STRUČNI RAD (PROFESSIONAL PAPER)
UDK: 343.98:[343.3/.7:004]

Associate Professor Svetlana Nikoloska, PhD
Faculty of Security- Skopje, “St Kliment Ohridski” University, Skopje
svetlana.nikoloska@uklo.edu.mk

Marija Gjosheva, PhD
Ministry of Interior of the Republic of N.Macedonia,
Sector for Cybercrime and Digital Forensics, Skopje

CRIMINAL INVESTIGATION OF CYBER CRIME

Cyber-crime is distinguished from classical and economic crime as a separate group of crimes that have their own specific criminal characteristics, which are emphasized in the very definition of this crime, which is the means of committing the crime and the object of the criminal attack. It is precisely the criminal characteristics of cyber-crime that necessitate the need for appropriate criminal investigation and the provision of relevant evidence through the application of legal measures and actions and the application of appropriate techniques to provide electronic evidence which is crucial to fully illuminate a criminal forensic event, prosecution of perpetrators of specific crimes. The purpose of this paper is the theoretical study of forensic research, by analyzing a practical example following the case studies method, in order to derive indicators of the specificity of the procedure for the elucidation of computer crimes and the specific approach to securing electronic evidence, as well as its storage. and adapting to the needs of the criminal procedure, is acceptable to the judicial authorities.

Keywords: *cybercrime, criminal investigation, forensic, digital evidence, criminal practice.*

are necessary preconditions for criminal investigation of this crime and enabling the initiation and successful completion of criminal proceedings against the perpetrators. Given that this crime according to its criminal characteristics, especially for the time and place of criminal activity has an international character, measures and procedures are needed for national coordination of investigators with the prosecution, but also international cooperation to assist, support and conduct joint forensic research.

2 TITLE AND PUBLIC FORMS OF COMPUTER CRIMINALITY

Cyber-crime is a general formulation that includes various forms and forms of criminal behavior. Namely, it is a crime that is directed against the security of information (computer) systems as a whole or in any part of it in different ways and by different means in order to gain some benefit for themselves or for another or to inflict it on another some damage (Jovasevic, 2002).

Cyber-crime is a crime related to information and computer systems and this category classifies all criminal behavior whether it is a threat to citizens' property rights or any other right, in terms of violation of human rights and freedoms, abuse of human rights. Personal data, violation of morality, as well as violation of property rights and interests of legal entities, which is an important element for this crime to be included in the scope of economic crime. Namely, the modern automation of the business process and the overall functioning of the legal entities, using computer technology, create opportunities for financial and bookkeeping and computer frauds, whereby illegal financial transactions are conducted illegally for the purpose of misappropriation. By perpetrators who are capable, in position, and knowledgeable of such criminal activity.

The computer is increasingly being treated as a means of committing a crime where both computer systems and networks are used in addition to the personal computer and by including opportunities for specific criminal behavior that result in the acquisition of unlawful gain or the infliction of property, financial or any other. Type of damage, or damage to the computer systems themselves and their contents. Thus, cyber-crime encompasses several different forms of criminal activity that are found in most definitions of the term cyber-crime, and several terms are used to cover the same or similar criminal acts where the computer occurs as a means of perpetration or an object of criminal activity, attack. These are the following terms: computer abuse, computer fraud, computer crime, information or technical crime.

Cyber-crime provides such an intellectual engagement to the offender that gives him the attribute of "perfect crime" (Đukleski, 2000).

In the theory of criminal law, criminology and criminology can be found several definitions of the term cybercrime, but international documents also have their own definitions for this type of criminal activity. With the introduction of

1 INTRODUCTION

The advantages of information systems and computer networks throughout social life do not remain unused by organized groups and individuals who use information in the field of computer science for illicit purposes, whether they are unlawfully benefiting or otherwise violating their rights and the freedoms of citizens, endangering the property of citizens, but also the overall security that encompasses the protection of national, racial, religious, social and economic citizens' rights no matter where they are on the globe. Criminals around the world do not choose the means of crime, and the computer is the perfect means to accomplish certain criminal purposes with little opportunity to detect them, because the cause is at one point on the globe, and the consequences can be in many places at completely different ends. From around the world, even the participants in the criminal network do not know each other, but it connects knowledge, power and skill in computer technology, but it also links the criminal purpose. The computer is becoming more and more a means of carrying out various manifestations of illicit, illegal and socially dangerous acts. Cyber-crime is synonymous with all forms of criminal behavior and plays an important role in criminal behavior, be it computer abuse as a means of committing criminal activity or as an object of criminal attack.

The international community recognizes the problem of cybercrime as a serious security problem, as a "benefit and quality" of the modern world and the rapid development of information technology. To investigate this one security phenomenon that poses a serious danger manifested through a number of emergent forms of criminal activity of a differentiated layer of perpetrators who skillfully use their knowledge, skills and abilities in criminal purposes, the term 'cyber-crime' must first be defined, to identify emerging shapes and forms and who are likely perpetrators. Namely, the original definition of cyber-crime was that: "any unlawful act whose successful execution is crucial to knowledge of computer technology" (Nikoloska, 2010).

Given that cyber crime is a modern form of crime caused or aided by the development of information technology, it also exhibits the hallmarks of organized crime and there is a difficulty in locating and identifying the most significant theoretical and practical problems related to its detection, proofreading. In this respect, it seems that criminal practice is ahead of theory for the simple reason that theoretical systems and subsystems of knowledge on the level of forensic methods for combating cyber crime have not yet been created (Angeleski, 1995).

National legislations accept the recommendations of international legal acts for harmonization of criminal substantive legislation and criminal procedural legislation in order to criminalize computer crimes, but also to provide for appropriate measures and actions to detect, clarify and provide evidence. These information technology and its abuse, the first definitions of the term cyber crime were given. Cyber crime has been defined as computer abuse in the sense of any activity related to the use of computer technology in which the victim suffers a loss or could have lost, and the perpetrator acts with the intention of gaining or could gain. (Parker, 1973). August Bequai defines cyber crime as committing crimes in which the computer appears as a means or object of protection, ie as the use of the computer to commit fraud, evasion or abuse with the aim of embezzling money or services or performing political or business manipulation that involves computer-directed actions. (Bequai, 1978). Cyber crime consists of crimes in which the computer appears as a tool, object or object for the execution or attempt of which a certain knowledge of informatics or computers is necessary (Brvar, 1982). Cyber crime refers to a special type of criminal behavior in which the computer system (understood as a unit of hardware and software) appears either as a means of perpetration or as an object of the crime, if the crime in another way or against another object could not be performed at all or would have other features (Ignjatović, 1991).

From a criminal-legal point of view, cybercrime covers the abuses of computer systems, programs and data that are incriminated in the Criminal Code of each country. These are crimes in which the computer is the object of a criminal attack (computer crime), Crimes in which the computer is a means of execution (computer related crime) and crimes that make illegal use of the Internet (net crime) (Nikač & Leštanin, 2019).

Cyber crime is defined in the Preamble to the 2001 Cybercrime Convention adopted in Budapest and is an activity that is directly directed against the confidentiality, integrity and accessibility of computer systems and data networks, as well as the possible misuse of these systems and data networks.

Cyber crime is characterized by great dynamics and numerous forms and forms and ways of execution that are directly related to the spread and opportunities provided by information technology and the rapid growth and development of computer networks and systems that have entered every home, every workplace. In all state institutions and commercial and other enterprises.

From the aspect of criminalistic characteristics that refer to the manner and means of committing the crime, criminal motives and goals of the perpetrators, time and place of perpetration, place of criminal activity, organization of perpetrators, special regularities in planning and committing crimes that have elements of computer crimes, they can be classified into several groups of computer crimes as follows:

- Property computer crimes (damage and unauthorized entry into a computer system, computer fraud, computer viruses, etc.).
- Violent computer crimes (wiretapping, cyber terrorism, cyber sabotage, cyber espionage, cyber vandalism, unauthorized intrusion or hacking,

incitement to racial and religious discrimination, child pornography, murder committed using a computer system, etc.).

- Economic - financial computer crimes (computer embezzlement, computer forgery, piracy, copyright abuse, making and using a fake payment card, etc.).

These cybercrime groups cover a number of specific crimes under national law, but national legislation follows international recommendations from international legal acts to codify new forms of cybercrime. However, the national legislations also adapt the criminal procedure laws in order to harmonize the existing ones and to create new measures and actions with which the electronic evidence can be more properly extracted, stored and presented.

3 CRIMINAL INVESTIGATION OF CYBER CRIME

Research on the state and movement of cybercrime indicates the existence of a large “dark number” of undetected and undeclared crime, but also reported crime where the perpetrators are undetected or unavailable. The problem is complex due to the existence of a growing number of computer social networks and a large number of their users, which facilitates the commission of crimes and hiding the perpetrators.

According to the official statistics of the most famous criminal police in the world FBI, less than 1% of cybercrime is detected from the reported 12%. The FBI has a specialized Computer Crime Unit - CAR (Cyber Action Team) that works with Interpol, Europol and other specialized agencies such as CERT (Computer Emergency Response Team) (Obradović et al., 2007).

From the very definition of the term cybercrime, the criminalistic characteristics of cybercrime are perceived, because almost everyone states that these are criminal acts where the computer appears as a means or object of a criminal attack. But from a forensic point of view in the field of forensic research, the computer again appears as technical in the process of providing electronic evidence. The function of the computer from a criminal point of view can be expressed in four and basic types (Bošković, 2000):

1. The computer as a means of committing a crime, where the perpetrator uses the computer to commit a particular crime, usually fraud, theft or embezzlement. It is a classic crime in the field of general crime and economic crime, which were committed in a specific way with the help of a computer, which is the basis for their separation from the traditional division of crime and reduced to the notion of computer crimes.
2. The computer as an object of attack, where the computer and the information contained in it are the ultimate target of a criminal attack, whether the computer is the object of damage, disabling or destruction, or

the information contained therein is to be accessed without authorization, of various motives. These criminal attacks can be carried out not only by persons who are employed, but also by persons outside the building where the computer equipment is located, using appropriate methods in order to unauthorizedly enter the computer system from another computer. In such situations, the perpetrator uses one computer, usually a personal computer, to access information contained in the second computer in an unauthorized and unauthorized manner. The first computer appears as a means of committing a certain computer crime, and the second computer is an object of attack by committing a crime. The computer as a means of organizing, planning, managing and carrying out criminal activities. For that purpose, the computer is mostly used in the field of organized crime, especially in the phase of preparation and planning of criminal activities, as well as in the procedure of control and supervision of the final realization, especially in achieving the financial effect.

3. The computer as a tool used by the police to prevent, clarify and prove crimes, because it provides complete, accurate and fast information, perceives the state, structure in the movement of crime, as well as to give certain forecasts, which gives the modern police adequate advantage over perpetrators."
4. The computer is also used in the process of extracting, analyzing and securing electronic evidence - digital forensics.

Criminal investigations are developed in separate disciplines, is different types of criminal investigations aimed at specific investigations of a particular group of crimes that have the same or similar criminal characteristics (Rejčel, 2010).

Criminal investigation is a complex process that requires expert knowledge in many areas, and this is possible only with the teamwork and expertise of expert and competent persons who, with their expertise, knowledge and skills, should contribute to successful planning, coordination and conducting investigations to clarify and substantiate computer incidents that have elements of a criminal offense provided for by the Criminal Code, and in particular when providing solid and unassailable electronic evidence, acceptable judicial authorities should lead the criminal proceedings and impose sanctions on perpetrators, but also for running a parallel procedure for determining the type and amount of illegal proceeds or any sort of causing a loss for victims of cyber-crime. To determine the type and amount of illegal proceeds, a financial investigation is conducted with the aim of determining the proceeds (type and amount), securing them in order to enable them to freeze and confiscate the proceeds and property of the perpetrators of cyber-crime.

Criminal investigation is specific to the provision of digital evidence, the existence and application of specific methods, means and ways of providing electronic evidence, but also the combination of digital evidence with other material and ideal evidence to illuminate and prove the crime. Situation and identification of the perpetrator or perpetrators, and first of all enabling quality criminal proceedings where, on the basis of relevant and substantiated evidence, appropriate action. In recent years, and even today, a major problem has been the acceptance of digital evidence by the judiciary, that is, judges who are somehow more likely to believe in material and ideal evidence. Or it would mean that the witness's faith would be worshiped faster than the digital evidence (as if there was any doubt or mistrust as to whether or not relevant evidence was provided). However, with training provided to judges and prosecutors, the situation is improving and in light of the criminal situation with elements of cyber-crime the measure of confiscation of computers and computer programs is applied in order to extract the digital evidence stored in computer memory (Nikoloska, 2013).

Criminal investigation begins from the first moment of obtaining any information that a computer crime has been committed, or that the information is directed to a perpetrator or group of perpetrators known to have committed computer incidents. Through operational checks that are planned and undertaken in a short period of time, general suspicions should be on a level of suspicion to take more serious steps or take measures and activities to establish the nature of the computer incident, then plan and provide digital evidence and finding and apprehending the perpetrators. These are measures carried out in the pre-trial procedure, also called pre-trial proceedings, but this is the stage where the emphasis is on criminal investigations, because without a well-conducted criminal procedure, there is no good criminal procedure, then the perpetrators are a "step forward or in advantage".

All omitted actions or measures in the pre-trial procedure make "loopholes or evidence gaps" that are difficult to fill in the criminal procedure phase, and hardly any court would impose a sanction without good and relevant evidence.

According to the FBI - United States, the pre-trial investigation of computer incidents takes place in several stages:

- Launching an investigation,
- Determine whether it is a computer incident and
- Analysis of evidence.

The first phase, investigating, involves: securing the scene of the incident, acquiring evidence, developing a hypothesis of the attack, and exploring alternative explanations.

The second phase, determining the nature of a computer incident, involves: incident analysis, analysis of the evidence gathered in the first phase together with alternative solutions, to determine whether it is a computer incident or something else (technical error, there is an incident but no features of any of the crimes provided for by law, etc.).

The third phase, analysis of the evidence includes: analysis of the evidence, preparation for the presentation of the computer incident with all the evidence before the competent authorities - the public prosecutor who should represent the indictment before the criminal court.

The computer incident investigation procedure generally contains the following procedures:

- Checking logs, logs, and other information about the suspect;
- Obtaining information from persons who might know certain details of the case;
- Control all stages of the investigation;
- Search planning (locating the compromised computer);
- Search of the suspect / suspect's resources (home, business premises, internet cafes, etc.
- Providing digital evidence and analysis.

The best combination in conducting an investigation or investigating computer incidents is the joint and team-to-start work of law enforcement authorities, which includes IT specialists, but who have appropriate criminal education or training needs find and extract significant evidence or assist in the selection of direct and indirect digital evidence.

Timely response, planning and teamwork are needed.

There is a general investigation or criminal investigation known to us where the authorities having police powers and in their jurisdiction are the detection of cyber-crime in collaboration with other police officers, the work of providing or obtaining operative information on the existence of elements of criminal activity of certain persons or criminals. Groups known in the area, their contacts with other persons from other areas in the country or foreign nationals. To obtain information on suspicious behaviors, especially of young and skilled PCs, as important operational information, their contacts with known criminals are most important. At this stage, general operational information is checked through operational contacts with persons from the criminal environment and measures and activities are planned to obtain more specific operational data and knowledge of criminal activity and whether that activity is related to computers and computer systems. Example: a known cheat has been in the company of young boys in the IT class for a long time. The question is what is the purpose of socializing? Are they scattered with money or expensive wardrobe bought online?

After obtaining more specific operational data, it goes to planning and implementation of other legal measures or is already in the process of criminal processing, but contacts with the competent Public prosecutor are already established at this stage and the provision of appropriate orders for the application of investigative and special investigations measures that are almost indispensable in computer incidents.

The generalized investigation procedure of computer incidents should be well planned and coordinated with the persons involved in the investigation process, the specification of their tasks according to the legal authorizations and the determination of the time and place of the implementation of the specific investigative measures (apartment overtaking) or the designation of specific investigative measures - who, over whom and for what period? In principle, investigating computer incidents, as well as other forms of criminal occurrence, should not be investigated spontaneously, but "step by step".

Each step within one of the phases of the investigation leads to the next step, thus providing control over previous activities within each of the steps envisaged. This is a 4-step investigation (Rosenblatt, 1995):

1. Initial investigation,
2. Tracking the attacker,
3. Detecting the identity of the attacker and
4. Arrest

Criminal investigations may be for a cyber-crime already committed, where the offense has caused a certain consequence: material, financial, human sacrifice, violation of personal integrity and morality, impaired national, racial or religious feelings, an act of pedophilia by displaying cyber pornography material etc. However, the investigation may be parallel to the criminal activity or it would mean that authorities are aware of the criminal event and are waiting for the right moment to be arrested and cleared, and the case (the police have been following a criminal gang that installs ATMs and extracts money, but in order to provide evidence, an ambush is waiting for the criminals to "attack the ATM." Either that would mean that there are two types of forensic investigation: a passive or completed computer incident and an active one computer incident.

Criminal investigation of an active computer incident is a complex work for many reasons. From a technical, legal and ethical point of view, it should be investigated whether measures are taken against criminals or persons who are only good hackers but not criminals.

Depending on the type and nature of the computer incident, appropriate measures are also taken at the time when the perpetrator commits the offense or when he or she is involved in a computer and there is suspicion that "something criminal" is involved with the rest of the computer network's criminal group and that to provide evidence, it is necessary to "catch when on" or "on line".

In the case of an on-line criminal attack, several situations are possible: that the offender is on the network and there is a realistic chance of a tactical "entry into the home to find the computer turned on and the offender logged in and then the investigators are at an advantage or the offender has not a time for destroying digital evidence (who is in contact, messages between them, email, etc.) ".

The results of the criminal investigation of the computer incident should be summarized and provided with answers to the main criminal questions.

The first steps are undoubtedly bound by more clues and of course more versions. The first step should be to answer the question: Is it a crime or something else, and then the other steps taken and the answer to the other eight golden criminal questions. According to Peter Stephenson, the research process is divided into seven separate steps (Đejms, 2009):

- **Step One: Eliminate Obviousity** - Based on What Is Obviously Possible - It Enables Computer Technology, Motivation and Possible Perpetrators are the primary elements that can determine whether it is a computer incident as a particular computer a crime, another crime or something else. The most important thing is to determine if a computer incident really happened because the computer system or computer program may crash and the action does not constitute a computer attack (Nikoloska, 2013).
- **Step Two: Developing a Hypothesis of Attack** - The process of developing a hypothesis requires an answer to the question of how a criminal attack occurred and how it was accessed in a computer system or network. In theory, the attack should be analyzed by mapping all attack vector capabilities (access routes to the victim's computer), analyzing access control and log files of the victim's computer, using the same type of forensic computer and the same operating system.
- **Step Three: Computer Incident Reconstruction** - This step requires the forensic test computer to simulate the attack computer as close as possible to the actual victim computer configuration (internal configuration, login, network connection). If a PC is attacked by a specific media and a physical image is obtained in the hard drive, using the appropriate program, it is then restarted on a forensic test machine and a correct mirror image (as a mirror image) is obtained. If you get the same result as the attacker got, the process of understanding how the computer is attacked does not necessarily lead to the attacker, but it certainly narrows the list of suspects (Nikoloska, 2013).
- **Step Four: Tracing Recovery to a Suspected Computer from the Attack** - The computer itself leaves traces in very accessible and hidden areas on the computer hard drive, so computer lovers know where the computer leaves traces or signs. A major advantage and chance for cybercrime investigators understands the operating system, hardware, and interface and communication functionality outside the computer, which hides certain traps, even for the most skilled hackers. Even with the viruses that the programmer writes, there may be clues to his identity, which the analyst can find.
- **Step Five: To analyze the computers that are the source, the target of**

the attack, and the ones that served as intermediaries - to "find signs along the way" that the attacker went through, all logins on every server, route, call switch. There are two dangerous situations in forensic data collection: data loss and alteration due to carelessness or "deliberate errors". Computer forensic data, which has not been handled properly, can be disputed in court. Most importantly, it is essential that the evidence is properly collected.

- **Step Six: Digital Proof Acquisition** - begins when information and / or physical objects are collected and stored for the purpose of examination. Key aspects of collecting forensic evidence are: the tools used to collect data; the techniques used to collect and store data; the tools used to analyze the data and the techniques used to analyze the data.
- **Step Seven - Preparing a Computer Incident Report** is the last phase of a computer incident investigation for any committed computer crime or it would mean summarizing the results of the investigation and preparing a criminal report or separate report to the Public Prosecutor's Office, but Organized Crime Prosecution is actively involved in cyber-crime, with charges being filed against the perpetrators. What is most important in cyber-crime is the handling of computer evidence throughout the research process from their provision, acquisition, to the preparation of forensic acts. Adequate provision, storage and handling of computer evidence are performed on the basis of special procedures and by specially trained persons in forensic techniques or forensics.

In the process of forensic investigation, it is important that "tactical forensic investigation is the study of past criminal incidents and potential criminal activities by examining the characteristics of how, when and where the activity took place to help develop a scheme, to investigate, to identify suspect and close the case.» (Rejčel, 2010). However, tactical actions and the application of appropriate measures and actions can contribute to the detection of ongoing criminal activity, ie detection of a criminal operation that takes place over a long period of time and for which the police have «knowledge» and certain facts level of «grounds for suspicion» important for undertaking certain activities for interception of electronic communication, but also undertaking other planning measures and activities in order to detect crime and provide evidence: For example, suspicions of misuse of payment cards with goods an operational combination can lead to the capture of perpetrators at the time of abuse. Interception of communications provides information about which ATMs will be «attacked», and operational information about setting a physical ambush by masked police officers and catching the perpetrators at the moment of withdrawing money from ATMs with fake payment cards. The tactics and technique of action are a key element of success, and a well-planned job is half done (Nikoloska, 2013).

4 MEASURES AND EFFECTS FOR PROVIDING ELECTRONIC EVIDENCE

The Republic of Northern Macedonia follows all the recommendations of the international conventions and other legal acts and several computer crimes are criminalized, in addition to the standard measures and actions, appropriate investigative actions are envisaged such as: Computer system search and computer data, Temporary seizure of computer data Expertise of electronic data and electronic devices and special investigative measures and actions, such as: monitoring and recording of telephone and other electronic communications in a procedure determined by a special law; monitoring and recording in a home, enclosed or enclosed space belonging to that home or business premises marked as private or in a vehicle and entering those premises in order to create conditions for interception of communications; secret surveillance and recording of persons and objects with technical means outside the home or business premises marked as private; secret inspection and search of a computer system; automatic, or otherwise, search and comparison of personal data and insight into realized telephone and other electronic communications (Criminal Procedure Law, 2010).

The police and other entities first take preventive measures to combat the emerging forms of cybercrime. Repressive measures are taken in order to locate, recognize and collect evidence of crimes and perpetrators, and then work on prosecuting the courts.

In addition to using the traditional criminal-operational tactical ways, actions, methods and means, the Law on Criminal Procedure provides for investigative actions that are applied to detect and shed light on computer crimes, but also provides electronic evidence as a special type of evidence in addition to material and ideal evidence, but special investigative measures are legally provided (Sessions, 1991).

4.1 Measures for finding and securing persons and objects and evidence

Search of computer system and computer data is a measure from Article 184 (Criminal Procedure Law, 2010) which is undertaken by order of a court, and upon the proposal of the public prosecutor. The executor of the order, the criminal police requests from which he uses the computer or has access to it or to another device or data carrier to provide access to them and to give the necessary notifications for the smooth realization of the purpose of the search. The person who uses the computer or has access to it or to another device or data carrier is also instructed to immediately take measures to prevent the destruction or alteration of the data, otherwise the person will be punished for non-compliance with the court order and is fined from 200 to 1,200 euros in denar counter value.

Temporary confiscation of computer data is a measure provided in Article

198 (Criminal Procedure Law, 2010) which is applied on the basis of an order for temporary confiscation of cases issued by the court upon the proposal of the judicial police or the public prosecutor for the purposes of the cases. shall be confiscated or which may serve as evidence in criminal proceedings shall be temporarily confiscated and handed over to the public prosecutor or a body designated by a special law or otherwise their custody shall be ensured. Seizure actions refer to data stored in a computer and similar devices for automatic or electronic data processing, devices used for data collection and transmission, data carriers and subscriber information available to the service provider. Upon a written request of the public prosecutor, this information must be submitted to the public prosecutor within the deadline set by him. The judge of the preliminary procedure, upon the proposal of the public prosecutor, may with a decision determine the protection and storage of the computer data found by conducting a search while it is necessary, and for a maximum of six months. After the expiration of this period, the data will be returned, unless they are involved in committing the crime of Damage and unauthorized entry into a computer system under Article 251, Computer fraud under Article 251-b and Computer forgery under Article 379-a all of the Criminal Code, if they are not involved in committing another crime with the help of a computer and if they do not serve as evidence of a crime. (Criminal Code, 2004)

As actions that provide evidence are:

- Expertise that is determined when to find or evaluate an important fact, a finding and opinion should be obtained from a person who has the necessary professional knowledge. The expertise is usually performed by experts registered in the register of experts in accordance with Articles 236 - 243. (Criminal Procedure Law, 2010) Experts should have a license for experts.
- The Macedonian legislator envisages the electronic evidence as relevant evidence in the criminal procedure which is legally provided by the application of the search actions and temporary seizure of objects.

4.2 Special investigative measures

In the process of criminal investigation, special investigative measures are applied when it is probable that data and evidence necessary for successful conduct of the criminal procedure will be provided, which otherwise cannot be collected. Out of a total of 12 special investigative measures for criminal investigation of computer crime, the following are applied: monitoring and recording of telephone and other electronic communications in a procedure determined by a special law; 2) monitoring and recording in a home, enclosed or enclosed space belonging to that home or business premises marked as private or in a vehicle and entry into those premises in order to create conditions for interception of communications; 3) secret surveillance and recording of persons and objects with technical means outside the home or business premises marked as private; 4) secret inspection and search in a computer system; 5) automatic, or otherwise, search and comparison of personal data; 6) inspection of realized telephone and other electronic communications, 7) simulated purchase of items; 8) simulated giving and receiving bribes; 9) controlled delivery and transport of persons and objects; 10) use of persons with concealed identities for monitoring and collecting information or data; 11) opening a simulated bank account and 12) simulated registration of legal entities or use of existing legal entities for data collection.

Special investigative measures are applied in accordance with the legal provisions provided in Articles 252-271 (Criminal Procedure Law, 2010). They are applied with a special order which may include the following persons: a person who has committed a crime, 2) a person who undertakes an action to commit a crime or 3) a person who prepares to commit a crime when the preparation is punishable under the provisions of the Criminal Code. The order may also apply to a person who receives or forwards shipments from the suspect or the suspect uses his means of communication.

The criminal police operatives coordinate with the public prosecutor in detecting and investigating cybercrime, and based on the needs, an investigation team is formed, led by the public prosecutor or an investigator authorized by him, but the team also includes a digital forensics expert. in order to professionally deal with electronic evidence.

5 ELECTRONIC (DIGITAL) EVIDENCE

With the advent of digital video, the notion of digital proof has also been introduced. IOCE (International Organization on Computer Evidence) was established in 1997. TWGDE (Technical Working Group for Digital Evidence) held its first meeting on June 17, 1998 to develop organizational procedures and relevant documents. The Federal Criminal Laboratory in the United States was established in February 1999. SWGDE (TWGDE) changes its name to SWGDE (Digital Working Group for Digital Evidence), which meets at least once a year. SWGDE members are sworn in (judicial authorities) and non-sworn experts, which are scientific workers. The FBI sponsors the SWGIT (Scientific Working Group in Imaging Technologies), for the electronic processing of data and images for the needs of the justice system after pre-defining and specifying the terms for cavitation, storage, processing, analysis, transmission and output format – photography (Whitcomb, 2002).

When it comes to digital evidence, technology has enabled the creation of copies that are true to the original in every sense. In this case, the presentation of copies is generally acceptable, even though originals are available. In practice, it is even preferable to present copies to remove any doubts about the possibility of altering the original. Even the printed form of a digital document is considered valid, unless it can display all the information necessary for the process.

There are three categories of digital evidence in computer incidents (Nikoloska, 2013):

- Transient data or information that is lost after shutting down your computer, such as open working memory connections, resident memory programs, etc. This data can also be lost when the computer is shut down. It is also important that the acquisition procedure is precisely implemented by the end. Prior to shutting down the computer, sensitive and encrypted data should be immediately examined, located and extracted, since it may be impossible to access them after shutdown.
- Sensitive or hard disk data (CDs) that can be easily modified, such as recent log file access times, and so on.
- Temporary access data or data stored on a hard disk CD that can only be accessed at a specific time (encrypted data).

Digital evidence management is a complex task that requires the need to develop specific procedures for dealing with and managing digital evidence that also imply a certain responsibility for the authorities involved in the extraction and management of digital evidence, if the procedures are not followed.

Digital evidence analysis is the most subtle part of the pre-trial or criminal investigation process, because without a good analysis of each evidence individually and analysis of its relevance to other evidence and evidence, there is no case-file with full clarification of all facts and circumstances that contributed to the commission of the crime, the manner of the criminal act, the organization, the time period of the criminal act, and of course the determination of the type and amount of the crime committed. Damage or extent of damage caused or damage to the honor, reputation, morals and so on, the victim as non-pecuniary damage. The analysis of digital evidence follows their acquisition and formulation in which it can be compared to other evidence, which may be material (objects, images, text) or ideal evidence (testimonies, statement of a suspect, etc.).

The overall analysis is in fact an explanation of the causal links in the criminal situation itself and the answer to the golden criminal questions.

6 CASE ANALYSIS

The Sector for Cyber Crime and Digital Forensics in the Public Security Bureau at the Ministry of Interior filed criminal charges against the person AT with the Basic Public Prosecutor's Office in Skopje (44) from Skopje, for having committed the criminal offense "damaging and unauthorized entry into a computer system".

During 2015 year, the Ministry of Interior announced, A.T. unauthorized access to the computer system with an administrator user - computer server unit

"WIN-KLS5VM0LT8C" owned by the company "Nextsense DOO" from Skopje, which hosted the website www.exploringmacedonia.com and then obtaining the administrative privilege from the website, is unauthorized uploading of new files, which made the computer data unusable and useless.

From the submitted logs for all unauthorized logins to the host-server, it is clarified in the announcement, their analysis was performed where IP addresses were determined from which it was accessed with time and date, and with further investigation the user - the person AT was determined , as well as the perpetrator of the above mentioned crime.

In connection with this, a search was conducted in the home and premises of the reported person where the computers through which A.T. performed unauthorized access to the computer server owned by Nextsense DOO, Skopje. Due to the provision of data and digital evidence, an analysis and expertise was performed on the confiscated computer equipment found during the search.

Using special standardized information - forensic procedures and using special licensed forensic software, a large number of deleted fragments of accessible IP addresses, URLs from Google Chrome and Mozilla Firefox browsers, and digital photos were reconstructed.

From the found elements of Internet access, is accessed IP addresses and virtual memory media, it is stated in the announcement from the Ministry of Interior, it can be concluded that compared to the analyzed logs and attached files at the critical date and time from the damaged host server, they are the same according to IP addresses , URL paths and files obtained from the expertise of the temporarily confiscated computer equipment from AT, where it was concluded that the reported person had unauthorized access to the server. By using an administrator account to log in to the server computer unit, as a final part for accessing the contents attached to the specified computer system, you enabled and performed unauthorized entry, modification and damage of computer data - digital contents on a website hosted on the server, and thus made difficulty and normal functioning of the computer system - the host server and its contents (MIA, 2015).

7 CONCLUSION

"Technology is rapidly evolving in a world driven by social networks, online transactions, cloud computing, and automated processes. But with the technological evolution comes the progress of cybercrime, which continually develops new attack types, tools and techniques that allow attackers to penetrate more complex or well-controlled environments, and produce increased damage and even remain untraceable. In a world driven more and more by big data, social networks, online transactions, information stored or managed via internet and automated processes performed through the use of IT systems, information security and data privacy are permanently facing risks. With the development of new tools and techniques, cyber-crime is consistently increasing in terms of number of attacks and level of damage caused to its victims" (Bendovschi, 2015: 24).

"As a result, and to provide organizations with the best level of protection, IT security professionals must be attuned to the ever-changing landscape and the latest threats and attack methods." (Check point research, 2019: 21). "While threat actors were trying hard to keep a lower profile with their menacing activities, they could not escape our watchful eye. Indeed, never does a day go by that we do not see organizations under constant attack from the ever growing number of malware spreading at higher rates than ever." (Check point research, 2019: 3).

"Security is everyone's job today, from consumers, to system administrators, to executives. If you are doing business, you need to elevate the priority of security across your organization and data center. Over the years, cybercriminals have gotten more advanced and better funded. They are entire teams of highly trained hackers, and they have built it into a very profitable business. Cybercrime is big business. In many cases, states have built their own cyber-attack teams. These teams are no less important to their state strategies than their army or navy. And just like these cyber-attack teams are prepared to attack anyone, you too must be prepared to defend against anyone. Whether you know it or not, you are in a cyber-war." (Oracle, 2017: 2).

We are at war with cybercriminals. You need to make cyber security and defenses your top strategic concern.

8 REFERENCES

Angeleski, M. (1995). Osnovni kriminalistički teoretski problem na borbata protiv organiziraniot kriminalitet. *Naučen proekt: Konstituiranje na Republika Makedonija kako moderna pravna država – na tema: Pravnata država i organiziraniot kriminal.* Skopje: Praven fakultet.

Bendovschi, A. (2015). Cyber-attacks – Trends, patterns and security countermeasures. *Procedia Economics and Finance*, *28*, 24–31. https://doi.org/10.1016/S2212-5671(15)01077-1

Bequai, A. (1978). *Computer crime*. New York: Lexington Book.

Bošković, M. (2000). *Kriminalistička metodika II* (drugo izmenjeno i dopunjeno izdanje). Beograd: Policijska akademija.

Brvar, B. (1982). Pojavne oblike zlorabe računalnika. *Revija za kriminalistiko in kriminologijo*, *33*(2), 92–104.

Check point research. (2019). *Cyber attack trends analysis, 10*. https://www.checkpointdirect.co.uk/media/downloads/check-point-2019-security-report-volume-1.pdf

Criminal Code. (2004). *Official Gazette of the Republic of Macedonia*, (19/04, 114/09).

Criminal Procedure Law. (2010). *Official Gazette of the Republic of Macedonia*, (150/10).

Đejms, H. S. (2009). *Forenzika*: *Voved vo naučni istražni tehniki*. Skopje: Tabernakul.

Đukleski, G. (2000). Najčesti oblici na izvršuvanje na kompjuterski criminal vo SAD. *Godišnik na fakultetot za bezbednost*, *18*(1), 66–70.

Ignjatović, Đ. (1991). Pojmovno određivanje kompjuterskog kriminaliteta. *Anali Pravnog fakulteta u Beogradu*, *39*(1/3), 136–144.

Jovasevic, D. (2002). *Leksikon krivičnog prava*. Beograd: Službeni list SRJ.

MIA. (2015). *Кривична пријава за скопјанец за неовластено навлегување во компјутерски систем*. https://kanal5.com.mk/krivichna-prijava-za-skopjanec-za-neovlasteno-navleguvanje-vo-kompjuterski-sistem/a230266

Nikač, Ž., & Leštanin, B. (2019). Borba protiv cyber kriminala: krivičnopravni i kriminalistički aspect. *Kriminalističke teme Zbornik radova*, *XX*(5), 3–15.

Nikoloska, S. (2010). Kompjuterski krivični dela protiv slobodite i pravata na *čovekot* i građanite. *Horizonti*, *6*(6), 241–250.

Nikoloska, S. (2013). *Metodika na istrazuvanje na kompjuterski kriminalitet*. Skopje: Fakulteta za varnost, Van Gog.

Obradović, S., Mijalković, M., Perić, D., & Puača, D. (2007). Istraživanje kriminala na računarima. *Infoteh-Jahorina*, *6*(E-III-14), 455–459.

Oracle. (2017). *Anatomy of a cyber attack: The lifecycle of a security breach*. http://www.oracle.com/us/technologies/linux/anatomy-of-cyber-attacks-wp-4124673.pdf

Parker, D. (1973). *Computer abuse*. Menlo Park, Springfild: Stanford Research Institute; National Technical Information Service.

Rejčel, B. (2010). *Kriminalističko istražuvanje.* Skopje: Nampres.

Rosenblatt, K. S. (1995). *High technology crime — Investigating cases involving computers.* San Jose: KSK Publications.

Sessions, S. W. (1991). Kompjuterski kriminal-trend koji eskalira. *Priručnik za stručno obrazovanje radnika unutarnjih poslova*, *39*(1991), 220–223.

Whitcomb, C. M. (2002). A historical perspective of digital evidence: A forensic scientist's view. *International Journal of Digital Evidence*, *1*(1), 1–9.