CHALLENGES IN COMBATING THE CYBER CRIME

Mr. Sc Ahmet Nuredini, PhD Candidate
Professor in ISPE College
ahmetnuredini1@gmail.com

DOI:10.5901/mjss.2014.v5n19p592

Abstract:

The modern society today faces with the greatest achievements of technical and technological development, associated by rapid expansion of information technology and automation of work activities in all social life spheres. Such development in modern society has brought a large number of facilities on one side while, on the other side the presence of deliberate misuse of this technological achievement has also created a number of problems and risks towards individuals and groups in the society in general and national safety in particular. The approach how criminals (offenders) commit crimes has changed. Digital general approach has opened new opportunities for unscrupulous behavior. Millions of euros have been lost by businesses and customers from the use of computers as part of the commission of the crime. Computers and different networks can be used to attack victims or to prepare global violent acts such as terrorist particular among other. In absence of technology and trained personnel to deal with this new threat known as cybercrime, the security agencies are challenged by specialized cyber offenders which are known as hackers because apart from managing to break into state institution websites they are able to have unauthorized access to information classified as state secret and top-secret. Due to the global nature of computer crime, the general action in preventing and combating this type of crime, consists on building bridges of cooperation and coordinated action of all countries, and in this case of Kosovo in order to set international standards in the field of defense and security of information systems which standard would guarantee the success of a sustainable national perspective in combating threats from cybercrimes. In this paper, among others I will present the global aspect of cybercrime, the legal infrastructure defining cybercrimes and their forms, in, the role of security institutions in combating crime in general with particular focus on tackling cyber challenges, current threats and future threats related to cybercrimes, recommendations to combat these crimes, etc.

Keywords: crime, threat, cyber, security, classification.

Introduction

Cybercrimes represent one of the serious challenges for today's society. These crimes do not endanger the activities of public and private institutions but may endanger the person in its daily activities, private or professional sphere. Internet, as a new technology available to a vast number of users, it represents not only positive gain, but consequently it brings series of issues. The information technology today touches every aspect of life and humanity regardless of their location in the world.

Despite the benefits mentioned above, the rapid development of information technology has its negative side. The great achievements in this field opened new opportunities for anti-social and criminal behavior that previously were not achievable. The computer systems provide new opportunities for violation of the law, by creating potentials that push the perpetrators in committing various forms of crimes.

Cybercrime is a constant international threat affecting and acting beyond national borders, in such a way, making this form of organized crime as a global concern.

Cybercrimes may appear in various forms, depending on the way how it is committed and the intent of the perpetrators of these criminal offences, including online, fraudulent acts, thefts and cyber terrorism. This being said, the main reasons that facilitate the commission of this sort of crime is the globalization of technology and the revolutionary advancement of Information and Communication Technology(ICT), by having impact on criminal activities.

2. Aim and of objectives of the study

The main aim of this work it to reflect some general aspects of cybercrime, the weaknesses, challenges and threats of existing security systems of information from cybercrime. The essence of this work is to review the importance of this topic in our daily lives. The final intent of this work is to provide an overall and systematic examination, theoretical and practical study of this matter that it would enable scientific approach in the field of cybercrime and to enrich with new knowledge from this field by identifying the need for developments in international efforts to combat the cybercrime.

The modern research in this field of organized crime proved to us that the number of criminal offences against security of information is increasing along with the civilization of humanity and development of informative technology.

3. Global spread of cybercrime

The cybercrime thrat is considered as one of the main threats for national security in XXI century. Precisely, the actual core importance in this aspect, assaults against informative systems of private, state and international organizations, organized in most of the cases by organized transnational criminal organizations, during the periods of armed conflicts or tense situations by state authorities, raised a specific importance to the cyber threats in these current historic moments, because of the increased probability of terrorist attacks and assaults during armed conflicts, to be focused towards information systems and structural information strategically vital for the defense of NATO and EU member states.

Cybercrimes present a great problem for the global community. The internet is the aim and conductor of such activity, because of its transnational characteristic the combat of cybercrime requires a well-coordinated international effort. Cybercrime has now become a new form of permanent threat, considering that a cyber-attack may destroy a country without a need to involve any personnel that would have to go that targeted country.

The loss estimation as a result of cybercrimes is extremely high. In year 2009, the Federal Bureau of Investigation, assessed that the yearly losses from cybercrimes in United States of America(USA) is over 10 milliard € each year. During 2002, George W. Bush as a president of USA received a concern letter from a group of 54 experts from the field of information technology, national safety and intelligence agency. The letter emphasized that American nation is in great threat from a cybercrime threat more immense than the terrorist attack of 11 September 2001. The targets were critical infrastructure of US, including electric power, finance, telecommunication, health care, transport, water supply and use of internet, therefore requested a quick reaction to decide in order to avoid a possible national disaster.

The Interpol has ranked the combating of cybercrime in international level as one of top five priorities. The European Cyber Crime Center known as EC3, has the most important role in the fight against cybercrimes which closely cooperates with European community, internet companies such as 'Microsoft', 'Google', and 'Symantec', by also expanding its activities in online payment systems such as: VISA, Master Card and PayPal. The EC3 is considered as neuralgic point of combating cybercrime, considering as the defense mechanism of European Union (EU) against crimes through internet. The EC3 is comprised of 43 security experts that continuously take effective measures to protect the interests of the users (private or public) of digital networks and to destroy the criminal organizations behind the anonymous coding to communicate freely in internet, without being exposed to the risk of being tracked or revealed.

The practice showed us that the organized crime understood the importance and benefit that the phenomenon of cybercrime would provide. The anonymity that the internet offers raised the interest of organized crime by taking over this phenomenon. To illustrate, during year 2000 a group of 20 persons experienced in field of information technology and linked with several mafia families, managed to clone a e-banking service of a bank in Sicily, by embezzling 400 million $ that was given by the European community for regional development. Upon embezzlement, they used other on-line banking accounts for money laundering and erase the trace by implicating distinguished banks such Vatican Bank and few banks in Switzerland.

4. Cybercrime definition

Cybercrimes are means of unauthorized interception of computer systems and computer data through computers with intent to intercept the network and computer systems, in order to obtain personal data or manipulate with these data, use of computer resources for terrorism, intercept and obtain data from computer systems for financial, political and blackmailing purposes, unlawful hindrance of computer systems, acts against confidentiality, integrity and availability of the

computer system data etc. There are a vast number of actions that are connected with cybercrimes in social aspect such as copyright issues on distribution of protected material such as scientific publications, musical projects, audio, video and other business and academic activities. More important, the intention to intercept the state organizations and access to classified information of different states, today represent a major concern and challenge of national security in electronic communication and data. There are a great number of possibilities used to reach their intent through computer crimes. The most common ones are distribution of various computer viruses to network of organizations, use of vulnerabilities in computer systems, obtaining passwords and other personal details through email-messages and delivery of e-mails by unknown persons enabling unauthorized access to the email and obtaining personal data.

The traditional category of informatics crime committed through misuse of information technology has and continues to endure changes, as a result of continuous transformation of technology, by recoding new kinds of conduct, among them terrorism informatics that has to be criminally sanctioned as cybercrime, meaning that mostly the commission of traditional crimes by using as tool the information technology to accomplish their aim, or to commit a crime that has as an object to damage the information or computer systems.

5. Internet crimes

Internet crimes are the crimes committed in the internet or through internet. The perpetrator commits the criminal act in various ways through web pages. Forms and methods of committing the internet crimes vary, including distribution of erotic and pornographic material, hate crimes, prostitution, gambling, and destruction of data. The internet crimes can be applied as warfare against other state known as cyber warfare, money laundering known as cyber laundering through use of online financial services etc. Further we will review some of most common cases that occur related to cybercrimes.

5.1 Phishing:

"Phishing" is a deceiving method by use of email, that appear as official emails in search of potential victims, by pretending to be from their ISP, bank, or krijimi me pakice, with intent to gather personal and financial information. It is known also as a "spoofing mark" that is a method of stealing valuable information as passwords, credit card numbers, social insurance numbers, or bank numbers of authorized organization possesses. During this process the users are requested to visit a web page in the internet to recover their personal information through e-mail.

5.2 Identify theft

Identify theft is a crime committed mainly for personal gain, known as identify deceit. Through this crime, the identity of a person is stolen and used to commit a fraud by using the personal details of the victim, the insurance number, the bank account, or credit card number. The thief's of identify secure names, addresses, date of birth in order to apply for a loan on behalf of the victim. Internet is the most convenient place to commit an identity theft. It is easy for the criminals to use the credit bank details of a person in order to perform transactions that are done swiftly and without any previous personal intercommunication. "Background surfing" is a method that a thief may detect your password or Personal Identification Number(PIN), however this may be committed by means of attractive e-mail that contain a virus.

5.3 Credit card fraud

In credit card fraud, the attackers' unlawfully use someone's credit card topurchase goods and services through internet. The attackers may steal personal details by using different skills during transactions of a user in internet, or simply through social engineering skills.

5.4 Unauthorized downloading

Unauthorized download is considered a cybercrime. The authorized download from a website is permissible. However, any product that is copyright protected cannot be sold by any organization or an individual that is not authorized. Unauthorized downloading influences in sale of this product. Most of the crimes are committed because of available software tools to download. There are many issues that lead to illegal downloading such as, obtaining products with low price or free, there is no need for personal information, they are available worldwide. The entities that are most affected by illegal download through use of internet are: movies, programs, music, confidential and protected information, internet data etc.

5.5 Child pornography

Child pornography relates to activities involving sexual children conduct. The rapid development of computer technology provided access to production and distribution of child pornography. Not only girls and boys, but also infants have been victims of such abusive activities. The perpetrators abuse poor children, juveniles with limited abilities, and sometimes neighborhood children for sexual abuse. The children subject to sexual abuse through pornography suffer from mental depression, emotional recall, mood, fear and anxiety. The abused children as victims of pornography are severely traumatized because of illicit sexual abuse from perpetrators of this criminal offence. The children are forced to perform sexual act and often to perform sexual intercourse. The victimization of children is conducted in various and numerous forms. The victimization of the children unfortunately starts in an early stage. The children may be isolated and forced to become victims in any cost.

5.6 Fraud

The internet is uniform and is used as the most convenient market to promote business and services to the clients' worldwide. However, it is difficult to trace and identify the differences between the legal and fraudulent seller in internet, that deceive people through use of various opportunities that internet provides.

5.7 Cybercrime

Cybercrime is performed by use of computers in order to dispatch an electronic attack, through a system by committing multiple attacks in all computers worldwide. Cybercrime is a conjunction of terrorism and cyberspace. It is defined as a premeditated attack, political, motivated against information, computer system and programs, and data that lead to violence, against the targets from international groups or clandestine agents.

6 Kosovo Legal infrastructure regulating field of cybercrime

Considering the consequences leading to cybercrime, the states are obliged to conduct concrete steps in prevention and combating cybercrime, therefore the Republic of Kosovo, respectfully its responsible institutions has taken all necessary steps to penalize all illegal activities related to cybercrime. In Kosovo there was lack of legal infrastructure considering that criminal offences linked with security of information, including cybercrime were not foreseen in Kosovo Criminal Code or any specific law. In order to advance in the war against cybercrimes there was a partial amendment placed in legal infrastructure foreseen by special law "Law on prevention and fight against cybercrime". The purpose of the law is to prevent and fight the cybercrime based on concrete measures, to prevent, discover and sanction violations through computer systems, by providing observance of the human rights and safeguard of the personal information. The cybercrime is defined as "a criminal activity carried out in a network that has as objective or as a way of carrying out the crime, misuse of computer systems and computer data". The computer equipment may be used to commit crimes in several ways: as object of attack, as subject for attack-tool to commit crime, tool for planning, to cover or lead criminal activity, as symbol for deception, as tool to prevent, examine and prove the actions.

Even though the number of cybercrimes committed in Kosovo is relatively low considering the fact that during year 2012 there were 12 criminal offences, while during year 2013 there were 18 criminal offences recorded that were categorized as cybercrimes, however the number of these types of crimes is continuously growing.

Apart from the law on prevention and fight against cybercrime, there are other applicable laws that facilitate the fight of criminal groups and individuals that commit such criminal acts, the laws regulating further this issue are the Kosovo Criminal

Code, Kosovo Procedural Criminal Code, Law on Electronic Communications, and other provisions deriving from international conventions and Laws that regulate police activities such as National Strategy Against Organized Crime and other national and sectorial strategies.

Law on prevention and fight against cybercrime foresees 15 punishable criminal offences such as:

1.Unauthorized access in computer systems;

2.Unauthorized interception;

3.Unauthorized interception of non-public broadcasting of computer information, from, to, or within a computer system;

4.Unauthorized interception of electromagnetic emissions from computer systems containing non-public computer data;

5.Unauthorized transfer, modification, deletion, erasure of the computer data or their limitation without authorization;

6.Unauthorized data transfer from computer systems

7.Penal acts against confidentiality, integrity and availability of the computer systems data

8.Unauthorized transfer

9.Hindrance of computer systems operation

10.Unauthorized production, possession and attempt

11.Causing loss of asset

12.Child pornography through computer systems

13.Sequestration, copying and maintenance of data

14.Access, obtaining or record of communications

6. The role of state institutions in combating cybercrimes.

State institutions have a specific role in combating crimes in general and cybercrime in specific. The terrorist groups may have their harm intents to access the state systems of high value for the state and security structure such as the police, military and other state security agencies.

The increase of concern by national state agencies to prevent and combat the cybercrimes in informatics or informative systems, including the cyber terrorism against information systems that are part of critical or strategic structures of one country, requires development of co-operation to ensure judicial co-operation in the fight against organized cybercrime and terrorism. The specialized criminal groups to commit cybercrime develop their activities through computer viruses against individual users of internet and above all with sophisticated operations aiming to block the official addresses of private and public institutions such as banks, in order to unlawfully obtain the data or to infiltrate to classified information so to exchange them. The specialized perpetrators known as hackers, do often chose as a target the webpages of governments, ministries, courts, prosecution, security and intelligence agencies. The hackers possess highly specialized skills and professional experience, where they act quickly and efficiently. Therefore, the officials of state institutions encounter difficulties in detecting and resolving perpetrators despite their high dedication, therefore they have built their professional capacities and to co-operate not only with national state agencies but also international state agencies.

7. The role of Kosovo Intelligence Agency in fighting cybercrime

In the scope of national security institutions of Republic of Kosovo operate the intelligence service that in their focus have the collections of information from persons or members of groups that threat national security by committing cybercrimes.

The Kosovo Intelligence Agency (KIA) is a vital part of security section. Its primary role is the collection and analyzing of information for threats against the state and the population. The KIA is established as necessity of obtaining the information on time for intelligence, counter-intelligence, internal and external threats, international and national terrorism, organized crime, cybercrime, sabotage and all other issues related to intelligence and Kosovo security.

Apart from its role to gather information, the KIA performs the counter-intelligence activities. This activity covers the encountering and obstruction of cyber espionage and foreign intelligence services that are against the interests of the state. The agency is responsible of information protection and state information system, dealing with verification of security for all employees of the state institutions that have access to classified information. The essential role of KIA is to protect the state and its population. Preventing various crimes, including cybercrimes, terrorism and other threats against national security, the KIA contributes in the security and welfare of the society. It analyzes foreign and internal information, electronic communication through internet and gathers the information for un-information issues such as, propaganda, terrorism, sabotage, espionage etc. The KIA collects information from persons and members of the groups that threat national security with their incriminatory action including cybercrime.

8. The Kosovo Police role in fighting cybercrime

The Kosovo Police (KP) applies high standards of preserving the classified information. The data-center of KP is used for creating and functioning of entire service infrastructure such as servers, memory disks, network services etc. The entire service proceeding is done at the center where it is supplied with a robust server to perform the services needed.

Within the KP there is a cybercrime section functioning to investigate cases such as child pornography through internet, attacks in web-pages (governmental, various public institutions, business companies etc.), identity theft(purchase or order through credit cards), placement of scanners in ATMs, e-mail threats(against high profile public and institutional officials), fraudulent service activities through internet etc. The sector receives considerable number of requests from other states involving various cybercrime cases such as: web-page attacks, unlawful profit though services provided by web-page companies, use of unauthorized credit cards (identity theft) etc. Apart from the mentioned activities of the police regarding the fight against cybercrime, an important role has the co-operation with the prosecution office, the court and internet providers with bank representatives, customs and other institutions, depending on their needs. The close co-operation between relevant institutions is a primary or leading condition that cybercrime be prevented and fought efficiently and effectively. In regard to the international co-operation, we can assess it as positive but with intent to further develop it.

9. Challenges, current and future threat related to cybercrime

ost of the states have internal capacities and sources but they are insufficient to respond to cyber-attacks of major dimensions. The limited knowledge of internet of the users, motivation, the capability and facilitations that the criminals have to commit the criminal acts through internet, made the cyberspace an attractive environment for the criminals. The cybercrime is a phenomenon that touches upon a series of competencies, such as informatics, criminology, economy, justice etc. Therefore the cybercrime is to be considered as a complex phenomenon and the only way to confront it successfully is through a global approach in handling this problem. For this, there is a need for a co-operation between the experts of above mentioned fields in order to avoid partial solutions. The lack of membership of Republic of Kosovo in regional and international organizations in field of rule of law, remain the main challenges in fighting organized crime. Based on current assessments, there is no single state immune to the cybercrimes, therefore the local institutions in co-operation with international institutions need to be in alert and observe the activities of groups and organizations that may influence on the recruitment and financing of individuals for different cybercrimes.

10. Recommendations

During my analysis and research in this paper, in order to increase the efficiency in combating cybercrime i recommend:

- Further development and amendment of legislation to combat cybercrime in Kosovo, and full harmonization with international legislation. The foreseen cybercrime in the law on protection and fight against cybercrime needs to be incorporated in Kosovo Criminal Code.
- To increase the number of experts in the security organs and specialized units dealing with cybercrime.

- Advancement of inter-institutional cooperation between different structures of information technology for sensibilization of groups of interest and preventing the risk of their occurrence. The co-operation should be advanced not only within national security agencies but also with international security agencies.
- To supervise and filter the disaggregated information to prevent risks that could be brought through information in internet;
- Raising public awareness for proper use of resources in information technology in regard to cybercrimes.
- In order to advance the knowledge for applicable laws, the protection of privacy and intellectual property, with intent to sensibilize the methods and measures to prevent and combat the cybercrimes, there is a need to organize media debates, workshops and seminars with organizations for security and civil society.
- To create a global architecture of security of information in order to consider within the technical, operational, organizational, economical, judicial, regulatory and human dimension, and
- Drafting of National Strategy for Information Security.

12. Conclusions

During the analysis and research in this paper, the following conclusions have been reached: Technical-technological development associated by fast expansion of information technology and automatisation of work activities in all life spheres in modern society brought a number of facilitations, while on other side it brought a premeditated misuse of these technological achievements, while creating a number of problems and risks for individuals and groups, as well as for society in general. Because of its global character the computer crime, the general act in preventing and combating requires the advancement in co-operation and codified action of all states to combat effectively the cybercrime. The war against computer crimes is a duty of the entire society, which in Kosovo can be achieved by taking measures to create an international co-operation in harmonizing judicial legislation with developed countries under the European Convention of European Council.

Bibliography

- Bruce Schneier, Secrets and Lies: Digital Security in a Networked World, John Wiley Sons: first edition, 2000,
- Cybercrimelaw.net. A Brief History of Computer Crime Legislation, taken from:[http://www.cybercrimelaw.net/content/history.html], 15.08.12
- Computer Crime & Intellectual Property Section (CCIPS) at U.S. Department of Justice, Field Guidance on New Authorities That Relate to Computer Crime and Electronic Evidence Enacted in the USA Patriot Act of 2001. 2001.
- Horn, P. It's Time to Arrest Cyber Crime. Business Week Online, 2006 :taken from: [http://www.businessweek.com/technology/content/feb2006/tc20060202_832554.htm]
- Internet news. Scammers Hooking Bigger Phish, 2006; taken from: http://www.internetnews.com/stats/article.php/3642971],data: 01.09.2012
- Kshetri, N., Positive Externality, Increasing Returns, and the Rise in Cybercrimes.

  Communications of the ACM, 2009.
- Council Official Curriculum, “Computer Hacking Forensic Investigator”,

  Courseware Manual 3.0 Volume 2, 2009
- Computer Crime & Intellectual Property Section (CCIPS) at U.S. Department of Justice.
- International Aspects of Computer Crime. taken from: [http://www.usdoj.gov/criminal/cybercrime/intl.html], 10.04.2014
- Gurpreet Thillon, Principles of Information Systems Security: Text and Cases, Wiley, first edition, 2006,
- Cyber Crime Staff. “FDA Flub.” Peter Salus. “Net Insecurity: Then and Now (1969–1998.

- National Security Telecommunications and Information Systems Security.
- Willis Ware. “Security Controls for Computer Systems: Report of Defense Science Board Task Force on Computer Security.” Rand Online. 10 October 1979.
- Kosovo Criminal Code,
- Kosovo Criminal Procedure Code,
- Law no 03/L-166 on Prevention and Fight of the Cyber Crime
- Law no. 03/L-063 for Kosovo Intelligence Agency
- Law no. 04/L-076 for Police
- Law no. 03/L-196 on Prevention of Money Laundering and Terrorist Financing
- Law no. 04/L-064 on Kosovo Agency for Forensic
- Law no. 04/L-094 on Information Society Services
- Law no. 03/L-178 on Classification of Information and Security Clearance
- Law no. 04/L-109 on Electronic Communications