Cyber security strategy of Romania

I. Introduction

1. Background

The rapid development of modern information and communication technologies – a sine qua non condition for the edification of the Information Society - has had a major impact on the social environment, marking true mutations in the operating philosophy of economics, politics and the culture, but also in the daily life of the individual. In fact, at present, the easy access to technology information and communication is one of the prerequisites for the proper functioning of modern society.

Cyberspace is characterized by the absence of borders, dynamism and anonymity, generating equal both opportunities to develop knowledge-based information society and risks to its functionality (at the individual, state and even transborder).

Alongside the undeniable benefits that computerization introduces in modern society, it also introduces vulnerabilities, so the security of cyberspace should be a major concern of all stakeholders, especially at institutional level, where responsibility of elaborating and implementing coherent policies in the field concentrates.

Romania aims to develop both a dynamic information environment based on interoperability and specific information society services, and enforcement of citizens' fundamental rights and freedoms and the national security interests, in an appropriate legal framework. In light of this, there is a need to develop a cyber security culture among the ITC users, which are often insufficiently informed of potential risks and countering solutions. Widespread knowledge about risks and threats deriving from activities in the cyberspace, as well as means of prevention and countering them requires efficient communication and cooperation between specific actors in this field.

The Romanian state assumes the role of coordinator of cyber security activities at national level, in line with EU and NATO initiatives. The cyber security issue has become a priority for these bodies, which implement regulatory approaches required for the development of cyber defence mechanisms.

Cyber security incidents and major cyber attacks which some states and international organizations have faced in recent years have determined, at international level, the understanding of the need to adopt strategies and policies in the field of cybersecurity. Thus, there are now national cyber security strategies, such as those of Estonia, United States, Britain, Germany and France, which substantiate the need to further develop their capabilities to counter cyber attacks and which set the framework for action and cooperation between different government entities and NGOs in order to mitigate the consequences. According to these strategies, states' efforts aim at implementing security measures conducive to the growth of cyber infrastructure protection level, especially those supporting national critical infrastructures.

The rapidly evolving nature of cyber threats has required the adoption, including at NATO, of a new concept and a new cyber defense policy. To this end, NATO has redefined its role and area of action in the field and developed a plan of action to develop the capabilities required to protect own cyber infrastructure own and mechanisms for consultation between Member States and for assuring assistance in the event of major cyber attacks.

At the EU level, the adoption a European cyber security strategy, aimed at harmonizing the efforts of Member States to address security challenges in cyberspace and critical information infrastructure protection, is in progress.

At the same time, the EU has outlined the need for a policy on fighting cybercrime. Subsequent initiatives have started from realizing the increase in the number of computer crimes, the deeper involvement of organized criminal groups in cybercrime, and the need for coordinating EU efforts in countering these crimes. Given that the large scale, coordinated cyber attacks targeting cyber critical infrastructure of the Member States are a growing concern of the EU, there is an urgent necessity to take action to combat all forms of cybercrime, both at European and at national level.

Increasing capacity to fight cyber crime at national, European and international level requires, inter alia:
- increased cooperation and coordination between units responsible with countering cybercrime, other authorities and experts from the European Union;
- developing a coherent regulatory framework at EU level on the fight against cybercrime, in coordination with Member States and with European and international relevant authorities in the field
- raising awareness of costs and dangers posed by cybercrime.

In this context, Romania acknowledges the existence of such threats and supports a joint integrated approach, coordinated at both NATO and EU level, in order to offer a timely response to cyberattacks.

2. Scope and Purpose

The purpose of Romania’s cyber security strategy is to define and maintain an secure virtual environment, with a high degree of resilience and confidence, based on national cyber infrastructures, which would constitute an important support for national security and good government, to maximize the benefits for citizens, businesses and the Romanian society as a whole.

Romania's cyber security strategy sets out the objectives, principles and major directions for action for understanding, preventing and counteracting cyber security threats, vulnerabilities and risks and to promote Romania's interests, values and national objectives in cyberspace.

To ensure coherence and actionable efficiency, the strategy seeks to achieve the national security target concerning "achieving cyber security", while respecting the principles and characteristics of the National Defense Strategy and National Strategy for the protection critical infrastructure.

For ensuring Romania’s cyber security, the strategy sets the following objectives:

a) adapt the regulatory and institutional framework to the cyberspace threats dynamics;
b) establish and implement security profiles and minimum requirements for national cyber infrastructures, relevant in terms of the proper functionality of the critical infrastructures;
c) ensure the resilience of cyber infrastructure;
d) ensure security through understanding, preventing and fighting vulnerabilities, risks and threats to cyber security of Romania;
e) take advantage of the opportunities to promote the national interests, values and objective in the cyberspace;
f) promote and develop cooperation between the public and private sectors at national and international level in the field of cyber security;
g) develop a security culture by raising awareness of the population concerning the vulnerabilities, risks and threats originating from cyberspace and the need to ensure protection of their information systems;
h) active participation in the initiatives of international organizations which Romania is part of in defining and establishing a set of international confidence-building measures concerning use of cyberspace.

3. Concepts, Definitions and Terms

For the purposes of this strategy, terms and expressions have the following meanings:

- cyber infrastructure - information technology and communications infrastructure, consisting of systems, applications related electronic communications networks and services;

- cyberspace - virtual environment generated by cyber infrastructure, including content information processed, stored or transmitted, as well as actions taken by users in this;

- cybersecurity - normality resulting from the application of a set of proactive and reactive measures that ensure the confidentiality, integrity, availability, authenticity and non-repudiation in electronic information, resources and public or private services, in cyberspace.

Proactive and reactive measures may include political, concepts, standards and guidelines for security, risk management, and training awareness activities, implement engineering solutions to protect cyber infrastructure, management identity and management consequence;

- cyber defense - actions taken in cyberspace to protect, monitor, detect, counter aggression and ensure appropriate response against specific cyber threats to national defense infrastructure;

- operations in computer networks - complex process of planning, coordination, synchronization, harmonization and development of actions in cyberspace protection, control and using computers network to obtain superiority information, while neutralizing enemy capabilities;

- cyber threat - circumstance or event which constitutes a potential danger to cyber security;

- cyber attack - hostile action in cyberspace held to affect cybernetics security;

- cyber incident - event occurred in the cyberspace, whose consequences affect cyber security;

- cyber terrorism - premeditated activities carried out in cyberspace by individuals, politically motivated groups or organizations, ideological or religious which may cause damage materials or victims, likely to cause panic or terror;

- cyber espionage - actions taken in cyberspace in order to obtain unauthorized confidential information in the interests of state or non-state entities;

- cybercrime - all facts under criminal law or other special laws which constitute a social threat and are committed with guilt, through cyber infrastructure;

- vulnerability in cyberspace - weakness in the design and implementation cyber infrastructures and associated security measures which can be exploited by threat;

- security risk in cyberspace - the likelihood that a threat will materialize, exploiting a specific cyber infrastructure vulnerability;

- risk management - a complex , continuous and flexible identification, evaluation and counteracting cyber security risks process, based on the use of techniques and complex tools for preventing losses of any nature;

- identity management - methods for validating the identity of persons when they accessing any cyber infrastructure;

- cyber infrastructure resilience - the ability cyber infrastructure components to withstand a cyber incident or attack and return to normality;

- CERT-type entities - specialized structures within the meaning of art. 2 letter a) the Government Decision no. 494/2011 on the establishment of the National Response to Security Incidents Cybernetics - CERT-RO.

4. Principles

Ensuring cybersecurity should be the outcome of an approach based on risk assessment, resource prioritization, implementing and monitoring the efficiency of the security measures identified through the application of risk management and compliance and respecting the following principles:

- Coordination - activities are carried out in a unitary, based on convergent action plans for cyber security in accordance with the duties and responsibilities of each entity;

- Cooperation - all entities involved (in the public or private) are working at nationally and internationally, to ensure an adequate response to threats from space cybernetic;

- Efficiency - steps taken aimed at optimal management of available resources;

- Prioritization - efforts will focus on securing cyber infrastructure supporting national and European critical infrastructures;

- Dissemination - ensuring the transfer of information, expertise and best practices in order protect cyber infrastructure;

- Protecting values - cyber security policies will ensure a balance between the need for increased security in cyberspace and the preservation of privacy and other values and fundamental freedoms of citizens;

- Accountability - all owners and users of cyber infrastructure must take the necessary steps to secure their infrastructures and not affect other users;

- Separation of networks - reducing the likelihood of manifestation of cybernetic attacks, Specific Internet network on cyber infrastructures that provide vital State functions, using dedicated networks and separate Internet.

II. Challenges and opportunities

1. Threats, vulnerabilities and risks

Specific threats to cyberspace are characterized by sharp asymmetry and dynamics and a global nature, which makes them difficult to identify and counter through measures proportional with impact risks materialize.

Romania is currently facing threats to its critical infrastructure, originating from cyberspace. This is due to an increasing interdependence between cyber infrastructure and infrastructure such as that belonging to banking, transport, energy and national defense sectors. The globality of cyberspace is likely to increase the risks affecting both citizens, businesses and the government.

In general, cyber infrastructures may be affected by technical threats (i.e., deficiencies or technical failures), human threats (i.e., operating errors, actions voluntary) or natural threats (i.e., extreme weather, natural disasters).

Threats to cyberspace can be classified in several ways, but the most commonly used are those based on motivational factors and impact on society. In this regard, we can consider cybercrime, cyber terrorism and cyber war, having as source both state actors and non-state actors.

Threats from cyberspace materialize - by exploiting vulnerabilities of human, technical and procedural nature - most often in the form of:
- cyber attacks against the infrastructure supporting public functions or information society services, whose disruption or damage could constitute a danger to the national security;
- unauthorized access to cyber infrastructures;
- modification, deletion or deterioration of computer data or unauthorized illegal restriction of access to such data;
- cyber espionage
- causing patrimonial damage, harassing and blackmailing individuals and businesses, public and private.

The main actors who create threats in cyberspace are:
- persons or organized crime groups that exploit cyberspace vulnerabilities to obtain property or non-property benefits;
- terrorists or extremists who use cyberspace to conduct and coordinate terrorist attacks, communication activities, propaganda, recruitment and training, etc. fundraising for terrorist purposes;
- state or non-state actors which initiate operations in cyberspace, with the purpose of intelligence gathering in the governmental, military, economic fields or of ensuring the materialization of other threats to national security.

2. Opportunities

At the same time, cyberspace, which became a new area of interaction within modern society, offers a number of opportunities generated by its very specificity. Thus, the following opportunities which Romania can take advantage through cyberspace of have been identified:
- Supporting policies and promoting the national interests;
- Developing and supporting the business environment;
- Improving the quality of life through the development of the information society services;
- Improving knowledge and the support for national policy decisions in the Information age through ensuring adequate cyber capabilities and tools;
- Increasing knowledge and prediction capacity for early warning of national security risks and threats;
- Increasing technical capacity and human resource skills to achieve national security objectives.

III. Directions of action

Romania aims at ensuring of normality and reducing the risks in cyberspace
seizing opportunities by improving knowledge, capabilities and mechanisms
decision. In this regard, efforts will focus on the following directions:

1. Establishing the conceptual, organizing and actional framework required for ensuring cyber security:
- constituting and operationalizing a national cyber security system;
- completing and harmonizing the national legal framework in the field, including setting up and appling minimum security requirements for national cyber infrastructures;
- developing cooperation between the public and private sector, including through stimulating reciprocal information exchange concerning threats, vulnerabilities and risks, as well as cyber incidents and attacks.

2. Developing national risk management and reaction capabilities in the field of cyber security, based on a national programme and including the following aspects:
- consolidating, at the level of competent authorities, the potential of understanding, preventing and countering threats and minimizing risks associated with making use of the cyberspace;
- ensuring tools for developing public-private cooperation in the field of cyber security, including for the purpose of creating efficient early warning, alert and response mechanisms concerning cyber incidents;
- stimulating research, development and innovation capabilities in the field of cyber security<
- increasing the resilience level of cyber infrastructures;
- developing CERT-type entities in both the public and private sector.

3. Promoting and consolidating the security culture in the cyber field
- Development of awareness raising programs at the levels of the population, public administration and private sector concerning threats, vulnerabilities and risks specific to the use of cyberspace;
- Development of educational programs, within the compulsory education cycles, concerning the safe use of the internet and computing equipment;
- Appropriate professional training to people working in cyber security and the widespread promotion of professional certifications field;

- The inclusion of elements relating to cyber security in the professional training programs for managers in the public and private sectors.

4. Develop international cooperation on cybersecurity
- Concluding agreements of international cooperation to improve response capacity in the event of major cyber attacks;
- Participation in international programs in the field of cyber security;
- Promoting the interests of national cyber security cooperation formats to which Romania is a party

IV. National cyber security system

National cyber security system (NSCC) is the general framework of cooperation which brings together public authorities and institutions with responsibilities and capabilities in the field in order to ensure coordination of actions at national level for cyberspace security, including through cooperation with academia and business, professional associations and organizations NGOs.

The mission of the NSCC is to provide elements of knowledge, prevention and counteracting of threats, vulnerabilities and specific risks specific to the cyberspace that may affect national cyber security infrastructure, including consequence management.

For the purpose of this strategy, NSCC works as a unitary mechanism effective networking and inter-institutional cooperation in developing and implementing the prompt decision.
NSCC is acting on the following components:

The knowledge component - provide information support to develop proactive and reactive actions to ensure cybersecurity.

The prevention component - is the main reason of ensuring cybersecurity through creation and development of capabilities for the analysis and prognosis regarding its status.

The cooperation and coordination component - ensures uniform and effective networking mechanism in the NSCC.

The counter component - ensure effective reaction to threats or cyber attacks by identifying and blocking their manifestation. This is done in order to maintain or restore the cyber security infrastructure concerned and to identify and punishing perpetrators law.

NSCC's main functions are achieved through information, monitoring, dissemination, analysis, warning, coordination, decision, response, recovery and awareness and the adoption of proactive and reactive measures.

Proactive measures are aimed at:
- Updating and harmonizing the national safety regulators cyber environment in line with developments of reference;
- Implementation of policies, concepts, standards and security guidelines;
- Gathering data and information on shared threats, vulnerabilities and risks identified in cyberspace;
- Analyze, anticipate and forecast developments in the state of cyber security;
- Realization and effective cooperation between the public and private sectors, between holders of cyber infrastructure and state authorities to take measures to prevent and countering of threats and minimize the effects of a cyber attack;
- Training and raising awareness on the risks deriving the use of cyberspace;
- Interoperability with other national and international responsibilities in security;

- National cyber infrastructure protection and those belonging to NATO or EU under the administration of institutions or public authorities;
-Implement a management risk mechanism; :
- Ensuring a high degree of self adaptability, according to developments in space cybernetic;
- Ensuring the confidentiality, integrity, availability, authenticity information in cyberspace;
- Providing identity management in cyberspace;
- Operationalization capabilities for management of cybernetics security incidents, including management consequence;
- Develop mechanisms to increase culture safety.

Reactive measures are aimed at:
- Implementing contingency plans to minimize the effects of an cybernetic attack;
- Measures to ensure continuity of information flows and decision-making;
- Implementation of a plan with measures on ensuring the functionality of the safe public or private services systems;
- Recovering and restoring data;
- Identifying and implementing lessons learned from the application procedures incident management, management of the consequences of a cyber attack, as well as business continuity.

Efficient activities in NSCC depends essentially on cooperation between public and private cyber infrastructure and between the holders and state authorities' ability to undertake measures to prevent and counteract threats, investigation of the cyber attacks and minimizing their effects.

The Supreme Council of National Defense is the authority that coordinates the strategic level of NSCC activity. The Supreme Council of National Defense approves cyber security strategy of Romania and approved Rules of organization and functioning of the Council Operative on cyber security. Cyber security operative Council (COSC) is the body through which the unitary coordination of NSCC. COSC in part, has permanent members, representatives of the Ministry of National Defense, Ministry of Interior Affairs, Ministry of Foreign Affairs, Ministry for Information Society, the Romanian Intelligence Service Information, Special Telecommunications Service, the Foreign Intelligence Service, Service 15/17 Protection and Guard, National Registry Office for Classified Information and Secretary of the Supreme Council of National Defense. Leadership is provided by a COSC president (presidential adviser on national security issues) and a Deputy (Adviser to Prime Minister on National Security). Technical coordinator of COSC is Romanian Intelligence Service, under the law.

.

The Government of Romania, through the Ministry for Information Society, ensure coordination for other public authorities that are not represented in the COSC, to achieve government policies consistency and implementation strategies for electronic communications, information technology, information society services, and the National Response Centre for Cyber Security Incidents - CERTRO
- Ensure the development and dissemination of public policies for preventing and counteracting incidents of cyber infrastructures, according to the competence area. The Romanian Government will draft a law on cyber security, which it will submit Parliament's approval, according to the law. All the institutions that are represented in the COSC cooperate with international bodies EU, NATO, OSCE, etc., each in its field of competence.

V. Cooperation between the public and private domain

Developing the cooperation between the public and private cyber security purposes is a priority for action in international bodies or alliances to which Romania is part, given that cyberspace brings together both cyber infrastructure owned and operated by state and private entities.

The main guidelines to ensure cyber security, by cooperation between public and private, must pursue:
- Cooperation based on trust between the state and business at all levels;

- Increased protection of the cyber infrastructure by correlating measures undertaken with resources available in the public and private sectors. Cyber security responsibility lies on all stakeholders, taking into account the complementary interests in this area to ensure the legality of operations conducted, combating cybercrime and Infrastructure Protection Critical interconnected cyberspace and is based on Mutual Trust.

The main objectives of cooperation between the public and private sectors aimed at:
-Exchanging information on threats, vulnerabilities and risks;

Developing early warning capabilities and response to cyber incidents and attacks;
- Conducting joint exercises on cyberspace security;
- Development of educational programs and research;
- Development of safety culture;
- Joint response in the event of major cyber attacks.
Mentioned objectives requires cooperation between the public and private sector, including prevention, awareness and promote opportunities in the cyber domain.

VI. Conclusion
Ensuring the cyber security is based on cooperation at national and international level to protect cyberspace by coordinating the actions of national guidelines and measures at international level in cooperation formats to which Romania is a party.
Given the dynamism of global developments in cyberspace and our objectives in the development of the information society and implementation of large-scale electronic services, it is necessary to develop a national program in detail, which - based on benchmarks provided by this strategy - to ensure development and implementing concrete cybersecurity projects.

NSCC operational measures efforts should be harmonized with the size of critical infrastructure protection, with the process of developing capabilities of CERT. The best option, NSCC must have a flexible and adaptive encompassing identification and prediction capabilities, resources and operational procedures prevention, response and countermeasures, and tools for documentation and sanction cyber attacks authors.

It is necessary to implement at national level the minimum standards of procedural and cyber security infrastructures, to substantiate the effectiveness of the actions protection against cyber attacks and to limit the risk of incidents with significant potential impact.

Public authorities with responsibilities in this area will allocate the necessary financial resources for cyber security through policies planning. In order to ensure increased capacities to identify, assets and design for properly management measures risk or incident response and cyber attacks is a priority trade development Information and transfer of expertise between the authorities responsible in the field, cooperation development between the public and private sectors and expand cooperation with the media NGOs and the academic community.

The NSCC will be the platform for cooperation and harmonization of existing capabilities for CERT nationally, drawing tools offered by them, and will work to strength the expertise in cyber risks, by stimulating synergies between the different plans cyber security action (military and civil, public-private governmental – non-governmental).

Given the rapid pace of issue development, this strategy will permanently be tested and reviewed, including in the broader context of defense strategy, continue to adapt the challenges and opportunities arising from a changing environment security.

Within 90 days of the entry into force of this strategy, COSC will develop a program for national cyber security risk management.