343.9:004]355.45-022.326.5 Review scientific article

HIGH-TECH CRIME - FORMS AND SECURITY RISKS

Marija Gjosheva, PhD
Department of Cybercrime and Digital Forensics
Ministry of Interior Affairs of the Republic of Macedonia
Email: gjoshevam@hotmail.com

ABSTRACT

In the era of high technology, which many consider the beginning of the 21st century, its application has found a place in our lives with all its positive and negative benefits, so fast that high technology has become a topic of today and not something that will bring us the future. We approached closer to the phenomenon of high-tech crime which by its characteristics is transnational and international. Thus stressed to the need for taking over a global action through closer international cooperation in the legal sphere as well as in the fight against high-tech crime, because without harmonization of measures and activities and without rapid and efficient exchange of evidence and information it is very likely a greater number of crimes to remain unpunished.

Keywords: high-tech crime, types and forms of endangerment, protection against high-tech crime, international institutions.

Introduction

The world is passing through the second "industrial revolution". Information technology now touches every aspect of our living. Daily activities for most people are affected by a computer. Businesses, governments, individuals and others use the benefits of information revolution. Despite the benefits in time and money, the computer has an impact on everyday life because the computer routines replace many human tasks. Computers are also used to store sensitive data of a political, social, economic and personal nature. They help in improving the economy and living conditions in all countries.

The computer has a large amount of data to store on the compact medium and high speed operation enables the most complex calculations to be realized in a few milliseconds.[70]

The development of information technology contributes to increasing the types of crimes in the area of high-tech crime especially with elements of cross-border organized and transnational crime. In many countries around the world which have developed informational structure which by its nature is very vulnerable to these kinds of attacks, high-tech crime is marked as one of the worst. Scientific and expert community has recognized the threatening danger from high-tech crime.[71]

Definition and types of high-tech crime

New technologies allow criminals new opportunities and fields of action. The mode of committing the crime in the past and today is very different. In the hands of people who are criminal, information technology can become a tool for danger or damage to life, property or dignity of the individual. The approach of classical security only brings stalled innovations in terms of high-tech crime. It is no longer feasible in this digital world because the information processing is distributed very quickly. Innovative solutions rely on new technologies and the traditional approach to security changes.[72]

The basic features of high-tech crime is the **use of the computer as an object of attack** and **as a means of committing the crime.** When it appears **as an object of attack,** the computer can attack two components- hardware and software. Damage, destruction or abuse of these two components is achieved through three core assets, namely: computerized viruses, worms and trojans. Unlike the first two, which when their creator send there is no more control over them, the third type is a danger which for us is of particular interest since it is a computer program that allows the sender to access the "infected" computer, and to have an insight into its data and manipulate with them without the owner being aware of it.

[70] Doctoral dissertation entitled "New challenges and threats of high-tech crime against national security" defended at 05.03.2017 the Faculty of Philosophy Ss. "Cyril and Methodius" Skopje - Institute for Security, Defense and Peace.

[71] The police and high-tech criminal - case studies and problem in the work of the Ministry of Interior Vladimir Urosevic, Sergei Ulyanov, Radoje Vukovic, Ministry of Internal Affairs of the Republic of Serbia.

[72] Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, Europe 2002, pp. 7, pdf.

When appearing **as a subject of attack or as a means of committing the crime,** it is a "relief" or facilitating the realization of a criminal activity with its help. Here, it is very important to note that the computer can be used as a tool for planning or covering up the crimes or the management of certain criminal activities. This feature is important because in the future it will be the point of connection between organized crime and high-tech crime.

According to the Convention on Cybercrime, the following manifestations and practices of the criminal acts of high-tech (cyber) crime are listed:

1. Computer fraud;
2. Identity theft (phishing, pharming and spam);
3. Financial theft and abuse;
4. Data and documents forgery;
5. Computer vandalism;
6. Making and use of computer viruses (viruses, worms and Trojans);
7. Computer sabotage and espionage;
8. Hacking (creating and abuse of botnet networks);
9. Unauthorized reproduction of legally-protected computer programs (software piracy);
10. Computer terrorism.[73]

Computer fraud

Computer fraud is the most widespread form of high-tech crime.[74] The numerous forms of fraud and their realization is virtually unlimited. Typical for computer fraud is that the offender and the victim does not come into direct physical contact, their contact is direct, but electronically.

The thing that characterizes computer fraud is that it is spread everywhere, in different forms such as: false advertisements which involves fictitious sale of all kinds of goods, when the victim make payments – they are deceived and do not receive the goods they had paid for, then unauthorized access to electronic mail and changing invoices for payments used by companies and concerning changes to the "Iban code" - that is a change of actual account at which should be paid in cash into a false account with a

[73] Cybercrime Convention was adopted by the Council of Europe on 23.11.2001 in Bucharest and entered into force on 01.07.2004 year Republic of Macedonia has ratified the Convention by law to ratify the Convention on Cybercrime adopted on 16.07.2004 year.

[74] Jugoslav Achkoski, Security of computer systems, computer crime and computer terrorism, Skopje, 2012, page 30, pdf

minimal change which is imperceptible to the victim. Thus the funds go to the account controlled by the criminals so they are gaining with a huge financial gain.

Most of the computer frauds are committed by international organized criminal groups operating in different countries in the world, and therefore the prosecution against them is very difficult.

Identity theft

Identity theft is complex problem that is spread throughout the world. The offenders can act alone, but they often form networks as they could operate around the world so the number of their victims becomes multimillion.

Computer criminals can overcome security measures for protection, to break through a database (detailed financial data such as bank accounts, data from credit cards, medical data to persons and other sensitive information), and data from personal documents: passports, identity cards, driving licenses etc. Also stealing the identity is easily executed through social networks, primarily because of the fact that large number of people have unprotected free - open profiles. Also, the offenders can easily come to the identity of any user of credit cards as one of the types of high-tech crime that is on the rise, for example by installing cameras over ATMs, setting "skimmer devices" to read data from credit cards which devices can easily be purchased online. Also, on the Internet can be found numbers of credit cards sold to certain forums where the membership in these forums is limited and not everyone can simply subscribe.

The main objective is financial gain. With all these stolen personal data of persons through illegal identity theft, cybercriminals can compromise people, to sell their personal information to other criminals of all types and levels, which can be used to carry out serious criminal acts such (terrorist financing, money laundering, human trafficking, illegal migration, computer terrorism etc.) that would affect the national security of the country.

Nowadays, as the best known and most common ways of identity theft through information system in order to abuse it, are Phishing, Pharming and Spam. Phishing attack involves activity by unauthorized persons through the use of fraudulent messages, email, create fake web pages of financial and other organizations in order to specify the user to disclose their confidential data, data such as bank accounts, credit card numbers, user names, pin codes and other approaches. Once the criminals obtain confidential information from a security nature, they can sell to them to other governments, private companies, in which way they can cause serious security breaches. Pharming is a form of remote attack which targets vulnerable web page and it redirects to a malicious web page.

This attack can be done by changing the file information to the embattled computer or by exploiting security flaws DNS (domain name system). DNS task is linking names with real addresses on the Internet, and for the compromised DNS is said that it is "poisoned". These attacks are concentrated on specific industries, such as financial and security. Also, if by pharming attack anyone comes to health information, they can be altered, that is, a particular therapy or blood test for example to the President of a country or the Premier to be changed, which means assassination of this person, which would cause a serious unrest in that country, thereby directly affecting the national security of the country. Spam is unwanted e-mail. It is a problem which many years creates concern among Internet users. Whether it comes to end-users, large companies or ISPs, spam except that asks users problems it causes financial losses. Despite major efforts to prevent spam with a variety of information tools, legal regulations, unwanted e-mail is still an unsolved problem in Information Systems. It can be freely said that many users are accustomed to spam and accepted as something inevitable.

Besides the disturbing character that the spam has with the end-users, the problems created by the spam have a broader importance. Namely, it could affect the reputation, damage and integrity of companies or individuals taking the time of the alien computer to perform the action, the space on the hard disk, network opportunities, etc. Addresses are being collected through daily internet search to obtain new addresses that later would be used to send spam messages. These addresses are later being sold to interested persons, mostly to spammers themselves who use them for mass messaging. Also it looks like an advertising message which offers certain products or services. In some cases spam message can contain scripts that gather all the information that you possess on a computer, network, or server. Also spam messages may contain malicious code, embedded macro viruses that after its activation on the device or the network will take all the information, images, documents that you own.

Financial theft and abuse

Financial theft and abuse are among the most common computer crimes, relating to unauthorized access to systems of financial institutions, such as systems of banks, processing centers serving banks and have large sets of financial data including personal data of customers, penetration of bank accounts, data from credit cards, and abuses of credit cards.

With data theft of cardholders and their pin codes, the criminals are making great abuses through the withdrawing large amounts of cash, they make forged payment cards with abused cardholder's data and use them in various countries around the world,

such as at ATM (cash dispenser) and POS terminals whereby perform illegal transactions of sale. There are various forums on the Internet, which for a certain amount are offering complete data from payment cards for sale (numbers of payment card data from owners of credit cards, PIN codes and CVV 2 code that is commonly used to carry out transactions on the Internet).

Lately there are frequent abuses when buying online that is e-commerce (online trading). When it comes to e-commerce, we can conclude that lately it is in development, we live the era of internet marketing which enables the exchange of products ever, anywhere at the speed of light.

The term e-commerce means transactions that are conducted online, and only on the web-based applications for trade (transactions through email are excluded), and covering goods and services in the material and the immaterial form. Mitigating circumstance in internet commerce is reduced risk to detect criminals, primarily because they do not need to appear in the shops, no need to set up a "skimmer devices" (devices for data theft from credit cards) at ATMs, do not need to produced forged payment cards and withdrawing cash from ATMs. To carry out illegal transactions online, criminals only need data from payment cards and CVV 2 code located on the back side of a payment card (in some cases not necessary, it depends on the website) and of course internet access .

As one of the largest financial theft and abuse which is also on the rise is Internet banking. It has become one of the best known and most widespread electronic services. Extremely convenient financial service that offers 24 hours service with no extra charge. However, online banking fraud is on the rise. Internet banking should be safe. The protection of personal user data is priority. Also Internet economy has become one of the strongest economies in the world. Most of our life now is done "online". Cybercriminals see great opportunity for financial fraud, theft, income from the stolen data and other valuable information.

These cyber-attacks directly targeting the business systems, large supply chains, as well as large business companies. These attacks mainly threaten individual security of person, then directly threaten the financial sector, affects the economic stability of the country, losing faith in the reliability of the state system, thereby reducing the financial gains of the state and thus it becomes economically weak, and when a country is economically weak it is an open field for many kinds of organized crime and corruption, and it affects the national security of the country.

Data and documents forgery

The rise of this activity is linked with the emergence of computerized color laser printers. These printers have the option of high-resolution printing, modification of documents, even creating fake documents. The quality of these documents are often not distinguished by the quality of authentic, and often there are attempts to counterfeit banknotes using the computer and peripherals.

Special emphasis should be put on data and documents forgery. The most popular is the personal documents forgery (ID cards, passports, driving licenses, health cards, etc.), also and educational certificates forgery, forging a various documents for economic purposes, for health purposes, etc. Using forged documents in election process in any country represents a major threat.

Computer vandalism

Cyber vandalism is a malicious hackers' act with performing disturbance of the functioning, modification and even destruction of the site. Cyber vandalism characterized as website defacement (destruction of the website) or Dos attacks (Denial of service). If in the past vandalism express itself by writing or drawing graffiti on walls in public places, or even further back by typing in caves, which undoubtedly was used as a means of communication "today it is done with WEB sites attacks". The affected websites must be temporarily closed to eliminate the damage, and return to normal original state. The immense possibilities offered by the Internet and its reach around the world, without borders or computer space allows this type of criminals to spread messages on the Internet that usually hate speech, as well as economic terms whereby damaging the economy and industry.

Cyber vandalism has a major impact on government sites as well as religious sites, and it may be political reasons or just for fun. For example, if the official website of the government, the president of a country, unauthorized change the contents and become threats from religious and national origin to a particular nation or written speech of hatred, it can cause protests, riots by members of that nation, which can easily escalate and thus become a threat to the national security of the state. In 2009, a computer vandalism- defacement was committed on the official website of the President of Macedonia, Dr. George Ivanov.

Preparation and use of computer viruses

A computer virus is a program, a correct computer code which represents being something else, it aims to do the unexpected, cumbersome and often undesirable situations, and it can do little or great damage to the computer (for example loss of data from the hard disk) . The activated virus can not only infect programs and documents on your computer, but can be reproduced and transmitted to other connected computers in the same way as biological viruses pass from one person to another.

Today viruses commonly spread through internet, when downloading various programs or via e-mail. To protect against the viruses we need to install an antivirus program to our own computer.

Today's viruses are much more powerful than they were in the early versions. Viruses can be activated by opening an e-mail (attachment), by clicking on spam by visiting suspicious sites, open spreadsheets (excel). However, the Internet represents the main "highway" transmission of viruses.

With the help of computer viruses, criminals can come to very confidential and sensitive government information, security information, financial data, personal information, research and medical data, etc. Usually if criminals come to such information, they can sell them in order to gain material benefit, unaware that if this information come into hands of wrong people, it can cause serious threats to security.

Computer sabotage and espionage

Computer sabotage exists in case someone destroys, deletes, conceals or otherwise disables data, program or damages the computer which is important for the state agency, institution, and public service. It is used for gaining economic advantage over competitors to promote illegal activities of terrorists or steal data or programs.

Spying can be motivated by political or economic reasons because many countries through the deployment of its secret services have come to disclosure of political, military, economic secrets to other countries. Computer espionage can be defined as one of the most modern forms of intelligence. Despite hackers and groups they organize unauthorized access to protected system; nowadays there are specialized secret government agencies that collected data intelligence nature by entering into the computer system of other countries. Computer espionage is the act or manner of obtaining secrets without authorization of the holder of the information (personal, sensitive, proprietary or confidential) from individuals, competitors, rivals, groups, governments and enemies, personal, economic, political or military advantage , using

illegal methods on the internet, network or individual computers. Computer espionage is a method used over the Internet. To carry out the computer espionage mainly, malware, including Trojan horses (special Trojans made to spy on the user), viruses, spyware (RAT, Keyloger) are used. Spying can fully execute the Internet by professionals from bases in some remote countries and so on.

Hacking

Hacking up is a penetration into certain information system and entering it. One of the biggest threats on the Internet is the existence of thousands of compromised computers. The networks of such computers are called BOTNET networks or "zombie thieves" and computers that are part of them are present in homes, schools, workplaces and government facilities worldwide. Mainly, they are under the control of one or several hackers-also known as "Bot master", and it is used in carrying out various types of attacks - from distributed attacks disabling services (Distributed denial-of-service, Ddos), sending unwanted messages by e-mail, using tools to capture pressed keypad (Key logger) to the spread of viruses, malware programs, etc. At the same time, the damage that can be caused by the use of such networks, is incomparably greater than the damage done to traditional discrete attacks.

It can be concluded that today BOTNET networks are one of the largest (if not the largest) security threat to the Internet community. The botnet network consists of a series of linked computers that cooperate and operated by a hacker or less group. Bot is an ultimate computer (or server), which is a member of the bot net network.

Unauthorized reproduction of computer programs (software piracy)

"Software piracy" covers a variety of activities: illegal copying programs, forging and distributing software, and exchanging programs. The software is one of the most valuable technologies in the Information Age.

Software pirates not only steal from the companies that produce software, but also inflict damage to consumers, shrink fund research and development of new software. With observance of the law, not only software piracy will be reduced, but would prevent a major economic problems. The fact that "Microsoft" logo is written on the disc or the software is originally installed on the computer, does not mean it is legal, simply stated, software piracy is illegal production and use of software products in abuse of copyrights.

Online sexual exploitation of children

Online sexual exploitation of children as a negative phenomenon is present in many criminal acts long time ago and it is growing globally. With the advent of high technology and global network of communication, the manner of its production and distribution facilitates and becomes easily accessible to a larger group of people, which has turned into an entire industry that ultimately tramples basic moral norms and the rights of children which have become a tool for earnings in the hands of international criminal network.

Regarding the online sexual exploitation of children, an abuse was observed (presentation and publication of pornographic material) through the social network Facebook, video streaming (watching live Internet) via Skype, etc. The reason for this trend is the easy availability on the Internet of children and lack of parental control in respect of persons with whom their children communicate through social networks.

Electronic money laundering

Using technology or electronic money transfer aids criminals in concealing the proceeds of criminal activities. The development of informal banking institutions and parallel banking systems, may allow you to avoid the supervision of the Central Bank, and can also allow evasion of cash receipts that have organized criminal groups.

Also, organized crime groups use the Internet as a communication (usually encrypted), thereby increasing market of digitally encoded technologies. Everyone need this type of technology especially banks that want to ensure the privacy and confidentiality of clients and their financial transactions. Cryptography represents them a powerful tool of criminal groups and terrorists to conceal their activities, and for authorities' additional difficulty for conducting investigations and collecting evidence.

High-tech crime mechanism of contemporary computer 'cyber' wars

Computer war (war in cyber space) is an internet conflict, including politically motivated attacks on information and information systems. Computer War is a new form of keeping a military gathering which application in the international community is increasing rapidly. But, its nature is specific and differs from the known forms of war. Computer war battlefield are communication and information content. Attackers can destroy infrastructures of unfriendly states if largely based on the same computer contents.

There are claims that the new tactic of computer war is causing damage to critical infrastructure in cyber space, and kept the damage. With the computer war attacker may have different strategic goals:

- Distribution of propaganda or causing panic between civilians;
- Permanent damage to the key elements of the technological infrastructure (power, communication centers, etc.).
- a collection of secret information;
- Attacks by viruses (Trojan horses, etc.).

Depending on the purpose you can use tools such as "zombie computers" that are used for DDOS attacks still allow obtaining control over the centers. The consequences of computer war are weakening or termination of the basic physical infrastructure. Critical infrastructure are the systems, and if they are destroyed that will affect economic security, banking, public health, physical security, communication, public transport, electronic commerce etc. and will cause implications for national security.

Cyber terrorism

Third major threat after chemical-biological and nuclear weapons is cyber terrorism. This is a special form of attack on computer networks and databases intended for use of force or threat to the government of a country for its ordering of a particular policy or making certain decisions, the use of cyberspace as a field for making illegally obtained money and using the internet to concealing the origin of illegally gained money (money laundering), in order to use them in financing of terrorist organizations or contemporary called cyber terrorism".

The object of attack may be important infrastructures (water, gas pipeline, electro-distributive facilities etc.), where breaking into computer systems of the control flight will cause plane crashes, activation of nuclear bombs, fear, panic among the population, large human victims. The terrorists have a large arsenal of weapons including chemical and biological weapons, which can cause ecological disasters and chemical pollution, opportunities for terrible poisonings of water systems. The terrorists use internet for dissemination of their goals, which consists mostly in spreading hatred, violence and racism.

Computer terrorism should also be distinguished from "Cyber War" manipulation of computers and computer networks in the context of inter-state conflicts. Computer war carries offensive and defensive activities of the state and the structure of international conflicts. Computer terrorism and computer war could match in the use of certain

methods such as Destruction of computer networks, but it does not mean that this is the same activity. Computer terrorists usually cooperate with weak states or states that are ineffective or corrupt security agencies in order to more effectively act.[75]

Conclusion

High-tech crime is not future, but present. High-tech crime has become more pronounced, it has applied innovation and is growing. With sophisticated information technology type of threats, the way of carrying out attacks, is more different from traditional types and forms of threats and attacks. From a broader perspective countries today face threats to their national security threats that are not traditional. The most important implications of these changes is to increase cooperation at the international level, ticking this need for cooperation between nations in order to successfully respond to threats posed by high-tech crime.[76]

High-tech crime is the kind of crime that often crosses the borders of a state, for example, the crime is committed in one state, the perpetrator is from another state and has caused damage to a third country. Hence, the best practice in combating high-tech crime is intensive cooperation at international level with police services from other countries especially through international institutions such as Interpol, Europol and SELEC.

States should adopt appropriate measures to regulate the investigation of these crimes, to collect evidence of the crime as possible. So, to successfully deal with high-tech crime requires cross-equal legislation and coordinated investigative process.

[75] Doctoral dissertation entitled "New challenges and threats of high-tech crime against national security" defended at 05.03.2017 the Faculty of Philosophy Ss. "Cyril and Methodius" Skopje - Institute for Security, Defense and Peace.

[76] James A. Lewis, „Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats" pdf.

Bibliography

1. COMMUNICATION FROM THE COMMISSION TO THE COUNCIL, THE EUROPEAN PARLIAMENT, THE ECONOMIC AND SOCIAL COMMITTEE AND THE COMMITTEE OF THE REGIONS (2001), Creating a Safer Information Society by Improving the Security of Information Infrastructures and Combating Computer-related Crime, Brussels: EU, accessed: http://eur-lex.europa.eu/legal-content/CS/ALL/?uri=celex:52000DC0890.
2. Convention on Cybercrime (2001), Strasbourg: Council of Europe, accessed: https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185
3.Gjosheva Marija, "New challenges and threats of high-tech crime against national security", unpublished PhD thesis defended at 03.05.2017 the Faculty of Philosophy Ss. "Cyril and Methodius" Skopje - Institute for Security, Defense and Peace;
4. Lewis James A. (2002), Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, Washington D.C.: Center for Strategic&International Studies, accessed on: https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/media/csis/pubs/021101_risks_of_cyberterror.pdf
5. Khadam Nadia, "Insight to Cybercrime", accessed on: https://www.academia.edu/2011205/Insight_to_Cybercrime?auto=download