Law Enforcement and Investigation of Cybercrime in Albania

Desara Dushi (Doctoral Candidate)
Erasmus Mundus Joint International Doctoral Degree in Law, Science and Technology
Supervised by University of Luxembourg,
coordinated by CIRSFID, University of Bologna
Dr. Nertil Bërdufi (Lecturer)
Hena e Plote (Beder) University, Albania

Abstract

Since 2000 until 2016, the Internet has expanded at an average rate of 918,3% globally; currently, around 4 billion people are online. Cyberspace today is one of the greatest legal challenges which have stimulated another form of crime, creating an environment for new methods of crime. Now, almost all crimes can be committed with the use of computers. This paper analyzes the procedures of cybercrime investigation according to the Albanian legislation such as handling of electronic evidence and the methods and tools of investigation. The paper deals also with the issues of cooperation with Internet Service Providers (ISP) and regional and international cooperation in the fight against cybercrime. Finally, the paper analyzes the work and progress of the new Cybercrime Investigation Units. This includes some interviews with cybercrime investigation agents providing information on the process of investigation of these crimes in Albania and the challenges faced by them.

Keywords: *cybercrime, evidence, investigation, Albania*

Introduction

Cybercrime has become one of the greatest legal challenges. Since 2000 until June 2016, the Internet has expanded at an average rate of 918,3% globally; currently, around 4 billion people are online (World Internet Usage and Population Statistics, 2016). Now, almost all crimes can be committed with the usage of computers. Viewing the current importance of this phenomenon on a global scale and at the national level, given the rapid growth of cybercrime in Albania in the recent years and the lack of reliable

studies in this field in our country, we decided to conduct a research on cybercrime investigation.

This study has to do with the analysis of the current situation in Albania related to the legal standards, mechanisms for investigation and prosecution of cybercrime, and the identification of problems and challenges encountered by investigators, prosecutors, police, and the Albanian government in the prevention and combating of cybercrime in Albania. Consequently, procedural measures and investigative tools used in cases of cybercrime investigation, handling of computer evidence, and tasks of computer crime investigators were described and analyzed. Included in the description are also the functions of the Department of Investigation of Cybercrime as a newly created body for the investigation of cybercrimes in Albania.

Criminal Procedure Code (hereafter CPC) in Article 149 provides the definition of criminal evidence as follows: *"Evidence is a notice (information) on the facts and circumstances relevant to the criminal offence, which are obtained from sources provided for by the criminal procedural law, in accordance with the rules prescribed by it and which serve to prove or not the commission of the criminal offence, its consequences, the guilt or innocence of the defendant and the extent of his responsibility"*. Based on this article, criminal evidence is considered as any notice giving a fact or circumstance relating to a specific offense that is taken from sources that is known and provided by the procedural law. This is done in accordance with rules set by it and serving to prove the commission of the offense or not, the consequences that derive from it, the guilt or innocence of the defendant, and his degree of responsibility as well as any interest for resolving the matter rightly (Elezi, 2013). Another element which should be considered when investigating a crime, especially cybercrime, is the jurisdiction. Jurisdiction is the right of the state authorities to resolve the issues involved in their functions by applying the law in any case (Schjolberg, 2013). Criminal jurisdiction is determined on the basis of the country where the criminal offense was committed or attempted to be committed, or where there is a consequences of the offense (Shegani, 2002). If the country is not known, then the jurisdictional powers are determined by the residence of the offender.

However, the determination of jurisdiction becomes more complicated in the case of cybercrimes where the perpetrator could be in a very great distance from the place where the crime was committed or where the consequences of crime came. In some cases, these distances exceed national boundaries. In these cases, the perpetrator is in a state, while the consequences of crime go to another country. Therefore, this leads to many difficulties on the part of the investigating bodies to investigate the related

crime caused by the lack or limitation of jurisdiction. In order to eliminate the possibility of being in a situation like the lack of jurisdiction, the Albanian government has adopted a series of bilateral or multilateral agreements which make adjustment to such cases. As regards the regulation of relations with foreign authorities in criminal matters, Article 10 of the CPC stated that they are regulated by international conventions recognized by the Albanian state, the principles, and the generally accepted norms of international law and the provisions of this code.

At the end of this paper, conclusions were drawn from the research study and some recommendations for Albania were provided. Thus, the result of the findings issued during the preparation of this study was achieved. Aspiration to join the great community of the European Union has made it possible for the country to have legislation in accordance with international standards, adapted in accordance with the EU legislation against cybercrime. However, only the existence of a suitable legal framework is not enough to fight cyber criminality. Effective implementation of this legal framework is essential. To achieve this goal, it is necessary to create or improve mechanisms against cybercrime, activation of all stakeholders affected by cybercrime, combating this phenomenon, increasing the awareness of the population and the country's government on the risks that endanger the country, and increasing regional and global cooperation in combating cybercrime.

1. Albanian Criminal Procedural Legislation Related to Computer Evidence

Procedural aspects of issues related to cybercrime are included in the actions and measures that apply specifically to this type of crime, as well as actions and measures to be applied in conventional crime. Here, we can mention the following provisions: With Law No. 10 054, date 29.12.2008 "*On some amendments to the Criminal Procedural Code*", Article 191 of the Criminal Procedure Code has been added to Article 191 which states that:

"Obligation to submit computer-based records: 1. In criminal proceedings regarding criminal offences in the information technology field, the Court, upon request of the prosecutor or the plaintiff, shall order the holder or the controller to submit the electronic data stored in the computer or in any other storage device. 2. During these proceedings, the Court shall order the service provider to submit any information about the subscribers, in connection with the services rendered by the provider. 3. When there is reasonable ground to believe that the delay may cause serious damage to the investigation, the prosecutor shall decide, by a reasoned decision, that it is obligatory to submit the computer-based records, set out in point 1 and 2 of

this article, and shall immediately inform the Court. The Court shall review the prosecutor's decision within 48 hours from the notification date."

As noted, the purpose of this article is to study the legal regulation of the relations between law enforcement organs and Internet service providers. It aims to define by law the obligation of cooperation between the parties in the cases specified in the law for investigative purposes of criminal acts in the field of technology information. However, this provision clearly states the cases when it can be ordered to present the computer data, which should be done only by court order.

Under the provision, the requirement for the submission of data to the court can be done not only by the prosecutor, but also by the injured accuser. Despite the adjustment of liability for disclosure of data, the missing of time limits within which must be given the decision of the court was noted. This is upon the application by the interested parties, as well as deadlines within which data should be filed by controllers and internet service providers. In this provision, the legislator uses the term 'controller' from the field of information technology. This term means "any natural or legal person, public authority, agency or other entity who, alone or jointly with others, store, process, manage, archive and therefore control personal data".[19]

Definitions of computer data, computer systems, and service providers are given explicitly in the Convention on Cybercrime of 2001. Thus, this was ratified by Albania with the law no. 8888, 25.04.2002 "*For the Ratification of the Convention on Cybercrime*".

Further in this Convention, the definition of "subscriber information" was defined as:

"...any information contained in the form of computer data or any other form that is held by a service provider, relating to subscribers of its services other than traffic or content data and by which can be established: a) the type of communication service used, the technical provisions taken thereto and the period of service; b) the subscriber's identity, postal or geographic address, telephone and other access number, billing and payment information, available on the basis of the service agreement or arrangement;

c) any other information on the site of the installation of communication equipment, available on the basis of the service agreement or arrangement" (Convention on Cybercrime, 2011). Here, subscriber means *"Any natural person, legal person, entity or association, part of a contract with a supplier of electronic communications services accessible to*

[19] See: Commissioner for the access to information and protection of personal data, information can be accessed at this web page: http://www.idp.al/index.php/sq/informacione/250-idp-sq/publikime/publikime-te-ndryshme/fjalor-terminologjik

the public for the provision of such services, or any beneficiary of these services through prepaid cards".[20]

Consequently, the Code of Criminal Procedure of the Republic of Albania specifically regulates the procedure of seizure of computer data in case of cyber offenses in Article 208 / a stipulating:

"*1. In criminal proceedings involving crimes in the information technology field, the court shall decide, upon request of the prosecutor, to seize the computer-based records and the computer systems. The court shall set forth in this decision the right to access, request and take data from the computer, and prohibits any further actions or obtaining of the data or of the computer system. 2. When there is reasonable ground to believe that the required computer-based records are stored in another computer, or part of it, and they may be, in a lawful way, accessed from or made available from the first computer, which is being controlled, the court shall order, upon request of the prosecutor, an immediate search or access to the latter computer. 3. Following the court decision, the prosecutor or the judicial police officer delegated by the prosecutor, shall take measures to: a) prevent further actions, or taking the computer, only a part of it, or another data storage device; b) extract and receive copies of the computer-based records; c) prohibit access to the computer-based records, or to remove these records from accessible computers; ç) provide inviolability of the respective stored records. 4. The prosecutor may authorize calling a computer expert, or an expert in protection of computer-based records, to carry out these actions. The expert may not refuse this task for unreasonable cause."*

As may be noted, this provision sets out in detail the procedure of sequestration of the computer data in case of the investigation of cybercrimes. In this provision, the legislator has determined the manner of sequestration of these data, the content of a court order for sequestration, as well as measures to be taken by the prosecutor or the judicial police officer in pursuance of this decision. Furthermore, the provision also provides possibility, but not the obligation to call an information technology expert who will assists in taking the measures prescribed in the provision. It is also noted that the expert has no right to refuse the task set without any reasonable reason. However, this is a kind of obligation given to the expert to obey the order of the prosecutor (Criminal Procedural Code, article 208/a).

Besides sequestration, Code of Criminal Procedure also provides expedited preservation and maintenance of computer data in Article 299/a. Through this provision, the legislator regulates the storage of computer data

[20] See: Commissioner for the access to information and protection of personal data, information can be accessed at this web page: http://www.idp.al/index.php/sq/informacione/250-idp-sq/publikime/publikime-te-ndryshme/fjalor-terminologjik,

when there are sufficient grounds to believe that it could be expected by the decision of the court for the seizure of data for risk loss, damage, or the alteration of the data. In these cases, the prosecutor orders the accelerated storage of risked data immediately (Criminal Procedural Code, Article 299/a). However, the same provision is regulated which is also the case when the data are in the possession of a person. In this case, the prosecutor is permitted to order the person to store data in a term up to 90 days. This is with the obligation of not disclosing the procedures and actions undertaken by the conclusion of the investigation. Through this way, the legislator prescribes by law the confidentiality of investigations by third persons involved in the event. However, this is done in order to ensure an impartial investigation and prevention of interference in the investigation or alteration of evidence by other people.

Even in this provision, the legislator has used technical terms from the field of information technology, such as the term "traffic data". The definition of this term is given in the Convention on Cybercrime, article 1(d) as: "*any computer data relating to a communication by means of a computer system, generated by a computer system that formed a part in the chain of communication, indicating the communication's origin, destination, route, time, date, size, duration, or type of underlying service.*" Article 299/b of the Criminal Procedure Code continues the definition of the accelerated conservation and partial disclosure of computer data. This provision states, in more detail, the obligations of the person charged by the prosecutor with the accelerated storage data traffic. This person should undertake to cooperate in the highest degree with the prosecution to identify the service providers and other necessary evidence. Under this provision, it includes:

1.1 Duties of the Proceeding Body

Detection and investigation of forms of cybercrime by the proceeding body were very complicated. Cyber changes and deletion of data are carried out without a trace. Even when there is an identification of certain persons working in these systems, the circle of offenders and type of computers itself does not facilitate the detection and investigation of this type of offense. Computer crime, as a new form of criminal activity, has great damages and consequences in the world. Thus, in every country, it requires all the organization of criminal politics nationally and internationally and the application of methods of modern criminal investigation for its discovering and deterrence. In any case, the computer criminal proceeding authority has a duty to apply these methods and tools based on the knowledge of experts who recognize the electronic and computer operation (Begeja, 2007). When it comes to computer evidence, these rules should be kept in mind (UNODC, 2013). The process of collecting, transporting insurance and computer

evidence should not change the test. In addition, computer evidence can be examined only by specially qualified persons. Therefore, any action taken during the blockade, transportation, or the storage of computer evidence must be documented.

The investigators who were present at the cyber scene should be careful when blocking computer equipment as evidence. This is because the inappropriate access of the data stored on the device might result to violations. Therefore, legal authority is needed before any further action. For this reason, police personnel found at the scene should immediately contact the prosecutor's office to inquire if they have proper jurisdiction (UNODC, 2013). Besides the legal issues in the case of the intervention of the data stored on the computer, police personnel should also be aware that the data on the computer or computer tests are generally very subtle. Therefore, only specially qualified personnel should be allowed to examine and analyze computer evidence.

1.2 Electronic Evidence

Electronic or computer evidence are materials that exist in electronic or digital forms (UNODC, 2013). Electronic evidence are essential not only for investigation and prosecution of cybercrime, but also for crime in general. Optimized legal framework for electronic evidence, together with law implementation and criminal justice capacity used to identify, collect and analyze electronic evidence, are essential for an effective crime response.

Electronic evidence like DNA and fingerprints are hidden. They overcome legal borders faster and easier, and they can be changed, damaged, or broken easily. Electronic evidence are also effected by time. Electronic evidence of crime scene should be collected, saved, and transported carefully. Furthermore, the police officer who is at the crime scene must have regard for the following: identify, block, recognize and provide all computer evidence at the scene; document all the scene, as well as special places where evidence was found; label and protect computer evidence; transport computer evidence in the safest way possible etc. (Zverlevski et al., 2014).

The collection of evidence at crime scene can be done only by the person who has the legal authority for the seizure of evidence, which in advance, makes insurance and documentation of the site. The staff at crime scene, who is not qualified, is not allowed to explore the content or get the information from the computer or any other computer device, but only to record what they see on the screen without touching anything. For a correct and successful investigation, it is essential that judicial police officers should be informed about the investigative values of computer evidence. This should

be done in order to evaluate the types of evidence at the scene and identify the equipment and materials found at the scene.

1.2.1 Electronic Devices as Possible Evidence

A *computer system* is composed of hardware and a software that processes data that are then stored in the hardware. Hardware is the mechanical and electronic parts of the computer system, whereas the software are data and computer programs.[21] Computer system and its components can be important evidence in the investigation or criminal proceedings. Hardware, software, documents, email and the attached files, Internet search history, discussions in chat rooms, photos, database, and financial records, all of them may be possible and valuable evidence for investigation of crime scene. The device itself, with the stored information in it, can serve as computer evidence.

Hand devices are mobile data storage devices that ensure communication, photography, video recording, navigation, entertainment, and personal information management. Hand devices such as, cellphones, smartphones, PDAs, multimedia computer equipment, pagers, and GPSs can contain applications, data or information, like SMS-s, messages, e-mail, internet navigation history, contact lists, photos, and financial records. However, all of these devices may contain valuable evidences used for investigation or lawsuit.

When electricity is cut, data or computer evidence can be lost. Computer data or evidence on some devices such as smartphones or cellphones can be overwritten or corrupted if the device remains activated. For these reasons, judicial police officers or investigators who go first on the scene should be careful not to lose the data stored on the blocked device that serves as material evidence.

Peripheral devices are those devices, which are connected to a computer or computer system to increase users accessing capacity and computer functions. The devices themselves, as well as the functions they perform, are all possible evidence. The information stored in the device can serves as an evidence, too, such as fax numbers and outgoing or incoming calls, recent documents scanned, copied or printed, and information about the reasons for using the device (UNODC, 2013). These devices can also be a source of other evidence such as fingerprints, DNA etc.

---

[21] See: Components of a computer system, available at: https://chortle.ccsu.edu/java5/Notes/chap01/ch01_3.html, and https://en.wikibooks.org/wiki/A-level_Computing/CIE/Computer_systems,_communications_and_software/Components_of_a_computer_system_and_modes_of_use/Types_of_hardware,

A *computer network* consists of two or more computers connected between them via a data cable or wireless connection. A network often includes printers and other peripheral devices such as hubs, switches, and routers. Computer systems and devices connected with them can constitute valid evidence for an investigation or proceeding. Also, the information contained may apply as potential evidence. Functions, capacity, and any other identifying information related to the computer system, components and connections, including internet protocol (IP) addresses of the local network (LAN), MAC addresses, addresses work interface card (NIC) etc, were also important.

1.3 Investigative Devices and Tools

In most cases, objects or devices containing computer evidence can be treated using standard tools. Agents investigating the crime scene must be careful with the evidence collection and packaging to avoid transformation, damage, or destruction. Computer evidence, computers and electronic devices where it is stored, are fragile and sensitive to extreme temperatures, humidity, shock, static electricity, and magnetic fields. For this reason, the investigator at the scene should take measures on documents, photographs, packs, transports, and stored electronic evidence to avoid alienation, damage, and the destruction of evidence (UNODC, 2013).

Research and interviews conducted with employees of the Albanian State Police who deal with cybercrime investigation shows that they are equipped with all necessary equipment and investigative tools to investigate these crimes. The Albanian State Police, in cooperation with the Programme of Assistance and Training International Criminal Investigation (ICITAP), United States Department of Justice (USDOJ), and the Office of Crime and Drugs of the United Nations (UNODC) has drafted in 2009 a manual guide for cybercrime investigation and computer evidence in service of the State Police. However, this guide describes in detail the types of computer evidence and how to deal with them step by step, including actions to be taken since the first moment on the scene, identification of the computer evidence, their documentation, collection, package, transportation and storage makes it a very valuable guide for the investigation of cybercrime. The content of this guide is not made public because of the sensitivity of instructions included.

2. Cybercrime Investigation Unit

In June 2014, the cybercrime sector and special structures near 8 district prosecution offices were established. For the first time in the Albanian prosecutor's office, a special unit for cybercrime offences started functioning.

Initially, this kind of investigation will be conducted in the Prosecutor's Office of Tirana, Durres, Elbasan, Vlore, Fier, Korce, and Shkoder.

Offenses subject of this sector[22] include: computer dissemination of materials in favor of genocide or crimes against humanity, threat due to racist and xenophobic motives through the computer system, dissemination of racist or xenophobic materials through the computer system, insulting due to racist or xenophobic motives through the computer system, computer fraud, computer falsification, unauthorized computer access, unlawful wiring of computer data, interference in computer data, interference in computer systems, and misuse of equipment.

Within the scope of the activity of this sector, serious immoral acts, pornography, fraud on works of art and culture, publication of another person's work with own name, unlawful reproduction of someone's work, violation of the rights to industrial properties, and violation of the rights to topography of semiconductor circuit were also included when committed through computer systems. This, however, is obvious based on the importance given to intellectual property protection from online crimes.

In General Prosecutor's Office, in 2014, the Directorate of Control of Investigation of Economic Crimes and Corruption (Task Force) was set up to control the investigation of corruption, economic crime, and investigation material in composition of the work of the Sector of Cyber Crime Investigation (Prosecution Office's Medium-Term Strategy for 2015-2017 and the Action Plan).

Another main objective is to strengthen the fight against cybercrime. Technological changes day by day, and crimes committed via computer are growing significantly. Thus, large amounts of income from crimes are generated and circulated on the Internet. Consequently, strengthening the fight against cybercrime is closely related with financial investigations which should be addressed in the searching, seizing and confiscation of crime incomes, and the investigation of money laundering on the Internet. In this regard, it is aimed at:

•Strengthening professional capacity and logistical structures investigation of cybercrime. Appropriate training of prosecutors and judicial police officers, familiarity with international legislation, and exchange of best international experience of computer crimes investigation;

•Strengthening public-private cooperation in the area of information technology;

[22] See: General Prosecution Office, for the first time in the prosecutors' offices in Albania, Cybercrime Investigation Unit starts to function, available at:http://www.pp.gov.al/web/Fillon_funksionimi_i_struktures_së_antikrimit_kibernetik_654_1.php#.VfSR29Kqqko

•Appointment of cyber experts in support of prosecutors and judicial police officers.

During 2014, 180 offenses were recorded in the area of cybercrime from which 76 were discovered with 86 authors; out of them, 10 were arrested, 2 were declared wanted, and 74 were free (Prosecutor General, 2014). This was compared with the same period, one year before 72 more offenses were recorded, with 17 more authors, and 1 more arrested author. State Police, in order to serve citizens better and to prevent and combat corruption and cybercrime, has put in function a software application for online reporting of cybercrime, which is located on the official website of the Albanian State Police.[23]

In this context, the Ministry of Justice recommended the General Prosecutor: "*severity of criminal policy towards security measures and punishment of criminal cases of organized crime [...] cybercrime; enhancing cooperation for strengthening and consolidation of joint investigation units, as well as specialized structures for prosecuting offenses of corruption, [...] and cybercrime [...]*". Obviously, cybercrime is increasingly given a greater importance thus making possible the further development of methods of investigation and prosecution of this crime.

As noted throughout this chapter, the procedures of investigation and prosecution of cybercrime in Albania are clear and accurate. In recent years, more and more importance is being paid to the investigation of such offenses, strengthening more and more measures in this field, including international cooperation. Within this cooperation, a manual for internal use for cybercrime investigators has been created with the support of UNODC. It is a quite detailed manual, including procedures, methods of action of investigators at the crime scene, types of evidence, the handling of electronic evidence, etc. Thus, this significantly facilitates the work of the investigators of cybercrime in Albania. Also, newly created cybercrime sectors in seven country prosecutors are another sign of increasing the awareness of the Albanian state for the phenomenon of cybercrime. Although these taken steps are in the initial stage and need a lot of work to achieve the standard required for a more efficient protection from the risk of cybercrime, it seems that Albania is in the right direction to combat this dynamic and dangerous phenomenon.

3. Research Analysis

This part provides an analysis of the Albanian reality related to the cybercrime in the country, as viewed by the eye of the best experts of this field that have been interviewed for the purposes of this research. The reason

[23] Material for the second meeting of GPP EU-Albania, priority nr.4. Domestic Relations

for choosing to conduct interviews is because it was thought to be the best way for discovering the challenges and real problems which the investigation bodies faces in practice.

The first question made to the interviewees is: in what aspects is the Albanian legislation more complete in the material, procedural or international unification aspects? The interviewees unanimously answered that regarding the international cooperation, the Albanian legislation is complete and efficient. This is based on the fact that the country has ratified all the international acts related to cybercrime and also other acts that have helped in the facilitation of the international investigation processes. Therefore, what the expert of the Security Policies highlights is that: "*We should act more rapidly in the implementation of those international acts that we ratify, in order to be coherent with the evolution of technology and cybercrime typology."* (Interview with Xh.Sh., 2015)

Furthermore, the Head of Cybercrime Unit at the Prosecution Office of Tirana declares that there is a problem in the field of international cooperation related to the letter rogatories seen as a procedure for obtaining international information for investigation purposes. Thus, he states that: *"Time, as regards cybercrimes, is very important and the letter rogatory is not the adequate solution for obtaining information about this kind of crime."* (Interview with A.G., 2015) Through this declaration, he stresses the need for the creation of accelerated procedures for the investigation of such a flexible crime which is also very fast in producing consequences. The same problem has been stressed also by the Head of Cybercrime Investigation Unit of the State Police, who states that: "*Letter rogatory is a serious problem, because in cases of cybercrime investigation, time is a very important element.*" (Interview with E.P., 2015) In such cases, procedures like the letter rogatory, that require a lot of time, constitute a big obstacle in the investigation of cybercrime. This is seen when it is well-known that in the cybernetic space, time passes very rapidly and it is crucial in achieving results. He declares that in avoiding this obstacle, the police have found another solution, which is by utilizing the international acts and by cooperating with private agencies such as Facebook. *"This method has given results in the fight against cybercrime, in cases in which information from Facebook was needed."* (Interview with E.P., 2015)

A key point of the interview was the question on the problems encountered during the investigation of cybercrime in Albania. Each of the respondents had different views. Nevertheless, all were unanimous when they stated that Internet Service Providers (ISP) do not have the facilities for the storage of the minimum information required by law, monitoring and identification of cases. This is because the ISPs use, based on the lack of facilities, the same IP for a certain number of users. In normal conditions, the

IP is the number that identifies an Internet user from another. Such an irregularity makes it more difficult to find the perpetrators. According to the expert of investigation of cybercrime in the forensic laboratory, something like this happens because in Albania, ISPs have not implemented IPv6 technology yet, which would make it possible to provide every user a unique IP. The forensic expert also notes that *"in the investigation field, there is a specialized human resources gap, but he stresses that the technology and equipment for the investigation of this crime exist and they are modern.*" However, what the expert of Security Policies stresses more regarding the problems of investigation is the problem of inspection and protection of digital evidence, as well as the presentation of evidence in court, which he notes that it is necessary to have specialized people to do something like that. Whereas the Head of the Cybercrime Unit, in the Tirana Prosecution Office maintains his view that the international letter-rogatory is the primary problem. This is then followed by the problem in infrastructure and equipment.

What has also been noted throughout this paper is that in the international arena as well as in the domestic one, the role and cooperation between national investigation authorities with the internet service providers is necessary. Thus, how is the Albanian reality? This question was asked to interviewees and the conclusion was clear: cooperation occurs because the law imposes it. As for concrete initiatives to strengthen this relationship between the relevant investigative authorities and ISPs, there is no such thing. Head of the Cybercrime Unit in Tirana Prosecution Office states: "We have sent a memo to the telecommunications office in connection with this matter, but in practice there is still nothing." Respondents emphasized that a strengthening of these relations is quite necessary to have the more positive achievements in the fight against cybercrime and cyber security.

A very important role in the fight against cybercrime is the establishment of special structures for combating cybercrime, which are those that enforce laws and regulations. Subsequently, the representatives of relevant institutions addressed the question whether they have these specialized units; and if yes, are they specifically dedicated to cybercrime? According to the respondents, such units have been created recently after a long absence. These are specialized units that focus only on cybercrimes. Such units are created at a local level in the prosecution offices and the police offices, as well as at the national level, which is ALCIRT. Forensic laboratory expert states that ALCIRT is not functional although it is the institution that should draft policies and coordinate nationwide cybercrime and security. He claims that in this area, there are no concrete results yet.

Respondents were also asked about the challenges (legal, technical, and institutional) facing the country in terms of cybercrime and critical

infrastructure. The Security Policy expert replied in this way: "There is a big challenge in this regard, as are retarded in this field. The positive moves in this area started very late even though they are international obligations." He stresses the need to identify the critical infrastructure as quickly as possible and that the political strategy against cybercrime must be approved. This has remained only a draft of ALCIRT, waiting to be approved.

Later access to technology and the Internet by the Albanian state and the confrontation with a new and very sophisticated kind of crime made it necessary to have experts that would deal precisely with investigating such crimes. For this reason, a number of individuals began to be trained in the field of cybercrime. Thus, how is the performance of such an activity, how much are trainings followed today in Albania, and who are the organizers of these trainings, domestic institutions or international organizations? According to the expert of Security Policy in Albania, trainings in the field of protection against cybercrime were held frequently. According to him, trainings were also conducted by Albanian trainers. He views it as a positive step and also as inclusion in school curricula of information about cybercrimes. Other interviewees noted that there are trainings related to cybercrimes, and most of them are made by foreign organizations, such as the FBI, ICITAP, PAMECA, and the CoE. Hence, they noted that the trained persons never stand in their assigned positions for a long time, which results both in economic costs and a lack of experts in the field.

During interviews with some of the leaders and best experts in the cybernetics field, a very important point was understood, especially for national security and for the business and private sector. This has to do with the security of data with which their employees work. Interviewees emphasized that there is a problem with the data that the employees receive intentionally or unintentionally by means of portable tools such as USB, especially when these tools are obtained from unsafe sources. This is because they can be infected, thus causing data losses. This has to do with the policies that have to be followed especially by state institutions. They have a high lack of security of their personnel as regarding the technology and the data that they can take or insert on the internal systems of the institutions due to the lack of knowledge. Therefore, it is necessary that there should be an increase in the awareness and trainings of staff on the safe usage, and on the distribution, transfer, and the receipt of data of the work on which they have access to.

Conclusion and Recommendations

Results of this analysis indicate that the Albanian legislation is in accordance with European standards and international conventions. Albania has signed and ratified all international conventions which cover protection

against cybercrime. Despite this fact, Albanian legislation still needs to be amended to be fully in accordance with the ratified conventions and to ensure the necessary flexibility for the prevention and prosecution of such dynamic crimes.

However, only the existence of a suitable legal framework is not enough to fight criminality, such as cybercrime. An effective implementation based on the practice of the legal framework is also crucial. To achieve this goal, the creation or improvement of mechanisms against cybercrime, the activation of all stakeholders affected by the phenomenon of cybercrime in combating this phenomenon, increase of the awareness of the population and the country's government on the risks that the country fases, and increased regional and global cooperation in combating cybercrime are necessary. The government should increase cooperation with ISPs, and they should increase the number of awareness by raising campaigns about the dangers of the Internet and online security.

Most law enforcement actors are not equipped with the necessary technological knowledge, whereas internet criminals are experts in computer technology. To combat these crimes, it is necessary to educate and develop human resources as one of the most reliable strategies. In addition, universities, schools of higher education, and academic institutions should open special courses designed to allow future generations of judges, prosecutors, and lawyers to be trained in this difficult, but very relevant and important area.

According to the study conducted in the context of this paper, after identifying the challenges and problems of the Albanian state in the fight against cybercrime, based on the analysis of the legal framework, achievements up to date, statistics and results obtained from the interviews conducted with specialists responsible for investigating, prosecuting and combating cybercrime, we were able to draw some recommendations to be followed by the Albanian government to improve the current situation regarding cybercrime in Albania. Thus, these recommendations are as follows:

- It is necessary to take measures for the separation and movement of data and information more securely, both within public institutions as well as private ones, with the aim of preventing and combating crime and ensuring appropriate security policies.
- Strengthening the existing institutions:

1. The identification of key institutions in the field of cyber security and to ensure that they have sufficient staff.
2. These institutions should have a mix of specialists, both from the legal field and from the information technology (IT), who must be constantly trained.

3. Updating the trainings curricula of the national public administration institutions and diplomatic academies.
4. Strengthening the national CERT, enabling it to have the capacity to respond to any incident.
5. There should be created conditions and taken measures to increase the cooperation and involvement of specialized agencies of law enforcement on a more adequate way of combating cyber crime.

- The creation of a public-private task-force is another necessary step in combating cybercrime more efficiently.
- Improving the operational capacity and response of law enforcement authorities against cyber attacks. In this context, it is necessary to increase the number of experts in the field of investigation and prosecution of cybercrime. This is possible by frequently organizing specialized trainings, and sending relevant officials for specializations abroad. Through these trainings, the specialization of experts in the field of cyber crime, their knowledge of domestic and international legislation in the field, and on the methods and ways of implementing this legislation in the most adequate and effective ways can be achieved. In this context, the training of existing staff is not only necessary, but also getting more specialists in this field since specialists in the field of combating cybercrime in Albania are very few.
- In addition to legal experts, experts in the field of information technology are also needed. This should be present in every structure of the police, prosecution, and courts that deal with the fight against cybercrime, in order to assist law enforcement with the right technical experience in a much more effective investigation of cyber attacks.

References:

Akhgar, Babak, Staniforth, Andrew & Bosco, Francesca (2014). Cyber Crime and Cyber Terrorism Investigator's Handbook. US: Elsevier.

Begeja. S (2007). Kriminalistika. Tirana.

Brunner, Elgin M. and Suter (2009). Manual. International CIIP Handbook 2008/2009, Center for Security Studies, Zurich: ETH.

Commissioner for the access to information and protection of personal data, information can be accessed at this web page: http://www.idp.al/index.php/sq/informacione/250-idp-sq/publikime/publikime-te-ndryshme/fjalor-terminologjik.

Computer Abuse: The Emerging Crime and the Need for Legislation. Fordham Urban Law Journal, 1983.

Convention on Cyber Crime of Concil of Europe (2001).

Criminal Procedure Code of the Republic of Albania (1995).

Csonka, P (2005). The Council of Europe Convention on Cybercrime: A response to the challenge of the new age? In Broadhurst, R. & Grabosky, P.

Eds. Cybercrime: The challenge in Asia, Hung Kong: University of Hong Press.
Elezi. F (2013). Provat penale dhe procesi i të provuarit, Tirana: Botimet Erik.
Elezi. I (2013). E drejta penale (Pjesa e posaçme). Tirana: Botimet Erik.
Elezi. I (2013). Kacupi. S, Haxhia. M, Komentari i Kodit Penal të RSH (Pjesa e përgjithshme). Tirana.
Gercke (2009). Impact of Cloud Computing on Cybercrime Investigation. Taeger/wiebe Inside the Cloud.
Internet Security Threat Report (2015). Symantec™ Global Intelligence Network. Vol. 20. April.
Internet Society (2015). Global Internet Report 2015, Mobile evolution and development of the Internet. Internet Society.
Law no.7895, date. 27.1.1995 "Criminal Code of Republic of Albania". Ammended
Magnin, Cédric J. (2001). The 2001 Council of Europe Convention on cyber-crime: an efficient tool to fight crime in cyber-space?, LLM Thesies, Santa Clara University.
Marcella Jr., A.J., Greenfield, R.S. (eds.) (2002). Cyber Forensics: A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, 2nd edn. Boca Raton: CRC Press.
Marcella, Albert J. and Menendez, Jr (2008). Doug, Cyber Forensics, Second Edition, A Field Manual for Collecting, Examining, and Preserving Evidence of Computer Crimes, US: Auerbach Publications.
Memorandum of Europian Commision no. 14/269 'Frequently Asked Questions: The Data Retention Directive'. Brussels, 8 April 2014.
Middleton,Bruce(2004). Cyber crime investigator's field guide. US: CRC Press LLC.
Recommendations No.R (89) 9, approved by the European Committee of Ministers of the Council of Europe on September 13 1989 and Report by the European Committee on Crime Problems: Computer-related crime.
Recommendations No.R (95) 13. approved by the European Committee on Crime Problems (CDPC) at its 44th plenary session May29-June 2, 1995: Concerning problems of criminal procedural law connected with information technology.
Rees Al (2006). Cybercrime Laws Of The United States, Compilation, CCIPS.
Reyes, Anthony, Brittson, Richard, OShea, Kevin and Steel Jim (2007). Cyber Crime Investigations Bridging the Gaps Between Security Professionals, Law Enforcement, and Prosecutors. US: Syngress Publishing.

Schjolberg & Judge Stein (2013). Crossing jurisdictional boundaries, A presentation at the Europol-INTERPOL Cybercrime Conference. September 24-25. Europol Headquarter.
Schjolberg & Judge Stein (2014). The Third Pillar for Cyberspace, An International Court or Tribunal for Cyberspace, Draft United Nations Treaty on an International Criminal Court or Tribunal for Cyberspace. Edition 9. June.
Shegani. A. E (2002). drejta penale e krahasuar. Tirana.
United Nations Office on Drugs and Crime (2013). Comprehensive study on cybercrime, Draft. UNODC, New York: February.
United Nations Office On Drugs And Crime (2013). Comprehensive Study On Cybercrime Draft February 2013, Chapter Six: Electronic Evidence And Criminal Justice. Vienna: UNODC.
Zverlevski Marko (2014). Andonova, Spasenka. And Millosheski, Vlladimir. Cybercrime handbook Skopje: OSBE.
World Internet Usage and Population Statistics: http://www.internetworldstats.com/stats.htm

Interviews

Interview with Prosecutor. A.G. Head of Cybercrime Unit at Prosecution Office in Tirana, July 2015.
Interview with E.P. Head of Cybercrime Investigation Unit at the Police Headquarters of Tirana. Tirana, July 2015.
Interview with M.Gj. Expert in Forensics Laboratory. Tirana, August 2015.
Interview with Dr. Xh. Sh. Expert in Security Policies, Police Academy of Republic of Albania.