International Journal of Social Science Research and Review

http://ijssrr.com
editor@ijssrr.com
Volume 5, Issue 7
July, 2022
Pages: 363-374

# Cyber Crimes in Kosovo in 2020

Frosina Tufa

Student in LLM in Department of Criminal Law. Faculty of Law / UBT - Higher Education Institution, Pristina. Republic of Kosovo

http://dx.doi.org/10.47814/ijssrr.v5i7.517

E-mail: frosinatufa@yahoo.com

## *Abstract*

The paper aims to compile the national and international definition of cybercrimes, their investigation and classification of the types of these computer crimes according to different world-renowned authors. The paper aims to describe the measures taken by countries such as Kosovo, Albania, Russia, the EU and the US in order to prevent and combat the cybercrime. It should be taken into account that cybercrime refers to illegal activities involving computers and computer networks, given the fact that nowadays special importance is given to technology, especially the internet and social networks. The internet has not only facilitated people's work, but in most cases it has also endangered their lives by causing very serious consequences. This is caused by the daily use of social networks and the dissemination of important information to us, which can lead to its misuse. In cybercrimes, usually, the first targets are people who have no knowledge of these diverse crimes. Therefore, the paper aims to make an understanding of the types of cybercrimes and study the phenomenon of cybercrime and its evolution in Kosovo and other countries with the use of analytical, historical, comparative and statistical methods. As a technique of data collection for the study, content analysis is used, which is usually applied when dealing with the data in textual form.

***Keywords:*** *Cybercrime; Victims; Cyber Attacks; Cyber Investigations; Preventive Measures; Forensics*

## *Introduction*

Criminality is antisocial behavior which is in conflict with legal and moral norms of behavior (Maloku,2019:174). Criminality represents the set of all actions that endanger and/or harm fundamental human values (protected by law) (Maloku,2021:60).

In today's society, the technology that continues to evolve, results in increasing the number of criminals and crimes in the cybercrime sphere. These activities are created by man himself, and therefore users who have negative goals, such as political or monetary gains, or even hindering the functioning of this system, are considered among the most intelligent opponents of this sphere.

We must pay special attention to the information or data that we consider important to us during the registration, because of the possibility of their misuse which may cause irreversible consequences. In such cases, governments apply certain measures to combat the cybercrime. The most common crimes that occur on computers are identity theft, fraud, and various psychological and sexual harassment including sexual abuse of children.

Such crimes can be committed individually and in an organized manner whilst they have in common the negative goal, such as loss of money, loss of life, destruction of the system, etc. Cybercrimes which are committed by a single person are committed by a so-called hacker, who manages to detect vulnerabilities in certain computers and gains access to them, which may cause big losses in different businesses.

According to William (2022), hackers are divided on the basis of certain crimes, such as white hat hackers, black hat hackers (who usually act for personal gain), hacktivists (hackers who access various websites and place a message of a religious, political, social nature), Phreakers (hacker of exploiting vulnerabilities on the phone rather than on a computer). As for organized cybercrime, so-called cyber terrorism is considered among the most dangerous attacks, which aims to spread a fear on the population by targeting military powers, banks, air, water and electricity control and many other points of importance to people (Johansen, 2020). Disrupting these services or even destroying their systems, cyber terrorism achieves through the use of various computer viruses (Haka, 2022). Cyber terrorism can also act on medical services, resulting in severe losses through access to the system, and the set goals (Janny, 2015). The very dynamic increase of this type of criminality (Maloku, 2015:119), as a form of organized crime, should undoubtedly be countered in a repressive and preventive manner.

In order to combat international organized crime, it is more than necessary that the competent governmental institutions harmonize legislation with world standards to cooperate among themselves, especially in the field of exchange of information that is important for Preventing and Combating Organized Crime (Maloku, 2015:461). Prevention of computer attacks from terrorism can be achieved with a special education against various cyber crimes (which will helps reduce the number of various scams), with a more dedicated regulation of the government towards criminal violations, etc. This paper is an attempt to highlight the growing phenomenon (Maloku & Maloku,2020:21) of this negative occurrence that has hit Kosovo.

## *1. Literature Review*

Authors Jasarevic & Maloku (2021) in their book Criminology (etiology and phenomenology of criminality) analyze and elaborate the etiology and phenomenology of criminality, they elaborate on various factors that influence the growth of criminality.

Also, Jararevic and Maloku (2021) in the book Criminal Procedural Law I and II (general and special part) the authors affirm that Criminal Procedural Law and Criminal Material Law constitute the right in a broader sense, which in itself imposes their close connection, because in the end they practically serve the same purpose, to achieve procedural criminal protection and security of society from criminality. The Internet offers us a very easy access to the information we need. Through the use of the internet, people are informed about the events that occur around the world. Therefore, the areas that can be targeted are diverse, such as: economical, criminological, legal medical, etc., as it happened in the first known attack on the Sri Lankan Embassy, by a group of so-called Tamil Tigers (1998), who through the use of the internet have sent 800 e-mails in order to raise awareness about the interruption of communication (Rai, 2019).

The number of cyber crimes is increasing, but a very big impact was also caused with the case of covid – 19 pandemic, where various crimes began to be committed as a result of this ambiguous situation (Stock, 2020).

Therefore, in order not to be a victim of these crimes, according to (Jacobs, 2019) people need to gain knowledge of the different types of crimes that are widespread on the internet, where among the most frequent crimes is the hacking of social networks, which nowadays, to people represents a special importance. As the ideal age to be a perpetrator of cybercrime, the age of Twenty (20) is usually considered as the cause of their desire and energy to enter cyberspace and commit various crimes (Yassir, 2012).

As a result of the impossibility of detecting the perpetrators of cyber crimes, the unstated intentions on monetary gain and the desire to cause damages through various forms of crimes, lower costs during online activity, as well as the lack of many reports has influenced the work to become more complicated in terms of the investigation into the detection of cybercrime perpetrators (Poonia, 2014). Therefore, any crime committed in cyberspace results in a lack of cyber security, the risk of which increases in cases of financial security of the individual and the government (Kaur, 2018). Among the years where cyber crimes took off were the years 2012-2013, because according to (Jahankhani, 2014) criminals in this sphere had realized that the profit that was realized through computers reduced the possibility of their detection and arrest compared to crimes that were committed physically.

## *2. Methodology*

The study focused on the analysis of the meaning of computer crimes and the determination of the methods of investigation of these cyber crimes. This study is based on the use of multiple research methods. Special scientific (Maloku, 2021:53). The historical method will reflect the birth and spread of cybercrime, and the development of global legislation on the prevention and combating of cybercrime. The descriptive method will also describe the definitions of the nation of "Cybercrime", the victims and their types that appear as a result of cybercrime, and the tools that are used to investigate these crimes.

Using comparative, theoretical and meta-analysis methods, the views of several different perpetrators will be presented (Maloku, 2021:170) regarding cybercrime. The comparative method is used to compare the measures applied by the different laws of the world and Kosovo legislation for combating cybercrime and for comparing a criminal offense from the Criminal Code of Kosovo and Albania.

While, through the statistical method, the most frequent cases of these crimes have been reflected through various applications that are usable nowadays. The research design is not experimental.

Since it is clear that this topic is inherently complicated, the paper also uses the content analysis method (Maloku, 2020:323) as a necessary method to study multidimensional research on cybercrime.

### Research Questions

1. What consequences can a cybercrime bring?
2. What measures are taken to prevent cyber attacks and how effective can these measures be given the difficulty of investigating these crimes?
3. What measures does the Republic of Kosovo foresee in comparison with the legislation of Albania?
4. Which apps increase the number of cyber crimes?

### *3. Results and Discussion*

### 3.1. History of Cybercrime

Crime is considered a problem, which mostly affects the quality of life not only of individuals but also the wider circle where we live (Maloku.2015:29). With the development of human society, various forms of criminality have also developed, and in particular the emergence and rapid development (Maloku, 2016:10) of cybercrime.  As a form of widespread criminality has appeared since 1960 and since that year the use of so-called hacking began.

Thus, with the constant introduction of hacking, during the ‘70s, there was a very well-known group, the so – called Phreakers, that with the use codes and signals achieved a new discovery on phone calls which helped the phone conversation at a little longer distance (Marie, 2019).

One of the main tools for the commission of various computer crimes, are computers which during the ‘80s came to market, by which people would manage to satisfy their interests (Marie, 2019). Mankind did not always have positive intentions, part of them were put into action to create some viruses, which would also be the first viruses for the purpose of collecting, namely stealing classified information. The highest fame hackers gained mainly in the ‘90s. After all these discoveries, from 2000 onwards, attacks on popular applications and businesses began. Among the most popular attacks is the cyber attack in Georgia, carried out on 20.07.2008, where a group of hackers so-called “zombie” carried out an attack against the Georgian President – Mikhail Saakshavili, on 20/07/2008. Entering their website and keeping it open 24 hours with the inscription win+love+in+Russia (Tidy, 2021).

In order to combat cybercrime, certain measures had to be taken, and the first step was made by the Russian Federation with a draft resolution, which was presented in 2003 in the General Assembly, on the topic “Developments in the field of information and telecommunication on the international security dispute” (Rexhepi, 2013). Meanwhile, after many discussions, Ban Ki-Moon (UN Secretary-General), together with a group of 15 experts, began their work in 2012 to establish measures and norms on cyber security (Haka, 2020). As for the European Union, in order to protect against computer attacks, managed to build an international defense against these crimes, which was called “The European Cybercrime Center” and the licensing of which took place in January 2013.

It should be noted, that according to Vatis (2009), there are two legal instruments against EU cybercrime:

- ○ European Legal Instrument dealing with the protection against cyber attacks, known as the “Council of Europe Convention on Cyber Crimes” of 2001 and
- ○ Eu Legal package, which regulates the various issues related to all types of cyber crimes.

In 2010, Law No. 03 / L-166-on the prevention and combating of cybercrime consisted of 29 separate articles (RKS Law - Law No. 03/L-166 on the Prevention and Combating of cybercrime).

### 3.2. Classification of cyber crimes

Cybercrime is divided into four main groups:

**1. Cyber crimes against individuals** (Jenny, 2015) :

Email Spoofing –   which means falsifying the email head.

Spamming – means sending mass emails for the purpose of collecting personal information.

Defamation – are cases that are usually carried out through computers, through the dissemination of information on various websites, this is mainly for the purpose of defamation.

Harassment and cyber stalking - among the most common forms and means when a person follows the activity of another person and does so through the above-mentioned applications.

- **Cyber Crimes against Property** (Mali,2009) :

Identity theft – the main purpose of this act is to modify the data of the individual and through it to obtain the property right, or even to extract money from his bank account, etc.

Intellectual property crimes – are crimes that are mainly related to copyright infringement, copying of various programs and their distribution.

Theft of Wi-Fi - which means the use of the internet which is paid by another person.

- **Cyber crimes against the organization** (Sharma, 2017) :

**Unauthorized access to a computer -** means illegal use of the computer, which includes two forms: alteration or deletion of data and computer espionage.

Virus – is a program that can infect other computer programs by copying themselves, slowing down the computer, and destroying many other programs on the given computer.

Sulma Salami – these crimes are known as financial crimes, because they relate to different amounts.

- **Cyber crimes against society** (Shaik, 2018) :

Falsification – when a person changes various data which are recorded on a particular computer.

Cyber terrorism – these attacks cause death, bodily harm, explosions, plane crashes, various economic losses, etc.

Web Jacking – in these cases hackers have access to another person's website, they can even make various changes within the site.

Pedophilia / Pornography – distribution of nude photos/videos of children, minors and adults.

### 3.3. Investigation of Cyber Crimes

Not always the work of computer criminals is very professional, often it can be detected during the act of commission, but because of the lack of knowledge of many types and their realization, such crimes cannot be observed.

According to Howard (2021), among the cases when the commission of the computer crime on the computer can be detected are the moments when:

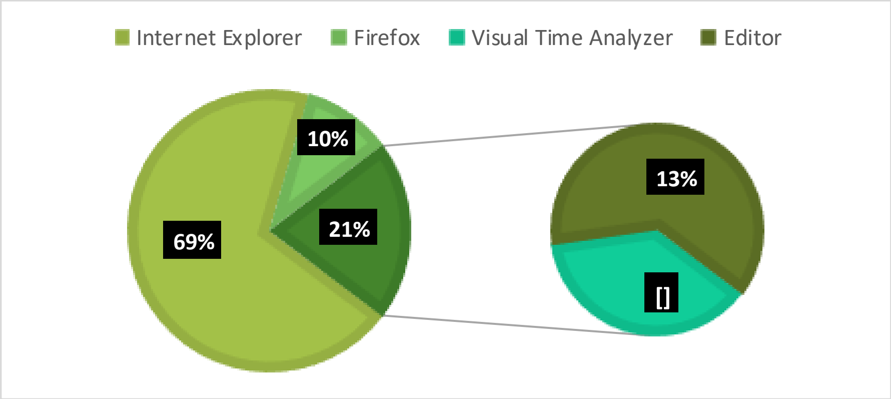
- The computer installs unnecessary programs;
- Mouse moves to the specified computer screen;
- Programs start to malfunction;
- Difficulty opening programs through passwords, etc.

For combating cybercrime, many different technological techniques are now known to be used in different police institutions. Therefore, an important role un the detection or investigation of such crimes is played by the means of communication. Among the most popular are the police informing the public, which is also known as an internal communication tool and external communication which means police informing the public about these cyber crimes, so that the public has knowledge about them and can protect themselves from such crimes. The most important part when investigating cyber crimes is the collection of evidence that will help solve certain crimes. The evidence collected is digital evidence because crimes are committed mainly on certain computers or digital devices (Stewen, 2022).

The analysis of these crimes is done through several important tools, and one of the most important forensic tools is;

○ Visual Time Analyzer –which tracks internet activity, time, work, project details, hours of use and history, etc. (Rexhepi, 2013).

**Graph nr.1:** Average use of computer programs



Source from: (Neuber M., 2021) - https://www.neuber.com/timeanalyzer/time-tracking.html

Based on Jay (2022), the time analyzer app can also determine the most used Page in a month or year, which helps to notify the public through these statistics and applications about the crimes that may occur on those pages that are most usable during the day, month or even year.

Among the forensic tools that detect crimes committed by mobile devices are WhatsApp forensic, iPhone analyzer, saft, etc., (Gashi, 2020).

According to Article 21 on investigation based on the Kosovo Law on prevention and combating cyber crimes, through various bilateral and multi-layered agreements, a special cooperation and multiple investigations on various cyber crimes could be realized... (RKS Law, Law No. 03/L-166 on the Prevention and Combating of Cybercrime).

### 3.3. Cyber Attacks in Kosovo for 2020

Cybercrime is a major concern for both the world and Kosovo. However, considering that Kosovo as not very developed country for protection against cyber attacks, it is not very ready to face them, because the measures that Kosovo can take against these attacks are minimal for a successful defense.Among the most frequent attacks in Kosovo are the theft of passwords of social networks (Konushevci, 2014). Compared to other countries, the number of cyber attacks in Kosovo is much lower. As the most frequent attacks that are carried out in Kosovo, can be mentioned: attacks of wealth gain, on banks, hacking of profiles of politicians, various scams, etc.Regarding statistics on cyber attacks around the world, the FBI in March reported that for 2020 there were 791,790 suspected cyber crimes and as a result of the appearance of the Covid-19 epidemic, the number increased approximately for 300,000 since 2019 (FBI, 2022).

**Table 1**. Victims for 2020 in Kosovo and around the world

| **Around the world** | | **KOSOVO** | |
|---|---|---|---|
| **AGE** | **VICTIMS** | **AGE** | **VICTIMS** |
| **20-29** | 70,791 | 16 – 70 | 73.2% |
| **30-39** | 88,364 | | |
| **40-49** | 91,568 | | |
| **50-59** | 85,967 | | |
| **Over 60** | 105,301 | | |

Source from: (FBI, 2022) https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

In fraudulent attacks, the most frequent victims were the age group under 25, while the second group that encounters numerous scams over losing money is old age (Maddison, 2022).

**Table 2.** Top 20 Countries Found to Have the Most Cybercrime

| **USA** | **23%** | **INDIA** | **3%** |
|---|---|---|---|
| **CHINA** | 9% | **RUSSIA** | 2% |
| **GERMANY** | 6% | **CANADA** | 2% |
| **BRITAIN** | 5% | **SOUTH KOREA** | 2% |
| **BRAZIL** | 4% | **MEXICO** | 2% |
| **SPAIN** | 4% | **JAPAN** | 2% |
| **ITALY** | 3% | **ISRAEL** | 1% |
| **FRANCE** | 3% | **ARGENTINA** | 1% |
| **TURKEY** | 3% | **KOSOVO** | 1% |

Source from: (Sumo, 2010) Top 20 Countries Found to Have the Most Cybercrime (enigmasoftware.com)

Given that many websites are always active, the hacking of the domestic websites increases and continues while in every 1 minute a cyber attack can occur, Therefore logging into different websites can also increase the number of crimes in this sphere.

According to Jay (2022), by the first half of 2020, only 4.83 cyber-attacks were recorded, and as a result, the US ranks first with a very increased number of cyber crimes.

### 3.4. Comparison of the Criminal Code of Kosovo and Albania

**Criminal offense *"Entering computer systems"***

3.4.1. Criminal Code of Kosovo

Chapter XXVI – Criminal offenses against property

Article 327 – "Access to computer systems"

- According to the Criminal Code of Kosovo, article 327, which is known as the criminal offense of accessing computer systems, any person, who intends to gain personally or for someone else a certain property benefit, or even cause consequences to the specified party, to interfere with the documents recorded in computer systems, will receive a fine and a sentence of imprisonment up to 3 years (Criminal Code of Kosovo, 2019).

- The sentence of imprisonment, starting from 6 months up to the maximum sentence of 5 years, shall be imposed on the person, who for personal property gain exceeds the amount of ten thousand (10,000 euros), (Criminal Code of Kosovo, 2019)

### 3.4.2. Criminal Code of Albania

Section III - Offences Against Public Order and Security

Article 293/c – *"Interference with computer systems"*

- According to the Criminal Code of Albania, article 293/C, which concerns the criminal offense of intrusion into computer systems, persons who create obstacles that present very serious problems, in order to obstruct the functioning of computer systems, by entering them and causing destruction in the interior of the recorded data, would be punished with imprisonment from 3 years to 7 years ( Criminal Code of Albania, 2017).

- According to the Criminal Code of Albania, the same article-293/C, when a certain person, by using a computer enters the internal systems of military computers, or that of health or any other system that is of great importance to the public, would be imposed to a sentence of imprisonment from 5 years to 15 years (Criminal Code of Albania, 2017).

**Comparison:** The Criminal Code of the Republic of Kosovo compared to the Criminal Code of Albania, as far as the determination of measures against cyber crimes is concerned, in this case, the Criminal Code of Kosovo, eventhough it is not formulated in a voluminous way enough to be ready to fight serious cyber crimes that can occur, but it is detailed, paying attention to the circumstances regarding the commission of these crimes.

On the other hand, the Criminal Code of Albania, the criminal offense "Entering the computer system" based on certain circumstances can sentence a minimum of 3 years and a maximum of up to 15 years of imprisonment, compared to the Criminal Law of the Republic of Kosovo, which for the same criminal offense foresees a sentence of imprisonment of a minimum of 6 months and a maximum of up to 5 years.

The penalties foreseen for cyber crimes in the Criminal Code of Albania are much more severe compared to Kosovo, this is probably due to the lower number of these crimes in Kosovo and bad drafting of the law on prevention and combating cyber crimes.

## *Conclusion*

Cybercrime is one of the most common problems that people face in their daily liver. These problems are increasing with the development of technology and the use of social networks. Therefore, in order not to be a victim of these crimes it is important that the public is informed about this area, because the consequences of these crimes can be very big, as well as economic attacks can cause huge money losses for both ordinary people and the state.

Usually, perpetrators of these computer crimes commit these crimes for personal interests. The perpetrators of computer crimes can be people aged 12 who are from a different country can cause a crime in a completely different country, so the risk of these types of crimes can be various. In order to commit a computer crime it is required a computer or a simple device and access to the internet through that device. Therefore, governments have applied laws to combat and prevent these crimes. The law applied by the Republic of Kosovo for combating and preventing these crimes is not drafted in such a detailed way as to pay attention to different circumstances. This law consists of 29 articles in which the meaning of cyber crimes and the circumstances that they may occur are defined. Regarding the investigations of these criminal offenses, the police institution should cooperate with the public on reporting and prevention of spreading of these criminal offenses. It should be taken into account that the detection and prevention of hacking and cyber offenses has become difficult and a problematic area. We conclude that this type of criminality, unlike other crimes, has a very high risk since as a weapon it uses a computer/device through which it can access the internet and cause harmful consequences to both individuals and governments.

## *Recommendations*

Cyber crimes, as mentioned above, are among the most widespread crimes in the world, due to the use of the internet. In order to prevent this crime, special care must be taken to disseminate personal information, because their misuse can cause irreversible consequences, such as loss of property, misuse of photographs, etc.

For cybercrime prevention, an international plan can also be created which should include first educating the community on their protection, strengthening the capabilities of cybercrime detection agencies and addressing them, an international cooperation on cybercrime. Above all, the government should deal with issuing preventive guidelines for these crimes in order to protect new users.

A better but not always safe protection would be if each person takes certain measures to prevent such crimes. Some measures that could help to protect against this particular crime are:

- Constant switching of passwords;
- Choosing stronger passwords, not assigning personal information as a password;
- Protection of computers with security applications;
- Avoiding bank card details;
- Non–responsese to false or fake messages or emails and;
- Attention to privacy policies;

Therefore, the caution that is given to these certain measures will help prevent and combat these cyber crimes.

## *References*

2020 Internet Crime Victims Reports. Crime Statistics, Federal Bureau of Investigation, Washington. Available at: https://www.ic3.gov/Media/PDF/AnnualReport/2020_IC3Report.pdf

Gashi, S. (2020). Kosova ndaj sulmeve Kibernetike.Kosova Live. Available at: https://kosovalive.org/2020/10/29/kosova-eshte-ndezur-ne-alarm-ndaj-sulmeve-kibernetike/Last accessed: 05.22.2022.

Haka, E. (2020). Krimi Kibernetik dhe Legjislacioni Ndërkombëtarë. Academia. Available at: https://www.academia.edu/19768726/krimi_kibernetik_dhe_legjislacioni_nderkombetar. Last accessed: 05.26.2022

Howard, P. (2021, Janar 08). Infosec Institute: Available at: https://resources.infosecinstitute.com/topic/computer-forensics-tools/ Last accessed: 05.27. 2022.

Jasarević, O., Maloku, A. (2021). *Kriminologija (etiologija i fenomenologija kriminaliteta*). Universitet u Travniku. Travnik. Bosna i Hercegovina.

Jasarević, O., Maloku, A. (2021). *Krivično procesno pravo I dhe II (opšti i posebni dio).* Universitet u Travniku. Travnik. Bosna i Hercegovina.

Jahankhani, H. (2014). Cyber crime Classification and Characteristics. Në A. H.-F. Ameer Al-Nemrat, & A. S. Francesca Bosco (Re.), *Cyber Crime and Cyber Terrorism Investigator's Handbook* (f. 152). Elsevier Science. Available at: https://www.researchgate.net/publication/280488873_Cyber_crime_Classification_and_Characteristics .Last accessed:06.06/.2022

Jacobs, L. (2019, Mars 12). 10 Types of Cyber Crimes. . . And Another 10 You've Never Heard of. Law and Crime. Available at: https://bestdsl.net/10-types-of-cyber-crimes-and-another-10-youve-never-heard-of/Last accessed: 09.06.2022

Jay, A. (2022). Important Cybercrime Statistics: 2021/2022 Data Analysis & Projections. Finances Online - Reviews for Business. Available at: https://financesonline.com/cybercrime-statistics/ Last accessed: 05.27.2022.

Jenny, S. (2015). Krimet Kibernetike dhe Klasifikimi i tyre. Bota Ndryshe: Available at: https://botandryshe.wordpress.com/ Last accessed: 05.18.2022.

Johansen, A. G. (2020). The ways to help protect yourself against cybercrime. Norton. Available at:https://us.norton.com/internetsecurity-how-to-how-to-recognize-and-protect-yourself-from-cybercrime.html. Last accessed: 05.23.2022

Karović, S., Maloku, A., & Shala, S. (2020). *Juvenile Criminal Law in Bosnia and Herzegovina With Reference to the Criminal Legal Position and Responsibility of Juveniles*. *Kriminalističke Teme*, (1-2), 107-122. Available at: https://krimteme.fkn.unsa.ba/index.php/kt/article/view/205

Kaur, N. (2018, Gusht). INTRODUCTION OF CYBER CRIME AND ITS TYPE. (C. E. Dr.A.Arul L.S, Re.) International Research Journal of Computer Science (IRJCS), 05(08), 435. Available at: https://www.academia.edu/37288317/INTRODUCTION_OF_CYBER_CRIME_AND_ITS_TYPE Last accessed: 06.06.2022

Kodi Penal i Republikës së Kosovës. Gazeta Zyrtare e Republikës së Kosovës / nr. 2 / 14 Janar 2019, Prishtinë. Available at: https://gzk.rks-gov.net/ActDetail.aspx?ActID=18413.

*Kodi Penal i Republikës së Shqipërisë*. Available at: https://www.pp.gov.al/Legjislacioni/Legjislacioni_Penal/

Konushevci, A. (2014). *Radio Evropa e Lirë*. Available at: https://www.evropaelire.org/a/26749258.html /Last accessed: 05.20.2022.

Ligji për parandalimin dhe luftimin e Krimeve Kibernetike në Kosovë. *Gazeta Zyrtare e Republikës së Kosovës / Prishtinë: Viti V / nr. 74 / 20 Korrik 2010*. Available at: https://gzk.rks-gov.net/ActDetail.aspx?ActID=2682 Last accessed: 05.18.2022.

Maddison, J. (2022). *Statistikat e sigurisë kompjuterike*. Fortinet Security. Available at: https://www.fortinet.com/resources/cyberglossary/cybersecurity-statistics Last accessed: 05.25.2022.

Mali, M. C. (2009). *Classification Of Cyber Crimes*. Lawyers Club India: Available at: https://www.lawyersclubindia.com/articles/Classification-Of-CyberCrimes--1484.asp#:~:text=Cyber%20crimes%20can%20be%20classified%20in%20to%204,Against%20Organization%204%20%284%29%20Cyber%20crime%20Against%20Society Last accessed: 05.27.2022.

Maloku, A. (2015). *Bashkëpunimi ndërkombëtar policor në luftimin e krimit të organizuar*. Regional Journal of Social Sciences Reforma. No.2. 2015 pp. 119-127.

Maloku, A. (2015). Fear of Violence and Criminality in the Region of Gjilan, Kosovo. Mediterranean Journal of Social Sciences, 6 (2 S5), 29–36. Doi:10.5901/mjss.2015.v6n2s5p29

Maloku, A. (2015). *Rregullimi ndërkombëtar ligjor për të parandaluar abuzimin e drogave dhe substancave psikotrope*. Balkan Journal of Interdisciplinary Research. Vol.1. No. 1. 2015. pp. 461-472.

Maloku, A. (2016). Karakteristikat e organizatave kriminale transnacionale. Buletini Shkencor Nr. 5 "DARDANIA. p. 10-24.: Qendra Kërkimore Zhvillimore – PEJA. Peje.

Maloku, A. (2019). *Fjalor i terminologjik i viktimologjisë*. Kolegji Iliria, Prishtinë,

Maloku, A. (2020). *Theory of Differential Association. Academic Journal of Interdisciplinary Studies*, *9* (1), 170. https://doi.org/10.36941/ajis-2020-0015

Maloku, A., Maloku, E. (2020). *Protection of Human Trafficking Victims and Functionalization of Institutional Mechanisms in Kosovo*. Acta Universitatis Danubius. Juridica, 16 (1), 21–44.

Maloku, A., Maloku, E. (2021). *Fajlor i terminologjisë juridiko-penale për gazetarë*. Kolegji Iliria, Prishtinë,

Maloku, E., Jasarevic, O., & Maloku, A. (2021). *Assistance of the psychologist expert in the justice bodies to protect minors in Kosovo*. EUREKA: Social and Humanities, (2), 52-60. https://doi.org/10.21303/2504-5571.2021.001649

Marie, B. H. (2019). *Phone Phreaking*. Encyclopaedia Britannica: Available at: https://www.britannica.com/topic/phreaking. Last accessed: 05.26.2022.

Neuber M., A. (2021). *Gjurmimi i Kohës*., Neuber Software: Available at: https://www.neuber.com/timeanalyzer/time-tracking.html Last access: 05.21.2022.

Poonia, A. S. (2014, Nënto-Dhjetor). Cyber Crime: Challenges and its Classification. International Journal of Emerging Trends & Technology in Computer Science (IJETTCS), Volume 3(6), 119. Available at: https://www.ijettcs.org/Volume3Issue6/IJETTCS-2014-12-08-96.pdf/ Last accessed: 10.06.2022

Rexhepi, K. (2013. *Krimet Kibernetike - Kosovë.*, nga Akademia: Available at: https://www.academia.edu/21816119/Krimet_Kibernetike. Last access: 05.20.2022

Rai, D. (2019, Nëntor 13). Cyber Crime and Cyber Security : An overview. Pleaders - Intelligent Legal Solutions: Available at: https://blog.ipleaders.in/cyber-crime-and-cyber-security-an-overview/ Last accessed:06.06.2022

Stock, J. (2020, 08 04). Interpol: Krimet kibernetike kanë arritur nivel alarmant gjatë pandemisë.GazetaExpress. Available at: https://www.gazetaexpress.com/interpol-krimet-kibernetike-kane-arritur-nivel-alarmant-gjate-pandemise/

Shaik, D. N. (2018). Classification and Provisions of Cyber Crimes. Toppr Law: Available at: https://www.toppr.com/guides/business-laws-cs/cyber-laws/classification-of-cyber-crimes/ Last accessed: 05.27.2022.

Sharma, V. (2017). *Classification of Cyber Crime and its differentiation from Conventional Crime*. Available at: https://www.linkedin.com/pulse/classification-cyber-crime-its-differentiation-from-vivek-sharma Last accessed:27.05.2022.

Stewen, B. (2022). Cybersecurity Guide. Available at: https://cybersecurityguide.org/careers/cybercrimeinvestigator/#:~:text=A%20cybercrime%20investigator%20investigates%20a%20number%20of%20crimes,computers%20that%20can%20be%20used%20in%20prosecuting%20crimes. Last accessed: 05.27.2022.

Sumo, K. (2010). Top 20 Countries Found to Have the Most Cybercrime. Enigma Soft: Available at: https://www.enigmasoftware.com/top-20-countries-the-most-cybercrime/ Last accessed: 05.26.2022.

Tidy, J. K. (2021). *The three Russian cyber-attacks the West most fears*. BBC News: Available at: https://www.bbc.com/news/technology-60841924 /Last accessed: 05.25. 2022.

Vatis, M. A. (2009). *The Council of Europe Convention on Cybercrime*. (S. &. LLP, Re.) Available at:http://static.cs.brown.edu/courses/csci1800/sources/lec16/Vatis.pdf#:~:text=The%20Convention%20on%20Cybercrime%20is%20an%20international%20treaty,the%20Council%20of%20Europe%20%28COE%29%20in%20Strasbourg%2C%20France.3 /Last accessed: 05.18.2022.

William, L. (2022). *What is hacking? Types of hackers/ Introduction of Cybercrime*. (Krishna, Producenti) GURU Education : Available at: https://www.guru99.com/what-is-hacking-an-introduction.html Last accessed: 05.23.2022

Yassir, S. N. (2012, February). Cybercrime: A threat to Network Security. Available at: https://www.researchgate.net/publication/342210727_Cybercrime_A_threat_to_Network_Security Last accessed: 10.06.2022

## Copyrights