CYBERSECURITY AND HUMAN RIGHTS

Adrian Cristian MOISE [1]

e-mail: adriancristian.moise@gmail.com

Abstract

Cybersecurity is a broad term which comprises the protection of critical information infrastructure, as well as elements which are considered critical information infrastructures, such as information networks of small and medium-sized enterprises, or personal computers. Cybersecurity consists in a process involving the entire society, where each individual is preoccupied with implementing it. Also, cybersecurity may consist in developing a cybernetic code of conduct for the appropriate use of information and communication technology and in spreading an authentic security policy providing the standards which the users of cybersecurity will expect to meet.
The Internet offers unprecedented opportunities for enforcing human rights and plays an increasingly important role in our everyday lives. Within this context, it is essential that all actors, both public and private, respect and protect human rights on the Internet. Steps must also be taken to ensure that the Internet operates and evolves in ways that fulfil human rights to the greatest extent possible.

Key words: Internet; human rights; cybersecurity; cybercrime; information and communication technology

The Internet is a communication and social interaction space, a virtual space, created by technological and information means, which creates facilities of use and allow access to information and geographic, social or cultural interactions. Also, the Internet is a phenomenon which by its ampleness and complexity presupposes interdisciplinary approaches: historical, technical, economical, sociological, cultural, psychological, juridical and political.

An important feature of the Internet network is its neutrality, which refers to the idea that individual networks, which form Internet, can be controlled by users, rather than its owners and operators. While the network operators are in the unique position to manage their resources, the supporters of the neutrality of network consider that they are unreliable to use their knowledge for the good of the community of the Internet users.

1. Cybersecurity

Cybersecurity is a broad term which comprises the protection of critical information infrastructure, as well as elements which are considered critical information infrastructures, such as information networks of small and medium-sized enterprises, or personal computers. Cybersecurity aims at preventing malicious cybernetic incidents which affect both critical information infrastructures and non critical information infrastructures. These malicious cybernetic incidents can include, for example, DOS attacks, spam, phishing, and other cybernetic crimes (Singer, P.W., Friedman, Allan. (2014). *Cybersecurity and Cyberwar*. Oxford: Oxford University Press, pp.34; Mitra, Ananda. (2010). *Digital security. Cyber Terror and Cyber Security*, New York: Chelsea House Publishers, Infobase Publishing, pp.45).

The purpose of the cybersecurity is to protect goods and resources of organizations from the organizational, human, financial, technical point of view, so that to allow them to continue their mission. The final objective refers to the fact that organizations must ensure that no significant prejudice is caused to them. Thus, this objective consists in reducing probabilities that a threat materialises, in limiting the tried prejudice or deficiency and ensuring that, following a security incident, the normal functioning can be restored in an acceptable frame time and at a fair cost.

Cybersecurity consists in a process involving the entire society, where each individual is preoccupied with implementing it. Also, cybersecurity may consist in developing a cybernetic code of conduct for the appropriate use of information and communication technology and in spreading an authentic security policy providing the standards which the users of cybersecurity (partners, entities, suppliers) will expect to meet.

For the purpose of designing a cybersecurity process, we appreciate that is important to

[1] "Spiru Haret" University of Bucharest, Romania

correctly identify the goods and the resources which must be protected, so that the scope of the security necessary for an efficient protection is precisely determined. This requires a global approach of security, one which has to be multidisciplinary and comprehensive. What are requested here are both a set of basic principles relating to ethical behaviour, responsibility and transparency, incorporated in an adequate legal framework, and a practical set of procedures and norms. At the same time, these principles must be applied both at national level and at the level of the international community, and must be compatible with international directives in force.

The necessity to elaborate a cybersecurity strategy is motivated by the following reasons: (Seger, Alexander. (2012). Council of Europe. Global Project on Cybercrime. *Cybercrime strategies*, Strasbourg, pp.6) society's dependence on cyberspace, which means that security, resilience and trust in information and communication field represent a problem of national interest; economic role and possibilities of information and communication technologies and the intention to maximize benefits and exploit their opportunities; the fact that cybernetic attacks, especially those committed against critical information infrastructure, could represent a threat to the national security. Thus, cybersecurity strategies are related to security and national defence strategies.

Concepts, purposes of cybersecurity combine the technical and political dimensions (national interest and security), by which cybersecurity is typically defined as being the protection of confidentiality, integrity and availability of data and information systems, in order to enhance security, resilience, authenticity and trust in the field of information and communication technology.

I consider that a cybersecurity strategy must have as objective also the protection and promotion of human and state of law rights. We also feel that a cybersecurity strategy must pay most attention on the protection of critical information infrastructure within the public and private sector against: some unintended incidents caused by the malfunctioning of technology, human errors, natural disasters, etc.; intentional attacks, including botnet attacks which are launched to perturb critical information infrastructure, unauthorized access and interception of data and communications or handling or destruction of information data and systems.

A cybersecurity strategy tends to focus on the technical, procedural and institutional measures, such as risk and vulnerability analyses, early warning and response, incident management, exchange of information, creation of bodies in the field of cybersecurity, such as *Computer Emergency Response Teams* (CERTs) and *Computer Security Incident Response Teams* (CSIRTs), which contribute to the intensification of international cooperation and other measures in order to ensure protection of cybernetic space.

Criminal justice or other measures that have to be taken against cybercrime are not found all the time among the priorities of a cybersecurity strategy. Cybersecurity strategy and cybercrime strategy are two complementary strategies (Dupic, Emmanuel. (2014). *Droit de la Sécurité intérieure*. Paris: Gualino Lextenso Éditions, pp.247-248). We consider that complementarity is obvious in terms of attacks committed against confidentiality, integrity and availability of information and communication technology and services built on it. Thus, while cybersecurity covers a wide area of technical and procedural measures to respond to international attacks launched against information and communication technology and to ensure confidentiality, integrity and availability of information and communication technology from its prevention to its protection and its recovery, cybercrime strategies focus on the response of criminal justice to attacks committed against the confidentiality, integrity and availability of information and communication technologies.

Cybersecurity is an interdisciplinary field at the intersection of technological, legal, sociologic, economic and political fields. For each country, the approach of national cybersecurity must reflect the vision, the culture and the civilization of a nation, as well as responding to the specific needs of security within the local context where this is introduced.

As cybersecurity has a global dimension and deals with a wide range of aspects, it is necessary to be developed a general culture of cybersecurity for the purpose of increasing the level of understanding of each user.

2. Human rights and fundamental freedoms on the Internet

The Internet is more than means of communication. This led to the occurrence of a virtual space, where users present a specific behaviour. This virtual space or cyberspace began to interact with the real world in domains such as: fundamental rights and freedoms, right to private life, use of personal data, etc. Consequently, a series of new behaviour rules with compulsory character which regulate social relations regarding the Internet, *the Internet Law*, appeared. The

Internet Law represents the "totality of juridical rules which regulate in a specific manner the social relations which are established through Internet" (Cimpoeru, Dan. (2012). *Dreptul internetului*, Bucharest: C.H. Beck Publishing House, pp.11).

The principles of Internet Law have their origins in international standards regarding human rights and derive from the Charter of Human Rights and Principles for the Internet, which has been developed by the Internet Rights and Principles Dynamic Coalition (Internet Rights and Principles Dynamic Coalition – IRP is an international open network convening individuals and organizations working to support the observance of human rights in online environment and in the entire range of domains of elaboration of policies on Internet. The Internet Rights and Principles Dynamic Coalition is based on the United Nations Internet Governance Forum) and inspire from the Association for Progressive Communications' Internet Rights Charter and other pertinent documents.

The Charter of Human Rights and Principles for the Internet which is based on WSIS Declaration of Principles of Geneva and Tunis Agenda for the Information Society, interprets and explains the standards of human universal rights within a new context, which is Internet. The Charter also emphasizes the fact that human rights are applied in both *online* and *offline* environments, and the standards regarding human rights as defined in international law are not negotiable.

The Charter of Human Rights and Principles for the Internet identify the principles of Internet policy which are necessary to observe the human rights in Internet era, to support the extension of Internet capability to be an environment for cultural, social, economical, political and civil development.

The Internet offers unprecedented opportunities for enforcing human rights and plays an increasingly important role in our everyday lives. Within this context, it is essential that all actors, both public and private, respect and protect human rights on the Internet. Steps must also be taken to ensure that the Internet operates and evolves in ways that fulfil human rights to the greatest extent possible.

To help realise this vision of a right-based Internet environment, the ten Rights and Principles are: (The Charter of Human Rights and Principles for the Internet (2014). The Third Edition, May 2014. Retrieved 28 December 2015 from http://internetrightsandprinciples.org/site/).

"**Universality and equality**

All humans are born free and equal in dignity and rights, which must be respected, protected and fulfilled in the online environment.

Rights and social justice

The Internet is a space for the promotion, protection and fulfilment of human rights and the advancement of social justice. Everyone has the duty to respect the human rights of all others in the online environment.

Accessibility

Everyone has an equal right to access and use a secure and open Internet.

Expression and association

Everyone has the right to seek, receive, and impart information freely on the Internet without censorship or other interference. Everyone also has the right to associate freely through and on the Internet, for social, political, cultural or other purposes.

Privacy and data protection

Everyone has the right to privacy online. This includes freedom from surveillance, the right to use encryption, and the right to online anonymity. Everyone also has the right to data protection, including control over personal data collection, retention, processing, disposal and disclosure.

Life, liberty and security

The rights to life, liberty, and security must be respected, protected and fulfilled. These rights must not be infringed upon, or used to infringe other rights, in the online environment.

Diversity

Cultural and linguistic diversity on the Internet must be promoted, and technical and policy innovation should be encouraged to facilitate plurality of expression.

Network equality

Everyone shall have universal and open access to the Internet's content, free from discriminatory prioritisation, filtering or traffic control on commercial, political or other grounds.

Standards and regulation

The Internet's architecture, communication systems, and document and data formats shall be based on open standards that ensure complete interoperability, inclusion and equal opportunity for all.

Governance

Human rights and social justice must form the legal and normative foundations upon which the Internet operates and is governed. This shall happen in a transparent and multilateral manner, based on principles of openness, inclusive participation and accountability".

3. Cybersecurity and final users

The notion of final user refers to persons who currently use information and communication technology.

Final users, who do not pay special attention regarding the protection of information systems against malware programs, become a huge source of vulnerability for critical infrastructure information. Also, they have the possibility to opt for installing in their information systems of programs which ensure protection of information systems. But, in order to achieve this, final users must have a certain degree of knowledge regarding the threats of cybernetic security and the adoption of some appropriate technical protection measurements. In this regard, a series of resources within the governmental sector and the private sector were used to prepare final users to determine them to be aware of the role of cybersecurity (International Telecommunication Union. (2009). *Cybersecurity: The Role and Responsabilities of an Effective Regulator*, The 9th ITU Global Symposium for Regulators, Beirut, Lebanon, pp.16).

The focal interests of the society are represented in many countries by a multitude of groups of the civil society which can have different forms and functions. The groups of the civil society manifest a growing interest in the field of cybersecurity in order to understand the social aspects which cybersecurity address (International Telecommunication Union. (2009). *Cybersecurity: The Role and Responsabilities of an Effective Regulator*, The 9th ITU Global Symposium for Regulators, Beirut, Lebanon, pp.16). These aspects refer, among others, to: human rights, civil liberties, right to privacy, consumer protection. We emphasize that over the recent period were created several non-profit organizations (The Society for the Policing of Cyberspace, Richmond, British Columbia, Retrieved 28 December 2015 from: http://www.polcyb.org/) of the civil society which have preoccupations regarding cybersecurity and cybercrime.

In conclusion, we appreciate that the reaction of civil society is a source of information for political decision-makers which try to adopt a holistic approach of cybersecurity beyond the interest of the government and of the business environment.

CONCLUSIONS

The Internet can be considered an instrument which allows the development of monitoring in digital environment on a very large scale (International Telecommunication Union. Cybercrime Legislation Resources. (2011). *Understanding Cybercrime: A Guide for Developing Countries*. Second Edition. pp.17. Retrieved 28 December 2015 from http://www.itu.int/ITU-D/cyb/cybersecurity/docs/ITU_Guide_A5_12072011.pdf). This situation creates the occurrence of some dangers to human freedoms: freedom of expression, freedom of association, freedom of movement (right to freely browse on Internet), right to knowledge and information, right to respect for private life, family and correspondence.

In the digital world, any activity leaves a trace. Some persons know how to cover or to erase a trace. The Internet users are responsible for the personal information they publish on social networks. All over the Internet people are encouraged to provide personal information, preferences and habits and disclose their personal locations. Some companies acquire possession of large amounts of personal data from their clients. Frequently, users are not informed by these companies as regards the purpose and the way of using this data, even if they consented to transmit it. Thus, by the inappropriate use of personal data, the users themselves could be threatened by possible dangers in the virtual space.

An important number of companies which carry out their activity on Internet, such as providers of social networks and services, take advantage of this situation. Thus, these companies carry out big profits by trading and exploiting personal data, which the users either freely sent it or were collected without their knowledge (Stein Schjolberg, Solange Ghernaouti-Helie. (2011). *A Global Treaty on Cybersecurity and Cybercrime*, Second Edition. Oslo: AIT Oslo Publishing House, pp.38-39). Criminal organizations know how to illegally get personal data and use it in order to generate substantial profits. Some criminals in the IT area commit the theft of identity crime in order to use personal data of the users for other criminal purposes.

The main organizations within the public and private sector which carry out activities on Internet consider protection of personal data and private life in the digital area a constraint with negative impact on commercial activities carried out on Internet rather than some fundamental human rights. These organizations forget that protection of personal data is a condition necessary for self-determination to protection of freedom of expression and human dignity, to freedom and democracy. Protection of personal data is a principle within the Universal Declaration of Human Rights (The Universal Declaration of Human Rights, Retrieved 28 December 2015 from

http://www.ohchr.org/EN/UDHR/Documents/UDHR_Translations/rum.pdf), which helps in consolidating democracy, social justice and fight against discrimination and violence. Public and private organizations must propose solutions regarding the security in the cyberspace, which have to be viable and convincing at national and international level, in order to allow to law enforcement bodies to act efficiently without infringing the fundamental freedoms.

The significance of the word *security* must be re-examined within its social and cultural environment. The same is valid for the word *freedom,* which can have different significances in different contexts.

In a global, interconnected and interdependent world, the objective regarding cyberspace security is to provide viable solutions to keep the national sovereignty, for the administration of the cybersecurity and for the fight against cybercrime and terrorism both at national and international level. At the same time it is necessary to be drawn up measures to stimulate a correct use of personal data and private life in digital field for any person.

As for the cybersecurity, it is necessary to know who controls it. And it is important to be redefined the concept of *network neutrality* as regards the fight against cybercrime and, also, to be kept the individual liberty and the civil liberty (Stein Schjolberg, Solange Ghernaouti-Helie. (2011). *A Global Treaty on Cybersecurity and Cybercrime*, Second Edition. Oslo: AIT Oslo Publishing House, pp.40).

Measures of cybersecurity, either technological, procedural, organizational or legal, must comply in a complementary and coherent way with the needs of the informational society. In this regard, human rights and democratic values for a secure and sustainable informational society will be protected.

Cybersecurity legal policies must establish, review and modify the relevant infrastructures which sustain information and communication technology. This requires update of criminal legislation, procedures and policies regarding cybercrime to approach the cybernetic incidents and to fight against cybercrime. Also, we consider that it has to be reviewed with priority the criminal legislation, the procedures and the policies regarding cybercrime in order to prevent, investigate or prosecute of all forms of cybercrime.

Cybersecurity legal measures must refer to the following aspects: security in electronic communications; use for criminal purposes of information systems; protection of personal data and private life; certification, digital signatures and Public Key Infrastructure-PKI-, etc.

Fight against cybercrime imposes also the modernization of law enforcement agencies, the creation of structures specialized in cybercrime, as well as the professional training in the field of cybercrime of law enforcement bodies.

REFERENCES

Cimpoeru, D., 2012 - *Dreptul internetului*, Bucharest: C.H. Beck Publishing House

Dupic, E., 2014 - *Droit de la Sécurité intérieure*. Paris: Gualino Lextenso Éditions.

Mitra, Ananda, 2010 - *Digital security. Cyber Terror and Cyber Security*, New York: Chelsea House Publishers, Infobase Publishing.

Stein, Sch., Solange, Ghernaouti-Helie, 2011 - *A Global Treaty on Cybersecurity and Cybercrime*, Second Edition. Oslo: AIT Oslo Publishing House.

Seger, **Al., 2012 -** Council of Europe. Global Project on Cybercrime. *Cybercrime strategies*, Strasbourg.

Singer, P.W., Friedman, **All., 2014 -** *Cybersecurity and Cyberwar*. Oxford: Oxford University Press.

*****, 2009 - International Telecommunication Union -** *Cybersecurity: The Role and Responsabilities of an Effective Regulator*, The 9th ITU Global Symposium for Regulators, Beirut, Lebanon.

*****, 2009 - International Telecommunication Union. Cybercrime Legislation Resources**. -. *Understanding Cybercrime: A Guide for Developing Countries*. Second Edition.