Journal of Forensic Sciences & Criminal Investigation

Juniper Publishers key to the Researchers

Research Article
Volume 2 Issue 1- : February 2017

J Forensic Sci & Criminal Inves

The Vulnerability of Cyberspace - The Cyber Crime

Doris Karina Oropeza Mendoza*

Independent Research Professional, México

Submission: January 23, 2017; **Published:** February 21, 2017

***Corresponding author:** Doris Karina Oropeza Mendoza, Independent Research Professional, Doctor in Public Law, México, Tel: +521 22 88 26 93 15; E-mail: doropeza1012@gmail.com

Abstract

The benefits offered by ICTs to the millions of users around the world have allowed diverse activities in the physical world to be transferred to the digital environment, communication efficiency and the exchange of data and information have facilitated the realization of economic and commercial activities, as well as social, entertainment, education, research, in all of them there is the imminent risk of being a victim of criminal behavior that puts at risk the personal and patrimonial security of users, therefore fundamental is the fight against this threat.

Keywords: Cyber crime; Cyber security; ICT

Introduction

A secure digital environment is a subject of great importance in the current reality in the information society and the new economy that set the course of the culture, economy and progress of the world today. Daily traffic on the Internet increases considerably, thousands of users access various websites to consume some product or service of the many that digital companies currently offer, however, the digital ecosystem is highly vulnerable to attacks by digital criminals which endanger the safety of users, who may be damaged in their property or in their person. Therefore, it is vital for each nation to have an up-to-date legal system capable of effectively protecting users against any criminal behavior typical of this technological environment. Therefore, this paper aims at exposing, in principle, a brief theory about "The Cyber Crime", and its elementary aspects that must be recognized by the legal system.

A brief theory about cybercrime

For legal science, crime is an object of study of extreme importance in its objective of generating knowledge for its application in favor of social welfare. The security of each person (person in the broad sense of human rights and also of corporations that have legal recognition subject to rights and obligations) is fundamental to preserve the peace and order that favor the development of humanity, therefore, the criminal conduct perpetrated against these ends, are analyzed by the law scholars, for their effective control. The digital environment created through ICTs is a platform parallel to the physical world, where an international community joins in which, day in and day out, thousands of human beings interact for different purposes, in such a way that the search for a cyberspace that guarantees security, order and peace, is a fundamental theme for the study in legal science, in the search and support to the government, to counteract the criminal behavior that to the detriment of the virtual environment, have strengthened while progress of ICTs has spread throughout the world.

The view on electronic crimes must be specific in its treatment and investigation by the parties legally interested and by any user of cyberspace, unlike the physical world, cybercrimes have a unique structure that conditions the typology of crime, the scene of the crime, the instruments to perpetrate the crime, among many others, so that their persecution and even prevention must be regulated in a particular way, only in essence, has the same vector with the physical world as the common object of damaging the legal space of the other, affecting his person or his property. When we talk about cybercrime, it is fundamental to talk about two fundamental areas, on the one hand the subject of crime in its broad context and on the other of cyber security, two of the fundamental pillars for the creation of effective and efficient public politics with defined objectives. In this first section we analyze the basic concepts for these pillars:

I.**Crime in its broad context:** It has been considered generalized the term criminality, in order to cover several aspects that involve the behaviors with legal-criminal consequences due to the use of the ICTs. These aspects refer to cyber-crimes, computer crimes, cyber-delinquents or cyber-crime, cyber-victims, mainly. All of them are issues that must be united in a complete analysis on the subject and must converge in any norm

created. As part of an adequate analysis, it has been considered necessary first to establish definitions on each of the terms mentioned above, since in many cases there is the problem of the indistinct use of terms such as cyber-crimes, cybercrime or computer crimes, when each has its special branch of study, which limits its correct use for doctrinal and normative purposes. In the first place we must make a separation between the illicit conducts carried out in the physical space and those in the virtual world, that is to say, the typical behaviors, be they actions or omissions, that have juridical-penal consequences under the classic theory of the crimes, are perceived by our senses in an immediate and natural way, on the contrary the illegal behaviors perpetrated in the virtual environment are those that exclusively our senses can perceive through the use of an electronic device and whose platform of communication is essentially Internet.

Therefore, we make the following fundamental division: the first one is called physical crimes, and the second is an electronic crime, this classification now allows us to make a much more precise definition of the various concepts used for crimes committed through Use of ICT. In the space of crimes there is a classification that by its characteristics has legal and penal consequences in the physical environment; these are the so-called, computer crimes. On the other hand, we have the electronic crimes whose manifestation is carried out in the virtual environment; usually the name of this type of crimes is accompanied by the prefix cyber, which directly must lead to distinguish the virtual origin of the conduct committed. Faced with the classification mentioned above, the essential concepts are defined, which will allow us to create a firm theory of such illicit behaviors:

II.**Computer crimes:** Computer crimes are crimes committed in physical space, whose legal and penal consequences are those already known in the physical environment. This type of offense has as typical behavior the abusive use of a physical resource of the ICTs, without authorization of its owner or custodian. This behavior, despite being in the classification of traditional criminal conduct, should be framed in electronic crimes, as an ICT resource, in addition to the criminal uses the electronic device in order to access the data contained and perpetrate another or other crimes involving an exclusively virtual order. In order to clarify this section, the definition given to this type of crime is quoted by the United States computer fraud and abuse act, which defines it as "intentional access to a computer without authorization or excess of authorized access" [1]. There are many debates about the limits of the interpretation of unauthorized access; Matthew B. Kugler cites three points of view [2]: the first focuses on unauthorized access when evading a restriction based on computer code, to this is known in strict sense to the piracy or hacking.

The second approach is based on the subject of contractual law, which ensures that access is unauthorized when it exceeds the terms of the services given to a computer, program or website, and finally considers the existence of the crime under social rules (We must also understand it as rules of behavior) of Internet users, access in these cases is exceeded when the majority of users consider it unacceptable. In such a way that we can define to the electronic crimes like those criminal behaviors, which are perpetrated through the use of the diverse technologies of the Information and Communication, considered harmful, that violate to the users of these technologies.

III.**Cybercrime:** While there is no conclusive definition of what cyber-crime is, in the near future some experts have provided an analysis of what it is; Felicity Gerry and Catherine Moore offer us a congruent definition: "criminal activity making use of computers and the Internet" [3], for his part David Wall, does not define what is, but methodologically tells us what is not separating, as he points out, cybercrime of non-cybercrime, has called it the modus operandi of cyber-crime, and classifies three forms of crime:

i. Crime against machines (hacking, attacks),

ii. Crime using machines (fraud) and

iii. Crime in the machines (pornography, hate speech and offenses in social networks) [4].

Cyber-crime is an undesirable reality in all countries of the world where technology is present, to a greater or lesser extent, despite Soumitra Dutta and others: "it is in rapidly developed countries, where the role of the Internet presents a new and more potential power in its global role" [5]. The key difference between traditional delinquency and digital crime lies in David Wall's "computer nature, network structure and global reach" [6].

Parties in Cybercrime

The three general parts that converge in the cybercrime are:

a)Cyber victims: Any user in cyberspace can be the victim of a criminal attack, so if the minimum security measures are not available, being part of the triangle that constitutes the perpetration of electronic crimes is a latent risk. It should be pointed out that being a user is only a potential victim, and only acquires such category when the damage has been perpetrated.

b)Cyber offenders: This category is made up of those individuals who, using ICT as an instrument, carry out an offense classified as a crime. We might think that these are professionals with professional knowledge in telecommunications or software, but this is not always the case, in this regard Johannes M. Bauer and William H. Duton, make us worryingly the following: "Just as the Internet has tended to democratize access to information, it also tends to democratize some criminal activities, making them easier for non-computer experts to use the Internet to eat crime, such as fraud, leading some to talk about "Democratization of cybercrime" [7]. In addition, the deterritorialization that the Internet allows, favors expert criminals to operate in more

 How to cite this article: Doris K O M. The Vulnerability of Cyberspace - The Cyber Crime. J Forensic Sci & Criminal Inves. 2017; 2(1): 555576.

complex ways that make their capture and verification of crime more complex, an example of which is organized crime, according to David Wall, e-delinquents, are acting in a collaborative way, as these are literally distributed over the Internet and are not geographically located in one place [8].

c) The State: The third part of this structure is made up of government offices specialized in cyber crime, these entities have three functions:

i. the protection of Internet users in their crime prevention work,

ii. the reparation of the damage caused to the cyber victims, and

iii. The pursuit of cybercriminals for prosecution and punishment.

The benefits offered by the Internet, such as the often automated interaction, the screen-to-person deal, and global interconnection can be a double-edged sword in cyber security, hindering the task of persecuting government agencies; In addition, the ability of cybercriminals can exceed the level of knowledge and experience of the authorities, so that prevention and e-safety education for Internet users are the best weapon against this stalking. In a delimited manner, according to specific behaviors, we can name as parts the following, worth mentioning, pointed out by Part Johannes M. Bauer and William H. Dutton, have made an interesting classification of the actors that intervene in the various cyber-crimes [9]:

i. Experts in cyber security

ii. Internet users

iii. Insiders: people within an organization who can undercut security, inadvertently exit a laptop on a train, or intentionally leak information

iv. Spammers

v. Hackers: those cracking systems for well-intentioned purposes, "white hats", and those with malicious intentions "Black hats"

vi. The criminals

vii. The terrorists

viii. The states

ix. Businesses and industries providing cyber security infrastructures, devices and software, such as anti-virus software

x. Internet governance communities focused on cyber security, including boards and standards committees.

The cybercrime in the web

There are some programs on the net that hide the user's identity, which can be a paradise for cybercriminals. In addition to the open network that we know, there is what has been termed a dark network (Dark web), which through some programs it is possible to keep the identity anonymous the user not to reveal the IP address, in addition to keeping the communications secret between the parts; It is a superimposed network [10] on the Internet, the logical or physical map of communication this type of networks, has a strict control, in addition the destination of the content is well determined; José María Berceló, explains that these types of networks are a system based on Hash tables, as substrates (understood as base or origin) where the location of values are determined [11], these systems can assign node identifiers consistently In a space where there are many identifiers; so the identified values are assigned an identifier, called a key, the protocol of the superimposed network, maps the keys in a single node among the connected, the messages are routed progressively, to the peers through overlap paths, of this form, it adds, each node sends the message to its node of its routing table that has a nearer identifier in the space of identifiers [12].

Values, key spaces and routing strategies allow the anonymity of the user with this type of system. One of the best known systems in the dark web is the program called Tor [13] which comes from the acronym the onion router, whose meaning is "Onion Routing". This is a program that must be installed on the computer to make use of it, and then it is possible to access the private information that is handled in it; according to the portal of this software, anyone can be user: family, business, activists, researchers, media, and army [14]. A noble use of such software, is the possibility of communication in countries where there is an important control of the Internet and the information that circulates, especially in cases where the government is considered as a repressor, however, the darkness that offers, it also becomes a space of opportunity to engage in criminal behavior, such as the transfer of child pornography, or communications for terrorist purposes. According to data from Verizon (2016), the 89% of the breaches, is due to financial or espionage motive [15], to say of Johannes M. Bauer and William H. Dutton [16], the most common electronic crimes that both companies and individuals can suffer are:

i. Spam: sending unwanted emails and spamdexing

ii. Theft of intellectual property: such as illegal downloading of copyright such as music or movies.

iii. Ransom ware: A particular form of malware that disables a computer or an e-mail account until the redemption is paid for its removal.

iv. Vandalism: how to deface a website.

v. Hacker a computer, for use by a web server for the purpose of carrying out other crimes such as phishing, spam, email attacks, click zombie fraud, zombie spam.

vi. Phishing: sending emails or other electronic messages

 How to cite this article: Doris K O M. The Vulnerability of Cyberspace - The Cyber Crime. J Forensic Sci & Criminal Inves. 2017; 2(1): 555576.

to acquire sensitive information, misleading a person to send money.

vii. The distribution of malware: this crime consists of installing a virus or other malicious code on computers or devices with access to the Internet, damaging even the operating system of the same.

viii. Data breaches, loss or theft of computers or electronic storage devices.

ix. Identity theft: through a computer system or email, criminals obtain personal data, making use of an identity for fraudulent access to credit card data, bank account, or even moral damage to a person.

x. The misuse of social media in ways that can harm users: same that translates into events such as cyber bullying or identity theft.

xi. Internal threats, such as a disgruntled employee or other privileged information intended to undermine security protocols.

xii. Cyber espionage: espionage by the government or companies to the information that circulates in the network, including the electronic mail or the information of a computer.

xiii. Cyber war: the attack that affects Internet networks, the Internet of things, websites.

Some of the successful attacks on companies in 2016, in accordance with Cyberedge [17]:

I. Malware (viruses, worms, Trojans, ransom ware)

II. Phishing /spear-phishing attacks

III. SSL-encrypted threats

IV. Denial of service (DoS/DDoS) attacks

V. Advanced persistent threats (APTs) / targeted attacks

VI. Web application attacks (buffer overflows, SQL injections, cross-site scripting)

VII. Watering hole attacks

VIII. Drive-by downloads

The need to fight against Cybercrime

Today's world is at a turning point for the future of the next generations, ICTs are a fundamental tool for the progress and development of nations, especially the Internet is an instrument of push for global, regional and local economy, for the advances in favor of education, health, among others, this has been recognized by the international community, in this regard the former secretary general of the United Nations, Kofi Annan, said: "The digital revolution has caused a surge unprecedented changes in technology. Used in a responsible way, it can greatly increase our chances of overcoming poverty and achieving the other priority objectives we pursue" [18], it is important to highlight the argument that warns: in a responsible way, since only with the correct use of such technologies can increase the profits, which discards any conduct contrary to order. Given the important benefits that ICTs offer for development, cybercrime "weakens or even decimates innovation, innovative sustainability and innovation-driven economic growth" [19]. In 2016, ten of the countries with telecommunications, technology, healthcare, government, retail, education, financial services and manufacturing industries were successful victims of cyber-attacks and occupy the first ten places are [20]:

i. Brazil 89.1%,

ii. France 82.4%,

iii. Canada 82.0%,

iv. Germany 77.8%,

v. United States 75.2%,

vi. Japan 74.6%,

vii. Mexico 74.4%,

viii. Singapore 72.9,

ix. United Kingdom 71.1%, Australia 63.2%.

Data provided by IBM, the average cost of data breach in the world in 2016 was of $4 million [21]. In a world where more than 40% of the world's population is currently using the Internet, according to data from the International Telecommunication Union [22], cyber-attacks represent a threat to the world's progress and stability, according to the economic forum within the global risk technological category, cyber-attacks can cause severe negative impacts especially for the business sector, the United States is the country with the greatest concern on the issue [23], nevertheless it is a risk that is extends to the whole world. Such is the gravity of the cybercrime that it is estimated that "crimes against data (the data that flow through the Internet) will affect a quarter of the population in the world in the year 2020" [24], therefore it is fundamental to have effective legislation and public policies to prevent, stop, investigate, prosecute and punish criminal behavior in the use of ICTs, especially the Internet, as well as the strengthening of cooperation between public and private sectors.

The legal battle against cybercrime

For the reasons mentioned above, the fight against these behaviors is a priority, for it exists two tools: the legal norms and the systems of technological security. In cyberspace, if the authorities try to follow the same line of "defense", the efforts made therefore would be useless, in a virtual platform, which as we have seen is a paradise for cyber-criminals for the ease with

which a crime may be committed. Therefore, it is required that the punitive force of the State be applied through the two tools mentioned above, which are explained in the following lines:

a)Tool 1: Technological security systems: In the fight against cybercrime, non-normative regulation is a tool that arises from social norms, called Netiquette, as well as architecture or code. Larry Lessig has published pioneering research on the subject, pointing out as a form of regulation in cyberspace, what has been called as a code, which is the use of Internet architecture or browsers, to create barriers that prevent comment various cybercrimes through the use, mainly, of the codification that can hardly be coded, which makes it not only a form of regulation, but crime prevention. Neal Kumar, speaks of a more restrictive form of crimes, and refers to monetary costs, as previously said, the electronic crime has a minimum cost or almost equal to zero, so the author points out that "the legal system must rely more on the costs of perpetration, the lack of perpetration costs is a high factor that explains the increase in cybercrime, the fact that committing a crime is cheap weakens the power of social norms" [25]. According to cyber edge group 2016, companies have several barriers that prevent them from establishing effective defenses against cyber-attacks:

i. Low security awareness among employees

ii. Too much data to analyze

iii. Lack of skilled personnel

iv. Lack of budget

v. Lack of management support/awareness

vi. Poor integration/interoperability between security solutions

vii. Lack of effective solutions available in the market

viii. Inability to justify additional investment

ix. Too many false positives

Implementing defense mechanisms would greatly reduce successful cyber-attacks, however, attackers continually develop more powerful software that cannot be identified by security systems or even break existing security codes, thereby diminishing the possibility of Prevention of cybercrime, and makes necessary the appearance of enforcement to punish the criminal conduct perpetrated.

b)Tool 2: The legal norms: It is undeniable that under the legal order society can be brought closer to an environment of order and peace, under the prevailing reality in which ethical and moral standards are not enough, which created the need for law, let alone in a society that is increasingly degrading, requires an entity with sufficient power to impose order and protect society in general from individuals who leave the sphere of order and violate stability, responsible for it is the State whose powers have been conferred, as said Jean-Jacques Rousseau under the social contract, which must necessarily move to cyberspace. Cyber security is the key word in the fight against cybercrime, it has been defined as: "technologies, processes, and policies that help prevent and / or reduce the negative impact of events in cyberspace that can happen as the result of deliberate actions against information technologies by a hostile or malicious actor" [26].

The global nature of the Internet and the non-existence of physical boundaries make cyber security a matter of common concern to everyone, the struggle cannot focus on a local or regional space to make the Internet a safe space for interaction. Sometimes users have to sacrifice their privacy, and even their security to access some web services or mobile applications, which is why it is indispensable to have legal measures to protect the user from falling into the hands of cyber-criminals. The right to privacy is intrinsically linked to the right to freedom of expression. Frank la Rue, pointed out that privacy "is the presumption that individuals must have an area of autonomous development, interaction and freedom, a" private sphere "with or without interaction with others, free from state intervention and Excessive unsolicited intervention by other unsolicited individuals" [27].

A.International legal instruments for cyber security: The World Summit on the Information Society urged governments around the world to prosecute cybercrime and noted the need to create effective and efficient national and international instruments and mechanisms to promote international cooperation among, inter alia, responsible for implementing the law on cybercrime. The vision of electronic crimes from the legal area cannot leave aside aspects that are interdependent and that in themselves are strengthened, such as respect for human rights and sustainable development, democracy and governance, while respecting the limits of the interaction in cyberspace, in favor of the creation of norms and public policies, attached to the social needs without contravening fundamental interests, and extending its protection to the diverse legal goods that are exposed with the illegal behaviors. There has been talk of respect by the authorities for the trend of free behavior of cyberspace, but this should be in accordance with the fundamental principles of respect for human rights, for which article 29 of the universal declaration of human rights in which it is mentioned:

i."Everyone has duties to the community in which alone the free and full development of his personality is possible.

ii.In the exercise of his rights and freedoms, everyone shall be subject only to such limitations as are determined by law solely for the purpose of securing due recognition and respect for the rights and freedoms of others and of meeting the just requirements of morality, public order and the general welfare in a democratic society.

iii.These rights and freedoms may in no case be exercised contrary to the purposes and principles of the United Nations."

One of the first documents on the subject, which is significant when trying to regulate a category as sensitive as criminal matters in the electronic environment, is "NETmundial multi stake holder statement" that was the result of the NetMundial conference [28], as a set of global proposals and discussions that presents a scheme of the necessary regulations for the evolution toward a governance in the Internet ecosystem, which has no binding force. As one of the pillars on which the discussion of the issues in NetMundial was based, it was the internet governance principles in which it was agreed that the rights that are protected in the physical environment should also be protected in the digital environment, in addition, the principles that were agreed in NetMundial are: freedom of expression, freedom of association, accessibility, freedom of information and access to information, development, cultural and linguistic diversity, unified space and non-fragmented, open and distributed architecture, favorable environment for innovation and creativity, open standards. It is fundamental to point out three principles that must be taken into account when regulating the subject of electronic crimes, such as the privacy principle, which was stated in the declaration that "it must be protected, which implies the right not to be subjected to arbitrary or unlawful surveillance, as well as the collection, processing and use of personal information.

Procedures and legislation regarding communications surveillance, interception of personal information, mass surveillance, should be reviewed with the intention of defending privacy and rights," the second principle is the protection of intermediaries, which considers that "the limitations of responsibility for intermediaries must be implemented in a way that respects and promotes economic growth, innovation, creativity and the free flow of information. In this way, cooperation between all parties should focus on stopping illegal activities within due process"; and lastly the fundamental principle of security, stability and resistance on internet, believes that "the network must remain secure, stable, resilient and reliable". Effectiveness in addressing risks and threats to the security and stability of the Internet depends on close cooperation between different stakeholders [28]. Another two documents of transcendence to national laws, to harmonize the fight against cybercrime and promote cooperation between states for this purpose:

a.The resolutions of the United Nations general assembly 55/63 and 56/121 on combating the use of information technology for criminal purposes: These documents seek to ensure that member countries harmonize their legislation under the following principles [29]:

i.States should ensure that their laws and practice eliminate safe havens for those who criminally misuse information technologies;

ii.Law enforcement cooperation in the investigation and prosecution of international cases of criminal misuse of information technologies should be coordinated among all concerned States;

iii.Information should be exchanged between States regarding the problems that they face in combating the criminal misuse of information technologies;

iv.Law enforcement personnel should be trained and equipped to address the criminal misuse of information technologies; Legal systems should protect the confidentiality, integrity and availability of data and computer systems from unauthorized impairment and ensure that criminal abuse is penalized;

v.Legal systems should permit the preservation of and quick access to electronic data pertaining to particular criminal investigations;

vi.Mutual assistance regimes should ensure the timely investigation of the criminal misuse of information technologies and the timely gathering and exchange of evidence in such cases;

vii.The general public should be made aware of the need to prevent and combat the criminal misuse of information technologies;

viii.To the extent practicable, information technologies should be designed to help to prevent and detect criminal misuse, trace criminals and collect evidence;

ix.The fight against the criminal misuse of information technologies requires the development of solutions taking into account both the protection of individual freedoms and privacy and the preservation of the capacity of Governments to fight such criminal misuse;

b.Council of Europe Convention on Cybercrime [30]: it is a normative benchmark of an international nature, which obliges the treaty countries to cooperate with each other in order to combat cybercrime. This treaty have the finality of: "Prevent actions directed against the confidentiality, integrity and availability of computer systems, networks and computer data, as well as misuse of such systems, networks and data facilitating their detection, investigation and prosecution National and international level and to provide agreements that allow for rapid and reliable international cooperation" [31].

Legal jurisdiction on the internet

Another aspect to be addressed is the issue of the jurisdiction of courts seeking to exercise their power and protect users, that is to say, How to know the competent authority in case it has been the victim of an electronic crime? The issue of jurisdiction on the Internet is not a simple matter precisely because of the global nature of it, however, some authors such as the case of Joel Reidenberg have simply pointed out that "the transmission of Internet protocols were designed to be geographically

independent but there are users and technologies within the physical boundaries and these endpoints provide the justification and ability for sovereign states to assert their authority" [32], so Internet Protocols (IP), are the tools which serve the authorities in order to determine precisely whether they are competent to investigate and, where appropriate, punish matters brought to their notice without infringing the sovereignty of another nation or even the jurisdiction of a state in a particular country. Thus, even on the Internet, which lacks geographical boundaries, the issue of jurisdiction is treated in the traditional way, i.e., the delimitation of IP addresses, reduce the treatment given to the Internet to confine it for jurisdictional purposes to have a Geographical limit.

Conclusion

Cybercrime is one of the contemporary threats that jeopardizes the development and progress of the Internet, severely affecting the various activities that millions of users in this platform carry out around the world. The figures are not encouraging, as we could see, cyber-attacks have a high impact in several countries around the world, their negative affects must be tackled, innovation and user confidence must be guaranteed, legal instruments and technological mechanisms are two fundamental tools to achieve this. The strengthening of national laws and international cooperation are weapons in the fight against crime in the digital environment.

References

1. 18 U.S.C.A. § 1030 (a)(2) Fraud and related activity in connection with computers. Legal Information Institute, USA.
2. Matthew B Kugler (2016) Measuring Computer Use Norms. Universidad Chicago Law School, USA, p. 2.
3. Felicity Gerry, Moore Catherine (2015) A slippery and inconsistent slope: How Cambodia's draft cybercrime law exposed the dangerous drift away from international human rights standards. Computer law & security review 31: 628-650.
4. David S Wall (2015) Dis-organised Crime: Towards a Distributed Model of the Organization of Cybercrime. The European Review of Organised Crime 2(2): 71-90.
5. Soumitra Dutta, William H Dutton, Ginette Law (2011) The New Internet World: A Global Perspective on Freedom of Expression, Privacy, Trust and Security Online. The Gobal Information Technology Report 2010-2011 - World Economic Forum in collaboration with INSEAD, comScore, and the Oxford Internet Institute.
6. Wall David S op. cit. note 4, p. 79.
7. Johannes M Bauer, William H Dutton (2015) The New Cybersecurity Agenda: Economic and Social Challenges to a Secure Internet.
8. Wall David op. cit. note 4, p. 79.
9. Bauer, Johannes M, Dutton, William H op. cit. note 7, p. 10.
10. Yolanda Panadero (2013) Redes Programables: Como Añadir Inteligencia A La Red Según Cisc. CISCO.
11. The data to be communicated, using computer language.
12. José María Barceló Ordinas (2008) Protocolos y aplicaciones de Internet. Editorial UOC, Spain, pp. 180.
13. https://www.torproject.org/
14. Tor, Who uses tor?
15. Verizon (2016) Verizon 2016 Data Breach Investigations Report.
16. Johannes M Bauer, William H, Dutton op. cit. note 7, p. 3.
17. Cyberedge (2016) 2016 Cyberthreat Defense Report. USA, p. 19.
18. Kofi A Annan (2000) 'We the peoples' The role of the United Nations in the 21st century. USA.
19. Emile Loza de Siles (2015) Cybersecurity and cybercrime: Intellectual Property and Innovation. Technology & Cybersecurity Law Group, USA, p. 5.
20. Cyberedge op. cit. note 17, p. 7.
21. Ponemon Institute LLC (2016) 2016 Cost of Data Breach Study: Global Analysis, USA, p. 1.
22. International Telecommunication Union (2015) Measuring the Information Society Report 2015. Switzerland, p.2.
23. World Economic Forum (2016) The Global Risk Report (11th edn). Geneva.
24. IDC (2015) IDC FutureScape: Worldwide Security 2016 Prediction, Massachusetts, USA, p. 1.
25. Neal Kumar Kaytal (2001) Criminal Law in Cyberspace. Georgetown University Law Center, University of Pennsylvania Law Review 149: p. 9.
26. David Clark, Thomas Berson, Herbert S Lin (2014) At the Nexus of Cybersecurity and Public Policy, Computer Science and Telecommunications Board. National Research Council of the National Academies Press, USA, p. 2.
27. Frank La Rue (2013) Promotion and protection of all human rights, civil, political, economic, social and cultural rights, including the right to development, USA.
28. Global Multistakeholder Meeting on the Future of Internet Governance (2014) NETmundialMultistakeholder Statement.
29. United Nations, General Assembly (2001) Resolution adopted by the General Assembly. Combating the criminal misuse of information technologies, USA.
30. Signed by 69 countries of the European Union and non-member States it has 51 ratifications.
31. Council of Europe (2001) Convention on Cybercrime. Europe.
32. Joel R Reidenberg (2005) Technology and Internet Jurisdiction. University of Pennsylvania Law Review 153: 1951.