AGORA International Journal of Juridical Sciences, www.juridicaljournal.univagora.ro
ISSN 1843-570X, E-ISSN 2067-7677
No. 1 (2015), pp. 62-66

CYBERCRIMINOLOGY
TRANSITION FROM TRADITIONAL CRIMINAL TECHNIQUES TO CYBERCRIME

G. M. Șinca

Șinca George Marius
Ministerul Afacerilor Interne
*Correspondence
Inspectoratul General al Poliției Române
Direcția Operațiuni Speciale
E-mail: sinca.george@politiaromana.ro

Abstract

In the last decade innumerable profound analyses of the cybercrime phenomenon were carried out that have led to predicting a future cyber-attack called the cyber war. Until now there hasn't been a real threat of this kind. From a criminology point of view, these two worlds, the real one and the virtual one, are totally different, so it's up to us, the observers, theoreticians and practitioners to elucidate the connection between these two worlds.

The transition to cybercrime by law breakers, made with a minimum effort, minimum investment and resources offered by the wide world users, sees that they could launch themselves into a no limits race.

Investigating methods and techniques for traditional crime improved because of the technological evolution within the last years. Unfortunately the phenomenon of transition from traditional crime techniques to cybercrime has not been studied enough. Measures were taken regarding the law breaker and the crime but the research area of studying the cause of crime, remained untouched, which is a great disadvantage for the justice system, both for authority structures and civil ones, leaving behind an opened door for a new superior level of crime.

Key words: cybercrime, transition, crime, threat, cybersecurity, internet

Introduction

Social reaction towards cybercrime is not nonexistent, on the contrary, along with technological evolution, access to information and to the user himself, is present but in a more attenuate way.

Once we access this big information cloud, called the Internet, we assume certain risks by utilizing this virtual environment, threats that stalk our every access.
Cybersecurity can be assured as long as each person develops a security culture; the reason behind it is simple, they must understand their role as a potential victim and the imminent threats that they are exposed to by modern communication methods.

The incidents regarding cybersecurity and the major cyber-attacks that some states and international organizations have fought with have determined the international

awareness of the need to adopt strategies and politics in this area of cybersecurity. So in the present there are national cyber security strategies like the ones from Estonia (after the cyber-attack from 2007, NATO opens the first Cybercrime Center Tallinn[1]), United States of America, Great Britain, Germany, France, which state the necessity of developing their own capabilities to fight cyber-attacks and set the action and cooperation frame between different governmental and non-governmental entities in order to limit the consequences. According to these strategies, a nation's efforts target the implementation of security measures which will lead to increasing the level of protection for cyber infrastructures, especially those who back up critic national infrastructures[2].

I. Similarities between traditional crime techniques and cybercrime techniques

In order to be more eloquent regarding the transition phenomenon from traditional crime techniques to cybercrime, I will show you a small crime comparative case between those two areas, the real one and the virtual one.

Of course the comparison between those two techniques is limited by many aspects such as concrete ways to make a crime, as well as ideological aspects or criminological regarding the subjects of cybercrime (regarding both a passive and an active subject).

Traditional Techniques		Cybercrime
Theft: *Breaking and entering with the intention of stealing*		**Hacking:** *Infiltration into a device or a communication network by means of unauthorized access.*
Fraud: *Obtaining by all means of communication financial data and information from a person with the intention of committing a crime*		**Phishing:** *A computer trick that sends spam messages to the victim in order to obtain data and financial information of a person for criminal purposes.*
Blackmail and Abuse: *Illegal or abusive use of position in order to obtain undue benefits, bribery, power or influence*	**INTERNET**	**Internet Blackmail and Abuse:** *Illegal access via data networks to control various personal, industrial and/or governmental databases, or blocking and altering them. The aim is to blackmail the victim in order to obtain money or satisfy other requirements.*
Fraud: *Deception, fraud, bad faith act in order to make a profit by harming another person's rights.*		**Internet fraud:** *Creating a profile similar to the victim by illegally obtaining information about him/her and using that information to commit crimes of fraud and deceit, usually to get material benefits*
Identity Theft: *The personification or representation of another person using personal data and its history to gain access, information or favors / benefits*		**Identity Theft:** *Creating a profile similar to the victim by illegally obtaining information about her and using those information to commit crimes of fraud and deceit. Usually to*

[1]http://www.nato.int/docu/update/2008/05-may/e0514a.html
[2]Strategia de Securitate Cibernetică a României, http://www.cert-ro.eu/files/doc/StrategiaDeSecuritateCiberneticaARomaniei.pdf, accesat astăzi 17.10/2014.

		get material benefits
Children abuse and exploitation: C*hild abuse and exploitation with indecent purposes, the most common cases are child pornography and sexual abuse*		**Children abuse and exploitation:** *Facilitate abuse (usually sexual) and their exploitation through modern communication devices.*

Table no. 1

*The *Italics* in this table are just an exemplification for a better comparison

Of course there are more crimes than shown in table number 1, but these are the most common ones on an international level. For a more plastic representation of this case I would like to bring into discussion a study belonging to Google Inc. security team that was published in 2010, which stated that they analyzed 240.000.000 web pages collected by Google's malware detection infrastructure for a period of 13 months and found that 11,000 domains were involved in malicious contamination (Fake AV)[3].

From a minimal perspective regarding the number of people in the world (~7.269.164.300 inhabitants[4]) compared with users of social networks (~1.82 milliard[5]) it seems that the fourth part of the world population socializes online. A report by the Electronic Privacy Information Center (EPIC) says that users spend 700 billion minutes per month on Facebook only. Looking at these numbers I realize that the chances are that only a small percentage of them (ex.0.001% = 7,000,000) may be infected with a computer virus at any second by accessing link traps.

As a logical deduction I can say that the offender's temptations and diversity of possible crimes are directly proportional to the number of users (potential victims) connected in the virtual world.

Paying more attention to the availability of information via computer systems penetration without authorization, a recent study done on 4,000 young people aged between 15 and 18 shows that 17% of them know how to find information via unauthorized commercial penetration, and one third of this group admits using such tools.

The study shows that 67% of young people surveyed have tried at least once to access a friend's email or a social network account without authorization[6].

Besides these factors, security risks regarding a computer system have been increased due to other factors strictly related to security culture. The most important are:

a. Increasing globalization;
b. Free flow of information;
c. Difficulty of securing contemporary computer systems;
d. Lack of user awareness and education in safety culture;

---

[3]Conference - The Nocebo Effect on the Web: An Analysis of Fake Anti-Virus Distribution, Google Inc., San Jose, CA, 27.04.2010, https://www.usenix.org/legacy/event/leet10/tech/full_papers/Rajab.pdf, accesat astăzi 20.10.2014.

[4]Populația lumii, http://www.worldometers.info/world-population/, accesat astăzi 22.10.2014.

[5]Statistică cu numărul de utilizatori în rețelele de socializare, http://www.statista.com/statistics/278414/number-of-worldwide-social-network-users/, accesat astăzi 22.10.2014.

[6] SANS, NewsBites, Vol. 11, Studiul Nr.39, 19 mai 2009, http://www.sans.org/newsletters/newsbites/newsbites.php?vol=11&issue=39, accesat astăzi 21.10.2014.

e. Unclear legislative regulations and certain jurisdictional issues.

II. Coverage area of cybercrime

Looking at the past year in terms of DDoS[7] type attacks, which essentially means overloading servers with signals from hacker-pirated PCs, I've asked myself a question as a starting point of this phenomenon which aims its attacks from and in all the countries. Which countries are targeted the most by this cyber-attacks? As a response, Google along Arbor Networks offered me the possibility to see, in real time, all the denial of service attacks (*DDoS – distributed denial of service/The flooding of a computer server with requests causing blocking or severe disruption of its operation*) across the world through *Digital Attack Map*[8]. Continuing my studies I realized that, in reality, this is a pattern, a criminogenic map that with very small changes / additions can be a milestone in the study of crime in the virtual environment. Arrangements for direct attack on Internet-connected devices are growing but among the most dangerous and widely used I may list the following:

Drive-by exploits, Worms / Trojans, Code Injection, Operating Kits, Botnet, Phishing, Compromise of confidential information, Rogue-ware / scare-ware, Spam, Targeted attacks, Theft / Loss / Physical damage, Identity Theft, Information Leakage, Search Engine Manipulation (SEP), False Digital certificates.

If these crimes have as an object the access and illegally manipulate the devices used by us and the information about us, then to be able to understand this aspect we need to deepen our understanding regarding the cross-border nature of everything that we may see as a risk, threat, or even cyber-attack, because technology is with us 24/7 (*gadgets, smartphones, computers and tablets, etc.*). It's a necessity and an obligation to ensure that we are living in a decent environment, if not, a safe one. Therefore the range of cybercrime is directly proportional to the range of connectivity of any device to any communication network.

III. Transboundary nature of cybercrime

Computer language is common for those who use computers, no matter the country they are in or the language they speak. This common language, and easy means of communication between users via a specialized network (the most eloquent example being the Internet or by a simple telephone line) leads to virtually limitless possibilities of connecting computers in the most remote corners of the world, and access the latest important information, with almost no effort. For geniuses in science, aces in this kind of activity, there are no obstacles and even if there were, with tenacity, everything can be overcome. Therefore, it is very difficult to prove an offense in computer science using classical methods of crime investigation, and the possibility that the offender is living in another area of the world, where the arm of the law cannot reach, is high[9].

Recalling the case of direct attacks on the websites of Bank of America, Wells Fargo,

---

[7] **D***istributed* **D***enial* **o***f* **S***ervice = Negare de Serviciu*

[8] DDoS Digital Attack Map, http://www.digitalattackmap.com/#anim=1&color=0&country=ALL&time=16092&view=map, accesat astăzi 22.10.2014.

[9] I. Vasiu, L.Vasiu, "*Informatică Juridică și Drept informatic*", Ed. Editura Albastră, Cluj-Napoca, 2009, pp.119-120.

PNC and many other banking institutions by Cyber fighters of Izz ad-din al Qassam, who after physical attack on the WTC towers began a direct DDoS attack which led to the failure of these institutions, the result was the setting up of services in different states and departments to track and determine cybercrime and cyber criminals. The first police service like this was founded in France, under the name of Information Security Club. They began with minimum provisions set by each country member of the European Community, and recommending provisions to be included in the laws of country members.

As a result, the Romanian Government issued Decision No. 271/ 2013 for the approval of the *Romanian cyber security strategy and national action plan on the implementation of national cyber security.*[10]

Amid the profound transformations that are found in cyber revolution regarding communication and access to information, many others have emerged, where new phenomena have diversified into areas such as organized crime, terrorism, cybercrime, etc.

Among all these criminal activities, Cybercrime has the most obvious international implications. The ease with which the Internet allows overcoming conventional boundaries may surprise even users. The question is, do we know which criteria should be applied to deter a competent country to follow and train for this type of crime? As a generic response, we have a system provided by Interpol (from the international research of fraud) to help investigators. It is based on national, permanent, contact points (Reference Points for computer-related crimes - NCRP's) from other connections, to profiles of international bodies and contacts from national institutions involved in fighting this phenomenon. It also provides an international legal framework established by mutual legal assistance treaties[11]. It recalls the golden rule of European criminal law regarding jurisdiction establishment from case to case differently depending on national legislation.

IV. Cyber revolution – offender in transition

With the emergence of cybernetics and subsequently virtualization, new opportunities in classic crime arise. At first it was a colossal effort to transpose the offense from one plan to another but with the passing years the transition is almost complete.

Offenses are almost perfectly adjusted to computerized environment and the offender has developed a new sense, which allows (even intuitively) to commit acts with much lower effort than "classics".

Recently offender classifications and typologies have been studied. We already understand that from the results of an offender's personality investigations and the shape of certain typology, we can assume a good knowledge of all the general and special aspects (psychological, sociological, cultural, anatomy, physiology, etc.) that influence or become a trigger for committing crime. The offender is reduced and tagged to a particular social category that have a behavioral diversity.

Each of them are unique, characterized by a multitude of physiological features,

---

[10] Publicat în Monitorul Oficial, Partea I nr. 296 din 23.05.2013.

[11] Gh. Alecu, A. Barbăneagră, R*eglementarea penală și investigarea criminalistică a infracțiunilor din domeniul informatic*, Ed. Pinguin Book, București, 2006, pp.252,253.

psychological and social attitudes which are not exactly found in all criminals.

This is why finding a typology of offenders is difficult, if not, almost impossible.

Legal aspects of crime are extended beyond defining, identifying, explaining their concept and structure. They are also extended to finding specific classification criteria in detecting and cataloging their general and specific characteristics.

Let us never forget that we can't see the face and body of a hijacker or other particularities so that you, the common user, or possible victim, could identify him and categorize him as a threat and could stay away from him.

On the contrary, taking advantage of these strengths, which he acquired through years of evolution of cybercrime, he will impersonate someone providing trust. This is especially true in cases of child pornography or sexual harassment, where "feelings" develop over time. These are false feelings created in order to blackmail, harass or exploit you. This may take the form of apps or reliable web interfaces, known to be safe and helpful, just to have your personal data sold and used by many marketing and advertising firms databases (false antivirus case[12]).

When we focus on the offender in the IT environment we must not let ourselves be influenced by the fact that he operates in a virtual environment and not physical. This is precisely why a cybercriminal can choose and work in any area of interest, such as identity theft or exploitation and harassment through social networks or fraudulently obtaining access through phishing method.

The Criminal matrix (Black Box) exhibits very well the theory regarding the committing of the offense in relation to its author. Committing any offense involves the whole being of the author, his cognitive-affective and volitional potential.

In psychological terms, the implementation of the criminal project is preceded by the specific process of the criminal offense conception.[13]

M. Rogers proposes a further reclassification of cybercriminals putting them in separate groups depending on the objectives and technological level "used", as follows:

Novices / Toolkit, technological beginners with very little technical skills and know-how principles; they use already designed software through the How-To User Guides downloaded from the Internet.

Cyber-Punk, able to write small programs themselves, which they use mainly for "misappropriation / impersonation" of web pages, spam applications or credit cards theft.

Interns, employees or former employees of an organization or company. They damage the company's system because of a personal vendetta. Their attacks are not based on technical skills, but rather on their exact knowledge about the level and type of existing security within the organization.

Coder / programmer, writing code exclusively to damage / destroy other systems.

Old-Guard Hackers, usually simply called hackers, highly skilled in the field, without criminal intent, which embrace the original first generation ideology of hackers; their interest lies in the intellectual-cognitive hacking.

Professionals and cyber-terrorists, they are the most dangerous, specialized professionals in industrial espionage and government, national security and intelligence agencies, etc.[14].

---

[12] Site folosit ca şi sursă de obiecte înjectate cu malware: http://malwarealarm.com/, accesat astăzi 20.10.2014.

[13] N. Mitrofan, V. Zdrenghea, T. Butoi, *Psihologie Judiciară*, Ed. C.E.P. „Şansa", Bucureşti, 2000, p.275.

Of course this list is not at all conclusive, but these are the main categories.
From a criminological point of view, the offender / murderer profile from the virtual environment is not well distinguished from traditional criminals. Possibly some features are screened and may not be valid or found in a new world of crime, where the evolution and development of the new methods require at least a general average IQ. I say this because fundamentally, their classification by temperament, psychological, social, physical or environmental factors that influence "career" offenders are identical. What distinguishes them, putting them in two different spheres, is the environment in which they operate. Criminal activity and social reactions are triggered as a response to their activity. An embodiment of this aspect, criminal personality was implemented in theory, validated by the research of the three giants - Kimberg, De Greef, Di Tullio - which revealed the basic features of the offender, such as:

- Self-centeredness: the offender would be highly individualistic and selfish;
- Lability: a poor mental and moral constitution of the offender;
- Lack of affection: cold, devoid of compassion for others;
- Aggressive: violence, hardness;
- Lack of self-control, psychological inhibition, etc.

J. Pinatel argues that the presence of these personality traits makes a person a criminal, only if they present a state of social danger too.[15]
This theory is not necessarily accepted when it comes to the characterization of cybercriminals. A good example would be that lability may not be found in this type of offender. The reason is that, in order to create a conjuncture in which you produce an offense in a virtual environment you need a certain intellect and a strong mental constitution which is not found in the feebleminded or the insane's criminal typology.
Among the most important types found in the virtual crime that have migrated from traditional crime, we have the following:

- Aggressive offender: he is considered the author of facts of violence, destruction of property, assaults to human dignity. He may cause remote damage through remote access applications, through breach of trust or by obtaining unauthorized access.
- Acquisition offender: a person who commits crimes against property, goods, cash values, etc. This type of offender is the most common, motivated by poor material circumstances or belonging to organized crime groups with oriented to such crimes.
- Professional offender: a person who commits criminal acts systematically, in order to gain livelihoods. Here we can find computer professionals who try to overcome their limits and complete their financial situation.
- The offender who is devoid of sexual brakes: This type of criminal commits sexual acts and is characterized by lack of moral sense and concern for the victim, he is characterized by brutality and has unrestrained sexual impulses. A dangerous type of offender, usually using social networks and blogs to find victims and later on, through this communication channel, to take advantage of them by various means of coercion. There is another typology, the one that after recording an act of perversion or other explicit sexual acts, they offer the recording via the internet to the general public for

---

[14] R. Chiesa, S. Ducci, S. Ciappi, Pr*offiling Hackers: The science of Criminal Profiling as Applied to the World of Hacking*, Ed. CRC Press, New York, 2009, p. 42; Rogers, M., *The Psychology of Hackers: The Need for a New Taxonomy*, 1999, http://www.infowar.com.
[15] Valentin Mirişan, *Criminologie*, Ed. Editura Imprimeriei de Vest, Oradea, 2000, p.72,73.

various purposes.

- Occasional offender: He is characterized by the fact that he doesn't have an innate tendency toward crime, he commits the crime under the influence of temptations caused by professional factors or external environment factors. Even the employees of a company can involuntarily produce such acts and sometimes they are not aware of that until after the occurrence. Note: this typology is not strictly dedicated to them.
- Ideological offender: The ideological (political) offender is the person who commits criminal acts based on political, scientific, religious ideas and beliefs etc. Attacks on government, civil or religious institutions, that promote an ideology contrary to any hijacker's ideologies is one of their preferred methods[16].

V. Cyber security and international (eu) legislation

Cybercrime can have many consequences, and in some extreme cases it may affect the economy or even national security. Security management systems become extremely important to ensure the absolute confidence necessary to carry out activities involving information systems and to comply with existing legal requirements.

The security requirements of a systems are very complex and are based on various aspects: operational, economic, technical, political, legal, societal and human resources aspects; having these in mind, the fight against cybercrime is fundamental.[17]

Rapid development of information and communication technologies has brought to the surface many negative aspects. On one hand, it allows a type of crime which would not be possible without information systems, and on the other hand, offers increased opportunity to commit traditional crimes.

Before the era of distributed intelligence issues, the main concern for security was to keep compeer data confidential, which could be achieved by simple physical protection (for example, by locking with a key or locking the room where the information was being kept).

Nowadays, with privacy, there are other important issues[18], security systems have become very complex and a concern for all organizations, whilst at the same time being utilized as a legal requirement.

At EU level, measures have been taken on this new challenge; among the many decisions there is the Directive 2009/136 / EC which requires an adequate level of privacy protection and security of personal data transmitted or being processed in connection with the use of electronic communications networks internal market.

Directive 2009/140 / EC of the European Parliament and of the Council from November 25th, 2009 requires taking appropriate technical and organizational measures to manage the risks concerning the security of networks and services.

Directive 2006/24 / EC of the European Parliament and of the Council states that

---

[16]Ibidem, p.85-88,91.

[17] Comunicarea Comisiei Europene, Către o politică generală de luptă împotriva criminalităţii cibernetice, COM(2007) 267 final; D. B. Hollis, An e-SOS for Cyberspace, Ed. Harvard International Law Journal, Vol. 52, Nr. 2, 2011.

[18] L. Vasiu şi colab., The tri-dimensional role of information security in e-business: A managerial perspective, Honolulu, Hawaii, USA, 2003; L. Vasiu şi colab., Three Strategic Dimensions of information Security in e-Commerce: A literature review based conceptual model, Surfing the Waves, Management Challenges, Management Solutions, Australia-New Zealand, 2003, p.1-10.

computer data are subject to appropriate technical and organizational measures to protect against accidental or legal destruction, accidental loss or alteration, storage, processing, unauthorized or unlawful access; data are subject to appropriate technical and organizational measures to ensure that their access can only be obtained by specially authorized personnel and data are destroyed at the end of the retention period, except those that have been accessed and retained.

European Convention of 2001 and the Framework Decision 2005/222 / JHA of February 24th, 2005 on attacks against information systems and the Proposal for a Directive of the European Parliament and of the Council on attacks against information systems and repealing Council Framework Decision 2005/222 / JHA [SEC (2010) 1122 final, SEC (2010) 1123 final] provides for liability of legal persons: a legal person can be held liable when the lack of supervision or control made an information crime possible.

In addition, Regulation (EC) No. 45/2001 provides that the entire processing of personal data by EU institutions and bodies which may present specific risks in relation to the rights and freedoms of data subjects are subject to prior checking the EDPS (European Data Protection Authority).The proposal of a Global Treaty in Cybersecurity and Cybercrime Field and building an International Criminal Court to prosecute cybercrime has been made[19].

Such a treaty, or a set of UN treaties, including treaties in the field of cyber security, cybercrime and other cyber treaties, would be a legal framework for peace, justice and security in cyberspace and would represent a turning point in regulating this field. Many large states, reluctant to sign and ratify the European Convention on Cybercrime, strongly support the adoption of the United Nations Treaty[20].

Recent efforts seem to indicate support for such an approach. Thus, international organizations and institutions such as the UN, Council of Europe, the Group of 8 (G8), ITU, (United Nations Office on Drugs and Crime (UNODC the only global intergovernmental body on crime prevention issues), Organization of American States (OAS), Economic Community Of West African States (ECOWAS) and the OECD have made and are making efforts to harmonize legislation[21].

Conclusions

Starting from the premise that there is no possibility of 100% security, technology surprises us with new innovations that we do not think of until we find ourselves involved as an active or passive part thereof. I, personally, glimpse great opportunities for all humanity: guaranteed development opportunities for the better, along with progress, criminal opportunists appear who, for various reasons, will make their presence felt. In conclusion, first for myself and then for the rest, I would say that the offense is with us always. There is no cure for this phenomenon but what we can do is to create our own security culture, to know not only our rights but the risks as well as vulnerabilities. Whether we are talking about traditional crime or about the one taking place in the virtual

---

[19] Vezi S. Schjolberg şi S. Ghernaouti-Helie, *A Global Treaty on Cybersecurity and Cybercrime*, A doua ediție (2011); S. Schjolberg, *An International Criminal Court or Tribunal for Cyberspace* (ICTC), A paper for the EastWest Institute (EWI) Cybercrime Legal Working Group (2011).

[20] Vezi http://www.cybercrimelaw.net/Cybercrimelaw.html, accesat astăzi 22.10.2014.

[21] I. Vasiu, Lucian Vasiu, "*Criminalitatea în Cyberspațiu*", Ed. Universul Juridic, Bucureşti, 2011, pp.73-74, 124-125.

environment, our needs and obligations are, and remain the same. There is a statement that says *that we are the product of our society*. I do not deny this but I would add something, *society can produce the elite providing that you are the first who wants it and does something about that.*

Bibliography

1. D. B. Hollis, *An e-SOS for Cyberspace*, Ed. Harvard International Law Journal, Vol. 52, Nr. 2, 2011;
2. S. Schjolberg şi S. Ghernaouti-Helie, A Global Treaty on Cybersecurity and Cybercrime, A doua ediție (2011);
3. S. Schjolberg, *An International Criminal Court or Tribunal for Cyberspace (ICTC)*, A paper for the EastWest Institute (EWI) Cybercrime Legal Working Group (2011).
4. I. Vasiu, L. Vasiu, "*Criminalitatea în Cyberspațiu*", Ed. Universul Juridic, Bucureşti, 2011, pp.73-74, 124-125;
5. SANS, NewsBites, Vol. 11, Studiul Nr.39, 19 mai 2009;
6. R. Chiesa, S. Ducci, S. Ciappi, *Proffiling Hackers: The science of Criminal Profiling as Applied to the World of Hacking*, Ed. CRC Press, New York, 2009;
7. I. Vasiu, L. Vasiu, "*Informatică Juridică şi Drept informatic*", Ed. Editura Albastră, Cluj-Napoca, 2009;
8. Gh. Alecu, A. Barbăneagră, *Reglementarea penală și investigarea criminalistică a infracțiunilor din domeniul informatic*, Ed. Pinguin Book, București, 2006;
9. L. Vasiu și colab., *The tri-dimensional role of information security in e-business: A managerial perspective*, Proceedings of the 3rd Hawaii International Conference on Business, Honolulu, Hawaii, USA, 2003;
10. L. Vasiu și colab., T*hree Strategic Dimensions of information Security in e-Commerce: A literature review based conceptual model, Surfing the Waves, Management Challenges*, Management Solutions, Proceedings of the 17th Australia-New Zealand Academy of Management Conference, 2003, p.1-10;
11. N. Mitrofan, V. Zdrenghea, T. Butoi, *Psihologie Judiciară*, Ed. C.E.P. „Șansa", București, 2000;
12. V. Mirișan, *Criminologie*, Ed. Editura Imprimeriei de Vest, Oradea, 2000;
13. *Strategia de Securitate Cibernetică a României*;
14. http://www.nato.int.