Legislative Aspects of Cybersecurity

Cezar PEȚA
"Alexandru Ioan Cuza" Police Academy, Bucharest, Romania
petacezar@yahoo.com

Abstract

The world we live in is becoming more and more dependent on information, information technology and communications. All governments should take actions to be prepared to face the new challenges that the cyberspace can bring. The main characteristics of cyberspace are no borders, dynamism and anonymity, creating both opportunities to develop knowledge-based information society, but also risks to its functionality.

Cybersecurity represents the state of normality resulting from the application of a set of proactive and reactive measures that ensure the confidentiality, integrity, availability, authenticity and non-repudiation of information in electronic format, the public and private resources and services in cyberspace. Proactive and reactive measures may include policies, concepts, standards and guidelines for security, risk management, training and awareness activities, implementation of technical solutions to protect cyber infrastructure, identity management, consequence management.

Index terms: security, cybernetics, cyber space, information, communications

Due to globalization and development of information technologies at the beginning of XXI century world is increasingly interdependent and interconnected. Due to the development of new information technologies have emerged threats, vulnerabilities and security risks both nationally and internationally.

Specific threats cyberspace is characterized by asymmetry and strong dynamic and global nature, making them difficult to identify and proportionate measures to counteract the impact of risks materializing. These threats arising in a virtual environment, are in all cases the most dangerous, because the moment of attack is the most difficult to predict and its countermeasures may be most often planned and implemented timely.

The world we live in is becoming more and more dependent on information, information technology and communications. The dependence of increasingly growing of information technology generates a number of advantages and disadvantages. The fact that many public and private companies have become totally dependent on information systems to perform important activities is a major but may be without adequate protection, a disadvantage.

Thus, given the potential dangers that may arise, governments everywhere take steps to be prepared to face new challenges that can occur in cyberspace, because, the daily life of every citizen, the national economy and the national security of any state currently depend on the stability and security of cyberspace.

The fast development of modern information and communication technologies - a sine qua non for building an information society - had a major impact on all social, marking true changes in operating philosophy

of economics, politics and the cultural, and the daily life the individual. Basically, now, easy access to information and communication technology is one of the prerequisites for the proper functioning of modern society. [3]

The main characteristics of cyberspace are no borders, dynamism and anonymity, creating both opportunities to develop knowledge-based information society, but also risks to its operation (individually, state and even border showing).

All these challenges have led identified the concept of „cyber security" which covers the main threats and vulnerabilities and the need for governments and other international bodies to develop a security strategy appropriate to their computer networks.

Cyber security is a challenge that must be tackled through cooperation between various national actors, and institutions, private companies and non-governmental organizations, and international level through cooperation among states, regional and global organizations, given that cyber security is a problem overall. The issue of cyber security has become a priority for the European Union (EU) and NATO, which carries regulatory steps needed to develop cyber defense mechanisms.

Cyber security threats have become more serious in recent years. Cyber security incidents and major cyber attacks have faced in recent years some countries and international organizations have awareness at the international level, the need to adopt strategies and policies in the field of cyber security. They are not limited by borders and an increase in frequency and sophistication. Universal membership of cyberspace, security risks posed by the global nature of cyber attacks and their effects require international cooperative efforts to ensure the security of information systems.

This involves the creation and funding of institutions to deal only cyber security, cyber crime prevention making plans for the opportunity to have a quick response if such events have their ability to find people or organizations for them so that they are brought to justice and, not least, the ability to replace or repair damaged parts as soon as the digital network.

The creation of these institutions must, however, be based on legal regulations. Thus, there is a now national cyber security strategy, such as those of Estonia, U.S., UK, Germany and France, which substantiates the need for steps to develop their own capabilities to counter cyber attacks and set the framework for action and cooperation between different governmental and nongovernmental entities to limit the consequences. According to these strategies, the actions of nations aimed at implementing security measures that lead to higher levels of cyber infrastructure protection, particularly those supporting national critical infrastructures. [3]

Being a defence alliance, NATO identified and recognized early in the last decade, the severity of cyber threats and the importance of protecting networks. Cyber defence appeared on the NATO agenda Summit in Prague in 2002 and was later confirmed as a priority at the Riga Summit in 2006. A policy in this area has been agreed for the first time, the Heads of State and Government at the Bucharest Summit in April 2008 [8]. The rapid development of sophisticated attacks and character placement basis in the centre led NATO security agenda documents Lisbon Summit (Strategic Concept and Summit Declaration) in 2010 confirmed this.

New Strategic Concept NATO qualifies as cyber threats directly targeting vital national security infrastructure that can reach levels likely to jeopardize „the prosperity, security and national stability and Euro-Atlantic integration." Consequently, this type of challenges require the development of the Alliance's ability to prevent, detect and defend against their recovery after their emergence, consolidation and coordination of national cyber defence capabilities.

The European Commission has published, together with the High Representative of the Union for Foreign Affairs and Security Policy,

a cyber security strategy and a proposal for a Directive on the network and information security (NIS). Cyber security strategy, called „A cyber space open, safe and secure," the vision of the EU's overall on the best ways to prevent and manage disruptions and cyber attacks. Its aim is to promote European values of freedom and democracy and to ensure the growth of the digital economy safe. [6]

They feature a number of specific actions aimed at increasing the resilience of cyber infrastructure, reducing cybercrime and strengthening the EU's international cyber security and cyber defence.

The strategy defines the vision EU cyber security through five priorities:

a) Obtaining a resilient cyber infrastructure;

b) Drastically reducing cybercrime;

c) Developing a cyber defence policy and capabilities needed in the context of the Common Security and Defence Policy (CSDP);

d) Development of industrial and technological resources necessary for cyber security;

e) Establishing a coherent EU international policy on cyberspace and promote the fundamental values of the EU.

Through the international policy in cyberspace, the EU aims to:

a) Promote the fundamental values of the EU;

b) Set rules for responsible behavior;

c) To support the implementation of existing international law in cyberspace;

d) To assist countries outside EU in terms of capacity building in cyber security;

e) Promote international cooperation in this field.

EU has adopted many measures to protect its citizens against online crimes. Among them we can mention:

a) Establishing a European Centre for Cybercrime;

b) Legislative proposal on attacks against information systems;

c) Launch a global alliance against child sexual abuse committed through the Internet;

d) Development and funding of a network of national centres of excellence for combating cybercrime.

A European approach to cyber security is a key component of an overall strategy in this area. Through this directive might require all Member States, major Internet service operators, operators of critical infrastructure (egg e-commerce platforms and social networks) and service operators in the energy, transport, health and in banking obligation to ensure a secure and reliable digital environment throughout the EU. [6] The Directive provides Member States adopt security strategies and information networks to designate a national competent authority in this area which have adequate financial and human resources to prevent, manage and resolve risks and incidents.

And Romania, as a member of the EU, implemented, although quite late we consider new matters set out in the EU Strategy. Thus in 2013 the Romanian Government approved the decision no. 271 of 15.05.2013 „Cyber Security Strategy of Romania" and „national action plan for implementation of the national cyber security." This bill is the document that ends a set of laws that, since 2003, by Law no. 161 of 19.04.2003 on measures to ensure transparency in the exercise of public dignities, public functions and business environment, the prevention and punishment of corruption, and later in 2011 by adopting the Government Decision no. 494 of 11.05.2011 on the establishment of the National Security Incident Response Cybernetics - CERT-RO.

Thus is established by Law 161 National Electronic System for public information system in order to ensure access to information and service delivery to individuals and businesses. For the first time in the enactment encounter the term „e-government" and "e-administration". Thus the government stresses need for information

systems introduction in the governance and administration e-Government is the use of central public administration authority's information technology applications in order to [1]:

a) improving access to information and public services of central public administration authorities;

b) elimination of red tape and simplify working methodologies;

c) improving the exchange of information and services between the central government;

d) improving the quality of public services at the central government level.

E-Government is the use by local authorities of information technology applications in order to [1]:

a) improve access and provide information and public services of local authorities by citizens;

b) elimination of red tape and simplify working methodologies;

c) improving the exchange of information between the components of local authorities;

d) improve the effectiveness, efficiency and quality of public services to the local authorities.

The establishment of the two systems „The e-government" and „e-administration system" in central and local government level are designed to provide access to information and service delivery to individuals and businesses. Operators are obligated to use security standards and procedures to ensure high reliability and safety of the operations in the National Electronic System in line with international practices in the field.

In Title III of the law shall regulate, for the first time, preventing and combating cybercrime specific measures of prevention, detection and punishment of offenses committed through computer systems, ensuring respect for human rights and data protection. The need for information systems security and data protection authorities and institutions shall generate competent in the field, service providers, NGOs and other civil society representatives:

a) Conduct joint and cybercrime prevention programs;

b) To promote policies, practices, policies, procedures and minimum standards of security of information systems;

c) To organize information campaigns on Cybercrime and the risks they are exposed to users of computer systems.

At the national institutions responsible for the creation and updating of databases on Cybercrime has the following structure: Ministry of Justice, Ministry of Interior (MAI), Ministry of Information Society, the Romanian Intelligence Service (SRI) and the Foreign Intelligence Service (SIE). These institutions should carry out special programs for training and retraining of personnel involved in preventing and combating cybercrime.

Stipulated in the law defining the offense find information as: [1]

a) The input, modify or delete, without right to restrict computer data without right, access to these data, resulting in inauthentic data in order to be used in order to produce legal consequences;

b) The act of causing the loss of property of a person by entering, modifying or deleting computer data, by restricting access to such data or by preventing in any way the operation of a computer system in order to obtain a benefit for himself or another.

To ensure international cooperation in combating cyber crime by this act shall be established, within the Department for Combating Organized Crime and Drugs Prosecutor of the Supreme Court of Justice, Department of cybercrime.

Also on the line of international cooperation in combating cybercrime can highlight signature at NATO Headquarters in Brussels, the „Memorandum of Understanding for cooperation in cyber security" between NATO Cyber Defence Management Board (CDMB) and S.R.I. This

document formalizes the exchange of information and best practices between SRI and NATO, but also assist in crisis situations and participate in joint activities that are related to cyber security issues. [5]

Numerous „attacks" that took place and aimed, in addition to private institutions and institutions of central and local public administration, which took place both internationally and nationally, and revisions of the EU Strategy to combat cyber crime led to the establishment, by government decision, in 2011, of the National Centre for Cyber Security Incident Response - CERT-RO, the independent structure and R & D expertise in the field of cyber infrastructure protection. CERT-RO is a specialized organizational entity that has the capacity to prevent, analyze, identify and respond to cyber incidents. [4]

In the CERT-RO the early warning system and real-time information on cyber incidents is established. This alert system is established in order to: [4]

a) Real-time warning and issuing reports on the distribution and nature of the incident;

b) Collaboration with national authorities responsible for ensuring cyber security, to prevent and eliminate the effects of incidents.

To identify and stop attacks affected entities CERT-RO cooperate with SRI and the Special Telecommunications Service (STS). CERT-RO is ready to respond in case of a cyber attack within the limits provided by law. However response strategy for cyber security incident is highly dependent on the response capacity of the affected entity. It is responsible for managing the affected system therefore has the means for immediate action.

Dan Tofan, technical director of CERT-RO stated that „there are situations in which the entity can not manage incident alone, and in this case the cooperation between both entities becomes very important. Cooperation in case of scale attacks is essential." [5] It supports the fact that cyber attacks can be detected through various technical means and beyond, and there is no general method or technology used in all cases. Detecting these attacks involve human resources and information systems specialist in analyzing phenomena in cyberspace.

With regard to remedy the effects, it is to analyze the technical incident to determine its characteristics, identifying more precise affected systems (computers, network equipment, etc.). And implementing a strategy for disinfection and recovery losses. CERT-RO is supporting technical bodies authorized to conduct investigations and remediation of structures affected by cyber effects.

The general objectives of attackers in cyberspace are roughly the same, namely to obtain various information that can subsequently bring various benefits (egg financial, political).

The main question, which many specialists ask themselves, is whether is Romania ready to cope with a cyber attack? Are we ready or not for such an attack?

This question is of great interest since the last time Romania was the target of two large-scale cyber attacks that targeted high-profile entities such as state institutions. In January, the computer security company Kaspersky Lab has announced that several states, including our country, have been the target of a cyber espionage campaign called Red October - ROCRA. The campaign targeted the national resources of our country, the information will be sold on the black market is also directed against NATO and the EU.

Espionage was carried out, it seems, in the last five years and were initiated from a server located in Russia, after which it expanded in Germany covering not only our country but also other states in the Southeast and the former USSR In Romania, cyber espionage aimed computers governmental institutions, aiming at avoiding confidential documents that later were to be sold for different amounts of money. S.R.I. timely informed of the institutions targeted cyber attack by using a Trojan at the moment of his and performed in cooperation countermeasures to restore

normal operation of the networks. In this case, CERT-RO identified four IP addresses in Romania who have been victims of this attack, whose identity was not disclosed.

The second cyber attack took place in late February. All company Kaspersky Lab has announced new cyber attack detection, called MiniDuke that targeted government institutions in several European countries, including Romania. Impact of the incident was estimated by the S.R.I. that is greater than the Red October operation, due to the complexity of technology and resource use. Representatives S.R.I. stated that the attack could be carried out by a state entity.

Regarding the involvement of entities in cyber attacks would not be a novelty or something that is not credible. We argue that these statements by U.S. President Barack Obama stressed during a press conference in California with his Chinese counterpart Xi Jinping. It appeals to the fact that "in his country and China to the common rules of the game are respected in cyber security." Since the U.S. pointed towards China in connection with the massive data thefts, the Chinese president said that this phenomenon is a problem, but remained faithful to the Beijing, ensuring that the country was „a victim of cyber attacks." Barack Obama noted that „in terms of technology incredible progress," he and his Chinese counterpart recognize that „the issue of cybersecurity, the need for rules and common approaches are becoming increasingly important. It is crucial that, as two of the biggest global economic and military powers, China and the U.S. must reach a solid agreement on this issue." [7]

U.S. President claims that cyber security is a particularly important aspect of national security.

Bibliography

[1]. Law no. 161 of 19.04.2003 on measures to ensure transparency in the exercise of public dignities, public functions and business environment, the prevention and punishment of corruption, published in the Official Gazette, Part I no. 279 of 21.04.2003.

[2]. Parliament Decision no. 30 of 04.11.2008 on the approval of the country's National Defence Strategy, published in the Official Gazette, Part I no. 799 of 28.11.2008.

[3]. Government Decision no. 271 of 15.05.2013 approving Romania's cyber security strategy and national action plan on the implementation of the national cyber security, published in the Official Gazette, Part I no. 296 of 05.23.2013.

[4]. Government Decision no. 494 of 11.05.2011 on the establishment of the National Security Incident Response Cybernetics - CERT - EN, published in the Official No. 388 of 02.06.2011.

[5]. CyberSecurity (2013, Mar. 07) [Online]. Available: http://www.ziare.ro

[6]. Information Security Strategy (2013, Mar. 11) [Online]. Available: http://www.tribunaeconomica.ro

[7]. Security Strategy (2013, Apr. 02) [Online]. Available: http://www.agerpres.ro

[8]. Aspects of Cybersecurity (2013, Apr. 05) [Online]. Available: http://nato.mae.ro