Borderless Crime - Computer Fraud

Raluca Georgiana POPA
Department of Economic International Relations,
Bucharest Academy of Ecomomic Studies
ROMANIA
jpopa1961@yahoo.co.uk

Starting from the consideration that fighting cybercrime is a continuous process, the more the types of old crimes are committed today through modern means (computer fraud) at distances of thousands of kilometers, international cooperation is vital to combat this phenomenon.
In EU countries, still under financial crisis "the phrase", cybercrime has found a "positive environment" taking advantage of poor security management systems of these countries.
Factors that led criminal groups to switch "their activities" are related to so-called advantages of the "gains" obtained with relatively low risk.
In Romania, more than any of the EU member states criminal activities set as target financial institutions or foreign citizens, weakening confidence in financial systems and the security of communication networks in our country, people's confidence in electronic payment instruments and those available on the Internet.
Keywords: *Computer Crime, International Cooperation, Security, Computer Fraud, Computer Systems*

Expand information crimes in our country, is another aspect of the offense or another phase of its development to modern society.
We can say that some crimes have acquired a descendent character due to the used means that have evolved, but the same cannot be said about computer crimes that took a great extent, being in continuous growing
In Romania these types of crimes are on a lower step, reporting our country to other developed countries, because the nature of such offenses is favorable to any more or less developed country , the only difference consists of the mode of operation and other factors, but objective part is one and same, no matter where there is crime
Computer along with other equipment, is now the technical complex by means of which the criminals' illegal maneuvers are operated.
In the last fifty years, statistics show that computer crime has become a growing phenomenon
The computer could allow encryption of information, thus preventing access of investigators to them, and this is a possibility highly exploited by criminals, including terrorists.
The first laws against crimes committed by means of a computer, contained, in essence, provisions against acts of penetration database, of deceit and sabotage, and software piracy that is normally regulated by copyright law. It has also proved that drug trafficking, illegal arms trade, child pornography, online shopping, various forms of economic crimes and even some crimes on environmental protection, can be made by means of a computer.
Thus, at the end of 1986, the spectrum of these crimes has been extended to all offenses using automatic data processing as a tool for action, then it was also approached the term "Computer Aided Crime".
Cybercrime phenomenon has engulfed the economy, today no serious criminal organization cannot be imagined without computer support, and investigators must bear them in mind in their action research.
Evolution of organized crime in Romania in recent years is closely related to the evolution of cybercrime and the increasing use of ICT technology in committing crimes. Analyzes effected at the level of the

European bodies on Cybercrime trends, define organized crime as an important branch of organized crime in EU countries.
Following this development, in Romania too, a number of studies and assessments have been made, that identified some common characteristics of this type of crime taking place in our country or the perpetrators are Romanian citizens.
Thus, these activities aimed at obtaining financial products i.e. credit and payment systems offered by financial institutions and banking that members of these crime networks access fraudulently, causing significant damage.
Cybercrime has become a phenomenon both by the large number of cases recorded, the organization of those who commit such acts, in criminal groups, and by shifting groupings who are committing crimes such as international traffic of cars and people, to the crimes in the area of cybercrime.
Trend of organized crime, defines cybercrime as an important branch of organized crime in EU countries, according to analyzes conducted in the European organizations .

OECD expert group in 1993, defined computer actions such as: "any unethical or illegal behavior regarding unauthorized automatic data treatment and / or data transmission", definition whose utility is currently useful , even if spectacular development occurred on the design and use of computer .

Another definition is given by UNAFEI (United Nations Asia and Far East Institute for the Prevention of Crime and the Treatmet of Offenders), by computer crime, it is understood: ”any offense in which a computer or computer network is the subject of an offense, or a computer or computer network environment is the instrument of making an offense ". In the narrow sense, "any offense the offender interferes without authority with automatic data processing processes, represents a computer crime. [1]

According to ENISA (European Agency for Network and Information Security Agency), computer crimes are classified as:

- Computer fraud, computer forgery, damage to databases and computer programs, computer sabotage, unauthorized access to computers, unauthorized interception, reproductions of fraudulent schemes, no right to alter data or computer software, computer espionage, unauthorized use of a computer or computer programs protected by law .

The main factors for gang diversion to computer crimes are tied to large financial gain in a relatively short time and with relatively low risk. This phenomenon affects the image of Romania, as criminal activities that target financial institutions or foreign citizens, weakening confidence in financial systems and the security of communication networks in our country, people's confidence in electronic payment instruments and those available on the Internet. Examining criminal cases, involving a number of defendants prosecuted and aim at computer crimes, it appears that their commission is made by the same types of actions, namely: misleading persons in the circumstances of the conclusion of online contracts and introduction of computer data in a computer system. However all these having as a result in any losses in buyers’ property who have good faith and confidence in how to complete online business.

The prosecution bodies in Romania, (Service for Combating Organized Crime Valcea), have been reported by many foreigners on the fact that since 2005 they have been misled over the Internet by an organized criminal group , meaning that accessing sites E-bay or other companies specialized in selling products online, they have been in contact with them and negotiated by e-mail or telephone trading conditions of goods, especially agricultural machinery and mobile phones , and after they transferred the money to Romania, by Western Union or other payment method, representing an advance or the total price of

the contract object, the "so called" sellers have stopped all contact with victims. [2]

Finally, companies Ebay and Paypal have made complaints and have presented data and information from which content results that the organized criminal group held computer data ,by wise utilization were rigged users' legitimate accounts of the two companies, thus creating localized damage to their property .

In February 2005, the Singapore citizen Y.S., visited sites Ebay, in the idea of buying brand mobile phones Nokia9500, circumstance in which he established contact with the holder of the e-mail redbear925@hotmail.com who convinced him to transfer to Romania on behalf of defendant M.N., through Western Union Quick payment in two installments, Singapore's total of $ 18,860 . It is observed that the tenderer has induced the victim the idea that he represents a prosperous company, specialized in online transactions and also has imposed him his own rules for conducting the transaction, meaning that money would be transferred by Western Union, which was happened, and the good be sent by international delivery service, UPS, rules that have no relation to services Ebay si Paypal.

A brief analysis of the modalities of operation of criminal groups that operate online, thus, they, in 2005-2008, by unlawful accessing of accounts belonging to companies specialized in online sales, by creating trap sites and accounts in which content that falsely offered for sale various goods, mainly agricultural machinery and mobile phones, and by online launching of fraud auctions have damaged more foreigners, who were caused a very large aggregate loss .

The organizer and coordinator of the organized criminal group, caught in criminal activity, according to the "skills" of each, and who were raising sums of money that came from fraudulent electronic auctions .

Criminal activity consists in no right access to computer systems, no right possession of computer data, and e-mail used for cheating victims.

Ultra Electronics values at $ 50 billion/ year the global market of cyber security. "And this market is growing 10% a year, twice faster than the entire information technology sector," says director Cassidian Cyber Security Solution within EADS (European Aeronautic Defence AND Space Company N.V). [3]

The Ministry of Communications and Information Technology made an eFraud Portal and is currently managed by the Department of cybercrime in the Ministry of Interior and Prosecutor's Office specialized section of the High Court of Cassation and Justice. Portal gives everyone the opportunity to appeal, on-line, any chance of possible fraud or other illegal activities on the Internet, www.efrauda.ro.

Mission to Romania of the United States Agency for International Development (USAID) in cooperation with the Ministry of Communications and Information Technology has initiated since 2002, the project RITI dot-Gov, and currently has developed a "Quick Reference Guide" for the enforcement of legal provisions relating to computer crime and providing assistance to law enforcement authorities, and for all those involved in crime prevention information, implemented in Romania by Iternews Network Inc.,an American non-profit organisation.

The latest survey conducted by Computer Crime Institute and Federal Bureau of Investigation (FBI) in 2003 indicated losses of $ 201,797,340 for 538 U.S. companies and institutions surveyed.

In Romania, was made in 2003 by specialized research computer 200 offenses half of which were fraudulent electronic auctions, 30% of goods ordered on-line fraud, 10% unauthorised access and 10% referring to other crimes (Nigerian letters, viruses, child pornography, use of false

identities), transmission of viruses, child pornography, use of false identities.[4]

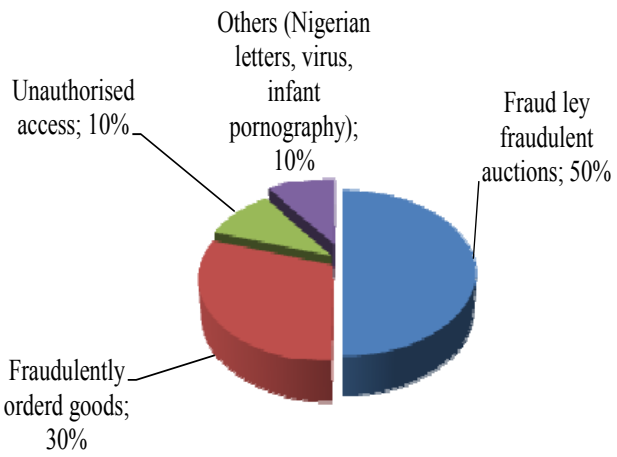

Fig.1. Computer fraud distribution. Source: data taken from www.securitatea-informatica.ro

As a result of this evolution in Romania have made a series of studies to identify the main causes generating:

- High performance technology used by criminals;
- Lack of preparation and training specialized personnel in the prosecution;
- Delayed reaction of the victims, this assuming minimal chances of identifying cybercrime and other measures to recover damages;
- The appearance of retention phenomenon , of the damaged, to report crimes to prosecutors;

EC (European Commission) Report supports the development by 2012, of the European emergency plan in case of cyber incidents, and supports national emergency plans and suggest the establishment of cyber attacks simulations, it also suggests the establishment of effective networks of intervention in emergency event of the global information. [5]

Recent events have shown that new and more sophisticated cyber attacks in terms of technology can disrupt or even destroy vital societal and economic functions. Examples include attacks on networks from the French Ministry before the G20 summit, the EU system of sale of emissions certificates and, recently, on the European Service for External Action and the Commission itself.

The Industry, Research and Energy Commission of the European Parliament, in the draft Report, "on critical information infrastructure, achievements and next steps: towards a global cyber security"-" All these developments in recent years unsolicited, which do not exhaust the efforts to enhance cyber security in the EU space, demonstrate that Internet security is a pertinent issue. It becomes obvious that the Internet is a critical infrastructure and the Internet disruption could lead to substantial losses and security risks, affecting a large number of European citizens and businesses. In addition, rapid technological developments require that prevent Internet attacks, repair and resistance reactions global network to be based on a comprehensive framework based on the flexible, innovative and long-term reaction. This framework should ensure effective interaction between governments, businesses, individuals and all other interested parties. Lastly but not least important, the increased strength of the Internet is possible only when there is an international system of cooperation and international rules." [6]

Border cybercrime materialized by cyber attacks causes great damage and it is possible a scenario in which a perpetrator able to launch attacks can interrupt the communication range. If only a small

percentage of important information hub sites are compromised, the chain reaction is likely to fragment the Internet. On the other hand, critical networks, such as those which are banking, have special equipment and protocols and are not connected to the Internet, so the only way to be compromised is the inside way. [7]

Moreover, in a modern society that the crisis becomes more acute as the use of the Internet to purchase goods, pay bills, or solve other everyday problems becomes a necessity, but such actions seriously jeopardize confidence people in the fairness of transactions online and generate a phobia in using electrical equipment. Another terminology used to define this type of crime is, cybercrime, which is crime performance using computer technology. Activities on economic and financial crime have exploded with unprecedented evolving practically together with the improvement in telecommunications and information technology assets, consisting of up almost means faster and "safer", of acceptance and transfer of money.

A computer operator can bring financial harm to a company by entering false data, the possibility of theft of money.

If one has to appreciate the extent of this type of crime, we can say that for them there is an impediment because computer technology is unevenly distributed in the world, with reference to the internet network and almost no existing means of protection .

But there are no borders for the "pirates ", they are forming organized criminal groups. Cybercrime is characterized mainly by committing crimes via computer, and they consist of:

- computers are used with predilection to commit financial crime, not necessarily as an instrument of crime, but chose to enter the database in order to extract and or enter information to initiate microchips for cell phones, to examine checks company, bonds and other negotiable instruments for counterfeiting [8]
- theft from distance of large sums of money from private accounts were the accounts of banks, commercial or material transfer tax;
- purchase of goods over the Internet that are paid illegal credit card numbers illegally using them without the owner's consent;
- offering for sale goods on the Internet at tempting prices, after opening a bank account and after deposit of amounts ,the account is abolished and goods are not dispatched
- entering the large database of companies, with the destruction or theft of database information;
- use computer for terrorism purposes;
- infringement of intellectual property;
- identity theft.

The context of the current crisis worsens the transformation of hacker activity in an industry organized crime, due to the exploit on personal information, which affects individual and socio-economic life.

IGPR (General Inspectorate of Romanian Police) and (BSA) Business Software Alliance signed a Protocol providing for prevention, and combating software piracy and the purpose is to establish cooperation between the two parties on the issues mentioned.

This Protocol, which is valid for two years, involves the initiation of projects, programs, campaigns and information activities, outreach to consumers and businesses, to reduce the risk of infringement. [9].

In 2011, specialized structures within IGPR, conducted over 180 inspections, claiming 46 cases to prosecute. [9].

IGPR, pursuant to provisions under Law no. 218/2002 on organization and functioning of the Romanian police with subsequent amendments and the Law. 8/1996, as amended, on copyright and related rights, carries out through its specialized structures, specific measures to:

- prevent and fight against financial and economic crime, in using information technology;
- declare offenses under the regime of copyright and related rights and conducting investigations on them.

For example, during 2011 as well, there were found 144 economic crimes, of which 40 were tax evasion and following the

checks carried out by the Fraud Investigation Department of the IGPR to protect business environment against illegal acts illegal affecting competition relationships and market economy mechanisms , were found 144 new crimes. [9]

Computer system, SIRENE (Supplementary Information Requested at the National Entries) appeared due to the need for data exchange and additional information from the Schengen and it is designated for storing information by the Romanian authorities and the European common data exchange, border monitoring, that is SIS, respectively (Schengen Information System).

With the lifting of internal border controls of Schengen Member states, there was a need in render Schengen Information System operationally, which contains minimum information about persons or property pursued by legal proceedings, and data and information obtained through the SIRENE Bureaux are established in each Schengen member state. [10]

In our country, to assess the exact scale of this type of crime, there were identified certain features, which as I described, go beyond borders and often, the perpetrators are Romanian citizens.

Among the features identified on cybercrime in Romania we can mention with the predilection for :

- financial condition (payment systems, credit and payment products);
- organization of criminal groups, with highly specialized young people;
- transnationality of these actions, using the other states systems;
- specialization, continuous improvement of operating systems;
- refocus criminal groups who commit computer fraud, on companies, thus committing large damaging , hard to recover due to operating modalities.

These "activities" aim at getting with predilection for financial products, credit, payment systems offered by financial and banking institutions, criminal networks that members of such fraudulent networks access, causing significant damage to both natural persons, companies, even affecting economies countries.

Cybercrime, aims however, at mostly economic and financial field, in order to obtain illicit revenues by some criminal groups. Economic and financial crime is more difficult to identify and proved, is much more complex than other traditional forms of crime, by the severity of damage caused , the number of people affected and by propagation in a long time as well.

"Cybercrime" is known as computer fraud, is part of computer-related crime leading technology, based on the rapid evolution of computer technology and communications, has created high possibility regarding criminal activity.

Cybercrime prevention is related to how information systems are protected, the use of permanent protection systems.

Also in this respect, the European Commission proposes a common policy to combat these types of fraud and developing a coherent European policy framework and public awareness about the costs and dangers of cybercrime.

Another approach to crime information, can be analyzed in terms of other definition, namely that "achieving direct or indirect, physical or logical, deliberate or non deliberate actions, aimed at changing one or more states of a system and subsystem information" legally and can be thus grouped :

- crimes for which committing were used information and computer technologies;
- crimes where computers and computer networks are targeted attack.

The need for international reporting mechanism for Internet Service Providers (ISP-Internet Service Provider) in respect of illegal material distributed via the Internet is reported more than 10 years.

Transition to the Information Society in Romania, as a relevant component development requires not only information and communication infrastructure, but also legislative gaps on computer activities, the

computerization process and, in general, the information technology.

Change, modernization and adaptation to new technologies represents our country's response to the conditions of acceptance of Romania into the European structures. [11]

Development of information technologies in recent decades due to the need for storage and rapid transmission of information with the least cost revolutionized global commerce, directly or retail trade, redefining the traditional principles of marketing, electronic commerce became synonymous with profit growth.

With this type of commerce, also occurred offenses on electronic commerce. The analysis on these offenses provided under the law no. 265/2002 referrers to crimes of:

- forgery of electronic payment instruments;
- possessing counterfeiting equipment specific to electronic payment instruments;
- conduct fraudulent financial transactions;
- acceptance of financial operations performed fraudulently.

For example, "no right to a network connection", addressing purely technical, simply connecting to Wi-Fi signal (radio waves) can be often automatically, depending on device settings used by the alleged offender without his knowledge, case that his guilt cannot be established.

Analyzing the many technical means that allow "access", meaning, "the program, run a program to intercept, to establish, communicate, store / archive / store or retrieve data from any other use of a sources provided by computers, including data or computer programs, computer systems, computer networks or databases" [12]

With the use of virtual worlds, criminals have found an ideal means to "launder money" that hide the origin and actual possession of their income from illegal activities.

Economy of virtual worlds like SecondLife has no fiscal rules in the real economy. Freedom of action is virtually unlimited and documents formalism nonexistent, guarantees on transactions are secured by the same methods that e-commerce already uses in the real world.

Law speaks in all criminal modes of money laundering, on goods in the ordinary meaning, they are physical, material, having a perceptible physical existence. To these it might be added intangible goods traded, and some virtual goods, which by their features already mentioned, although sensory perceptible, they do not have a physical existence, but, by real-virtual correspondence, the tangible features with physical existence .

Furthermore, by assigning a value, as are the spellings, these assets become property values, some made extremely important by design. [13]

As in case of theft of goods in cyberspace, the law does not provide conformance to features, nor associates the economic value to this new categories of goods .

Thus, it remains an area where the legislator should intervene and adapt the legal text, making it applicable to virtual space as well, by the simple and extensive definition of goods or indicating the extension of regulation on illicit activities in cyberspace.

Internet can be also used as a " comfortable umbrella " for transactions outside virtual worlds, for automating transfer of money, without possibility on the phenomenon to be monitored.

Within the national regulatory space, notions of "money laundering" by means of computer or "cyber terrorism", do not currently have an impact, the subject being studied and treated accordingly, losing itself in general usual concepts, giving substance to field cybercrime through legal practice.

So, by definition, cybercrimes (cybercrime), are all crimes committed by electronic means and investigating these types of crimes involves certain challenges:

- the opportunity to acquire a transnational or organized character and the effects arising for prosecution;
- virtual place of the offense;
- data theft;

- difficulties with intercepting communications (encryption communications interception servers);
- management of electronic evidence;
- organs of the criminal investigation are limited to legislation and national jurisdiction;

These issues generate new management tools, leading to fighting cybercrime:

- establishment of preventive measures current threats (SIRENE application);
- liability to be established since the early space;
- harmonization of national legislation;
- agreements with Internet service providers, financial institutions, credit, etc.
- specialized professional staff, with the evolution of new information technologies;
- use of international instruments of cooperation in the field (SIRENE, SIS).

As electronic media become more accessible to all, cybercrime is diversifying and intensive, far outstripping the traditional fraud and forgery.

In this context, a European strategy is not simply a desire, but an important necessity.

Thus, the Prevention and Combating Crime Service, in its Progress Report for 2011 states that, in 2011 increasing trend of crimes against systems / computer data or committed using information technology, is fully revealed by statistical indicators pursued , represented as the number of cases recorded, as well as the number of cases solved or remaining in work progress.

It is also noted that, besides false informatics (work of "phishing") and the actual computer fraud, deception committed through information technology represented by fictitious goods auction sites specialized in electronic commerce is a big part of notified facts, which are the subject of cases registered or resolved during 2011.

Undermining access accounts belonging to users of e-commerce sites, financial institutions or social networks, unauthorized access to systems followed by blackmail or misuse of confidential data obtained (electronic payment tools data) represents ,with credit card fraud (compromised ATM), capturing information on the magnetic strips of credit cards, forgery of electronic payment instruments), manifestation forms of cybercrime in obvious increase.

Transnational character, whether it is given by where the facts are committed , or it is about the location of victims represents an objective factor to increase in cybercrime, with recruitment by means of increasingly sophisticated "arrows", and their specialization as needed (opening bank accounts, transport of money or creating money laundering networks comprising Romanian and foreign citizens, as well.

The transboundary nature of computer crime, the specialized networks located abroad, respectively, still remains one of the difficult problems to overcome in operational solution on the files recorded .

Not least ,the effective investment in creating/ purchase of criminal schemes, investment in technology and development of counterintelligence activities, determines that the groups investigated present an increasingly higher danger.

Specific analysis of cases solved, for 2011 also confirms the trend observed in recent years on the migration of people from organized crime to ordinary computer crime, especially in the fraudulent operations with electronic payment instruments.

Such facts remains a significant source of revenue for prominent members, without the latter to become directly involved in crime enforcement.

” Regarding credit card fraud, counties Prahova, Vâlcea, Teleorman, which are known as the manifestation areas of the phenomenon of computer fraud.

Counties of Vâlcea, Arges, Constanta, Teleorman as well the City of Bucharest keep being areas with high criminal potential for computer crime, being equally noted facts both in the field of credit card fraud, and computer crimes area in ”stricto sensu”, as well .

In 2011, 873 cases were resolved, an increase of 62.87% compared to 2010, when 536 cases were solved".(14).
Cybercrime is an ascendant "process", involving numerous domestic and international organizations in this respect, all countries are "united front" against this scourge.
"Models of computer attacks:
(i) Access user-attack in this class requires access to system by users having certain privileges, as the following steps:
- obtaining information- a complete search is effected ,in order to get data to identify security vulnerabilities. This process is often like being authorized by instruments such as "nmap" or instruments or tools that target a specialized application such as a Web server. Vulnerabilities can exist in the system components , may result from errors on system administration ,or can be reflected in poor security policies of the system.
- operation- of a security breach is done to gain access or obtain system information for their use in future cues. In the early stages of an attack vulnerability may come from information such as computer name or names of user accounts
- damages -the desired effects as a result of an attack are ,for example, changing data, access to classified information or establishing permanent connections that can be used for ongoing access. The final step in this attack is changing logos files, so the attack cannot be not identified
ii) Access to components- an attack of this category does not require user access to the system. These attacks create denial of services by sending improper requests. In some instances, such a request may result in loss of certain weaker system components . In other cases, the extra time needed for processing such a request is sufficient to slow processing much down . Steps in this attack are:
- obtain information – is identified a component of the system and a communication port
- operation- messages are sent to the port;
- damage - loss or overloading a component application or network service;
(iii) The application content- these types of attacks send improper data application rather than the network components. In this situation traffic is properly formatted. The problem is related to the content of traffic and as in the case of attacks on access to network , these examples do not require an attacker to gain access to the user. The steps are as follows:
- Obtaining information – is done the identification on the target application. This can be either a network application such as a Web server or a browser or an application such as Microsoft Office, where emails are used to transmit data to applicants;
- Exploitation- the content is directly or indirectly sent to the target application;
- Damages – following such attacks user files are deleted, configuration changes a user's account or user files are exported. [15]

Conclusions

Thus, UNAFEI, ENISA, DIICOT, EA DS, FBI, USAID, SIRENE, jointly elaborated projects, guidelines for application of the law on computer crime, and providing assistance to law enforcement authorities and to all those involved in crime prevention information.
UE also, supports in 2012, an European emergency plan in case of cyber attacks and make recommendations for the establishment of effective networks for urgent intervention in the event of information worldwide.
IGPR and BSA, signed a protocol providing for the prevention and combating software piracy.
Dimensions of cybercrime, was exemplified by specific data provided by authorized institutions (DIICOT, IGPR), the transboundary nature may also be highlighted by the interest of many countries, for this, and targeting the economic and financial with predilection for
.

Thus, SIRENE, appeared due to the need for data exchange and additional information from the Schengen area and it is designated for storing information by the Romanian authorities and the European common data exchange, border monitoring, SIS ,respectively.

Several definitions have clarified the notion of computer fraud, which means because of the state known beyond the frontiers of the country, manifested globally, which required the need for a mechanism for "reporting" international internet service providers (ISP-Internet Service Provider).

Computer fraud is not just stealing goods from virtual space, criminals have found an ideal means to "launder money" and hide the origin and actual possession of their income from illegal activities.

One can thus conclude that any or all means would set, as the means information is developed, there is virtually impossible to have a "percet sync" in terms of prevention.

Practically taking advantage of this situation, computer fraud is growing and diversifying extensively, and establishing comprehensive strategies on international instruments of cooperation, (SIRENE, SIS), becomes necessary.

For examples, we can say that computer fraud in Romania concerns with predilection for financial institutions or foreign citizens, thus reducing confidence in financial systems on the network security.

Expansion of information technologies, in addition to positive effects on socio-economic and political life of the world, generated, as mentioned, and some behaviors outside the law, taking forms that did not exist previously. But in a society that supports economic and social repercussions daily cybercrime, daily use is made of computers in all areas of socio-economic life.

Computer fraud can have a very high price in economic terms, for all the world, everything depends on their extent, and the problem of defining computer crime may appear as a new concern for societies where access to new technology was delayed and where some states precautionary measures have not yet established.

References

[1] www.criminalitatea-informatica.ro
[2] *Data delivered by Service for Combating Organized Crime Vâlcea-Indictment*, 2011.
[3] www.europarl.eu/meetdocs/2009-2014
[4] www.securitatea-informatica.ro
[5] bursa.ro
[6] V. Patriciu ș.a, *Internet and Law*, Editura ALL BECK, București, 1999, p 21.
[7] I. Vasiu, *Cybercrime*, Nemira, București, 1988, p 121-122
[8] *Bulletin of Information and Documentation MI*, anul, XII, nr. 6 (53), 2002.pg 131-133 (Bulletin of information)
[9] EuroAvocat.ro/20/04/2011
[10] Directive 95/46/CE
[11] *Reason presentation for Bill NO. 365/2002, as to e-commerce.*
[12] T. Amza ș.a., *Cybercrime*, Ed. Lumina Lex, București, 2003, p.14.
[13] https//marketplace.secondlife.com/p/
[14] www.diicot.ro/pdf - *Directorate for Organised Crime Crime and Terrorism* / no 4/CD/2012-Prelucrare, pg 39-45.
[15] http://www.ciminalitatea-informatică.ro

Raluca Georgiana POPA is a PhD student in the field of Economy and International Affairs at the Academy of Economic Studies. She graduated the Faculty of Law within the University of Bucharest and she has a master in economy. Currently, she works within the Management Authority of the General Programme 'Solidarity and Management of Migration Flows', programme which sets out to support the common policy on the management of the external borders of the European Union and to help implement the common policies on asylum and integration.