizens in the development of the new security environment.

CICS intends to identify the institutional communication mechanisms and the proper framework to conclude partnership agreements with NGOs and public authorities in order to ensure expertise transfer in the national security field.
Introduction

The complexity and diversity of risks and threats, increasingly interconnected and characterized by multiple causes, require an integrative, systemic and comprehensive approach on security goals, especially on the protection of the vital components for the safety and the normal development of social and economic life.

The actions aimed at protecting the critical infrastructures exceed national boundaries and imply common efforts to identify and assess potential vulnerabilities. Therefore, the protection of critical infrastructures – an essential factor in maintaining stability and security – requires increased involvement of the main international actors (state and international organizations) in order to elaborate and adjust strategies in the field. These strategies should provide risk identification and early warning systems, at the same time with the opportune adoption and promotion of decisions/efforts to prevent and counter threats.

The issue has become a major preoccupation for the intelligence agencies, which carry out activities in order to gain knowledge, anticipate, prevent and counter threats to critical infrastructures, helping other government institutions to ensure national security.
I. Critical Infrastructure Role and Importance for Security and Stability

International Context

The issue of critical infrastructure has increasingly emerged as a topical subject by the end of the 20th century and the beginning of the 21st, because of rising asymmetric risks.

The 9/11 terrorist attacks marked the beginning of a “new age” in international relations\(^1\), a crucial moment for the international community to extend the concept of “critical infrastructures” worldwide and to adopt unitary measures embedded in national and regional strategies, to protect them against risks and threats, mainly terrorist ones.

Important developments in the legal and institutional field have taken place, aiming at defining and protecting critical infrastructures both in the United States and within NATO and the EU member states.

➢ The Senior Civil Emergency Planning Committee has carried out actions to elaborate and implement unitary strategies on identifying, assessing risks, and protecting infrastructures deemed critical by the organization, according to NATO’s goals\(^2\).

➢ The EU has undertaken a series of measures aimed at establishing the legal and operational framework for identifying and improving critical infrastructure protection, especially after the terrorist attacks in Madrid (2004) and London (2005).

Among such significant developments, we mention the following:

• the launch, on December 12, 2006, of the European Program for Critical Infrastructure Protection (EPCIP), including 11 sectors and 32 vital services at the European level;
the adoption, on December 8, 2008, of the Council Directive no. 114/2008/EC on identifying and designating the European critical infrastructures and assessing the need to improve their protection.

Defining and Identifying Infrastructures

Taking into account the critical role of infrastructures in supporting all mechanisms ensuring the stability and operational security of the economic and social systems, the specialized literature proposes the following three main categories:

- **Common infrastructures** representing a framework structure, ensuring the construction and functioning of a system;

- **Special infrastructures** playing a consistent role in the functioning of systems and processes, with a high degree of stability and security within the regional complex of economic and social life mechanisms. These types of infrastructures, subject to dysfunctions and vulnerabilities, which also exist in an insecure climate, may be considered "critical";

- **Critical infrastructures** are, in general, vital for the stability, security, and safety of systems and processes, playing an important role in the economic, social, political, and military field. These infrastructures’ criticity degree is determined by the significant consequences triggered by their disruption or destruction, including for a very short period.

Although approaches vary, having as a starting point the common elements regarding the importance of safe operation and the induced effects, the concept of “critical infrastructures” may be assimilated to any functioning economic entity providing products, goods and public services vital for the entire society and whose
destruction, degradation or breakdown have a major economic and social impact, at micro- and macroregional levels. ⁴

An infrastructure or set of infrastructures may be considered critical due to:

- their uniqueness, and also their complementarity within a certain infrastructure;
- their vital role in ensuring the stability, reliability, safety, functionality and, especially, the security of systems;
- their enhanced vulnerability to direct threats, as well as to threats targeting the systems/processes they are part of;
- their particular sensibility to different conditions and, mostly, to unexpected developments.⁵

The assessment of critical infrastructures can be achieved according to the following criteria⁶:

- physical or presence criterion – assessing their place among the other infrastructures, their size, dispersion, endurance, reliability etc.;
- functional or role criterion – what exactly “does” the respective infrastructure;
- security – the infrastructure role in ensuring the system’s safety and security (assessed in terms of effects triggered by the alteration of basic conditions);
- flexibility – some of the common infrastructures may become, under certain circumstances, “critical” and the other way around;
- unpredictability – showing that some of the common or special infrastructures may become, in a given context, critical.
The critical infrastructures can be operationally configured taking into account their role as integral parts of a system or process, and their own elements completing a network, as follows:

- *the parts represented by infrastructure nodes*: employees, departments, contractors, subcontractors (institutions with which they collaborate/cooperate), facilities, and equipment;

- *the interactions* (links) established among nodes: services, hierarchical guidance (change/reorientation), schemes and link networks of critical importance in order to assess security, efficiency, sustainability, durability;

- *the critical infrastructure features* (people, installations, equipment, systems) and their assessment according to the degree of security, efficiency etc.

According to various factors, stages and situations, determining causes (terrorism-related risks, extreme weather conditions or serious technological risks) and especially social and economic consequences which may cause a snowball effect, the infrastructures can meet, at a certain point, the essential criteria for being included in or excluded from the *critical* category.
The European Council Directive no. 114/2008/EC of December 8, 2008 on identifying and designating the European critical infrastructures and assessing the need to improve their protection defines the critical infrastructures, as follows:

„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”.

This document defines the European critical infrastructure as „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 cross-cutting criteria. This includes effects resulting from cross-sector dependencies on other types of infrastructure”.

The stability and security climate is determined by the good functioning of critical infrastructure networks, whose protection represents an essential condition in order to avoid severe disruption of society’s viability.

According to the above-mentioned Directive, the protection consists in “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”.


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

(Text with EEA relevance)
Types of Risk Factors against Critical Infrastructures

Ensuring an effective critical infrastructure protection requires deep knowledge of the elements affecting them:

A. Vulnerabilities

Vulnerabilities represent those facts, processes and phenomena diminishing the capacity to react to existing or potential risks, or favouring their emergence and development, with consequences on the functionality and use of critical infrastructures. They are the consequences of systemic dysfunctions, triggering gaps at the level of information and decision-making processes, ties and relations between the system components or of the inter-systemic relations, negatively affecting economic and social functionality, balance and stability.

Non-identifying or improperly managing the dysfunctions may trigger risks and risk factors, threats, state of danger or aggressions against national security goals, values, interests and necessities.

Critical infrastructure vulnerabilities may be the consequences of objective elements, triggered by potential human intervention or by improper operation and administration.

Within the context of critical infrastructure protection measures, the assessment of individual and systemic vulnerabilities represents a key element.

B. Risk Factors

They refer to domestic and foreign developments, elements, conditions and circumstances, sometimes accompanied by actions, determining or favouring the materialization of infrastructure threats, generating insecurity.

Critical infrastructure risks can be classified according to:

- the structure and extent of breakdown, failure, intervention, degree of probability, as well as human action potential;
• the driving factor and vulnerabilities of a system or systems;
• the nature, as well as the degree of ambiguity and incertitude.

The importance of identifying and preventing the emergence of risk factors implies a comprehensive risk assessment, starting with the dysfunctions and vulnerabilities.

C. Threats

They represent capabilities, strategies, intentions, and plans posing an increasing risk to critical infrastructures, materialized in attitudes, gestures, acts, and facts triggering unbalance or instability and creating dangerous situations affecting national security.

D. State of Danger

It usually highlights the consequences of a materialized threat or the imminent aggression against critical infrastructures.

E. Aggressions

They represent violent or non-violent actions, carried out by an entity (states, pressure groups, non-state actors, power centres etc.) by military, electronic, psychological or information means, based on strategies or plans.

Probability versus Impact

The critical infrastructure vulnerability is represented by the relationship between the probability of a real threat against its good functioning and the inducted consequences.
**Risk Matrix Template**

- **Low probability (below 50%)**
  - **High impact**
    - These are the most ‘dangerous’ incidents, because most people tend to focus on low probability rather than major impact, delaying preparations until it is too late.

- **Low probability (below 50%)**
  - **Low impact**
    - Most probably minor incidents will occur, the crisis unit being able to manage them properly with adequate training and employing reaction procedures.

- **High probability (over 50%)**
  - **High impact**
    - All efforts must focus on these events, as they have been envisaged and have a major destructive potential.

- **High probability (over 50%)**
  - **Low impact**
    - There are high chances for minor impact incidents to occur, but their impact is low, due to their increased frequency, and the teams are prepared/ready.
National Infrastructure System

The national infrastructure system, due to its characteristic development, technical performance, and security level, creates real premises for the emergence of vulnerabilities and risk factors generating significant imbalances with major social and economic impact, at the national and macro-regional level.

Thus, the negative effects of the precarious technical condition of the specialized transport infrastructure are highlighted by the increased operation time, poor performance of activities, with direct impact on competitive services complying with high quality and safety standards.

Similarly, the energy, oil and gas systems (the study focusing on those targeted by the European Directive) face major dysfunctions generated by insufficient rehabilitation measures, leading to poor technical exploitation performance.

The insufficient physical protection of these infrastructures allows the increase in a. - the theft of transported goods and b. - the risk of deliberate and aggressive interventions, leading to major disruptions at the level of the distribution system of public elements/services, with a severe economic and social impact.

In November 2010, the Romanian legal framework in critical infrastructures protection was strengthened with two acts in the area of critical infrastructures protection, regarding the identification, designation and protection of critical infrastructures⁹, in accordance with the Directive 114/ 2008/ EC. Government’s Emergency Ordnance nr. 98 was approved and modified by the Law nr.18 from 11 March 2011.

The Romanian Intelligence Service was appointed responsible authority for the IT&C and national security sectors, together with other institutions.
Critical Infrastructure Risk Management Diagram

**RISKS**
- Intensive exploitation of installations and equipments;
- Degradation, amid lack of resources for maintenance/ modernization;
- Poor/Improper operation of installations and equipments;
- Lack of adequate guard and protection measures.

**CRITICAL INFRASTRUCTURES**

**CRITICAL LEVEL**
- Influence on the economic and social activity;
- Generating unbalances at the level of horizontally-linked entities;
- Extent of damage (material and human losses) in case of accident.

**Public-Private Partnership**
- Owners or administrators ensuring:
  - funds;
  - maintenance;
  - protection.

**Institutions in charge of**
- legislation;
- control.

**Information flux**

**Common Protection Measures**

**Early Warning System**

**Initiative**

**Opportune Intervention System**

**Physical**

**Technological**

**Relevant authorities counterterrorism and emergency authorities**
II. Romanian Intelligence Service Competences in Ensuring Critical National Infrastructure Protection

SRI Activity Coordinates on Critical Infrastructure Protection

Under the law, the Romanian Intelligence Service operates in this area through:

A. Intelligence Measures

Their goal is to identify any type of threats to critical infrastructures, as well as vulnerabilities, state of danger and risks, and to brief the legal beneficiaries on all security issues.

The Romanian Intelligence Service has the responsibility to inform constantly and in due time the decision makers (according to the Law nr. 51/1991 and 14/1992) and to cooperate with other structures nationwide (according to the Law nr. 535/2004).

The intelligence activity related to critical infrastructure focuses on actions and operations permanently carried out in order to plan, search, obtain, check, and analytically process data and information on critical infrastructure protection, as well as on briefing relevant decision-makers.

Reliable, accurate and topical information – mainly with anticipative/predictable character – is the early-warning instrument for the authorities in order to implement appropriate counter measures and avoid emergencies or “strategic surprises”.

Moreover, highlighting, in due time, real emergency developments and their potential effects improves crises management.

The information related to critical infrastructure protection is a national security element, defined as an intelligence activity product, including elements of novelty, related to situations/phenomena/facts/state of
facts, which represent or may represent threats or sources of risk to national security or risk vectors.

Therefore, the following are among SRI responsibilities:

- collect first hand data and information on risk factors affecting the integrity and functionality of critical infrastructures;
- elaborate assessments and comprehensive analyses on critical infrastructure security, allowing the identification and understanding of potential threats;
- provide relevant authorities and relevant decision-making institutions with information on situations/ potential risks to critical infrastructures.

Secret data dissemination to beneficiaries is based on the “need-to-know” principle, decision-makers in various activity areas receiving information according to their legal competences. The individuals having access to certain classified information in order to fulfil their duties are granted a corresponding security clearance, according to the legal norms on the access to classified information.

Having in view the necessity to increase the efficiency of its activity, the Romanian Intelligence Service increasingly needs an institutionalized, opportune and effective feed-back from its legal beneficiaries, on critical infrastructure issues allowing it to adjust and tailor its capabilities to meet the need for knowledge/ information of the authorities and to set its tactical and operational priorities.

The information activity is considered to have reached its purpose when the beneficiaries receive relevant intelligence products. Beneficiary’s feedback – confirming, assessing, denying/ amending the analytical product content or requesting additional data – triggers a new process/ analytical cycle, which is likely to end in a new information product.
As far as the internal activity regulation and planning is concerned, the *Intelligence Strategy* – a programmatic document translating national security and defence strategies into the SRI responsibility – includes critical infrastructure protection among its priority directions of action, ensuring human, material and financial resources, as well as intelligence and operative capabilities to that end.

**B. Measures Ensuring Physical Protection of Critical Infrastructures in case of terrorist threats**

SRI is the national antiterrorism authority and technical coordinator of the National System for the Prevention and Countering of Terrorism (NSPCT), therefore such measures are applied gradually, according to the threat level, based on intelligence and specialized risk assessments. They include coordination or action measures:

- security clearance for counterterrorism protection/intervention, when such a threat is imminent – NSPCT specialized forces tasks;
- counterterrorism intervention, when a terrorist attack occurs – SRI’s main responsibility, with NSPCT support;
- counterterrorism - anti-hijacking and counterterrorism checks, as well as counterterrorism measures at civilian airports – SRI’s responsibility.

The prevention and countering of terrorism – one of the most important threats to critical infrastructures – is carried out observing the domestic legislation, international conventions to which Romania is part, as well as relevant international regulations. Specific responsibilities are included in domestic normative acts.
C. Measures Deriving from SRI’s Role as National Cyber-Intelligence (CYBERINT) Authority

The computer systems through which most critical infrastructures operate are increasingly targeted by increasingly well-organized and complex cyber attacks. The attacks against national or private computer systems, related to critical infrastructures, become more dangerous and difficult to prevent. They can be launched by organized crime groups mainly in order to obtain financial resources, but also by hostile states, to achieve political goals.

From this point of view, SRI’s transformation and modernization process is aimed at establishing the Service's institutional concept and architecture, ensuring an adequate response to such threats (prevention, protection, reaction and consequence management in case of cyber attacks), through the creation, in 2008, of the National CYBERINT Centre, designed as:

- a collaborative platform for the institutions within the National Security Community;
- a cooperation interface with similar NATO structures.

D. Physical, Judicial and Procedural Protection Measures for Classified Information on Critical Infrastructures

The Romanian Intelligence Service, as national authority protecting classified information, carries out activities related to the security of classified information managed by the authorities, public institutions or legal persons, within its sphere of competence, according to the Law nr.182/ 2002 on classified information protection and other subsequent normative acts.

In order to exercise all its responsibilities in the implementation of these regulations, the specialized department of the Service ensures:

- protection of NATO and EU classified information, managed by SRI;
- general coordination and control of classified information protection measures within SRI’s sphere of responsibility, to prevent the disclosure of state secrets, respectively of NATO/EU classified information;
- establishment of national standards for classified information protection;
- oversight of efforts meant to protect classified information and state secrets, undertaken by authorities and public institutions, as well as by entirely or partially state-controlled economic agents and other legal persons;
- cooperation with relevant security authorities and specialized structures of partner agencies on classified information protection;
- specialized assistance to the entities handling classified information and observation of law by applying sanctions, according to the legislation.
Romanian Intelligence Service’s Public Communication on Critical Infrastructure Protection

In 2009, the Romanian Intelligence Service, through the Centre for Information on Security Culture, has initiated a public communication project called “Critical Infrastructure Protection - Main Direction to Achieve National Security”.

Its main goal is to inform on critical infrastructures and the role and place of SRI in ensuring their protection.

The project was launched on May 12th, 2009, in Brașov, during a round table called “Critical Infrastructure Protection and Public-Private Partnership. Main Direction to Achieve National Security”, in partnership with the Eurisc Foundation. The event was attended by representatives of local public authorities, defence institutions, law enforcement and national security agencies, companies operating in critical infrastructure sectors (transports, utility providers, IT&C), as well as of local media.

The main topics focused on the concept and the need to achieve critical infrastructure protection, according to the European Council Directive 114/2008, respectively the need to launch a dialogue/partnership with companies and institutions holding such infrastructures or being involved in their development or protection, as well as on the explanatory elements of the relationship between critical infrastructures and national security.
Conclusions

Economic and social developments, implicitly predictable and unpredictable threats, effects on the population and the economies of the countries and federations, at the national and international level, highlight the need for urgent critical infrastructure protection measures, such as:

- the strengthening of inter-institutional cooperation at the national, European and macro-regional level;
- the involvement of critical infrastructure administrators/operators in legal and enforcement efforts;
- the development of relevant expertise;
- the establishment of an optimal and efficient framework for ‘early warning’ and pre-emptive intervention against risks that could affect the infrastructure systems integrity and functionality.
Appendix: European Programme for Critical Infrastructure Protection

Launched on December 12th, 2006, the European Programme for Critical Infrastructures Protection (EPCIP) mentioned 11 sectors and 32 associated vital services, at the European level:

<table>
<thead>
<tr>
<th>Sector</th>
<th>Product or service</th>
</tr>
</thead>
</table>
| I. Energy | 1 Oil and gas production, refining, treatment and storage, including pipelines  
2 Electricity production  
3 Electricity, gas and oil transport  
4 Electricity, gas and oil distribution; |
| II. Information and Communication Technologies | 5. Information systems and networks;  
6. Command, automation, and instrumentation systems;  
7. Mobile and fixed telecommunication services;  
8. Radio communication and navigation services;  
9. Satellite communication services;  
10. Broadcasting services; |
| III. Water Supply | 11. Drinking water supply;  
12. Water quality control;  
13. Dam building and water quantity control; |
| IV. Food | 14. Food supply, safety and security; |
| V. Health | 15. Medical and hospital care;  
16. Drugs, serums, vaccines and pharmaceutical products;  
17. Bio-laboratories and bio-agents; |
| VI. Financial | 18. Payment services/related structures;  
21 Government financial systems; |
| VII. Defence, Law Enforcement and Security | 20. Country defence, public order and national security;  
21. Integrated border management; |
| VIII. Administration | 22. Government;  
23. Armed forces;  
24. Administration and services; |
IX. Transport

25. Emergency services;
26. Road transport;
27. Rail transport;
28. Inland waterways transport, short-sea and ocean shipping;
29. Air transport;

X. Chemical and Nuclear Industry

30. Production, processing and storage of chemical and nuclear materials;
31. Pipelines for dangerous chemical products/materials;

XI. Space

32. Air traffic.

Notes:

1 Smith, Michael N., Counter-Terrorism and the Use of Force in International Law, The Marshall Center Papers, No.5, November 2002
5 Prof. Rizea, Marian, PhD.; Marinica, Mariana; Barbasura, Alexandru; Conf. Dumitrache, Lucian; Ene, Catalin, Euro-Atlantic Critical Infrastructure Protection, Printing House of the National Intelligence Academy ‘Mihai Viteazul’, 2008, Bucharest, p.7
6 Alexandrescu, Grigore, PhD.; Vaduva, Gheorghe, PhD., Critical Infrastructures: Dangers and Threats. Protection Systems, Printing House of the National Defence University ‘Carol I’, Bucharest, 2006, p. 8
7 Critical Infrastructures, published in the SRI’s magazine ‘Profil’, nr.10, March 2006, p. 23, Bucharest
9 Government’s Emergency Ordinance nr.98/2010 regarding the identification, designation and protection of critical infrastructures and Government’s Decision nr.1110/ 3 November 2010 regarding the structure, attributions and organisation of the Inter-institutional working group for the protection of critical infrastructures.