Analele Universității "Dunărea de Jos", Galați - Fascicula XXII
***Drept şi Administrație Publică* Anul I, Nr. 1 – 2008**
Galati University Press ISSN 1843 -8334

Adriana TUDORACHE

COMPUTER-RELATED CRIMES

Abstract

The rapid growth and globalization of information technologies has dramatically changed the way people communicate. Millions of people pay bills, consulte professionals, conducte research and make connections with family and friends in cyberspace. As cyberspace continues to become an integral part of life, cybercrime or computer crime poses new challenges to the criminal justice system. The global nature of cybercrime raises difficult legislative problems of jurisdiction as criminals use offshore servers and Internet sites to avoid domestic regulations. Crime in cyberspace, such as cyberterrorism, cyber-money-laundering, cybergambling, Internet fraud and cyberstalking, can occur instantaneously, and offenders targete victims in other countries where the offence is not easily detected.

The seriousness of cybercrime is reflected in the fact that cyberspace has become the target of terrorists and organized crime groups.

Fifteen years ago, cartoonist Peter Steiner drew two dogs sitting in front of a computer, one saying to the other, "On the Internet, nobody knows you're a dog." This iconic adage, cute in its day, is now a warning.

Cybercrime is estimated to be a $600 billion market and looks set to grow in 2009 as the complexity of cybercrimes intensifies. The year 2008 concluded to be a year of an exponential increase in the activities of cyber criminals. Every day, criminals are invading countless homes and offices across the world – not by breaking down windows and doors, but by breaking into laptops, personal computers, and wireless devices via hacks and bits of malicious code.

Billions of dollars are lost every year repairing systems hit by such attacks. Some take down vital systems, disrupting and sometimes disabling the work of hospitals, banks, and 9-1-1 services around the world.

The capabilities and opportunities provided by the Internet have transformed many legitimate business activities, augmenting the speed, ease, and range with which transactions can be conducted while also lowering many of the costs. Criminals have also discovered that the Internet can provide new opportunities and multiplier benefits for illicit business. The dark side of the Internet involves not only fraud and theft, pervasive pornography and pedophile rings, but also drug trafficking and criminal organizations that are more concerned about exploitation than the kind of disruption that is the focus of the intruder community.

Defining Cyber Crime

Cyber crime encompasses any criminal act dealing with computers and networks (called hacking). Additionally, cyber crime also includes traditional crimes conducted through the Internet. For example; hate crimes, telemarketing and Internet fraud, identity theft, and credit card account thefts are considered to be cyber crimes when the illegal activities are committed through the use of a computer and the Internet.

Cyber crime is the latest and perhaps the most complicated problem in the cyber world. "Cyber crime may be said to be those species, of which, genus is the conventional crime, and where either the computer is an object or subject of the conduct constituting crime" (13). "Any criminal activity that uses a computer either as an instrumentality, target or a means for perpetuating further crimes comes within the ambit of cyber crime"(12).

A simple yet sturdy definition of cyber crime would be "*unlawful acts wherein the computer is either a tool or a target or both*".

Reasons for cyber crime

Hart in his work " The Concept of Law" has said 'human beings are vulnerable so rule of law is required to protect them'. Applying this to the cyberspace we may say that computers are vulnerable so rule of law is required to protect and safeguard them against cyber crime. The reasons for the vulnerability of computers may be said to be:

1. *Capacity to store data in comparatively small space*

The computer has unique characteristic of storing data in a very small space. This affords to remove or derive information either through physical or virtual medium makes it much more easier.

2. *Easy to access*

The problem encountered in guarding a computer system from unauthorised access is that there is every possibility of breach not due to human error but due to the complex technology. By secretly implanted logic bomb, key loggers that can steal access codes, advanced voice recorders; retina imagers etc. that can fool biometric systems and bypass firewalls can be utilized to get past many a security system.

3. *Complex*

The computers work on operating systems and these operating systems in turn are composed of millions of codes. Human mind is fallible and it is not possible that there might not be a lapse at any stage. The cyber criminals take advantage of these lacunas and penetrate into the computer system.

4. *Negligence*

Negligence is very closely connected with human conduct. It is therefore very probable that while protecting the computer system there might be any negligence, which in turn provides a cyber criminal to gain access and control over the computer system.

5. *Loss of evidence*

Loss of evidence is a very common & obvious problem as all the data are routinely destroyed. Further collection of data outside the territorial extent also paralyses this system of crime investigation.

Cyber criminals

Who is behind such attacks? It runs the gamut—from computer geeks looking for bragging rights…to businesses trying to gain an upper hand in the marketplace by hacking competitor websites, from rings of criminals wanting to steal your personal information and sell it on black markets…to spies and terrorists looking to rob our nation of vital information or launch cyber strikes.

The cyber criminals constitute of various groups/ category. This division may be justified on the basis of the object that they have in their mind. The following are the category of cyber criminals:

1. *Children and adolescents between the age group of 6 – 18 years*

The simple reason for this type of delinquent behaviour pattern in children is seen mostly due to the inquisitiveness to know and explore the things. Other cognate reason may be to prove themselves to be outstanding amongst other children in their group. Further the reasons may be psychological even.

2. *Organised hackers*

These kinds of hackers are mostly organised together to fulfil certain objective. The reason may be to fulfil their political bias, fundamentalism, etc. The Pakistanis are said to be one of the best quality hackers in the world. They mainly target the Indian government sites with the purpose to fulfil their political objectives. Further the NASA as well as the Microsoft sites is always under attack by the hackers.

3. *Professional hackers / crackers*

Their work is motivated by the colour of money. These kinds of hackers are mostly employed to hack the site of the rivals and get credible, reliable and valuable information. Further they are ven employed to crack the system of the employer basically as a measure to make it safer by detecting the loopholes.

4. *Discontented employees*

This group include those people who have been either sacked by their employer or are dissatisfied with their employer. To avenge they normally hack the system of their employee.

Romanian Legal Framework on Cyber crime

1. *International conventions:*

- National Convention on Cybercrime, Budapest, 23.XI.2001
- Declaration on freedom of communication on the Internet, Strasbourg, 28.05.2003

2. *Laws :*

- Provisions on preventing and fighting cybercrime (The cybercrime related provisions are incorporated in Title III of the Anticorruption law no 161/2003 published in the Official Monitor no 279 from 21 April 2003)
- Government Emergency Ordinance no. 79 of 13 June 2002, concerning the general regulatory framework for communications
- Law no.365 of 7 June 2002 on electronic commerce
- Government Ordinance no. 34 of 30 January 2002 on access to, and interconnection of, electronic communications network and associated facilities
- Government Ordinance no. 31 of 30 January 2002 on postal services
- Government Ordinance no. 20 of 24 January 2002, concerning public acquisitions by means of electronic bids

- Law no. 676 of 21 November 2001, concerning the processing of personal data and the protection of privacy in the telecommunications sector
- Law no. 455 of 18 July 2001 on Electronic Signature

3. *Guide for applying the Cyber crime law*
www.riti-internews.ro
www.mcti.ro

The occurrence of cyber crime has become a serious and growing threat. High priority is given at European level to tackling the problem.

The 2007 Internet Crime Report cites the top ten countries by amount of perpetrators of online crime. In descending order, the top ten list includes the United States, the United Kingdom, Nigeria, Canada, Romania, Italy, Spain, South Africa, Russia, and Ghana.Our country ,along Nigeria is considered to be a "hotspot" for cyber crime.

Operating as a full member of the European Union since January 2007 requires new solutions – compared to the existing methods – to tackle the phenomenon of cyber crime. Due to the complexity of the issue, which recently has more and more serious consequences (e.g. cyber terrorism, attacks on financial and banking data bases etc.) and to the fact that it has no border limits, proper measures have to be taken at national level to ensure that the law enforcement personnel have the necessary tools to counteract cyber criminality.

In matters related to cyber crime, Romania applies the provisions of Law no. 161/2003 regarding certain measures to ensure the transparency and the exercise of public dignities, public functions and business environment, preventing and sanctioning corruption and of Law no. 39/2003 on organized crime. The Council of Europe Convention on cyber crime was also ratified by Romania through Law no. 64/2004. Effective measures to counter organized crime, including cyber crime were set out by the National Strategy on Fighting Organized Crime and its action plan, approved by GD no. 1171 from September 2005.

To step further in addressing in an efficient manner the countering of the cyber crime, assistance is longer needed to identify the possible gaps of the existing legislation in the field, set out a methodology and working procedures for dealing with such cases, to prepare the professionals (prosecutors and police officers) in advance investigation techniques of the cyber crime and provide them with the necessary software applications to support such tasks.

Frequently Used Cyber Crimes

1. *Unauthorized access to computer systems or networks*

Unauthorized access to computer systems or networks means any person who secures access or attempts to secure access to a protected system.
This activity is commonly referred to as hacking. The Romanian law has however given a different connotation to the term hacking, so we will not use the term "unauthorized access" interchangeably with the term "hacking".

2. *Theft of information contained in electronic form*

This includes information stored in computer hard disks, removable storage media etc.

3. *Email bombing*

Email bombing refers to sending a large number of emails to the victim resulting in the victim's email account (in case of an individual) or mail servers (in case of a company or an email service provider) crashing

4. *Data diddling*

This kind of an attack involves altering raw data just before it is processed by a computer and then changing it back after the processing is completed. Electricity Boards in Romania have been victims to data diddling programs inserted when private parties were computerizing their systems.

5. *Salami attacks*

These attacks are used for the commission of financial crimes. The key here is to make the alteration so insignificant that in a single case it would go completely
unnoticed. E.g. a bank employee inserts a program, into the bank's servers, that deducts a small amount of money (say Rs. 5 a month) from the account of every customer. No account holder will probably notice this unauthorized debit, but the bank employee will make a sizable amount of money every month.

To cite an example, an employee of a bank in USA was dismissed from his job. Disgruntled at having been supposedly mistreated by his employers the man first introduced a logic bomb into the bank's systems.

Logic bombs are programmes, which are activated on the occurrence of a particular predefined event. The logic bomb was programmed to take ten cents from all the accounts in the bank and put them into the account of the person whose name was alphabetically the last in the bank's rosters. Then he went and opened an account in the name of Ziegler. The amount being withdrawn from each of the accounts in the bank was so insignificant that neither any of the account holders nor the bank officials noticed the fault.

It was brought to their notice when a person by the name of Zygler opened his account in that bank. He was surprised to find a sizable amount of money being transferred into his account every Saturday.

6. *Denial of Service attack*

This involves flooding a computer resource with more requests than it can handle. This causes the resource (e.g. a web server) to crash thereby denying authorized users the service offered by the resource. Another variation to a typical denial of service attack is known as a Distributed Denial of Service (DDoS) attack wherein the perpetrators are many and are geographically widespread. It is very difficult to control such attacks. The attack is initiated by sending excessive demands to the victim's computer(s), exceeding the limit that the victim's servers can support and making the servers crash. Denial-of-service attacks have had an impressive history having, in the past, brought down websites like Amazon, CNN, Yahoo and eBay!

7. *Virus / worm attacks*

Viruses are programs that attach themselves to a computer or a file and then circulate themselves to other files and to other computers on a network. They usually affect the data on a computer, either by altering or deleting it. Worms, unlike viruses do not need the host to attach themselves to. They merely make functional copies of themselves and do this repeatedly till they eat up all the available space on a computer's memory. 170 The VBS_LOVELETTER virus (better known as the Love Bug or the ILOVEYOU virus) was reportedly written by a Filipino undergraduate.

In May 2000, this deadly virus beat the Melissa virus hollow - it became the world's most prevalent virus. It struck one in every five personal computers in the world. When the virus was brought under check the true magnitude of the losses was incomprehensible. Losses incurred during this virus attack were pegged at US $ 10 billion.

The original VBS_LOVELETTER utilized the addresses in Microsoft Outlook and emailed itself to those addresses. The e-mail, which was sent out, had "ILOVEYOU" in its subject line. The attachment file was named "LOVE-LETTER-FORYOU. TXT.vbs". The subject line and those who had some knowledge of viruses, did not notice the tiny .vbs extension and believed the file to be a text file conquered people wary of opening e-mail attachments. The message in the e-mail was "kindly check the attached LOVELETTER coming from me".

Since the initial outbreak over thirty variants of the virus have been developed many of them following the original by just a few weeks. In addition, the Love Bug also uses the Internet Relay Chat (IRC) for its propagation. It e-mails itself to users in the same channel as the infected user. Unlike the Melissa virus this virus does have a destructive effect. Whereas the Melissa, once installed, merely inserts some text into the affected documents at a particular instant during the day, VBS_LOVELETTER first selects certain files and then inserts its own code in lieu of the original data contained in the file. This way it creates ever-increasing versions of itself. Probably the world's most famous worm was the Internet worm let loose on the Internet by Robert Morris sometime in 1988. The Internet was, then, still in its developing years and this worm, which affected thousands of computers, almost brought its development to a complete halt. It took a team of experts almost three days to get rid of the worm and in the meantime many of the computers had to be disconnected from the network.

8. *Logic bombs*

These are event dependent programs. This implies that these programs are created to do something only when a certain event (known as a trigger event) occurs. E.g. even some viruses may be termed logic bombs because they lie dormant all through the year and become active only on a particular date (like the Chernobyl virus).

9. *Trojan attacks*

This term has its origin in the word 'Trojan horse'. In software field this means an unauthorized programme, which passively gains control over another's system by representing itself as an authorised programme. The most common form of installing a Trojan is through e-mail. E.g. a Trojan was installed in the computer of a lady film director in the U.S. while chatting. The cyber criminal through the web cam installed in the computer obtained her nude photographs. He further harassed this lady.

10. *Internet time thefts*

Normally in these kinds of thefts the Internet surfing hours of the victim are used up by another person. This is done by gaining access to the login ID and the password.

11. *Web jacking*

This term is derived from the term hi jacking. In these kinds of offences the hacker gains access and control over the web site of another. He may even mutilate or change the information on the site. This may be done for fulfilling political objectives or for money.

Combating cyber crimes

A prerequisite for combating computer-related crimes is to criminalize acts of computer wrongdoing.

The next crucial element of any international effort against cybercrime is to facilitate technology transfer and engage in capacity-building. Legal and technology experts need to cooperate closely without any barriers whatsoever. The digital divide between the legal and technical matters need to be closed at the national, regional and global levels to effectively put up a fight against what is essentially a global crime wave. Crime has grown so fast in the "bottomless world of cyberspace" that legal and law enforcement bodies should "step up to the plate",

In order to control cybercrime, it is important to strive for harmonization in criminal law to develop a seamless mutual assistance framework. Technology will continue to grow and, as it did, new criminal opportunities would be created.

the worldwide proliferation of new information and communication technologies has given rise to more forms of computer-related crime, which pose threats not only to the confidentiality, integrity or availability of computer systems, but also to the security of critical infrastructure. Technological innovation gives rise to distinct patters of criminal innovation.

When combating such crimes, a number of forensic problems challenge investigators, prosecutors and judges. Effective investigation and prosecution of computer-related crime often require tracing criminal activity through a variety of Internet service providers or companies, sometimes across national borders, which may result in difficult questions of jurisdiction and sovereignty. Computer-related crime, therefore, necessitates international cooperation, which requires countries to be equipped with the necessary legal, procedural and regulatory tools. A number of regional and interregional efforts have been undertaken in recent years, leading to several significant accomplishments. In order to bring those efforts to fruition, it is necessary to support a wide range of research on the various aspects involved in combating computer-related crime to foster an active partnership between government and the private sector.

Computer-related crime includes theft of telecommunications services or computer services by using hacking techniques. Servers and websites could be targets of denial-of-service attacks, viruses and worms. Computers were also used as instruments to commit crime, such as modification of data, electronic vandalism, forgery and counterfeiting, information piracy, industrial espionage and copyright infringement. There were many types of computer-related crime involving attacks on banks or financial systems, as well as fraud involving transfer of electronic funds. Other problems involve telemarketing and "phishing" or spoofing spam. Existing offences such as extortion and harassment are also carried out online. In recent years, increasing attention has been devoted to the relation between terrorism and the Internet, as the Internet was being used to facilitate terrorist financing and as a logistics tool for planning terrorist acts.

Conclusions

Undeterred by the prospect of arrest or prosecution, cyber criminals around the world lurk on the Net as an omnipresent menace to the financial health of businesses, to the trust of their customers, and as an emerging threat to nations' security. Headlines of cyber attacks command our attention with increasing frequency. According to the Computer Emergency Response Team Coordination Center (CERT/CC), the number of reported incidences of security breaches in the first three quarters of 2008 has risen by 54 percent over the total number of reported incidences in 2007. Moreover, countless instances of illegal access and damage around the world remain unreported, as victims fear the exposure of vulnerabilities, the potential for copycat crimes, and the loss of public confidence.

Cyber crimes—harmful acts committed from or against a computer or network—differ from most terrestrial crimes in four ways. They are easy to learn how to commit; they require few resources relative to the potential damage caused; they can be committed in a jurisdiction without being physically present in it; and they are often not clearly illegal

The laws of most countries do not clearly prohibit cyber crimes. Existing terrestrial laws against physical acts of trespass or breaking and entering often do not cover their "virtual" counterparts. Web pages such as the e-commerce sites recently hit by widespread, distributed denial of service attacks may not be covered by outdated laws as protected forms of property. New kinds of crimes can fall between the cracks, as the Philippines learned when it attempted to prosecute the perpetrator of the Love Bug virus, which caused billions of dollars of damage worldwide.

Effective law enforcement is complicated by the transnational nature of cyberspace. Mechanisms of cooperation across national borders to solve and prosecute crimes are complex and slow. Cyber criminals can defy the conventional jurisdictional realms of sovereign nations, originating an attack from almost any computer in the world, passing it across multiple national boundaries, or designing attacks that appear to be originating from foreign sources. Such techniques dramatically increase both the technical and legal complexities of investigating and prosecuting cyber crimes.

The growing danger from crimes committed against computers, or against information on computers, is beginning to claim attention in national capitals. In most countries around the world, however, existing laws are likely to be unenforceable against such crimes. This lack of legal protection means that businesses and governments must rely solely on technical measures to protect themselves from those who would steal, deny access to, or destroy valuable information.

Self-protection, while essential, is not sufficient to make cyberspace a safe place to conduct business. The rule of law must also be enforced. Countries where legal protections are inadequate will become increasingly less able to compete in the new economy. As cyber crime increasingly breaches national borders, nations perceived as havens run the risk of having their electronic messages blocked by the network. National governments should examine their current statutes to determine whether they are sufficient to combat this kinds of crimes . Where gaps exist, governments should draw on best practices from other countries and work closely with industry to enact enforceable legal protections against these new crimes.

REFERENCES

1. Duggal Pawan - The Internet: Legal Dimensions
2. Duggal Pawan - Cybercrime
3. Dorothy E. Denning and Peter J. Denning, Internet Besieged, Addison-Wesley Publishing Co., 1997.
4. Nagpal R - Defining Cyber Terrorism
5. Peter J. Denning (editor), Computers Under Attack, Addison-Wesley Publishing Co., 1990. A collection of reprinted articles from computer software journals, mostly from the 1980s.
6. Peter G. Neumann, Computer-Related Risks, Addison-Wesley Publishing Co., 1995. A collection of terse anecdotal reports in book format.

ASSOCIATED PRESS, "How Romania became a center of cybercrime," William J. Kole
http://www.msnbc.com/news/981284.asp?0si=-&cp1=1
ComputerWeekly, "Romanian man charged with releasing Blaster worm variant," Paul Roberts
http://www.computerweekly.com/Article124773.htm

The Register, "Transylvanian hackers put the bite on," Mike Kemp
http://www.theregister.co.uk/content/55/31493.html
http://www.cybercrime.gov/
http://www.fbi.gov/cyberinvest/cyberhome.htm
http://www.usdoj.gov/criminal/cybercrime/reporting.htm
http://en.wikipedia.org/wiki/Cybercrime
http://www.cybercrimelaw.net/laws/coantries/canada.html accesat la 01.08.2007
http://pim.belmt.be/pisa/fr/iur/mfocrimewet.htm accesat la 01 august 2002
http://europa.eu.irtt/ISPO/bonii/t_itidex.html
http://www.just.ro/ accesat la 01.02.2005
http://www.pcsj.ro/indicatori.htm accesat la 01 .02.2005
http://www.scj.ro/stat2004.asp accesat la 01.02.2005
http://www.poliiiaromana.ro/date_sta.tistice 2004.htm accesat la 01.02.2005
http://www.sri.ro/ accesat la 01.02.2005
www.efrauda.ro
http://www. insse.ro/
www.droi-technologie.org
The Computer Security Institute
http://www.gocsi.com/