International Journal of Multicultural and Multireligious Understanding

http://ijmmu.com
editor@ijmmu.com
ISSN 2364-5369
Volume 10, Issue 4
April, 2023
Pages: 625-635

Cyber Crimes Investigation

Lumi Millaku

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

http://dx.doi.org/10.18415/ijmmu.v10i4.4723

Abstract

This paper aims to make the definition of cybercrimes, their investigation and the classification of the types of these computer crimes. Also, the paper aims to describe the measures taken by states to prevent and fight cybercrimes. One of the biggest modern challenges is undoubtedly the online "war", which with the rapid technological development day by day is taking on large proportions in Kosovo as well. The fight against cybercrimes and the institutional confrontation for security and the prosecution of these crimes remain challenging for the state of Kosovo. Cybercrime, also called computer crime, refers to the use of a computer as an instrument for illegal purposes, such as committing fraud, trafficking in child pornography and intellectual property, stealing identities, or violating privacy. Cybercrime, especially via the Internet, has grown in importance as the computer has become central to commerce, entertainment and government. (Dennis, 2022)

Keywords: *Cyber Crime; Computer Crime; Fraud; Criminal Code of Kosovo*

1. Introduction

The authors Jasarevic and Maloku (2021a.2021b) have analyzed the criminological and criminal procedural aspect of criminality exceptionally well, while the sociological aspect of criminality has been analyzed by the authors Shabani and Maloku (2019a, 2019b). The development, growth and use of communication and information technologies, (TKI) has always been associated with a significant increase in criminal activities. The Internet is increasingly being used as a tool in the hands of organized crime and terrorism.

Unlike other well-known crimes, computer crimes are distinguished by the fact that they are easy to learn how to use, require very few resources, but the action of which causes serious and extensive damage, can be carried out in a certain jurisdiction without being physically there, and what is more prominent, often, their illegality is not so comprehensible.

Under this perspective, new forms in the field of computer crime are a constant challenge to legislators, law enforcement agencies and international organizations. Instruments on state barriers, as well as internal instruments, are needed to monitor TKI from the risk of criminal activities.

The very dynamic increase of this type of criminality (Maloku, 2015a, 2018), as a form of organized crime, must be opposed in a repressive and prejudiced manner.

In order to fight international organized crime, it is more than necessary that the competent institutions of the states harmonize the legislation with world standards and cooperate with each other, especially in the field of exchanging information that is important for preventing and fighting organized crime. (Maloku), 2015c:461).

Crime is considered as a problem, which mostly affects the quality of life not only of individuals but also of the wider circle where we live (Maloku. 2015b:29,). With the development of human society, various forms of criminality have also developed, and in particular, the emergence and rapid development (Maloku, 2016a, 2016b, Gabela & Maloku, 2022,2023) of cybercrime as a fairly widespread form of criminality, has appeared since 1960 and since year, the use of the so-called - hacking or hacks also began.

Cybercrime is more than a science. Analyzing the data and investigating the root cause will help you bring that person to justice, whether in civil or criminal court. (NathansInvestigation, n.d.)

Recently, this new type of crime has broken the previous limits of time and physical extent, crossing state borders. So, it is no longer enough for a state to have preventive measures against this phenomenon, but the cooperation of two or more states is also necessary to have results in preventing and fighting this phenomenon. (Shkëmbi, 2015)

This paper presents an attempt to highlight the growing phenomenon (Maloku & Maloku, 2020:21) of this negative phenomenon. This paper contributes to the existing scientific literature, especially in the legal field. Moreover, this paper can contribute to the work of criminologists, victimologists and sociologists. (Qerimi, Maloku, & Maloku, 2022)

2. Methodology

This study is based on the use of multiple research methods. (Maloku, 2021:53). Because of the research intricacy, numerous approaches have been modified to help each other solve the problem (Maloku, Qerimi &; Maloku, 2022:176). The scientific methods used in this paper are mainly methods of analysis, synthesis and comparison, which help to analyze, synthesize and compare the theoretical views of local and foreign authors. (Maloku & Maloku, 2020:323). Such research enables us to obtain relevant knowledge with the help of scientific methods and research techniques — scientific knowledge (Maloku, Kastrati, Gabela & Maloku, 2022:138). This study is focused on the analysis of the meaning of computer crimes and the determination of the investigation methods of these cybercrimes. The defined object of research requires the use of different methods and scientific knowledge from many scientific disciplines, in particular, the paper will use theoretical analysis methods, comparative methods and the unity of inductive-deductive methods. (Maloku, 2021:76)

The research in this paper has the characteristics of scientific theoretical research, which is necessarily qualitative in nature. (Qerimi, Kastrati, Maloku, Gabela, & Maloku, E. 2023). The scientific methods used in this paper are historical, descriptive, analytical and statistical methods. Through the historical method, the birth and spread of cybercrimes will be reflected, and the development of legislation on the prevention and combating of cybercrimes.

With the method of description, the description of the definitions of the notion "Cybercrime", victims and their types that appear as a result of cybercrimes and the tools used to investigate these crimes will be made. The analytical method is mainly based on the in-depth legal analysis of the provisions of the community and domestic acts in the cyber field.

While, through the statistical method, the most frequent cases of these crimes have been reflected through various applications that are usable today.

The research design is not experimental. As a technique for collecting data for the study, content analysis was used, which is usually applied when dealing with data in text form. In this case, content analysis focuses on deriving an understanding of the types of cybercrimes.

3. Results and Discussion

3.1. History of Computer Crimes

For computer criminality as a new form of organized crime in the contemporary world, from the scientific point of view, until now there has not been any common position regarding the definition or the beginnings of the appearance of this form of criminality. Some think that this is a new category, whose beginnings are related to the appearance of the first electronic digital computers, towards the middle of the last century, but there are also those opinions that say that the first misuses came even earlier, that at the beginning of the twelfth century, when the first mechanical calculators appeared.

In order to prove the exact period of the appearance of computer criminality, first of all it was necessary to determine the period when the first abuses committed on computers, or with their help, in fact computers, which have been before computers.

In this regard, some authors connect the beginnings of the appearance of computer crime with the application of the first mechanical calculators, which may have even led to the first manipulations with their help. (Vula, n.d.)

3.2. Ways of Committing Cybercrimes

Computer systems have become a vital part of the way of life. In order to understand and analyze the phenomenon of cybercrime more clearly, it is important to determine the place, role and ways of using the computer in this field.

The use of computers in the field of cybercrimes is done in five basic ways:

a) The computer as an object of attack;
b) The computer as a means of execution (modus operandi):
c) The computer as a tool for the organization, planning and leadership of criminality;
d) The computer as a symbol for deception:
f) The computer as a tool for stopping, disclosing and examining criminal offences. (Shkëmbi, 2015)

3.3. Classification of Cybercrimes

Cybercrimes can be classified into 4 major categories.

a) Cybercrime Against the Individual

- Email spoofing;
- Spamming;
- Defamation;
- Harassment & Cyberstalking.

b) Cyber Crime Against Property

- Identity theft;
- Intellectual property crimes;
- Theft of internet time.

c) Cybercrime Against the Organization

- Unauthorized access to the computer;
- Denial of service;
- Computer contamination/viruses;
- Email Bombing;
- The Salami attack;
- Logic bombs;
- Trojan horse.

d) Cybercrime Against Society

-Forgery;
- Cyber terrorism;
- Web Jacking;
- Pedophilia/pornography. (BotaNdryshe, n.d.)

3.4. Investigating Cybercrimes

3.4.1. What is a Cybercrime Investigation?

A comparison of cybercrime investigations and physical-world criminal investigations reveals a primary difference: evidence in criminal investigations is primarily digital in nature.

A cybercrime investigation is the process of investigating, analyzing and recovering forensic data for digital evidence of a crime. Examples of evidence in a cybercrime investigation include a computer, cell phone, car navigation system, video game console, or other networked device found at a crime scene. This evidence helps cybercrime investigators determine the perpetrators of a cybercrime and their intent. (Maryville University, a.d.)

Cybercriminals can make their crimes visible and, at times, more subtle. Here are some areas they will target and why you need a trained private investigator to help.

Your computer has unexpected software installations:

- The mouse moves by itself and indicates the goal
- Programs do not work or do not open
- Files have been deleted or moved
- Passwords have been changed without your knowledge
- Money is missing from your accounts, or you receive a call or bill for a purchase you never made.
- Denial of service attacks
- Hacking or unauthorized access
- Email fraud (NathansInvestigation, n.d.)

Cybercrime investigators perform many tasks including:

- Determining the nature of a cybercrime;
- Conducting an initial investigation;
- Identification of possible digital evidence;
- Conducting digital forensics on devices;
- Provision of equipment and digital evidence;

Presentation of evidence in the judicial system. (Maryville University, a.d.)

3.5. Cyber Crime Investigation Techniques Include

Conducting background checks: Determining the when, where, and who of a crime sets the stage for an investigation. This technique uses public and private records and databases to discover the background of individuals potentially involved in a crime.

Information Gathering: This technique is one of the most critical in cybercrime investigations. Here, investigators ask questions such as: What evidence can be found? What level of access to resources do we have to gather evidence? The answers to these and other questions provide the basis for a successful investigation.

Conducting Digital Forensics: Cybercrime investigators use their digital and technological skills to conduct forensics, which involves using technology and scientific methods to collect, store and analyze evidence during an investigation. Forensic data can be used to support evidence or to confirm a suspect's involvement in a crime.

Tracking the perpetrators of a cybercrime: With information about a crime in hand, cybercrime investigators work with Internet service providers and telecommunications and network companies to see which websites and protocols were used in the crime. This technique is also useful for monitoring future activities through digital surveillance. Investigators must seek permission to conduct these types of activities through court orders. (Maryville University, a.d.)

3.6. How to Protect Against Cybercrime

These steps will help mitigate the necessary steps a criminal would use to gain entry.

- Do not click on unknown links
- Never download software that is not known
- Avoid giving out personal information if the source cannot be trusted
- Have a firewall installed
- Make sure all your software is up to date
- Change your passwords regularly and change them
- Avoid public WiFi
- Keep personal information off the cloud
- Always back up your data. (NathansInvestigation, n.d.)

For the investigation of computer crimes, Computer Forensics also plays an important role, which handles, analyzes and examines evidence.

The analysis of these crimes is done through several important tools, and as among the most important tools of forensics is;

Visual Time Analyzer – which tracks internet activity, time, work, project details, usage hours and history, etc. (Timesheet, 2022)

Through Time Analyzer, the most frequent use of a web page can also be determined, which helps to inform 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 the year.

Among the forensic tools that detect crimes committed by mobile devices are whatsapp forensic, iphone analyzer, saft, etc. (Cybercrime Statistics, 2022)

According to Article 21 on the investigation based on the Law of Kosovo on the prevention and combating of cybercrimes, all states and other organizations at their request can cooperate with the

Kosovar authorities and these investigations can be carried out through bilateral and multilateral agreements. (LAW No. 03/L-166 On the prevention and combating of cybercrimes, 2022)

3.7. Penal Code of Kosovo

Article 125

Disclosure of classified information and non-retention of classified information

Anyone who discloses or fails to retain classified information is punishable under the Information Classification and Security Clearance Act.

Article 199

Violation of Confidentiality of Correspondence and Computer Databases

1. Anyone who without authorization opens a letter, telegram, facsimile or any other closed document or delivery or electronic communication of another person, or in any other way violates the confidentiality of such materials or without authorization keeps, conceals, destroys or delivers to another person a letter, telegram, facsimile, electronic communication or any other closed document or delivery of another person, shall be punished by a fine and imprisonment of up to six (6) months.
2. Anyone who without authorization intervenes in the computer database of another person or uses those data or makes them available to another person, shall be punished with a fine and imprisonment of up to one (1) year.
3. When the criminal offense referred to in paragraph 1. or .2 of this article is committed with the purpose of obtaining material benefit for himself or for the other person or to cause damage to the other person, the perpetrator is punished with a fine and imprisonment for up to three (3 years.
4. When the criminal offense from paragraph 1., 2. or 3. of this article is committed by the official person in misuse of his position or authorizations, for the criminal offense from paragraph 1. or 2. of this article, the perpetrator is punished with imprisonment of three (3) months to three (3) years, while for the criminal offense from paragraph 3 of this article, the perpetrator is sentenced to imprisonment from one (1) to five (5) years.

Article 200

Unauthorized Disclosure of Confidential Information

1. The lawyer, defender, doctor or other person who without authorization discloses the confidential information about which he was made aware during the exercise of his profession and which he is legally obliged to keep secret, shall be punished by a fine or imprisonment up to a (1 year.
2. The person is not criminally liable according to paragraph 1. of this article if he disclosed confidential information for public interest if such interest outweighs the non-disclosure of confidential information.

Article 232

Abuse of Children in Pornography

1. Anyone who produces pornography with children or uses or involves the child for the creation or production of live performances, shall be punished by imprisonment of five (5) to fifteen (15) years.
2. Anyone who sells, distributes, promotes, displays, transmits, offers or makes available child pornography shall be punished by imprisonment of three (3) to ten (10) years.

3. Anyone who provides for himself or another person or possesses child pornography, shall be punished with a fine and imprisonment of one (1) to five (5) years.
4. An attempt to commit a criminal offense under this article is punishable.
5. For the purposes of this article, the expression "live display" means the actual display, including through means of information and communication technology, of:

5.1. Of a child engaging in sexually explicit conduct, whether real or simulated; or
5.2. Genitalia of a child for primarily sexual purposes.

Article 301

Issuing Bad or Fake Checks and Misuse of Bank or Credit Cards

1. Anyone who, with the purpose of obtaining an illegal financial advantage for himself or another person, gives or puts into circulation a check for which he knows that there is no cover, a fake check or a forged credit card and in in this way realizes financial benefit, is punished with a fine and imprisonment of up to three (3) years.
2. Anyone who, with the purpose of illegally obtaining material benefit for himself or another person, uses a credit card or check without authorization or uses a bank card in a bank machine to withdraw cash, knowing that the withdrawal such is not covered by the account balance or by the overdraft or anyone who uses the credit card even though he knows that at the time of payment he will not be able to pay the corresponding amount and thus realizes a financial benefit, is punished with the penalty from paragraph 1. of this article.
3. When the criminal offense from paragraph 1. or 2. of this article results in financial gain that exceeds the amount of five thousand (5,000) Euros, the perpetrator is sentenced to imprisonment from six (6) months to (5) five years

Article 327

Access to Computer Systems

Anyone who without authorization and with the intention of unlawfully obtaining material benefit for himself or another person or causing damage to another person, changes, publishes, deletes, destroys or destroys data or computer programs or in any other way accesses another's computer system, shall be punished by a fine and imprisonment of up to (3) three years.

If the criminal offense from paragraph 1. of this article results in financial gain exceeding the amount of ten thousand (10,000) Euros or in material damage exceeding the amount of ten thousand (10,000) Euros, the perpetrator shall be punished with a fine and imprisonment of six (6) months. up to five (5) years. (Kosovo Criminal Code)

3.8. Law on the Prevention and Combating of Cybercrime

Article 1

Purpose

This law aims to prevent and fight cybercrime with concrete measures, prevent, detect and sanction violations through computer systems, offering respect for human rights and protection of personal data.

Article 9

Criminal Offenses Against the Confidentiality, Integrity and Availability of Data of Computer Systems

1. Illegal access to computer systems is a criminal offense and its perpetrator is punished with imprisonment from six (6) months to three (3) years.
2. When the criminal offense from paragraph 1 of this article is committed for the purpose of obtaining computer data, the perpetrator shall be sentenced to imprisonment of six (6) months to four (4) years.
3. When the criminal offense from paragraphs 1 and 2 of this article is committed by violating the security measures of computer systems, the perpetrator is punished with imprisonment of three (3) to five (5) years.

Article 10

Interception Without Authorization

1. The unauthorized interception of non-public transmissions of computer data, from, to, in, or within a computer system, is a criminal offense and its perpetrator is punished with imprisonment of six (6) 4 months to three (3) years. If it is committed by a member of a criminal organization, its leader is punished with imprisonment of one (1) to five (5) years.
2. The unauthorized interception of electromagnetic emissions from computer systems, which hold non-public computer data, is a criminal offense and its perpetrator is punished with imprisonment of one (1) to five (5) years.

Article 11

Unauthorized Transfer

1. Changing, erasing, destroying computer data or limiting them without authorization is a criminal offense and its perpetrator is punished with imprisonment of one (1) to three (3) years.
2. The unauthorized transfer of data from computer systems is a criminal offense and its perpetrator is punished with imprisonment of three (3) to five (5) years.
3. The unauthorized transfer of data from their database with computer systems is a criminal offense and its perpetrator is punished with imprisonment of three (3) to five (5) years.

Article 12

Impeding the Operation of Computer Systems

Serious obstacles to the functioning of computer systems, by entering information, transferring, changing, erasing or destroying computer data or by limiting unauthorized access to such data, is a criminal offense and the perpetrator is punished with imprisonment of three (3) months to three (3) years. If it is committed by a member of a criminal organization, its leader is punished with imprisonment of one (1) to five (5) years.

Article 13

Unauthorized Production, Possession and Attempt

1. The production, sale, importation, distribution or offering available in any form, without right, of a device or computer program designed and adapted for the purpose of committing any criminal offense, shall be punished by imprisonment of one (1) up to four (4) years.
2. Producing, selling, importing, distributing or making available, in any form, without right, password, access code or other computer data that allow full or partial access to the computer system for the purpose of performing any criminal offense is punishable by imprisonment of one (1) to five (5) years.
3. Possession, without right, of the device, computer program, password, access code or computer

data for the purpose of committing any criminal offense, is punishable by imprisonment of one (1) to six (6) years.

4. The leader, for attempting to commit the criminal offense, according to paragraph 2 or 3 of this article, is punished with imprisonment from three (3) months to one (1) year.

Article 14

Criminal Offenses Related to Computers

1. Entering information, changing or erasing computer data without authorization or restricting access to such data without authorization, resulting in inauthentic data, with the purpose of using them to acquire a right, is an offense criminal offense and its perpetrator is sentenced to imprisonment from six (6) months to three (3) years. If it is committed by a member of a criminal organization, it is punishable by imprisonment of one (1) to five (5) years.
2. For attempts to commit a criminal offense, according to this article, the perpetrator is sentenced to imprisonment from three (3) months to one (1) year. (Law No. 03/L-166 on the Prevention and Combating of Cybercrime)

3.9. Cases of Cybercrimes in Kosovo

In the table provided by the Police, you can see the enormous increase in identity theft and access device cases in 2022, compared to 2021.

Also, based on the data, the situation is also alarming in terms of breaking the computer systems.

While the violation of the secrecy of correspondence and databases, in the aspect of official presentation, has significantly decreased during 2002 compared to the previous year.

Cases of cybercrimes	**2021**	**2022**
199 Violation of confidentiality of correspondence and computer databases	17	2
327 Introduction to Computer Systems	189	131
336 Identity Theft and Access Device	19	38

Source: (Nacionale, 2022)

4. Conclusion

Cybercrimes are among the most frequent problems that a person can face in everyday life. These problems are increasing with the development of technology and the use of social networks.

Usually, the perpetrators of these computer crimes carry out these crimes for personal interests. Persons as young as 12 years old can also be perpetrators of computer crimes, who from a different country can cause a crime in a completely different country, therefore the risk from these types of crimes can be diverse. What is needed to commit computer crimes may only be the need for a computer or a simple device and access to the Internet through that device.. It should be noted that the detection and prevention of hacking and cyber crimes has become difficult and has become a field problematic. In conclusion, we concluded that this type of criminality, unlike other crimes, has a very high risk because it uses the Internet as a weapon through which it can be accessed and cause every possible consequence, both individual and state.

References

1. *BotaNdryshe*. (n.d.). Retrieved from https://botandryshe.wordpress.com/(2015)/04/25/krimet-kibernetike-dhe-klasifikimi-i-tyre/.

2. Gabela, O., Maloku, A. (2022). Genocid: osnovni aspekti u poimanju, shvatanju i istraživanju zločina. Univerzitet u Sarajevo. Institut za istraživanje zločina protiv čovječnosti i međunarodnog prava. Sarajevo.

3. Gabela, O., Maloku, A. (2023). Genocid: fundamental aspects of understanding, comprehending and investigating crime. University of Sarajevo: Institute for Research on Crimes against Humanity and International Law. Sarajevo.

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

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

6. *CybercrimeStatistics*. (2022, February 15). Retrieved from 73 Important Cybercrime Statistics: 2021/2022 Data Analysis & Projections - Financesonline.com.

7. Dennis, M. A. (2022, december 15). *Britannica*. Retrieved from https://www.britannica.com/topic/cybercrime.

8. Kodi Penal i Republikes se Kosoves. (2019, January 14). *Gazeta zyrtare e Republikës së Kosovës*. Retrieved from https://gzk.rks-gov.net/ActDetail.aspx?ActID=18413.

9. Ligji Nr. 03/L-166 Për Parandalimin dhe Luftimin E Krimit Kibernetikë. Gazeta Zyrtare e Republikës së Kosovës / Prishtinë: Viti V / Nr. 74 / 20 Korrik 2010.

10. *Ligji nr.03/L-166 Per parandalimin dhe luftimin e krimeve kibernetike.* (2022).

11. Maloku, A. & Maloku, E. (2020). SOCIOLOGICAL PERSPECTIVE OF SUICIDES / Sociological Perspective of Suicides. Uluslararası Ekonomi İşletme ve Politika Dergisi , 4 (2) , 319-334 . DOI: 10.29216/ueip.784154.

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

13. Maloku, A. (2015b). 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.

14. Maloku, A. (2015c). *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.

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

16. Maloku, A. ., Qerimi, I. ., & Maloku, E. . (2022). The Scope of Crime by Social Origin in the Region of Gjilan. Academic Journal of Interdisciplinary Studies, 11(4), 172. https://doi.org/10.36941/ajis-2022-0107.

17. Maloku, A., Kastrati, S., Gabela, O., & Maloku, E. (2022). Prognostic scientific research in planning and successful management of organizations in the security sector. Corporate & Business Strategy Review, 3(2), 138–150. https://doi.org/10.22495/cbsrv3i2art12.

18. 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.

19. Maloku, Ahmet. (2016b) Medunarodna saradnja u borbi protiv transnacionalnog organizovanog kriminala. Universitet u Travniku. Pravni Fakultet. Travnik. Bosna i Hercegovina.

20. Maloku, Ahmet. (2018). Drustvena dezorganizacija i obiljezja kriminaliteta na podrucju regije Gnjilane (Kosovo) u periodu 2010-2014. Univerzitet u Sarajevu: Fakultet za kriminalistiku, kriminologiju i sigurnosne studije. Sarajevo.

21. Maloku, Ahmet. (2021). "DEVIANT BEHAVIOR OF JUVENILE DELINQUENTS" (2021). UBT International Conference. 76. https://knowledgecenter.ubt-uni.net/conference/2021UBTIC/all-events/76.

22. 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.

23. *Nacionale*. (2022). Retrieved from https://nacionale.com/drejtesi/sulmet-kibernetike-rriten-ne-kosove-cak-kryesisht-mediet-ekspertet-alarmojne-per-gjendjen.

24. NathansInvestigation. (n.d.). *NathansInvestigation*. Retrieved from https://www.nathans-investigations.com/cyber-crime-investigations/

25. Qerimi, I. ., Kastrati, S. ., Maloku, A. ., Gabela, O. ., & Maloku, E. . (2023). The Importance of Theory and Scientific Theories for the Scientific Study of Genocide in the Context of the Contribution to the Development of the Science of Genocide. *Academic Journal of Interdisciplinary Studies*, *12*(1), 183. https://doi.org/10.36941/ajis-2023-0016.

26. Qerimi, I., Maloku, A., & Maloku, E. (2022). Customary law and regulation: Authenticity and influence [Special issue]. *Journal of Governance & Regulation, 11*(4), 289–299. https://doi.org/10.22495/jgrv11i4siart9.

27. Shabani, Alisabri, Maloku, Ahmet. (2019a). Sociologjia.. Kolegji Iliria, Prishtinë.

28. Shabani, Alisabri, Maloku, Ahmet. (2019b). Tema te zgjedhura nga Patologjia Sociale. Kolegji Iliria, Prishtinë.

29. *Timesheet*. (2022, 02 16). Retrieved from Timesheet time tracking - track working time on computer (neuber.com).

30. Vula, V. (n.d.). *PDFSLIDE*. Retrieved from https://pdfslide.net/documents/kriminaliteti-kompjuterik.html?page=2.

Copyrights