# CYBER SECURITY STRATEGIES IN THE INTERNET ERA

**Cătălin-Ionuț NASTASIU**

"Nicolae Bălcescu" Land Forces Academy, Sibiu, Romania

DOI: 10.19062/2247-3173.2016.18.2.19

***Abstract:****The characteristics of the new security environment require new coordinates, especially when we talk about the cyber environment. The threats from this environment have become increasingly large, which led to the appearance of the Cyber Security Strategies at national level as well as NATO and EU level.*

*The real concern is that the cyber attacks have increased in the last years. This thing is the result of the development of technology and easier access to a computer or internet.*

*Cyber Security strategies are created to determine the risks and threats and what are the courses of action in case of a cyber attack, what are the steps to follow in order to minimize the effects and catching the attacker.*

***Keywords****: cyberterrorirsm, cyber attacks, cyber space, security, cyber security, cyber defence.*

## 1. INTRODUCTION

Cyber security threats have become increasingly serious in recent years. They are not limited by borders and an increase in the frequency and degree of sophistication. Universal membership of cyberspace, the security risks involved in cyber attacks and global character of their effects require international cooperation efforts for ensuring the security of computer systems.

The Web spread on a global scale, has evolved. Worms and viruses have been transformed from simple threats in serious security challenges and perfect tools of Cyber espionage. Attacks can be executed through the involvement of a large group of processing units that generate requests for a service, resulting in blocking access to that service. If it has been seen as nothing more than some "protest jams", the cyber attacks had became a tool in the information war.

The organizations became dependent on cybernetic systems over the full range of human activities, including trade, finance, health, energy, entertainment, communications and national defense. Globally interconnected, digital information and communications infrastructure known as cyberspace, underpins almost every branch of modern society and provides critical support for the economy, civil infrastructure, public safety and national security.

## 2. WHAT IS ELECTRONIC WARFARE?

The rapid development of information technology and means of communication, which is a necessity today, had a major impact on the social, marking true mutations in economic philosophy, politics, cultural, etc. Practical, easy access to information and communication is a pillar of the functioning of society today.

The information has an especially important role for both, the individual and the organization, therefore requiring appropriate measures of protection. Information security protects the informational structure from threats. In this sense, information security is characterized as being that which produces and maintains confidentiality, integrity, and sustainability. Information security is achieved through the implementation of a set of policies, practices, procedures and organizational structures. These items must be implemented in such a way as to extend certain security goals.

Cyberspace is characterized by the absence of boundaries, dynamism and anonymity, generating opportunities for the development of knowledge based on information about society's risks[1]. If the society is based on information, it will become more vulnerable, and security of cyberspace must become a matter for all stakeholders, particularly at the institutional level, where attention must be directed towards the development of the security policy and its implementation.

Like any other actions, and he follows cyber-attack a number of predefined metedologii: obtaining vital information in relation to the proposed target, finding out and accurate understanding of the weaknesses of the target, exploiting vulnerabilities, actual attack itself for triggering the desired effect and carrying out actions aimed at covering traces of allowing identification of făptaşului. If we take into account the amount of human and material resources used in a classic war, waging a cyber warfare is shown to be much less than constisitoare, so it avoids the losses. This type of warfare is aimed at conquering and maintaining final information superiority over your opponent can be defined as an act of denial, exploitation, distortion or destruction of information and command, control and evolution of the enemy, protecting ones own[2].

Considering these features and their consequences, the cyber attack was defined as "any action to compromise the functionality of a network of computer systems, for political purposes or related to national security."[3]

Cyber warfare involves attacks motivated leading to sabotage and espionage and information in the information system. Cyber-warfare attacks can destabilize the networks, may affect essential services may alter or even steal information and classified data, encrypting every system. It's basically like an information war that can be used in his private public interest.

Cyber-terrorism is defined as a premeditated, politically motivated attack against computer systems, information, programs or sensitive data that lead to violence against non-combat and civil targets. The attacks are coming from the transnational groups or clandestine agencies. Cyber environment is severely affected by the implications of the globalization process in the development of information technologies because some hijackers may have access to certain systems which can be vital to a whole nation.

## 3. N.A.T.O. CYBER SECURITY STRATEGY

From year to year , growing cyber security threats are becoming more serious . These threats are facilitated by the lack of borders, that is the reason why it is recorded a growing degree of sophistication. Universal membership cyberspace security risks posed

[1] Hotărârea nr. 271/2013 pentru aprobarea Strategiei de securitate cibernetică a României şi a Planului de acţiune la nivel naţional privind implementarea Sistemului naţional de securitate

[2] Intelligence, Nr. 23, noiembrie-decembrie 2012, p. 5.

[3] Oona A. Hathaway, Rebecca Crootof, Philip Levitz, Haley Nix, Aileen Nowlan, William Perdue, Julia Spiegel, The Law of Cyber-Attack, Faculty Scholarship Series. Paper 3852, p.10.

by cyber attacks and the global nature of their effects require international cooperation efforts to ensure the security of information systems[4].

Cyber defense appeared on the agenda of NATO Summit in Prague in 2002 and was later confirmed as a priority at the summit in Riga in 2006. A policy in this area has been agreed for the first time , the heads of states and government at the Bucharest Summit in April 2008. The evolution of this new concept, the cyber attacks and because of their character and complexity, entered in the attention of all the member states and occupied the first place on NATO security agenda. The documents of the Lisbon Summit ( Summit declaration and Strategic concept acquis ) 2010 confirmed this thing[5].

Only the events in Estonia in the spring of 2007 prompted the Alliance to radically rethink its need for a cyber defense policy and to raise countermeasures to a new level . Therefore , the Alliance first developed a " NATO cyber defense Policy ", adopted in January 2008 , which established three central pillars of NATO policy in cyberspace[6] *: subsidiarity* represents the assistance provided on request only, in this mode is respected the principle of state sovereignty; *unnecessary duplication* expressed by avoiding duplication of structures or capabilities at international, regional and national level; *security* will be achieved through cooperation based on trust , taking into account the sensitivity of information related to the systems and possible vulnerabilities.

The new Strategic Concept qualifies as cyber threats directly targeting vital national security infrastructure, which can reach levels likely to endanger "prosperity, security and national stability and Euro-Atlantic integration". Accordingly, such challenges require the development of the Alliance's ability to prevent, detect and defend itself against their recovery after their occurrence, strengthening and coordinating national cyber defense capabilities. Tasks set by the Lisbon Summit, NATO cyber policy developed and Action Plan reflecting the main changes and demands urgent matter. NATO objectives defined in those documents, identified structures wich will be involved in Allied defense mechanisms for coordinated action[7]. Under the new NATO Strategic Concept, revised NATO Policy on Cyber Defence defines cyber threats as a potential source to collective defense in accordance with Article 5 of NATO. Moreover, the new policy and action plan for its implementation, NATO offer clear guidelines and a list of priorities agreed on how to advance cyber defense Alliance, including through increased coordination within NATO and with its partners.

In the events generated by strained relations between Russia and Ukraine, NATO need to strengthen their eastern border, they were adopted new security measures. The appliance and so the idea of creating based on voluntary contribution of NATO member countries, a Support Fund (Trust Fund) for the development of cyber defense capacity of Ukraine. Country's Supreme Council of Defense approved transmission of the decision by NATO and the NATO Summit in Wales since 4-5 September Romania declared its readiness to act as the nation's leading Support Fund for cyber defense of Ukraine. Romania, as a nation-leading involves defining the cyber security specialists, based on dialogue with the Ukrainian side, the technical requirements and architecture of a system to protect critical IT infrastructure against cyber threats. Another task of nation-leader as identifying other NATO member states that participant Trust Fund, so that it can provide the resources necessary for project implementation. In order cyber defense Romania can

[4] http://nato.mae.ro/node/435, accesat la data de 05.07.2015, ora 16:20

[5] "The NATO Summit at Prague, 2002" Paul Gallis http://fpc.state.gov/documents/organization/45219.pdf

[6] Idem

[7] "Jurnalul Academic" Decembrie 2010, Edi ţia 13
http://nato.md/uploads/Analize%20si%20comentarii/Jurnal%20Academic/JA_nr_13.pdf

collaborate with specialists in cyber security Ukrainians, bringing problems and incidents common plan, and with the support of the Fund for Support to counteract and neutralize cyberattacks against Ukraine.

## 4. ROMANIA'S CYBER SECURITY STRATEGY

Romania aims to develop a dynamic information environment based on interoperability and information society services , and ensure compliance of fundamental rights and freedoms of citizens in the interests of national security, in an appropriate legal framework . From this perspective it feels the need to develop a culture of cyber security and communications systems users often poorly informed about potential risks and solutions against them . Knowing widespread risks and threats derived from activities in cyberspace and how to prevent and counter them requires effective communication and cooperation between specific actors in this field[8].

Romanian state assumes the role of coordinator of activities at national level to ensure cyber security , in line with steps taken at EU and NATO. Cyber security incidents and major cyber attacks have faced in recent years some countries and international organizations have determined the awareness at the international level, the need to adopt strategies and policies in the field of cybersecurity .

Increasing capacity to fight cyber crime at national, European and international level involving[9]:

- increase cooperation and coordination between units responsible for combating 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 authorities and international relevance in the field;
- raising awareness of costs and dangers posed by cyber crime.

The purpose of the Romania cybersecurity strategy is to define and maintain a secure virtual environment with a high degree of resilience and confidence, based on the cyber-national infrastructures, which constitute an important support for national security and good governance, to maximizing the benefits citizens , businesses and Romanian society as a whole[10].

Romania's cyber security strategy sets out the objectives , principles and major action for understanding, preventing and counteracting threats , vulnerabilities and risks to cyber security and promoting Romania's interests , values and national goals in cyberspace[11].

To ensure cyber security strategy, Romania establishes the following objectives:

a) adaptation of the regulatory and institutional dynamics specific threats to cyberspace;

b) establish and implement security profiles and minimum requirements for national cyber infrastructure, relevant in terms of the correct operation of critical infrastructure;

c) ensuring cyber infrastructure resilience;

d) ensuring the security through understanding, preventing and countering vulnerabilities, risks and threats to cyber security of Romania;

e) the opportunities cyberspace to promote the interests, values and national goals in cyberspace;

[8] ANEXA Nr. 1, Strategia de securitate cibernetică a României
[9] Strategiei de securitate cibernetică a României, 2013 pag 5
[10] ANEXA Nr. 1, Strategia de securitate cibernetică a României
[11] Strategiai de securitate cibernetică a României, 2013 pag 6-7

f) promote and develop cooperation between the public and private sectors at national and international level in cyber security;

g) the development of safety culture by raising awareness of the population to vulnerabilities, risks and threats from cyberspace and to ensure their protection systems;

h) active participation in initiatives of international organizations of which Romania is part in defining and establishing a set of confidence-building measures at international level on the use of cyberspace.

Ensuring cyber security must be the result of risk-based approach, prioritizing resources, implementing and monitoring the effectiveness of security measures identified through the application of risk management and compliance with the following principles[12]:

- coordination - activities are carried out in a unitary, based on convergent action plans designed to ensure cybersecurity, in accordance with the duties and responsibilities of each entity;
- cooperation - all entities involved (in the public or private) working at national and international level to ensure an adequate response to threats in cyberspace;
- 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 to 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 fundamental values and freedoms of citizens;
- accountability - all owners and users of cyber infrastructure must take the necessary steps to secure their infrastructures and security infrastructures do not affect other owners or users;
- separation of networks - reducing the likelihood of manifestation of cybernetic attacks, specific Internet network on cyber infrastructures that ensure vital state functions using dedicated networks, separate Internet.

The national cyber-security system (NCSS) is the general framework for cooperation which brings together public authorities and institutions with responsibilities and capabilities in the field, to coordinate national actions to ensure the safety of cyberspace, including through cooperation with academia and business , professional associations and NGOs.

NCSS mission is to provide elements of knowledge, prevention and countering of threats, vulnerabilities and risk cyberspace that may affect national cyber security infrastructure, including consequence management.

## CONCLUSIONS

We live in the Internet age and that is why we can say that we are interconnected and unfortunately every day there are more and more cases where people have fallen victim to cybercrime. When I say cybercrimes I am talking about the identity theft, illegal money transfer etc. While information technology are increasing developed, the society becomes dependent on its scope and cybersecurity gradually falls into the category of areas of national interest.

[12] Ibidem , pag 8-9

Ensuring 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 in which Romania is part of.

Increased importance of cybersecurity in society led to the creation of new tools for detection and handling vulnerabilities, especially when considering the growing number of internet users. If we take into account the growing number of companies and organizations which use computers and computer network and thus can be accessed through them, we see that the number of cyber attacks is growing both in Romania and in other countries.

It is necessary to implement at national level the minimum standards of procedural and cyber security infrastructure, to substantiate the effectiveness of approaches to protect against cyber attacks and to limit the risk of incidents with potentially significant impact. Being new, cyberspace, have invested resources to develop programs and structures to provide security and safety systems, especially those of particular importance.

## REFERENCES

[1] Dragomir, D., *Război informaţional agresiv asupra sistemului bancar,* Cotidianul, 29 mai 2004.
[2] Howard, M., LeBlanc, D. ,*Writing Secure Code*, 2nd Edition, Microsoft Press, Redmond, Washington, 2003.
[3] Toma, Gh.. Liteanu, T., DEgeratu, C., *Evoluţia arhitecturilor de securitate sub impactul globalizării*, Editura ANI, Bucureşti, 2007.
[4] F. Dunnigan F. James, *The new global threat – cyber-terrorism*, Editura Curtea Veche, Bucure ști, 2010
[5] Codreanu Ion, Opris Marcel, *Cyberterorismul – o nouă ameninţare la adresa securităţii naţionale*, Bucureşti, Editura C.S.S.N, 2007
[6] Intelligence Magazine, No. 23/ nov-dec 2012
[7] Strategia de Securitate Cibernetică a României" disponibila la http://www.mcsi.ro/Transparenta-decizionala/21/Strategie_Cyber_23052011
[8] http://nato.mae.ro/node/435
[9] http://www.nato.int/docu/review/2011/11-september/Cyber-Threads/RO/index.htm