Cybercrime and its challenges between reality and fiction. Where do we actually stand ?

Raluca Simion[•]

Riassunto
Affrontando il tema della criminalità transnazionale, la criminalità informatica rappresenta una delle minacce più serie prodotte dalla globalizzazione. Questo articolo intende focalizzarsi su alcune politiche in questo ambito, innanzi tutto, definendo e delimitando concetti e trattando di argomenti che sono specifici della criminalità informatica. L'articolo si concentra, poi, sull'analisi di alcune minacce e sulle relative risposte e soprattutto sulle sfide poste dalla criminalità informatica e sull'evoluzione delle misure regionali e internazionali adottate per combattere questo tipo di criminalità.

Résumé
Si on parle de la criminalité transnationale, la cybercriminalité représente une de plus grandes menaces produites par la globalisation. Cet article veut offrir un point de vue sur les politiques dans ce domaine. Il s'agit de délimitations conceptuelles et d'arguments spécifiques de la cybercriminalité. L'article se concentre ensuite sur l'analyse de certaines menaces et leurs réponses et surtout sur les défis posés par la cybercriminalité et sur l'évolution des mesures régionales et internationales pour combattre ce type de criminalité.

Abstract
When speaking about transnational crime, cybercrime represents one of the major threats posed globally. The present article tries therefore to offer an accurate overview of criminal policies in the field. It starts with some conceptual delimitation and then presents arguments for the specificity of computer criminality. Threats and responses are briefly introduced in the context and then the author speaks extensively about the regional and international approaches, the challenges brought by the high tech crime to the law enforcement agencies and the possible evolutions of regional and international measures to combat this type of crime.

1. Introduction.

Cybercrime is a subject quite in fashion these days. Governments and media altogether seem fascinated by this argument and the evolution of the classical justice systems has clearly shown that it needs to be adapted in order to face the unique challenges of cybercrime. This article tries to bring together several issues which are currently under discussion in the global discourse in this field and to identify the difficulties that the law enforcement agencies need to deal with when fighting computer crimes.

[•] Ph. D. in Criminology at the University of Bologna, Legal Advisor of "Directorate of Criminal Law and Treaties, the Cooperation in Criminal Matters Unit", Ministry of Justice, Bucharest, Romania.

2. Cybercrime. The controversies of a definition.

On of the major polemics as regards cybercrime relates to its very definition. There is not consensus about that, as there is not consensus as regards the nature of cybercrime. The literature in the field is abounding with definitions of cybercrime, which are sometimes almost identical, sometimes quite different[1]. As it was well stated by the United Nations the term of cybercrime has been a topic for debate for the last 30 years and that the scholars have mainly concentrated in their articles on a three levels scheme: the computer as subject of a crime, the computer as object of a crime or the computer as instrumentality[2]. There were even opinions that the word cybercrime should be entirely deleted from the lexicon[3].

There were narrow definitions circulated such as the one mentioned by the Stanford Draft Convention which as it was well underscored by Gercke reduces cybercrime only to those crimes committed trough computer networks, leaving behind the actions that aim for individual computers, not neccesarily connected at the moment the crime occurs[4].

The original term of cybercrime, a product of the media, was strictly restricted to hacking activities[5]. Then, the concept of cybercrime, as Wall[6] well put it, meant " the occurrence of a harmful behaviour that is somehow related to a computer". Other definitions as it was correctly noticed by Yar[7] did not included only the illegal behaviours, but also the deviant behaviours. From a legal point of view this kind of broader definition could not stand up though.

When referring to cybercrime, despite the fact that is not offerring a definntion an interesting typology can be met in the provisions of the Council of Europe *Cybercrime Convention*, for the moment the only binding international instrument of this kind. This typology was adopted as a kind of working definition by the literature and also the actors that play a part in this field.

According to the substantial provisions of the Convention[8], under the generic name of cybercrime there are subscribed the four following categories: offences against the confidentiality, integrity and availability of computer data and systems, computer-related offences, content-related offences, offences

1 See Sette R., *Criminalità' informatica. Analisi del fenomeno tra teoria, percezione e comunicazione sociale*, Clueb, Bologna, page 27.

2 See the Background Paper of the Workshop *Measures to Combat Computer-Related Crime* of the *Eleventh United Nations Congress on Crime Prevention and Criminal Justice*, Bangkok, 18-25 April ,2005.

3 See Gordon S., Ford R., "On the definition and classification of cybercrime", in *Journal in Computer Virology*, n. 2, 2006, pp.13-20.

4 See for details Gercke M., *Understanding Cybercrime. A Guide for Developing Countries*, Draft April 2009, page 17 and following available at www.itu.int

5 See Wall D. S., *Understanding Crime in the Information Age*, Polity Press, 2007, page 10.

6 Wall D., "C*ybercrimes and the Internet"* , in Wall D. (Edited by), *Crime and the Internet,* Routledge, London-New York, 2001, page 2.

7 See Yar M., *Cybercrime and Society*, Sage Publications, 2006, page 9.The definition proposed by Thomas and Loader quoted in Majid Yar, Cybercrime and Society, page 9 "computer-mediated activities which are either illegal or considered illicit by certain parties and which can be conducted through global electronic networks".

8 A special chapter will be dedicated to the provisions of the Council of Europe Cybercrime Convention with special emphasis on the provisions related to substantial law.

related to infringement of copyright and related rights. As regards the content-related offences, it has to be said that the list offered by the Convention and its Additional Protocol from 2003 is not an exhaustive one, other illicit behaviours were included by the specialised literature in this category.

One can easily notice that despite the fact that the term cybercrime can be read in the very title of the Convention, it cannot be found in art 1 of the Convention which is entitled Definitions.

An important concept has to be reminded here, as it helps in understanding the categories of crime that could be included generically under computer crimes and that is computer systems. According to the paragraph a) of the first article "computer system" means *any device or group of interconnected or related devices, one or more of which, pursuant to a program, performs automatic processing of data.* The Cybercrime Convention Committee (T-CY) stated in its 2006 Meeting Report that the term of computer system has to be understood as covering not only desktop computer systems, but also "developing forms of technology, including modern mobile telephones and personal digital assistants"[9].

The lack of coherence as regards the definition of cybercrime was acknowledged also by the European Commission which admitted in its Communication *Towards a General Policy on the Fight against Cybercrime*[10] that terms such as cybercrime, computer crime, computer-related crime or high-tech crime are often used interchangeably. In the same Communication there are enumerated three categories of computer-crimes: traditional forms of crime(e.g. fraud and forgery) committed over electronic communication networks, publication of illegal content over electronic media and crimes unique to electronic networks (attacks against information systems, denial of service, hacking)[11].

As it can be well seen, the classification of the European Commission is almost identical with the one used in the Council of Europe Cybercrime Convention (with the exception of the offences related to infringement of copyright), being observed only slight conceptual differences, even though the offences comprised in the three categories are exactly the same. Unlike the *Cybercrime Convention* that does only enumerated the computer crimes, the Communication offers a operational definition of cybercrime "criminal acts committed using electronic communication networks and information systems or against such networks and systems"[12].

Before this Communication was issued, there were different orientations even among the law enforcement agencies, the concept being used rather in media, academic world or among the criminal justice actors[13]. Looking back at the beginnings, the concept has known a constant

9 See for the details T-CY Meeting Report T-CY(2006)11, 1st Multilateral Consultation of Parties, 22 March 2006, page 1, available at www.coe.int

10 Communication from the Commission to the European Parliament, the Council and the Committee of the Regions, *Towards a general policy on the fight against cybercrime*, COM(2007)267 final, Brussels, 22.5.2007, available at www.europa.eu

11 See the Communication, page 4.

12 The scholars' definitions are somehow concentrating around the same issues-see for example the definition proposed by Thomas and Loader mentioned earlier.

evolution. Although the term is inserted in a document that has no normative value, but it is rather connected to the criminal policies in the field, this could be a good starting point for future conceptual delimitation.

Now it remains to be seen if there is the ability to agree upon a common definition applicable at global level not only at regional level.

3. Nature of cybercrime. Towards a plea for its specificity.

In the academic discourse there are two orientations as regards the nature of cybercrime: one that has been launched by Peter Grabosky as "old wine in new bottles"[14] and the second one that was entitled by Majid Yar as the "novelty of cybercrime".

The first one practically states that the causality of cybercrime can be easily explained by appealing to classical theories and that they are just old crimes committing by using new techniques.

The second considers that computer crime is representing a totally new type of criminality that differs completely from the one committed in the real world.

I believe that we are indeed in front of a new type of criminality and its novelty comes from the environment where it is perpetrated. It is indeed true that the motivation of the cyberoffenders does not differ too much from that of the other criminals (at least not in the present days) and that many of the cybercrimes (with the exception of the so-called C.I.A offences) are just old crimes committed in a new environment.

On the other hand, even these traditional crimes such as fraud on line, if we are to take one of the most present computer crimes, are manifesting in a totally different way in the world wide web. If there were no differences, then no challenges would have appeared. But the location where they are taking place, the cyberspace, as we all call it today, creates many opportunities that cannot be encountered in real life. issues.

The question to raise is to what degree cybercrime presents certain particularities comparing to other crimes. Answering to that question could leave aside the opinions that these are just new concepts for old and I strongly believe that the uniqueness of Internet makes it quite impossible to adhere to this reductionist thesis.

Two of the main characteristics that confer its specificity come from the perceived anonymity and the transnational character. Of course, if one thinks of the transnational character, it can be met in the case of the already classical organised crime, but not to the same degree. These traits make difficult identifying the offender or the place where he lives and obviously, much more difficult to prosecute him and consequently to apply a sentence. This is what makes so important the need for an international instrument and for adequate adjustments of the internal laws. But this is not sufficient, as it will be seen.

4. Trends in cybercrime and responses. A glimpse in the criminal policies in the field.

4.1 Trends.

13 Yar M., *Cybercrime and Society, op. cit*., page 9.

14 See Grabosky P. N., "Virtual Criminality.Old Wine in New Bottles?", in *Legal Studies*, vol. 10, n. 2, 2001, pp. 243-249.

If the motives to commit cybercrimes are no different from those that stay behind the ordinary crimes, whether they are greed, revenge challenge, adventure, the opportunities are always dynamic in this case. Bearing in mind this, it has to be said that designing some valid and effective policies against this phenomenon proves to be quite a difficult task. To offer just an example, the legislation proves to be most of the times some steps behind the evolution of the cyberspace threats.

If we try to stick to the criminological theories and adopt the utilitarian approach, a crime would be committed when the benefits obtained from the crime would surpass the risks. The problem with the Internet is that because of its specificity, these risks are reduced to acceptable levels[15]. As it was correct noticed some while ago[16], the sophistication of the security measures determined an increase in the professionalization of the offenders and their need to work in organised groups.

This is confirmed by the Council of Europe reports on organised crime dating from 2004 and 2005[17] and more recently by the EUROJUST Reports 2007 and 2008[18] which showed that cybercrime had more and more ties with the organised crime. We have assisted in just a few years to a shift between the individual hacking, committed by rebel teenage geeks and the professional hacking, committed in an organized manner, as the cybercrimes are much more orientated on the economical aspect.

The last years major Internet threats, spam, spyware, phishing and pharming, are orientated to potential gains, taking advantage of the growth of E-commerce and do not follow the destructive pattern the classical viruses had not so long ago. Another trend is represented by the so-called *blended threats* which are mixing the characteristics of viruses, worms, Trojan Horses and malicious code[19].

Phishing, the so-called novelty of year 2004 designed with the purpose to get personal information and to use that information for fraud and identity fraud, continued to spread in 2005[20], to use more and more sophisticated methods and evolved into the more difficult to detect pharming.

New threats made their presence felt in 2006 and 2007. Starting from phishing schemes, more and more ID theft cases and financial fraud of banks were brought to the public attention. Additional to that, botnets, targeted attacks against governments and firms, web attacks, crimes committed in the virtual worlds

15 See Ghernaouti-Hélie S., "La cybercriminallité: reflects d'une certaine criminalité économique", in Auburger-Bucheli I., Bacher J-L. (sous la direction de), *La criminalité économique: ses manifestations sa prévention et sa répression*, L'Harmattan, Paris, 2005, pp.243-253.

16 Rogers M., "Organized Computer Crime and More Sophisticated Security Controls: Which Came First the Chicken or the Egg", in *Telematic Journal of Clinical Criminology*, 1999, www.criminologia.org

17 These reports are available at www.coe.int. The 2004 report was focused on cybercrime, fact that proves the attention the international institutions such as Council of Europe are granting to this type of criminality.

18 The reports are available at www.eurojust.europa.eu

19 See for details as well as a brief history of malware and current developments: Hughes L. A., DeLone G. J., "Viruses, Worms and Trojan Horses: Serious Crime, Nuissance or Both?", in *Social Science Computer Review*, 2007, pp. 78-98.

20 See Hunter P., "2005 IT Security Highlights- the day of the hacker amateur has gone, but there are still plenty of amateur users", in *Computer Fraud and Security*, January 2006, pp.13-17.

(e.g. Second Life) were among the top threats of the year 2007[21] . These latter threats continued to manifest in 2008 as well. The phishing schemes which aim practically at gathering mostly financial data, but also personal data in general, not only continued to develop, but according to the data brought forward by the specialised literature, experienced a significant growth, ever since the economic crises has begun to make its presence felt[22]. Of course one should not leave behind the Internet fraud that although not considered a computer crime *per se* has found ,due to the Internet characteristics, new forms of manifestation, the offenders changing their modus operandi from one year to another. For example, in 2008 the cybercriminals used extensively the already classical method of sending spam in order to commit identity theft, but the original element was represented by the fact that the unsolicited emails was allegedly coming from FBI officers or from a friend of the victim[23]. Botnets are the threats envisaged by the law enforcement agencies which are striving to find solutions to effectively deal with such a phenomena.

Another emerging problem is that of piracy. This is a very much controversial issue, because there are opinions that piracy related to software, music and films was incriminated as a consequence of corporate pressure and does contradict the free nature of the Internet. Lately, the P2P networks gave a lot of problems to the law enforcement agencies and not only for copy right issues but also because of child pornography[24].

The major threats on line can be extensively discussed and are making the object of numerous reports released from the industry or academia. Therefore, I have only tried to sum up here the main tendencies in order to have an overview of the issues the law enforcement have to confront with and consequently to better understand where the challenges are coming from. But the extraordinary dynamism of the Internet will turn the current threats into history as new and new menaces will intervene.

4.2. Responses. What criminal policies?

The responses offered by the state and the society to the threat posed by cybercrime consist in elaborating a legislative framework able to cope with the new types of crimes committed on the Internet, creating new security solutions and educating the Internet users so that they could protect themselves and avoid becoming a victim. We are speaking about a three layer approach that needs to be integrated in the transnational context of computer crimes. For that purpose to be fulfilled, concrete policies needed to be built up at national, regional and international level.

21 See Ifrah L., *Cybercrime: Current Threats and Trends*, page 4, available at www.coe.int

22 See for details and specific figures Brown I., Eduards L. and Marsden C., I*nformation Security and Cybercrime*, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1427776

23 See 2008 Internet Crime Report released by the Internet Crime Complaint Center, page 11-12, available at www.ic3.org

24 According to the *Council of Europe -Organized Crime Situation Report 2005*, surveys in 2003 suggest that 24% of the image searches in peer to peer applications are child pornographic images.

What does really mean policing the Net today? Can the Internet be so easily regulated? Are we talking about law enforcement, about private actors trying to regulate the Internet? What are the major trends in this respect? What are the best solution fit to deal with this? Kozlovsky[25] tries to define the classical model based on detention and punishment in opposition with what should be cyber-policing constructed on prevention strategies.

If the classical model is based on the efforts of the professional law enforcement agencies, the cyber-policing should be the result of a combination between the activities of public and private organisations. It is interesting to be seen how this model of policing is able to protect the potential victims and leave behind the traditional model that keeps concentrating on the offender.

The actual players involved in policing the cyberspace come from the private and public sector as well: the Internet users, the ISPs, corporate security organisations, state-funded public police and state-funded non-public police[26].

a. Legislation

When trying to solve the cybercrime problem, the states confronted with several problems. Their legislation was not adopted according to the new requirements of the IT. Domestic solutions had to be adopted or the existing laws had to be adopted. Sometimes, there were no procedural provision that could have assured the efficiency of the investigations. The globalisation of crime posed the problem of the cost of investigating and prosecuting transnational crime.

That is why the authorities soon realised that the domestic regulations were not enough and consequently the intervention of international and regional organisations was necessary in this respect.

Among them the UN, E.U, G8, OECD, Council of Europe. What these official organisations are mainly doing is building up an international legislation that can answer to the challenges of cybercrime. They are also trying to make public this new orientation in the criminal policies, to make people aware of the phenomenon.

The first initiative on computer crime was at European level, to be more precise, belonged to Council of Europe which organised in 1976 the Conference on Criminological Aspects of Economic Crime.

In 1983 OECD appointed an expert committee to discuss computer-related crime and to see how changes should be brought to the Penal Codes.

In 1990, UN gave a resolution on computer crime legislation and in 1994 was published the United Nations Manual on Prevention and Control of Computer-Related Crime.

G8 built up in 1997 a Subgroup of High-Tech Crime and the same year they adopted in Washington Ten Principles in the Combat Against Computer Crime[27].

25 Kozlovky N., A *Paradigm Shift in Online Policing. Designing an Accountable Policing*, http://crypto.stanford.edu/portia/pubs/articles/K146964995.html

26 The classification and detailed comments regarding each category in Wall D., *op. cit.*, pp.167-183.

27 Schjolberg S., *Computer Related Offences.* A presentation at the Octopus Interface 2004. Strasbourg 2004, available at www.coe.int

In 1997, Council of Europe created the Committee of Experts on Crime in Cyber-Space. The European Commission, Council of EU, USA, Canada and Japan had the possibility to send a representative to CoE. This gave the opportunity of a rapid alignment of the CoE policies with those of G8.

The co-operation was enhanced by the acting together of G8 and EU toward the "developments of a transnational network of actors"[28].

The *Cybercrime Convention* adopted by the Council of Europe[29] member states was created as a possible response to the global threat of cybercrime. It is in fact the only legal binding international instrument to tackle cybercrime and the result of several years of work. Apart from that, an *Additional Protocol to the Convention on Cybercrime*, concerning the criminalization of acts of a racist and xenophobic nature committed through computer systems was opened for signatures in 2003 and entered into force in March 2006[30].

As previously mentioned, The Convention offers a classification of cybercrimes in four big categories: offences against the confidentiality, integrity and availability of computer data and systems, computer-related offences, content-related offences, offences related to infringements of copyright and related rights.

An important part of the Convention is dedicated to the international aspects-international co-operation and to procedural measures. The transnational character of the computer crimes is one of the most problematic issues the law enforcement agencies have to face, as it will be shown further on. We are speaking about different jurisdictions and all the diversity that emerges from that. That is why the Convention tried by introducing the provisions related to international co-operation in computer cases to create some common standards and to fill up the gaps of the existing regional and international instruments in the field.

The Convention raised also some critics, especially from the American opponents but not only, who considered it too largely formulated and contradicting the American constitutional provisions such as the First Amendment. There were also persons who contested the big secrecy under which the Convention was drafted and the fact that there was no prior consultation of the civil society.

The Convention was signed also by non-member states of the Council of Europe. Among them, as lit emerged from the previous lines, USA which ratified the convention in 2006, after a long and controversial internal dispute. The fact that the Convention was signed also by countries from another continents would implicitly mean that it was intended to address the cybercrime issue

28 Norman P., "Policing 'high-tech' crime within the global context: the role of the transnational policy networks", in Wall D., *Crime and the Internet*, Routledge, London-New York, 2001, pp.184-194.

29 The Cybercrime Convention and the Explanatory Report are available at www.coe.int. It was opened for signatures in November 2001 and came into force at the 1st of July 2004. the main condition for entering into force was to be ratified by 5 countries, 3 from them had to be members of Council of Europe.

30 The Additional Protocol, the Explanatory Report and the list of ratifications and reservations can be found at www.coe.int. The main condition for entering into force was to be ratified by 5 countries. Italy did

globally. The next logical and legitimate question is if a regional organisation can assume such a task, bearing in mind that such an initiative is exposed to the risk of failure, as long as countries from other regions of the world would be reluctant to a regional initiative that does not come from their region.

b. IT Security

It is hard to bring forward in several lines the evolution of the IT industry and all the efforts this industry has undertake in order to improve the security measures designed for cyberspace. Suffice it to say that it is a very dynamic field, trying to keep up with the major threats the Internet posed.

That is why an extraordinary competition is taking place between different companies. Antivirus programs are not enough anymore, so firewalls, antispyware, antispam and more recently, antiphishing and antirootkit tools appeared on the IT market.

The evolution of the security market is toward all-in one products that is products that comprise, firewall, antivirus, antispam, antispyware, antiphishing and antirootkit protection in opposition to stand alone products. This measure proved to be much more efficient for companies and is starting to be adopted by individuals as well. It is much more convenient from a pragmatic point of view.

We know by now that the perfect product does not exist. Some are saying that the IT security is knowingly maintaining security wholes in their OS and products, so that they could justify their activity. Other scholars are questioning the figures periodically released by the big IT security industry companies, arguing that they are trying to create artificially the image of a growing threat, exaggerating the numbers so that their industry could prosper.

Whether these allegations are true or not, the role of the individual must not be passive just because he believes in the total efficiency of the security product bought by him.

Most of the times this wonder product proves insufficient unless combined with preventive measures which can be adopted if the people are aware of the potential dangerous to be found on line. This can only happen if the IT industry along with the authorities and the media are making some continuous efforts to educate the users.

c. The Role of Media in Educating the Internet users

Media plays a great role in educating the netizens. There are several trends referring to the relationship between media and crime generally[31]. The conceptions according to which the media is in search for spectacular subjects are entirely true, but media cannot be reduced only to that.

The European Court of Human Rights called the media the watchdog of civil society and

not signed it, Romania signed it and ratified it in 2009.

31 The interpretations of the relationship between crime and mass-media can be grouped intro three categories:
1. mass-media that causes criminal behaviour by broadcasting crimes, violences, aggression generally
2. mass-media that creates stereotypes regarding certain groups leading to the so-called moral panic phenomenon
3. mass-media determines the way in which criminality and punishment are consumed at popular culture level (see Carrabine, Igansky, Lee, Plummer, South, *Criminology. A Sociological Introduction*, Routledge, 2004, page 331 and following).

considered that in achieving its purpose, it is allowed to exaggerate sometimes. The importance the media plays when it comes to cybercrime is great.

Not only that the media can offer a real to life image of the cybercrime trends, but it could also contribute to the cybercrime prevention in the sense that by knowing the major threats and the state response, a person can prevent becoming a cybercrime victim or can be discouraged to turn into a cyber criminal. So the inputs offered by the press can be split into three : trends, policies and prevention.

For the purpose of our research, media can be really useful in the sense that we could find out to what extent the Romanian and Italian press for example are keeping the Internet users posted with the latest developments.

The question is to what degree is the press able to prevent us from becoming victims? Is it sufficient to speak about a new virus or spyware and its way of manifestation in some newspaper? Or is it also important to know how one can fight against them and prevent future attacks? I consider the impact the press can have on the potential victim an issue more important than the deterrent effect that could emerge from an article or a TV headline that presents how another group of hackers has been successfully been apprehended.

5. Reality vs fiction.

In order to understand if cybercrime is a real threat or just a product of media, state or private actors, I will start from three general statements that could be found in the above-mentioned Communication of the European Commission, namely:

1.”*the number of cyber crimes is growing and criminal activities are becoming increasingly sophisticated and internationalised*”;

2. “*clear indications point to a growing involvement of organized crime groups in cybercrime*”;

3.”*however, the number of European prosecutions on the basis of cross-border law enforcement cooperation do not increase*”.

These three points are revealing the main trends of the cybercrime phenomenon as seen by the law enforcement agencies at EU level. But are they true facts or they are just some myths launched by the press and the security industry and taken over by the LEAs as a justification for a serious of actions they elaborated? Can we currently speak about fear of cybercrime? We will try to answer to all that in the following pages.

a. The Game of the Statistics

The statistics have represented always an important aspect in the global discourse about cybercrime. But what kind of statistics are we talking about? The Communication of the Commission states that the number of cybercrimes is growing. On what is that statement based?

There is common knowledge about the lack of official statistics in this field. Taking into account the fact that computer-crimes have been introduced rather late as offences *per se* in the legislation on many countries, would be quite difficult to undertake longitudinal measures of crime[32] (charting of crime trends), as these crimes have no past category to be compared with. In any case, accurate official

statistics would offer a glimpse into the legal criminality. The most recent acknowledgement of the problem emerges from the *Council conclusions of 27 November 2008 on a concerted work strategy and practical measures against cybercrime*[33] which invites member-states in the medium term to work towards " developing(...) statistical indicators to encourage the collection of comparable statistics on the various forms of cybercrime".

Of course, this would not represent a true to life image of cybercrime, being well known that this type of criminality is amongst the least reported, so the black figure of crime gets to very high percentages. But at least it would represent a starting point. A more realistic image could be achieved by undertaken relevant crime and victimization surveys, activity that is underdeveloped as well[34].

Currently, most of the statistics are issued by IT security companies, from the private sector, that is why the figures they produce are often contested on the ground that they are not corresponding to true facts and they are only feeding an emergent industry that needs to justify its very existence .

These figures are taken over by the press and made available to the public together with rather apocalyptic comments and they are in a continuous crescendo. See for example the *Internet Security Threat Report* issued by Symantec in 2004 which said that the number of attacks blocked by their filters increased by 366% between July and December 2004[35] or the *Internet Security Report* issued by the same company in September 2007 which stated that " in the first half of the 2007, 212, 101 new malicious code threats were reported to Symantec, which was a 185% increase over the second half of the 2006"[36]

Let's take another example connected with one of the countries often associated with the cybercrime phenomenon-Romania which finds itself always in the reports issued by different organisations or private entities involved in the IT security area. If we should stick to some more recent examples, Romania has been mentioned in the 2007 *Internet Crime Report* released by the Internet Crime Complaint Center Report as being on the 5th place in the world when it comes to fraud[37]. The 2008 Symantec Security Report also has positioned Romania on the first place in Europe and on the 3rd place in the world among the countries that are hosting phishing sites.

When these reports were released, the Romanian media hurried to bring them to the audience's attention. All the televisions and major journals made of them the news of the day: a nations of cybercriminals. The statistics taken over from the Symantec Report were interpreted wrongly and the news were

32 Yar M., *op. cit.*, page 13.

33 Available at www.europa.eu

34 There are some countries where in the crime and victimization surveys have already been introduced items related to computer crime such as UK or USA, but in order to have a complete view of the phenomenon at a global level, this practice should be generalised.

35 See the *Symantec Internet Security Threat Report* VII(July-December2004) quoted in *Council of Europe Organized Crime Situation Report* 2005, page 41.

36 Quoted from David S Wall, "Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime", in *International Review of Law, Computers and Technology*, Vol. 22, no. 1-2, 2008, pp 45-63.

sounding like the country with the greatest number of phishers from Europe. But this is not what the report said.

Does this mean by any chance that cybercrime is a growing phenomenon in Romania? Can we possibly know that all the owners of the phising sites were Romanian, just because those sites were hosted in Romania?

What is the role played by media in this equation? Can we speak about a deliberately action of the media to create a fear of cybercrime? Is this just a part of big picture in which the myth of the Romanian hacker, cunning, highly intelligent, defrauding the poor westerners who in well faith tried to do on line transactions is brought to the attention of the Romanian reader? What is the line between reality and fiction? What should the mass-media do and what is actually doing? Too many questions and no clear answers, I am afraid.

As Grabosky emphasised "Overreaction may still be a useful strategy for organisational maintenance. One way to get attention (and resources) is to convince the world that the doom is imminent"[38]. But one just has to know exactly when to stop. And here comes the legitimate question how far the press has come with their stories.

There is no doubt the press is offering some valuable inputs as for what are the main trends when speaking about cybercrime, what are the major offences that occur and the modus operandi of the cyberoffenders.

But as the media is too much concentrated on the sensational and how to get the prime time, sometimes these episodes are exaggerated and much more important elements are left behind, such as how to prevent computer-crimes, how to avoid becoming a victim.

Important elements in the education of netizens can be gathered from the press, if the right articles are to be written. The press can contribute to the awareness raising of the Internet users and can represent a valuable actor in designing the prevention policies in the field. This is the right path the press should follow but for now it remains to be seen if the commercial would be left aside in order to follow this less spectacular direction.

b. Cybercrime and transnational organised crime

The concept of organised crime is much more disputed and controversial than that of cybercrime and my purpose here is not to bring to the surface all the polemics about it, but rather to discuss to what extent is cybercrime committed in an organised manner.

Different typologies of transnational organised crime have been sketched by the experts in the field, considering the transnational organised crime as an entity, an activity or concentrating rather on the effects of the transnational character of this type of crime[39].

I will therefore make use once again of the existing legal definitions, that is the definitions offered by the *United Nations Convention against Transnational Organized Crime,*

37 The statistics offered by the IC3 Report took into consideration the number of perpetrators.

38 Grabosky P., "Editor's Introduction", in *Crime Law and Social Change*, vol. 46, 2006, pp. 185-187.

39 See for details Cockayne J., *Transnational Organized Crime: Multilateral Responses to a Rising*

Palermo 2000. There are three definitions that are important from my point of view, if we are to relate them to computer crime: organised criminal group, serious crime and structured group. If one looks upon these definition gets to the conclusions that at least at an institutional level the option was made for a broader definition of transnational organised crime, that would encompasses all the currents in the field. The definitions are to be found in article 2 of the above-mentioned Convention, as follows:

-organized criminal group: *a structured group of three or more persons, existing for a period of time and acting in concert with the aim of committing one or more serious crimes or offences established in accordance with this Convention, in order to obtain, directly or indirectly, a financial or other material benefit;*

-serious crime: *conduct constituting an offence punishable by maximum deprivation of liberty of at least four years or a more serious penalty;*

-structured group: *a group that is not randomly formed for the immediate commission of an offence and that does not need to have formally defined roles for its members, continuity of its membership or a developed structure.*

All these elements can be easily recognised in the actual picture offered by cybercrime. The *Council of Europe Organised Crime Situation Report 2005* stated that although "the assumption that most cybercriminals are individual offenders (...), reports on organised forms of cybercrime have become more frequent in 2004 and 2005[40]".

Some years ago the economic profit as a motivation for committing computer-crime was rather rare, now it has become the common rule. It would be interesting to see if the proportion between organised cybercrime and cybercrime committed by individuals has not reversed in the last three, four years.

At least the official figures would indicate such a reversal which would come as no surprise taking into account the high percentages of Internet fraud, ID theft and skimming, that due to their transnational *modus operandi*, need the presence of organised groups.

What is important to be mentioned is the fact that there is an international legal framework that allows the states to bring to justice organised cybercriminals that are actioning in a borderless environment, namely the Internet.

Sometimes, the *Palermo Convention* represents the only legal instrument that can be invoked, especially in circumstances when between the issuing and executing countries (which are to be found on different continents) there is no bilateral or regional treaty into force.

c. Challenges for law enforcement agencies?

There is no doubt that cybercrime raised a lot of problems for the law enforcement agencies. Should computer crimes have been common criminality, these challenges could not have appeared, so I guess that indirectly the issues the police and judiciary have to face when tackling cybercrime are clearly stating that we

Threat. Coping with Crisis, International Peace Academy, April 2007.

40 See page 43 and 44 of the above-mentioned report available at www.coe.int

are taking about something really different compared with the traditional crime, something that needs special attention and special measures. There are a lot of discussions in the specialized literature as to what are the major challenges posed by cybercrime and therefore, I would not assume that my ideas would completely correspond with those belonging to the experts in the field. Still, I have tried to bring together three categories which would shortly be presented below:

c1.Challenges deriving from substantial issues

The appearance of the computer-crimes found the states somehow unprepared as there was no special legislation in place regarding computer crimes.

The situations such as the one created by the famous I LOVE YOU virus and the fact that there was no domestic provision in Philippines that would allow the criminalization of such a conduct has raised two issues that needed to be solved: the existence at national level of a coherent and adequate legislation in the field and secondly, the harmonisation of the domestic legislations so that the double criminality requirement which is essential in extradition procedures and mutual assistance in criminal matters could be fulfilled.

Regulating the Internet has proved until now to be one of the most difficult tasks of the public actors and the harmonisation of the legislation world wide might take some time from now on.

That would create the possibility for the offenders to take advantage of the legal gaps existing in some countries and to administrate their activity from there. Important progresses have been made, but still a lot remains to be done until a complete and coherent legislative framework could be created.

c.2 Challenges deriving from procedural issues

The *Communication of the European Commission*, previously mentioned, stipulates that the number of prosecution is not growing, despite of an increase in the number of cybercrimes. Referring to this problem Wall put it in a very plastic way that *the low prosecution rate is showing the absence of evidence or the evidence of the absence*[41].

He offers three possible explanations for this discrepancy: the exaggerated image created by the press, the lack of efficiency of the law enforcement agencies and the nature of the cybercrimes. The complexity of computer-crimes is not allowing for reductionist answers. The chance for being prosecuted for computer hacking in the USA is placed at 1 in 10 000[42]. As the above-mentioned examples, shows, there are countries especially those with a common law tradition where there is no principle of legality governing the prosecutorial phase, therefore, it will be no mandatory prosecution. The prosecution will rather take place in accordance with some very pragmatic criteria as related to the seriousness of the offence, the value of the prejudice. The criminal investigation would depend on the resources available and to the degree of prioritization established by the law enforcement agencies.

41See Wall D., "Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime", in *International Review of Law, Computers and Technology*, Vol. 22, no. 1-2, 2008, pp. 45-63.

Another problem would be represented by the fact that cybercrime requires a high degree of specialisation among the police officers, prosecutors and even judges.

The criminal investigation of computer crimes are circumvented to special requirements and techniques, starting from a computer search to preservation of computer data, real time collection of data etc. That means that for effective prosecution previous specialised training is needed. Some states already did that, others still need to develop valid training programs in this respect.

c3.Challenges coming from the transnational character

The transnational character of cybercrime represents one of the greatest challenges ever to the law enforcement agencies. Internet has no borders and consequently the cybercriminals can act from their homes affecting the lives of individuals located on the other side of the planet.

Without developing too much on it, it has to be said that transborder searches, positive conflict of jurisdictions and requests of mutual legal assistance in criminal matter can raise a lot a difficulties and can cause delays in solving cybercrime cases. The co-ordination between countries is in this context crucial, as long as we are talking about data extremely volatile and the classical channels of communication could in most of the times prove totally inefficient as timing and a response rate.

From this point of view, the challenges posed by the transnational character are maybe the most serious and with no effective solution developed up to now. It is important that organisations such as UN, Council of Europe or the European Union have become aware of the problem and now are trying to deal with this issue as effectively as possible.

6.Instead of conclusions or where to for the criminal policies in the field?

As it was well noticed[43] the initiative to harmonise the laws related to computer crimes came especially from well developed countries, mostly European countries or members of the G8 and this is definitely not enough. Due to the transnational dimensions of this type of criminality[44], it is of utmost importance to involve as much countries as possible in this harmonisation process and that means also developing countries where the IT market is still in an emergent phase.

This is the only valid solution if the slogan no safe havens for cybercriminals should prove to be really back up by concrete actions.

The Cybercrime Convention was a good starting point in this direction. Although the initiative of a regional organisation (Council of Europe), the Convention was open for signature for non-member states as well in the attempt to bring to a common nominator the legislation, procedural measures and provisions related to international co-operation at global level. Currently, the Council of Europe is very much involved into a wide campaign of publicising the Cybercrime

42 Bequai A., *Cybercrime.The US Experience, Computers and Security*, 1999 quoted in Yar M., *op. cit.*, page13.

43 See Sette R., *Criminalita' informatica, Analisi del fenomeno tra teoria, percezione e comunicazione sociale*, Clueb, Bologna, 2000, page 306.

44 A special chapter will be dedicated further on to this special issue.

Convention on other continents, such as Africa, South America or Asia[45]. On the other hand, the ratification process of the European countries that have signed the Convention in 2001 in Budapest is rather slow, there are still a significant number of member-states of the Council of Europe which have not ratified the Convention such as Great Britain and Spain while Germany ratified it only in the first half of 2009[46]. This is to some extent deligitimizing the Convention and makes the efforts to find new states interested in even greater as long as European level no propensity to speed up the process emerges.

On the other hand, at the international level it was felt that a regional effort although accessible to non/European countries would not be sufficient. In this context, the International Telecommunication Union (ITU) is currently developing a programme called "ITU Global Cybersecurity Agenda" which is a multi-layered agenda, one of its tasks being " the development of a model legislation on cybercrime"[47].

Although this programme is currently work in progress, it is presenting a clear positive advantage in comparison with the Council of Europe initiatives, in the sense that developing countries are also participating into it and this can confer indeed a global coverage. Additional to that, UN is currently struggling to bring together a treaty on cybercrime which would be applicable world wide and which could correspond even to the visions of the states which are not party to the Council of Europe Convention[48].

Despite the fact that it is too early to tell where the work of these organisations is heading, as it was well underlined, "the UN/ITU could support the standardization processes in the developing countries where the majority of the Internet users are located"[49]. .

In this context, the projects undertaken by ITU and UN could enjoy that global recognition that the Council of Europe could not possibly benefit up to now from due to its regional character and could develop an instrument able to be recognised and applied everywhere on the globe.

But harmonising the legislation is obviously not enough. This article has showed what are the major tendencies in the field and how fast everything is changing. In this context, repression is not sufficient anymore. Prevention policies are another aspect that needs to be taken into consideration more and more not only by the LEAs but also by the private industry as it is more and more clear that the fight against cybercrime is a fight that needs to be fought by all of us together.

45 For a complete overview of the activities undertaken by the Council of Europe in the framework of the Global Project of Cybercrime (the 2nd phase of the Cybercrime Project which should take place between 2009 and 2011), please see www.coe.int

46 See for an up to date overview of the ratification the Treaty Office of the Council of Europe webpage www.coe.int

47 For details see Gercke M., "National, Regional and International Legal Approaches in the Fight Against Cybercrime", in *Journal of Information Law and Technology*, Issue 1, 15 February 2008, pp. 7-14.

48 Conceptual differences in the field were met for example between Russia and USA, for details see US and Russia Differ on a Treaty ofr Cyberspace, NY Times, 27th June 2009, available at http://www.nytimes.com/2009/06/28/world/28cyber.html?pagewanted=2

49 Gercke M., *Ibidem*, page 10.

Bibliography.

- Brown I., Eduards L. and Marsden C., I*nformation Security and Cybercrime*, available at http://papers.ssrn.com/sol3/papers.cfm?abstract_id=1427776
- Carrabine E., Lee M., South N., Cox P., Plummer K., *Criminology. A Sociological Introduction*, Routledge, London-New York, 2004.
- Cockayne J., *Transnational Organized Crime: Multilateral Responses to a Rising Threat. Coping with Crisis*, International Peace Academy, April 2007.
- Communication from the Commission to the European Parliament, the Council and the Committee of the Regions, *Towards a general policy on the fight against cybercrime*, COM(2007)267 final, Brussels, 22.5.2007, available at www.europa.eu
- Gercke M., "National, Regional and International Legal Approaches in the Fight Against Cybercrime", in *Journal of Information Law and Technology*, Issue 1, 15 February 2008, pp. 7-14.
- Gercke M., *Understanding Cybercrime. A Guide for Developing Countries*, Draft April 2009, available at www.itu.int
- Ghernaouti-Hélie S., "La cybercriminallité: reflects d'une certaine criminalité économique", in Auburger-Bucheli I., Bacher J-L. (sous la direction de), *La criminalité économique: ses manifestations sa prévention et sa répression*, L'Harmattan, Paris, 2005, pp. 243-253.
- Gordon S., Ford R., "On the definition and classification of cybercrime", in *Journal in Computer Virology*, n. 2, 2006, pp.13-20.
- Grabosky P. N., "Virtual Criminality.Old Wine in New Bottles?", in *Legal Studies*, vol. 10, n. 2, 2001, pp. 243-249.
- Grabosky P., "Editor's Introduction", in *Crime Law and Social Change*, vol. 46, 2006, pp. 185-187.
- Hughes L. A., DeLone G. J., "Viruses, Worms and Trojan Horses: Serious Crime, Nuissance or Both?", in *Social Science Computer Review*, 2007, pp. 78-98.
- Hunter P., "2005 IT Security Highlights- the day of the hacker amateur has gone, but there are still plenty of amateur users", in *Computer Fraud and Security*, January 2006, pp. 13-17.
- Ifrah L., *Cybercrime: Current Threats and Trends*, available at www.coe.int
- Internet Crime Complaint Center, *2008 Internet Crime Report*, available at www.ic3.org
- Kozlovky N., A *Paradigm Shift in Online Policing. Designing an Accountable Policing*, available at http://crypto.stanford.edu/portia/pubs/articles/K146964995.html
- Norman P., "Policing 'high-tech' crime within the global context: the role of the transnational policy networks", in Wall D. (Edited by), *Crime and the Internet*, Routledge, London-New York, 2001, pp.184-194.
- Rogers M., "Organized Computer Crime and More Sophisticated Security Controls: Which Came First the Chicken or the Egg", in *Telematic Journal of Clinical Criminology*, 1999, available at www.criminologia.org
- Schjolberg S., *Computer Related Offences*. A presentation at the Octopus Interface 2004, Strasbourg 2004, available at www.coe.int
- Sette R., *Criminalità informatica. Analisi del fenomeno tra teoria, percezione e comunicazione sociale*, Clueb, Bologna.
- Wall D., "*Cybercrimes and the Internet"* , in Wall D. (Edited by), *Crime and the Internet*, Routledge, London-New York, 2001, pp. 1-17.
- Wall D., *Understanding Crime in the Information Age*, Polity Press, 2007.
- Wall D., "Cybercrime, Media and Insecurity: The Shaping of Public Perceptions of Cybercrime", in *International Review of Law, Computers and Technology*, Vol. 22, no. 1-2, 2008, pp. 45-63.
- Yar M., *Cybercrime and Society*, Sage Publications, 2006.