PESQUISA

RDBCI: Revista Digital Biblioteconomia e Ciência da Informação
RDBCI : Digital Journal of Library and Information Science

DOI 10.20396/rdbci.v15i3.8647632

FOR A CYBERSPACE INFORMATION POLICY: ADVANCES, PERSPECTIVES AND CHALLENGES

PARA UMA POLÍTICA DE INFORMAÇÃO NO CIBERESPAÇO: AVANÇOS, PERSPECTIVAS E DESAFIOS

PARA UNA POLÍTICA DE INFORMACIÓN EN EL CIBERESPACIO: AVANCES, PERSPECTIVAS Y DESAFÍOS

[1]Jakeline Amparo Villota Enríquez, [2]Mardochée Ogécime, [1]Maribel Deicy Villota Enríquez, Heriberto González Valencia

[1]Universidad Santiago de Cali, [2]Universidade Federal da Bahia

Correspondência
[1]Jakeline Amparo Villota Enríquez
Universidad Santiago de Cali
Cali, Colômbia
Email: javillota@hotmail.com
ORCID: http://orcid.org/0000-0003-3086-8268

Submitted: 23-11-2016
Accepted: 02-06-2017
Published: 26-06-2017

JITA: LH. Computer and network security.

RESUMO: O presente artigo consiste em descrever e analisar as políticas da informação no ciberespaço, tanto global como regionalmente, em diversas direções: programas, resoluções e projetos do setor informacional. Igualmente, se apresenta um panorama das mesmas na região Latino-Americana e o Caribe. Mediante uma análise documental da literatura relacionada com o tema, o artigo se fundamenta numa revisão de literatura levantada a partir de materiais científicos. Em consequência, conceitua-se o ciberespaço e caracterizam-se seus elementos, dimensões, estratégias e variações, analisando as políticas da informação do ciberespaço, partindo do cenário global para relacioná-lo, finalmente, com o da região da America Latina e do Caribe, com a ideia de abordar melhor a problemática. As políticas de Informação do Ciberespaço experimentam diferentes progressos em matéria da cibersegurança y temáticas relacionadas com as mesmas; resultantes das politicas da informação estabelecidas por cada Estado o Região.

PALAVRAS-CHAVE: Políticas de Informação. Ciberespaço. Cibersegurança. Cibersociedade.

ABSTRACT: This article is to describe and analyze the policies of information in cyberspace, both global and regionally, in different directions: programs, resolutions, and projects from the information sector. Likewise, an overview of the same is presented in the Latin American and Caribbean region. Through documentary analysis of the literature related to the topic, the article is based on a review of literature raised from scientific materials such as: books, thesis papers, dissertations, texts on internet sites and articles, resolutions, projects and decrees dealing with the same topic. As a result, cyberspace is conceptualized and its elements, dimensions, strategies and variations are characterized, by analyzing the information from cyberspace policy, based on the global stage to relate it, finally, to the region of Latin America and the Caribbean, with the idea of better addressing the problems. The cyberspace information policy experience a minor and slow process in the field of cyber war; resulting from the obstacle of international cooperation defined by the disparate ambitions of the State or region.

KEYWORDS: Information Policy. Cyberspace. Cyber security. Cyber society.

RESUMEN: Este artículo consiste en describir y analizar las políticas de la información en el ciberespacio, tanto global como regionalmente, en diversas direcciones: programas, resoluciones y proyectos del sector informacional. Igualmente, se presenta un panorama de las mismas en las regiones Latino-Americanas y el Caribe. Mediante un análisis documental de la literatura relacionada con el tema, este artículo se fundamenta en una revisión de literatura levantada a partir de materiales científicos. En consecuencia, se conceptualiza el ciberespacio y se caracteriza sus elementos, dimensiones, estrategias y variaciones, analizando las políticas de la información del ciberespacio, partiendo del escenario global para relacionarlo, finalmente con el de la región de América Latina y del Caribe, con la idea de abordar mejor la problemática. Las políticas de la Información del Ciberespacio experimentan diferentes progresos en materia de la ciberseguridad y temáticas relacionadas con las mismas; resultantes de las políticas de la información establecidas por cada Estado o Región.

PALABRAS CLAVES: Políticas de información. Ciberespacio. Ciberseguridad. Cibersociedad.

INTRODUCTION

The transverse nature of information and the use of ICTs in all sectors that constitute the heart of national life, such as: transport, energy, universities, libraries, nuclear power stations, culture, economy, will lead to the creation of a new deterritorialized place, meaning, the "cyberspace". Like any place, which is the competence of the State, in which the information of the Nation-State is recorded, circulated, stored and operated, special attention is required of all the lived forces of a Nation. However, by its scope, it becomes a challenge of control by the states, governments, decision makers in the field of information, legislators, etc. Since its elements constitute both the strategic parameters to be taken into account by the States and the actions to be taken through regional, national and / or international cooperation.

This space materialized by the internet as a tool of Information Technology and Communication, becomes an indispensable support of "globalization", capitalist and informational economy; it is also understood as one of the vectors of dissemination of democracy of values and freedom of expression. However, it constitutes a hegemonic and powerful tool, where the question of the privacy and sovereignty of States is constantly discussed. Cyberspace therefore establishes a space of conflict since it is where crime, terrorism, and competition between companies, individuals, ideas, powers of the State and military are developed. (Vera, 2104).

Thus, today, one can say that the interdependence that characterizes the international system nourish the relationships created by cyberspace. Despite the advantages involved, this reliance on information technology leaves States and society much more vulnerable to various types of attacks: computer attacks and instructions, cyber-terrorism, espionage of other states, etc.

In this sense, KEMPF (2012, p. 7) argues that: "Cyberspace presents ambiguous characteristics and marks a rupture with traditional boundaries in the sense of a universality of risk." Therefore, it cannot be concluded that there is a homogeneous distribution on the characteristics of cyberspace, on the contrary, it can be said that, for most actors, cyberspace presents significant differences in structure, which, at the same time impact safety conditions. The interests of disparity between the various actors, countries, and, even the regions themselves, are relevant factors to be taken into account.

It is important to highlight, for the understanding of this article that the concept of "Information Policies" refers to "a series of principles and strategies that guide a course of actions to reach an objective" (MONTVILOFF, 1990, p.11). Thus, information policies can be considered as a guiding framework for the action of a program, plan or activity. Politics is assumed as the decision of the government, which may be legislable or not.

This article describes and analyzes cyberspace information policies, both globally and regionally, in different directions: programs, resolutions and projects of the informational sector. Likewise, an overview of this issue is presented in our Latin American and Caribbean region. Therefore, we seek to conceptualize the term "Cyberspace" and characterize its elements, dimensions, strategies and variations; As a space beyond the virtual, emphasizing the different global and regional political approaches and analyzing their impacts on Latin American and Caribbean society.

It is necessary to know the initiatives taken by governments, non-governmental organizations, institutions at both global and regional levels to promote security in the context of the current Information Society. In the same way, understanding the dimensions of these Information Policies allows to create competencies in the resolution of the problems of the informational sector in the context of the digital revolution and to be informed about initiatives aimed at regulating cyberspace in a country or a region, Which will allow decision makers, users and information professionals to be aware of what is happening in their environment in order to be real agents of change.

The methodology applied in this study consists of a documental analysis of the literature related to the topic, both at the global and regional levels, so that from this perspective, we can better understand the scope of these information policies. This research was based on a literature review and a description of existing global and regional policies, their origins, especially their applications, in order to know their impacts on cyber society.

1. WHAT IS CYBERSPACE?

Basically, the term "Cyber" evolves from Norbert Wiener (1948), who conceptualized "cybernetics" as the "control and communication of the animal and the machine". The underlying idea is that humans can interact with the machines and that the resulting system strengthens an alternative interaction environment, which provides the basis for the concept of cyberspace. In the early 1980s, William Gibson (1984), the author of science fiction, used the term cyberspace in one of his books "Neuromancer". Thus, this word expanded in professional and academic circles; for years there have been many different definitions of cyberspace depending on the concerns and interests of the actors and authors.

For example, the author Gómez (2012) quote the definition of the Department of Defense of the United States of America, which considers cyberspace as:

> A global domain within the information environment consisting of an interdependent network of Information Technology (IT) infrastructures, including Internet networks, telecommunications, computer systems and embedded processors and controllers. (GOMEZ, 2012, p.170).

According to Ottis and Lorents (2011, p.4), the European Commission vaguely defined cyberspace as "A virtual space where electronic data of the world's computers circulate."

However, in the mercantilist logic in support of private initiative, the International Telecommunication Union (ITU) sees cyberspace as a place created through the interconnection of Internet-mediated computer systems. In fact, cyberspace includes:

> Users, networks, devices, software, processes, stored or current information, applications, services and systems that are directly or indirectly connected to networks whose safety depends on a set of tools, policies, security concepts, security safeguards, guidelines, methods risk management, actions, training, best practices, insurance and technologies that can be used to protect the assets of an organization and users in cyberspace [...]. That is why it must be ensured that the security properties of the organization's assets and users are achieved and maintained against the corresponding security risks in cyberspace. Security properties include one or more of the following: availability; Integrity, which may include authenticity and non-repudiation; and confidentiality. (ITU, 2008, p.6, 7).

According to Douzet (2014), Russians and the Chinese use little the term "cyberspace" or the idea of a space beyond borders, and pretend to talk about the Internet or information safety; taking these discussions to the field of the competence of States. In this sense, it refers to the Internet, precisely, as the global interconnection of authorized digital data processing equipment. Information and communication systems are not limited to the internet, but it is the Internet that has given origin to what is now known as "cyberspace".

In this way, within this study we will assume "cyberspace" referring to both the Internet and the space it generates: an immaterial space, in which de-territorialized changes take place among citizens of all nations, at an instantaneous speed that eliminates any notion of distance. Consequently, technically, we recognize that the Internet is the global computer network that connects enumerated autonomous networks, using the same system language. The qualification of the space that generates it, is subject to the contradictory representations, activism, politics, geopolitics, etc.

From this perspective, several authors believe that the internet and cyberspace are now unavoidable realities in the contemporary world and in geopolitics. Recent events have emphasized its importance in the security of national information. In this sense, ROBINE and SALAMATIAN (2014: 123) state that:

> The Internet is a network built on the real, made up of optical fibers, satellite links and machines that are located in terrestrial space; Cyberspace includes applications that explore the Internet and seem to escape from the earth's space, forming a new one.

2.1 Cyberspace: Layered Architecture

To better understand Cyberspace, it is evoked, its layered structure. This allows the decomposition of cyberspace as a yarrow which different layers can interact with each other (BRUNO, 2000). According to the authors, it can be divided into two, four, five or seven layers. And in all layers of this structure there are rivalries of power between authors, usually about technical issues, which limits are still very geopolitical. To simplify, the following four layers are presented, based on the perspective of Bruno (2000):

a)The first layer is **physical**; which is composed of submarine and terrestrial cables, a real backbone of the internet, radio, TV, computers and the physical infrastructure of the Internet that constitutes a set of equipment installed in the territory, subject to the limitations of the physical and political geography, that allow to construct, to modify or to destroy, to connect or to disconnect to the network. The authors Robine and Salamaatian (2014) show the importance and the strategic challenges of this infrastructure, since it is geo-located. Morenkova (2014) evokes, in the light of the recent revelations of Edward Snowden, a former analyst of the United States Department of Intelligence, who treats the independence of Russian IT infrastructures as a sine qua non National Security. Physical infrastructure was conceived as a perspective of opening and circulating information flows, without any integrated security. It was in this sense that one of the founding countries of the Internet, POUZIN (2013, p.23), estimates that, in order to "Secure the Internet, it must reconstruct it from the base".

b)The second layer is the **logical** infrastructure. This includes all services that allow the transposition of data between two points in the network, and thus, send and receive information, formatted in small data packets from the sender to the recipient. A logical architecture, based on a fundamental harmonization, a common language that allows all computers in the world to communicate with each other, under the Internet Protocol (TCP / IP). These services are routing (choosing a route by which data packets travel between two networks), naming (name that identifies network elements or users) or also addressing (which transforms the series of numbers that represent addresses in words intelligible to users). However, some aspects can be geo-located or not, depending on certain technical challenges (borrowed paths, domain names, IP addresses ...). Discussions and demands on this issue were addressed at the World Summit on the Information Society in 2003, where heated discussions arose because of the strong symbolic control exercised by the United States by the decision-making power of the Department of Commerce (ICANN), which evidence its cyberspace hegemony (RABOY & LANDRY, 2004).

c)The third layer is the **application layer**, made up of computer programs allowing everyone to use the Internet without deep knowledge of computer programming (web, e-mail, social networks, research engines, etc.). The recent revelations of Snowden demonstrate the problem of the worldwide success of software programs of some large companies (Google, Facebook, Amazon, etc.), which users trust their private data and are used ingeniously by marketing teams or services of intelligence of the countries. What Grumbach and Frénot

(2013) consider as the new black gold of the economy. Data does not evaporate in clouds, but is stored on servers managed by private or public entities, and often outside the territory of the entity.

d)The fourth layer is the one of **information** and **social interaction**, sometimes called cognitive or semantic. It is the users, the discussions and exchanges in real time around the world, the most difficult to capture (in certain measures) and represent geographically. This is not, however, less geopolitically relevant when it comes to determining, for example, that they are the most "friendly" countries on Facebook, in which languages the content is available in some regions of the planet, where or how the riots in social networks or disinformation campaigns against a government or an institution reach.

Also in the scientific literature, the author LÉVY (1998, p.104) has emphasized the conversation of this space in a terrain of geopolitical conflicts. In the author's conception, cyberspace designates "The universe of digital networks as a place for encounters and adventures, a terrain of global conflicts, a new economic and cultural frontier [...].

The conflicts that occur in cyberspace are characterized by their great diversity, whether techniques are used, objectives or their authors. Thus, to address fraudulent acts and activities related to cyberspace, the author Romani (2008) refers to a computer warfare to characterize actions aimed at paralyzing the information systems of an institution or a business, or to divert or distort the data. According to ROMANI (2008, p.11), there are three main modes of information warfare:

a) The **war on information**, which attacks the integrity of computer systems to perturb or disrupt its operation.
b) The **war for information**, which seeks to penetrate networks to retrieve information that circulates or is stored there.
c) The **war for the information**, which uses the computer vector for purposes of propaganda, disinformation or political action.

That is why, in the advent of the Information Society, in which information and communication technologies play a predominant role in the infrastructures of Nations and in the interaction among them; the information infrastructures try to be critical, since they can suffer incidents of different proportions that lead, for example, to dysfunctionalities. Thus, if they stop, the Information Society also stops, with serious consequences on the information assets of the real society (KEMPF, 2012).

Given this central role of information and communication systems and the extreme dependence of our societies, cyberspace tends to increase its territory more and more with the development of New Technologies of Information and Telecommunications (NICT), and its increasing interconnection and generalization of their usefulness in the daily life of States.

For this reason, the improvement of the protection and defense of information systems is an important national security issue where the constant intervention of the State, blocks of interests, organizations, etc., is revised according to its needs.

2. INTERNATIONAL CYBERSPACE POLICIES

Due to the global nature of cyberspace and the more active use of information and communication technologies (ICT), the cyberspace problem is reviewed from the universal and transnational nature, which affects countries, society and individuals. On the premise that the problem of information security would not be solved by the efforts of a single State or group of States or on a regional basis; addressing cyber incidents requires joint efforts by the international community as a whole. It is therefore pertinent to address briefly some global policies in order to promote cyber security.

3.1 The United Nations (UN)

The issue of information security has been addressed on the UN agenda since the Russian Federation in 1998 first introduced a draft resolution in the First Committee of the UN General Assembly. This resolution was adopted without a vote (A / RES / 53/70) and continued until it was a more detailed proposal, even though its contents were conflicting and probably unforgettable (UN, 2011). In the same way, the author ROJAS (2013, p.27) reports that:

> These draft resolutions became an annual frustration exercise: the Russian initiative, for many years, was rejected by some Western countries, but still has the undeniable merit of keeping alive the argument that a major legislative effort was needed.

In its section 3, resolution 66/24 invites all Member States to take into account the evaluations and recommendations contained in the report of the Group of Governmental Experts on developments in the field of information and telecommunications in the context of international security (UN, 2011, p.18); and continues to communicate to the Secretary-General his views and comments on:

a) The global assessment of information security problems.
b) Measures taken at the national level to strengthen information security and contribute to international cooperation in this area.
c) The content of the concepts referred to in paragraph 2 of the resolution.
d) Measures that the international community could take to strengthen global information security.

In a global framework, the United Nations (UN) has adopted several documents with respect to Information and Communication Technologies and security aspects. In this context, the first UN Disarmament and Security Commission of the UN General Assembly adopted several international resolutions and constituted a group of governmental experts (Rojas, 2013). This group presented a report in 2010 that promotes consensus among States on possible rules on the use of Information and Communication Technologies to adopt measures of confidence, stability and risk reduction, exchange of information on legislation and national security strategies relating to Information and Communication Technologies, and identifies resources for the least developed countries to strengthen their capacities.

In its Resolution 65/41 (UN, 2011), adopted in November 2011, the General Assembly of the United Nations decided to resume the work of the Group of Governmental Experts in 2012. These decisions should be based on the definition of confidence-building measures to strengthen Security or the search for a consensus on patterns of behavior in cyberspace. To this end, several United Nations Organizations are empowered to fulfill this goal.

3.2 International Telecommunication Union (ITU)

It is important to mention that the International Telecommunication Union (ITU) is a specialized organization of the United Nations, which main objective is the standardization of telecommunications, has jointly organized with the United Nations General Assembly, the World Summit on the Information Society, which held two meetings in 2003 and 2005, where the issue of Internet governance was discussed.

ITU works to establish an international framework to promote cyber security through a "Global Cyber security Program" and in 2008 created a high-level group of experts to propose a long-term strategy encompassing legal measures in order to remedy the failures of software products; as well as the prevention and detection of computer attacks and crisis management (ITU, 2009).

At the World Summit on the Information Society (WSIS) Forum in 2011, a high-level discussion was held on "Building trust and security in cyberspace". The Fourth Parliamentary Forum on "The triple challenge of cyber security: information, citizens and infrastructure" (ITU, 2011) was organized by the International Telecommunication Union, the Department of Economic and Social Affairs and the Inter-Parliamentary Union. The Economic and Social Council, the Department of Economic and Social Affairs and the ITU organized a special meeting on cyber security and development.

The Global Cyber security agenda, introduced by the ITU in 2007, continues to strengthen a framework of international response to the growing challenges. Since 2008, ITU has been collaborating with the "Multilateral International Alliance against Cyber branches (IMPACT)" and has established the first truly global multi-stakeholder alliance and the public and private sectors to combat them (ITU, 2008). According to Schjølberg (2008), ITU and IMPACT carried out in 30 of the least developed countries joint training programs on the creation of national IT incident teams, and 10 countries are currently developing their national teams.

With the publication of the handbook "Cybercrime: A Guide for Developing Countries" (ITU, 2009), ITU and the United Nations Office on Drugs and Crime signed a memorandum of understanding to collaborate globally, Member States to reduce the risks of cybercrime. In fact, the "National Cyber security Strategy Guide" was launched in 2011 to help governments develop their national strategies and responses (ITU, 2011).

Under the leadership of its General Secretary, ITU sought to strengthen its role in terms of cyber security, particularly with a view to a revision of the International Telecommunication Regulations in November 2012. The ITU General Secretary had already mentioned in The 2010, the idea of an international treaty, banning cyber war. According to BOCKEL (2012, p. 55), this will of the ITU is supported by China and Russia, they wish to use this space as one of the vectors of their approach to cyber security, as well as by most of the developing countries.

In contrast, some large Western countries opposed the idea of recognizing a legally binding basis for ITU's work on cyber security (BOCKEL, 2012). However, ITU agreed to play a useful role in developing national capacities (CERT creation, business strategies, etc.), particularly for developing countries.

3.3 Organization for Economic Co-operation and Development (OECD))

The Organization for Economic Co-operation and Development (OECD) is an intergovernmental body to which 34 countries, including Mexico and Chile from Latin America, belong. This agency is authorized to discuss public policies, seek solutions to common problems among members, identify best practices and coordinate national and international policies in various sectors, including the area of Information and Communication Technologies.

The OECD is also concerned, from an economic perspective, with cyber-attacks on businesses and their impact on the economy. According to Bockel (2012), the OECD published the guidelines on information systems security in 1992, which were updated in 2001, and a number of documents were issued, mainly on the protection of critical information infrastructure information.

During the ministerial meeting on the "Future of the Internet Economy", held in Seoul, Korea, from 17th to 18th of June 2008, a panel discussion was held entitled "Confidence-building" where some aspects were dealt with on cybercrime and identity theft in member countries. Thus, a cyber-security committee and cyber security working group were formed within the OECD and the functions of this group include the development of a list of confidence and security measures for cyberspace. However, from a geopolitical perspective, this discourse of trust has been due:

> To the will of the United States to turn that agency into a true "machine of trust-making" that played an important role during the "cold war", trying to establish measures of confidence in cyberspace, especially with Russia (BOCKEL, 2012, p. 56).

In fact, the "Seoul Declaration on the Future of the Internet Economy" (OECD, 2008, p.7 and 8), which resulted from the ministerial meeting, included the following recommendations on security and cybercrime, all of which aimed at "Strengthening trust and security", through policies that:

a) They protect critical information infrastructures against national and international security risks.
b) Reduce malicious activity online, by strengthening national and international cooperation among all communities of participants on their way to effective prevention, protection, sharing of information and response.
c) Promote research to respond to emerging security threats.
d) Strengthen cross-border cooperation between governments and enforcement authorities in the areas of cyber security improvement, anti-spam, and privacy protection, etc.

In June 2015, the OECD directorate of "Science Technology and Innovation" published the "Draft Council Recommendation on Digital Security Risk Management for Economic and Social Prosperity" (OECD, 2015). Establishes a series of principles intended to complement the processes of digital security of risk management. The document determines that the "interested parties" are governments, public and private organizations, individuals that develop in the digital environment the great totality or part of their economic and social activities. According to the Communications Regulatory Commission of the Republic of Colombia (CRC, 2015, p. 46): "This document establishes, for interested parties, the following general principles such as: knowledge, ability, empowerment, responsibility, respect for Human rights and fundamental values and cooperation ".

However, concerted efforts among Member States have led to consideration of the various dimensions of current cybercrime. Bockel (2012) referred to the lack of experience of the OECD with respect to cyber security. In fact, he states that: "This organization, however, should remain a mere forum for exchange among Member States for lack of real expertise on cyber security." (BOCKEL, 2012, p.57). On the other hand, the 2014 document of the Ministry of Defense of Spain on e-strategy revealed a dilemma caused by the diversity of perspective linked to the security and defense of Member States. This document reports that:

> While most national strategies aimed at addressing cyber security from a state security and defense perspective, the OECD's orientation has been essentially to coordinate initiatives to increase the global level of cyber security, although we can only increase the competitive advantages of the states of the new economy. Given this idea and, as many countries focus on articulating their national cyber security

> strategies, the OECD defines as a key policy objective of capacity building and the national industry sector in the area of cyber security. (MD, 2014, p.84).

3. CYBER STRATEGY OF THE EUROPEAN UNION

The European Union adopted in December 2002 the "European Security Strategy (ESS)" in which it planned a safe Europe in a better world. This document (EUROPEAN UNION, 2013) took into account the security context with the global challenges and the main threats. This security context, the product of the end of the cold war, is characterized by a growing openness of borders that indissolubly binds internal and external aspects of security. There has been a technological development that has increased Europe's dependence on interconnected infrastructure in areas such as transport, energy and information, thus increasing its vulnerability.

In the review of the ESS, in December 2008, the so-called "Solana Report" has already appeared with new threats and risks, security of information systems. As one of the new global challenges and major threats, the term "Cyber Security" was reported:

> Modern economies rely heavily on vital infrastructures, such as transport, communications and energy supply, as well as the Internet. The EU strategy for a secure "Information Society" in Europe, adopted in 2006, refers to the crime caused on the Internet. However, attacks on private or government IT systems in EU Member States have given a new dimension to this problem as a potential new economic, political and military weapon. Further work is needed in this area to explore a global approach to the EU, raising awareness and enhancing international cooperation. EUROPEAN UNION (2008, page 5).

Thus, in March 2010, the EU's internal security strategy was extended to several sectors to address serious cyber incidents. Among the threats identified, this strategy includes cybercrime, which "proposes a global, technical, cross-border and anonymous threat to our information systems and therefore proposes numerous additional challenges to the authorities. (EUROPEAN UNION, 2010a, p.14).

Europe, with its 1999 Common Security and Defense Policy, has developed defense programs and structures, such as the unitary body to protect each of its members against risks and threats. The most important security initiatives include:

a) The establishment of ENISA (European Network and Information Security Agency) in 2004 provides advice to the Commission and Member States on security and IT products (EUROPEAN UNION, 2009).
b) The Critical Infrastructure Protection Program (PEPIC), approved in 2004.
c) Europe's protection against cyber-attacks and large-scale disruption, improved preparedness, security and resilience.
d) Towards a general policy to combat cybercrime (EUROPEAN UNION, 2007).
e) The European Digital Agenda (EUROPEAN UNION, 2010b): in order to structure its main actions around the need to systematically address the following seven problematic aspects: 1)

> Fragmentation of digital markets; 2) Lack of interoperability; 3) Increase of cybercrime and risk of lack of confidence in networks; 4) Lack of investment in networks; 5) Insufficiency of research and innovation efforts; 6) Lack of literacy and digital literacy; 7) Loss of opportunities to face social challenges.

This agenda provides an insight into current and predictable problems and opportunities; and it will evolve based on the experience and rapid changes in technology and society. On the other hand, it proposes a set of legislative initiatives proposed in the framework of the Digital Agenda and distributed in the following points: a) a dynamic digital market; B) interoperability and standards; C) confidence and security; D) fast and ultra-fast access to the Internet; (E) promoting literacy, training and digital inclusion; F) benefits that favor ICT for EU society (EUROPEAN UNION, 2010b).

As for the Internet, the new situation provoked by Snowden's revelations about the United States' massive Internet surveillance programs creates an opportunity for Europe to become the architect of a transatlantic agreement that would establish the basic principles of Internet based on the respective democratic values. In this perspective, the inventor of the web, the British Tim Berners-Lee, has argued that it is important to create a global Constitution for the Internet (BERNERS-LEE, 2014).

According to Benhamou (2014), in this proposal, it would be appropriate to add a section prohibiting States from taking measures that could affect the operation of the network for all users. Also the creation of a transatlantic agreement that would establish an international legal exigency to the technological actions of the States that obstruct the good operation and the security of the network. Subsequently, it could be expanded by other democratic regimes to avoid new crises of confidence that weaken the global architecture of the Internet.

He also recalled the recent report of the European Union Senate on global internet governance, the development of a transatlantic treaty on internet governance is indeed a fundamental character for the countries of the European Union:

> The European Union must make its voice heard in the ongoing debate on the future governance of the Internet. But it is true that its credibility will be even stronger than it has, internally, rethought its digital future to conquer a real weight in cyberspace. (MORIN-DESAILLY, 2014, p.149).

Several steps have been taken in the European framework, but still need to converge efforts, especially to achieve technological independence. At the heart of the development of a European cyber security policy would be the comprehensive development of a European cyber security strategy. In order to keep pace with these challenges, the European Parliament proposed a resolution on the implementation of a Common Security and Defense Strategy. Other proposals include the creation of a council, a coordinator or a European cyber security agency.

3.1.Cyberspace in Latin America and the Caribbean

According to a study by the United Nations (UN, 2013), the available knowledge about the overall picture of cyber threats and responses from governments in Latin America and the Caribbean is incomplete. This study reports that: "All that is known about the cyber threats scenario in the region is based on sporadic reporting without solid foundation bases." (UN, 2013, p.1).

Therefore, in 2012, governments noted an overall increase in the frequency of cyber incidents compared to 2011, even when the definitive quantitative data were incomplete or unavailable. According to the UN report (2013, p.3):

> The minimum increase of cyber incidents evaluated during the period 2011-2012 recorded by a government was between 8% and 12%; while at the upper end, two other countries recorded a 40% increase. Most governments cited the increase at some point within this scale, although it is interesting to note that several reported that, overall, fewer incidents were detected.

In this sense, Martin (2015) argues that this perceptible disparity in the percentage of cyber incidents between states is due to the disparity of Internet users in Latin American countries. This is an important element of the context to be taken into account in the assessment of cyber risks. Thus, the author states that:

> It could easily be said that less-connected countries experience a statistically lower risk in their area where internet penetration is already well advanced by the simple effect of fewer potential victims. However, in the least connected countries, the large absentees are the individual users, especially those who are located on the periphery of the communication infrastructure network, such as rural areas and areas of extreme poverty. It has as a logical effect a low representation of attacks directed against public and private institutions. On the contrary, in the most connected countries, the population is directly involved in security issues and can have an effect on the actions to be carried out by their individual behavior and the expression of a political claim. MARTIN (2015, p.5).

On the other hand, the UN document (UN, 2013) reports that activism, or cybercrime for political reasons, received great media attention in 2012, and information provided by Member States shows that this form of cyber incidents is truly increasing in the region. According to the UN (2013, p.4), two countries reported:

> Coordinated cyber-attacks in response to legislative initiatives aimed at strengthening the enforcement of copyright laws and reforming tax codes. In both cases, ratification of the respective bills approached; hacking forums were saturated with plans to carry out large-scale cyber-attacks against government infrastructures if that legislation was not be banned.

Despite its greater visibility, activism did not replace pecuniary benefits as the main motivation underlying the invasion and illicit use of the internet in the region. Hackers continued to search for personal and financial data and feeding online black markets around the world. However, it is impossible to measure accurately,

> The quantitative impact and economic losses caused by the theft of information in the Americas and the Caribbean in 2012. The number is extremely high, probably higher than the losses caused by any form of crime, including drug trafficking. UN (2013, p.5).

The author Martin (2015), worried about the new trends of cyber incidents against our infrastructures, those that involve the main vulnerabilities in the availability of energy, communication services, necessary resources in the productive process, evidenced a lack of conscience and interest on cyber security issues. In fact, he says that "while infrastructures in Latin American countries present innumerable security flaws, some are not even protected by a simple password" (UN, 2015) quoted by MARTIN (2015, p.7).

It should also be mentioned that Latin American intelligence agencies lack personnel with a high level of knowledge, experience and understanding of the online threats scenario. In fact, some countries have worked to create units against cybercrime. However, these units often focus on digital forensics (finding the needle in the haystack), digital testing (discovery, preservation, management and presentation) and copyright anti-piracy. Thus, it is argued that:

> National authorities routinely encounter the development of the skills of staff responsible for cyber security and cybercrime, e.g. the involvement of technicians from various public institutions in courses on information security, incident management, social networking, Forensics and legitimate piracy. (UN, 2014, p. 91).

On the other hand, ICANN, in its report on the panorama of the cyberspace in Latin America and the Caribbean pointed to the problematic of the antiquity of the equipment of the Infrastructures of information. This report cited by the UN (2014) recalls:

> The problem of routing, one of the most important functions regarding the operationalization of the Internet [...]. However, in Latin America, the routing system is based on technologies that essentially have not been altered for more than 15 years. (OAS, 2014, p.93).

Lemarchand and Sidney (2014), in their approach to cyber security in emerging countries and Latin America, introduced the concept of ¨data heaven¨, referring to the true foundations of international cybercrime, which constitute a major obstacle to the fight against cybercrime. These digital paradises are defined as places where a criminal can act or lodge servers and illegal content with impunity. According to the authors, these paradises are constituted by:

> States or private sector actors providing lax structures, accommodation or laws; For example, they guarantee their clients not to follow up on any request for international cooperation, and in the form of tax havens, to promote the proliferation of cyber-criminal acts to judicial immunity, greatly hindering the efforts of the international community. (LEMARCHAND, SIDNEY, 2014, page 22).

Some authors argue that the cybernetic environment of Latin America and the Caribbean favor the development of cyber incidents. Thus, it seems obvious that the economic opportunity and the lack of legislation catalyze the preference of our region for cybercrime, which makes it even more difficult to approach regulatory actors. Thus, GONCHAROV (2012, p.13) showed this fact, when he states that "in contrast to the preference for paid and proxy servers that criminals in Eastern Europe show, those in Latin America prefer to use free hosting services" .

It should also be noted that, in contrast to global standards, cybercriminals in America use common money transfer services to pay for the goods and services of cybercriminals. Since that, it could lead to their identification by the authorities; so,

> Cybercriminals hire "mules" to carry out the transactions. In addition, systems such as Web money are being widely used, this is evidence of growing international collaboration among cybercriminals operating in Latin America and Eastern Europe. OAS (2013, p.17)

Faced with this multidimensional growth of cyber incidents in Latin America and the Caribbean, the parties involved need to develop strategies to deal with such incidents in their various forms. And, that requires the multiplication of efforts and the convergence of both national and regional actors for the security of our cyberspace.

4. FINAL CONSIDERATIONS

According to the above considerations, we can highlight that the main characteristic that has contributed to this development and dependence on cyberspace is the treatment of information and the scope of Information and Communication Technologies. In the so-called "information society", or cyber society (Joyanes, 1997), the premise is that information itself has a value capable of generating power (political, economic, social, etc.). The greater the efficiency with which it is treated and managed, the greater its benefits. Thus, cyberspace has undergone a huge and rapid development, translating as a new model of dependency in today's society, which contrasts with the less and slow progress in cyber security. For this reason, it also becomes a field to be regulated by the actors who choose to operate in cyber society.

Cyberspace's global information policies are designed to respond to new security concerns in Cyber society; However, States have a common line of cyber defense; At times, they are aligned to a great power like, for example; the United States. However, global information policies, based on global or regional cooperation, show disparate ambitions.

Information policies planned at the national level to address cyberspace threats are based on international cooperation, although in cyberspace, we are facing threats that border borders. However, in the name of national security, global and cooperative policies evolve in an environment of mistrust. As always it is recommended that in matters of e-strategies there are no friends; At times, many States favor bilateral cooperation with their close allies and refuse to raise these issues in a multilateral framework.

In the analysis of the cyberspace scenario in the Latin American and Caribbean region, it is perceived that, in addition to the efforts agreed upon by the various actors in our region, the need for highly trained professionals who can protect networks, diagnose intrusions and effectively manage cyber incidents when they occur. These problems are most prominent in regions with low percentages of training programs.

From the revision of literature we can deduce that the dependence of our region on technologically developed countries, on external private capital, for lack of awareness of the value of information, of human capital, of investment, of appropriate legislation, and of the age of information infrastructure are factors that create barriers to cyber security. That is why we need to join efforts to develop and create information policies for the development of an infrastructure and infrastructure ideal for the region, in accordance with the digital and technological revolution.

DOI 10.20396/rdbci.v15i3.8647632

REFERÊNCIAS

BENHAMOU, Bernard. Organiser l'architecture de l'Internet. **France-Diplomatie**, n^o 4, Avril, 2014. Disponível em: <http://www.diplomatie.gouv.fr/IMG/pdf/OrganiserlarchitecturedelinternetBernardBenhamou-2.pdf>. Acesso em: 24 Jun. 2017.

BERNERS-LEE, Tim. **An online Magna Carta: Berners-Lee calls for bill of rights for web**. (The Guardian, 12/03/2014). Disponível em: <https://www.theguardian.com/technology/2014/mar/12/online-magna-carta-berners-lee-web>. Acesso em: 23 Jul. 2017.

BOCKEL, Jean-Marie. Rapport D´Information. Sénat - Session extraordinaire de 2011-2012. **Enregistré à la Présidence du Sénat** le 18 juillet 2012. Disponível em: <https://www.senat.fr/rap/r11-681/r11-6811.pdf>. Acesso em: 24 Jul. 2017.

BRUNO, Vitorio. **Arquitetura de redes de computadores**. Universidade Federal de Santa Catarina. Departamento de Informática e de Estatística. Florianópolis, SC, 2000. Disponível em: < http://www.joinville.udesc.br/portal/professores/flavio/materiais/Redes.pdf>. Acesso em: 22 Jul. 2017.

CRC. Identificación de las posibles acciones regulatorias a implementar en materia de Ciberseguridad. **Documento de análisis y consulta**. Coordinación Relaciones de Gobierno y Asesoría. Todos por un nuevo país. Comisión de Comunicaciones. Colombia, Julio de 2015. pp, 4 – 84.

DOUZET, Frédérick. La géopolitique pour comprendre le cyberespace. **La Découverte**. 2014. pp 3 – 21. Disponível em: < https://www.herodote.org/IMG/pdf/Douzet.pdf>. Acesso em: 20 Jul. 2017.

GÓMEZ, Ángel. **El ciberespacio como escenario de conflictos**. Identificación de las amenazas. Centro Superior de Estudios de la Defensa Nacional: Febrero, 2012. pp. 169 – 203. Disponível em: <http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/126_EL_CIBERESPACIO_NUEVO_ESCENARIO_DE_CONFRONTACION.pdf>. Acesso em: 28 Abr. 2017.

GONCHAROV, Max. **Russian underground 101.** Trend Micro Incorporated Research Paper 2012.

GRUMBACH, Stéphane ; FRENOT, Stéphane. Les données, puissance du futur. **Le Monde Diplomatique**. France, n^o 3, Janvier 2013. Disponível em: <http://www.lemonde.fr/idees/article/2013/01/07/les-donnees-puissance-du-futur_1813693_3232.html>. Acesso em: 28 Jun. 2017.

ITU. **Repport-fourth parliamentary forum on shaping the information society.** The triple challenge of cyber-security: information, citizensand infrastructure”. ILO Conference Center International Labour Organization Geneva, Switzerland, 2011. Disponível em: <http://www.itu.int/net/wsis/implementation/2011/forum/inc/Documents/WSISForum2011OutcomeDocument.pdf>. Acesso em: 10 Mar. 2017.

JOYANES, Luis Aguilar. **Cibersociedad:** los retos sociales ante un nuevo mundo digital. McGraw-Hill. España, 1997.

KEMPF, Olivier. **Introduction à la Cyberstratégie**. Paris, Broché, 2012.

LEMARCHAND, Hugo; SIDNEY, Barbara. **Cybersécurité des pays émergents. États des Lieux. Les notes stratégiques**. CEIS. Paris, 2014. pp. 3 – 33.

LÉVY, Pierre. L´intelligence collective. Pour une anthropologie du Cyberspace. **La Decouverte/Poche**. Paris, 1998.

MARTIN, P. Edouard. Inseguridad cibernética en América Latina: líneas de reflexión para la evaluación de riesgos". **Documentos de Opinión**. Ieee. es. 2015.

M. D. Documentos de seguridad y defensa. Estrategia de la información y seguridad en el ciberespacio. **Escuela de Altos Estudios de la Defensa.** Ministerio de Defensa. España, Junio 2014. Disponível em: < http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/docSegyDef/ficheros/060_ESTRATEGIA_DE_LA_INFORMACION_Y_SEGURIDAD_EN_EL_CIBERESPACIO.pdf > Acesso em: 30 Jul. 2017.

MONTVILOFF, Victor. **Políticas nacionales de información -** Manual sobre la formulación, aprobación, aplicación y funcionamiento de una política nacional sobre la información. Programa General de Información y UNESCO, París: Unesco, 1990. Disponível em: < http://unesdoc.unesco.org/images/0008/000869/086995sb.pdf > Acesso em: 07 Ag. 2017.

MORENKOVA, Elena. De la sécurité informationnelle à la Cybersécurité: la redéfinition de la doctrine stratégique russe. **TRIBUNE.** Université de Paris, n. 586, v2, 2014. . Disponível em: <http://www.academia.edu/10278359/_De_la_s%C3%A9curit%C3%A9_informationnelle_%C3%A0_la_cybers%C3%A9curit%C3%A9_la_red%C3%A9finition_de_la_doctrine_strat%C3%A9gique_russe_Revue_D%C3%A9fense_Nationale_Tribune_n_586_D%C3%A9cembre_2014_pp._1-7> Acesso em: 20 Jul. 2017.

MORIN- DESAILLY, Catherine. L'Europe au secours de l'Internet : démocratiser la gouvernance de l'Internet en s'appuyant sur une ambition politique et industrielle européenne**. Repport d'information n° 696(2013-2014);** fait au nom de la MCI sur la gouvernance mondiale de l'Internet, déposé le 8 juillet 2014. Disponível em : < https://www.senat.fr/rap/r13-696-1/r13-696-11.pdf> Acesso em: 07 Ag. 2017.

OECD. **The Seoul declaration for the future of the internet economy**. Ministerial Session. Korea, June 2008. Disponível em: <http://www.oecd.org/sti/40839436.pdf>. Acesso em: 25 Jul. 2017.

OEA. **Tendencias de seguridad cibernética en América Latina y el Caribe**. Washington: SYMANTEC, 2014. Disponível em: < https://www.symantec.com/content/es/mx/enterprise/other_resources/b-cyber-security-trends-report-lamc.pdf > Acesso em: 25 Jul. 2017.
____. **Tendencias en la seguridad cibernética en América Latina y el Caribe y respuestas de los gobiernos**. Washington: TEND Micro, 2013. Disponível em: < http://www.trendmicro.com.au/cloud-content/us/pdfs/security-intelligence/white-papers/wp-

tendencias-en-la-seguridad-cibernetica-en-america-latina-y-el-caribe-y-respuestas-de-los-gobiernos.pdf > Acesso em: 07 Ag. 2017.
_____. **Reporte de seguridad cibernética e infraestructura crítica**. Washington: TEND Micro, 2015. Disponível em: < https://www.sites.oas.org/cyber/Documents/2015%20-%20OEA%20Trend%20Micro%20Reporte%20Seguridad%20Cibernetica%20y%20Porteccion%20de%20la%20Inf%20Critica.pdf > Acesso em: 07 Ag. 2017.

OTTIS, Rain; LORENTS, P. **Cyberspace:** definition and implications. Tallinn, Estonia: Cooperative Cyber Defence Centre of Excellence, 2011. Disponível em: <https://www.academia.edu/16137618/3rd_International_Conference_New_Functional_Materials_and_High_Technology_NFMaHT_2015?auto=download>. Acesso em: 06 Jun. 2017.

POUZIN, Louis. L'Internet doit être refait de fond en comble. **Les Échos**, n° 21442, 24 mai 2013. Disponível em : < https://www.lesechos.fr/24/05/2013/LesEchos/21442-102-ECH_louis-pouzin-----l-internet-doit-etre-refait-de-fond-en-comble--.htm> Acesso em: 30 Jul. 2017.

RABOY, Marc; LANDRY, Normand. La communication au cœur de la gouvernance globale. **Enjeux et perspectives de la société civile au sommet de la Société de l'information**. Canada: SMSI, Département de communication, 2004. Disponível em : < http://www.lrpc.umontreal.ca/smsirapport.pdf > Acesso em: 05 Ag. 2017.

ROBINE J.; SALAMATIAN Kave. Peut-on penser une cybergéographie?. **HÉRODOTE. La Découverte**. Paris, 2014.

ROJAS, Emilio. Cooperación internacional en temas de ciberseguridad. In. **Necesidad de una conciencia nacional de ciberseguridad. La ciberdefensa:** un reto prioritario. España: Ministerio de defensa, 2013. Disponível em : < http://www.defensa.gob.es/ceseden/Galerias/destacados/publicaciones/monografias/ficheros/137_NECESIDAD_DE_UNA_CONCIENCIA_NACIONAL_DE_CIBERSEGURIDAD_LA_CIBERDEFENSA_UN_RETO_PRIORITARIO.pdf > Acesso em: 07 Ag. 2017.

ROMANI, Roger. **Rapport D´Information. Sénat - Session extraordinaire de 2007-2008**. Annexe au procès-verbal de la séance du 8 juillet 2008. Au nom de la commission des Affaires étrangères, de la défense et des forces armées (1) sur la cyberdéfense. Strasbourg, France. Disponível em: < https://www.senat.fr/rap/r07-449/r07-4491.pdf > Acesso em: 07 Ag. 2017.

SCHJØLBERG, Stein; ITU Global Cybersecurity Agenda (GCA); High-Level Experts Group (HLEG). **Report of the chairman of HLEG**. Norway: ITU, 2008. Disponível em: < https://www.itu.int/en/action/cybersecurity/Documents/gca-chairman-report.pdf > Acesso em: 07 Ag. 2017.

SCHOENBERGER, Viktor; ZIEWITZ, Malte. Sciences and Technology- Law review. **Jefferson Rebuffed - The United States and the future of internet governance**. John F. Kennedy School of Government, Harvard University, The Colombia, 2006. Disponível em: < http://stlr.org/download/volumes/volume8/schoenberger.pdf > Acesso em: 26 Jul. 2017.

UIT. International Telecommunication Union, Rec. SERIES X: Data networks, open system communications and security. **Telecommunication security**. April, 2008. UIT-T X.1205

___. Recursos jurídicos contra el ciberdelito. **El ciberdelito: guía para los países en desarrollo.** Ginebra: Departamento de Políticas y Estrategias; División de Aplicaciones TIC y Ciberseguridad. Sector de Desarrollo de las Telecomunicaciones de la UIT, 2009. Disponível em: < https://www.itu.int/dms_pub/itu-d/oth/01/0B/D010B0000073301PDFS.pdf > Acesso em: 28 Jul. 2017.

UNIÓN EUROPEA. **Una Europa segura en un mundo mejor. Estrategia europea de seguridad**. Bruselas. 2013. Disponível em: < http://eur-lex.europa.eu/legal-content/ES/TXT/?uri=URISERV%3Ar00004>. Acesso em: 24 Jul. 2017.

UNIÓN EUROPEA. **Estratégia de segurança interna da União Europeia. Rumo a um modelo europeu de segurança.** Bélgica, 2010a. Disponível em: <http://register.consilium.europa.eu/doc/srv?l=PT&f=ST%2015670%202014%20INIT>. Acesso em: 24 Jul. 2017.

UNIÓN EUROPEA. **Uma Agenda Digital para a Europa**. Bélgica, 2010b. (Comunicação da Comissão ao Parlamento Europeu, ao Conselho, ao Comitê Econômico e Social Europeu e ao Comitê das Regiões). Disponível em: <http://ec.europa.eu/europe2020/pdf/europe2020stocktaking_pt.pdf>. Acesso em: 21 Jul. 2017.

UNIÓN EUROPEA. **Parecer do CES Europeu sobre a Comunicação da Comissão ao Parlamento Europeu, ao Conselho. Comitê Econômico e Social Europeu e ao Comitê das Regiões**. C255/98. 22.9.2010. Comunicação COM (2009). Sec. 149. Bruxelas, 30 de Março de 2009. Disponível em: <https://ec.europa.eu/transparency/regdoc/rep/1/2017/PT/COM-2017-134-F1-PT-MAIN-PART-1.PDF>. Acesso em: 18 Abr. 2017.

UNIÓN EUROPEA. **Informe Solana. Informe sobre la aplicación de la Estrategia Europea de Seguridad**. Ofrecer seguridad en un mundo en evolución. Bruselas: UE: Diciembre del 2008. Disponível em: <http://www.consilium.europa.eu/ueDocs/cms_Data/docs/pressdata/ES/reports/104637.pdf>. Acesso em: 24 Jul. 2017.

UNIÓN EUROPEA. **Comunicação da Comissão ao Parlamento Europeu, ao Conselho e ao Comité das Regiões**. COM (2007) 267 final. Novembro 2007. Disponível em: < http://eur-lex.europa.eu/legal-content/PT/TXT/?uri=CELEX%3A52007DC0267>. Acesso em: 22 Jul. 2017.

VERA, G. Roberto. La sociedad de la información en México frente al uso de internet. **Revista Digital Universitaria.** Volumen 5, num. 8, UNAM, México, 2004. Disponível em: <http://www.revista.unam.mx/vol.5/num8/art50/sep_art50.pdf> Acesso em: 05 Ag. 2017.

ISSN 1678-765X
9 771678 765041 17 >