This journal provides immediate open access to its content under the Creative Commons BY 4.0 license. Authors who publish with this journal retain all copyrights and agree to the terms of the above-mentioned CC BY 4.0 license.

DOI: 10.2478/seeur-2023-0065

DIGITAL FORENSICS AND COMPUTER CRIMES: THE CASE OF NORTH MACEDONIA

Deshira Imeri-Saiti
Faculty of Contemporary Sciences and Technologies,
South East European University, North Macedonia
d.imeri@seeu.edu.mk

Mentor Hamiti
Faculty of Contemporary Sciences and Technologies,
South East European University, North Macedonia
m.hamiti@seeu.edu.mk

ABSTRACT

The subject of the research refers to the aspect of digital forensics and computer crime and the latter is one of the reasons for the evolution of crime in general. Based on the growing trend of technology development and the increase in the number of digital crimes, a special emphasis is given to the statistical aspect of computer crime as well as measures to reduce the impact of computer crime, including the ethical and legal aspects in the Republic of North Macedonia (RNM).

To conduct this research, statistical data on computer crime in RNM from 2011 to 2020 were used, based on historical data of analysis, as well as comparison, correlation, and the ANOVA-test.

The highest number of crimes were registered in 2020 and a special feature is that a positive linear trend can be observed during the last decade. “Damage and unauthorized access to a computer system” took the first place in computer crimes according to the Criminal Procedure Law.

Key words: Digital forensic, Computer crime, Ethics, Law, North Macedonia.

INTRODUCTION

Digital forensics is causing a massive collision between two seemingly solid forces: the legal system and forensics that operate at a relatively slow and deliberate pace against the "blinding" speed of technology (Sammons, 2012). According to Internet Live Stats (2021), there are almost 3.5 billion Internet users in the world as of August 2016, covering nearly 46.1% of the world's population. Therefore, it can be assumed that cybercrime has evolved since the reporting of cybercrime incidents began, both with the collection of evidence from computers and with the increase in access to the Internet. Digital forensics according to Arnes (2018) is becoming increasingly important with the escalation of cybercrime and serious network-related crimes, where understanding the laws and regulations governing electronic communications, computer crimes, and data storage requires the continuous acquisition of new knowledge, methods, and tools. It is therefore critical that computer science and security students acquire a fundamental understanding of digital forensics, participate in public debates, and act as experts in a legal context.

Digital forensics is a new science, and the fact that this science deals with rapid changes in the computing environment, on the other hand, affects its scope in many disciplines (such as the legal system, law enforcement, business management, information technology and the nature of limit of the Internet) make it a very challenging field that requires continuous development of methodologies and tools to counter the ever-new changes of cybercrime (Hassan, 2019). In recent years, electronic exchanges have activated businesses and facilitated communication exponentially; however, they have also made the same information susceptible to a host of criminal activities, where the activity that has arisen due to developments in the use of network technology has caused billions of dollars in damages to governments and private industry (Zakaras, 2001). The United Nations (2021) draft resolutions on various aspects of cyber security have for the first time been forwarded to the United Nations General Assembly by its three main committees (Committee on Disarmament and International Security; Economic and Financial Committee; and the Social, Humanitarian and Cultural Committee). Perhaps the most important developments have been made in the Committee on Disarmament and International Security, which can be considered a unique forum for major “players” such as the US, China, and Russia to discuss the “high end” of threats to information security (ccdcoe.org, 2021).

The process of digital forensics investigations, as recommended by experts, should be carried out by specialist persons, who have a completely unbiased approach to ensure the credibility and image of the organizations where the investigation will be carried out (Horsman, et al., 2012). According to Hassan (2019), digital forensics is categorized into relevant types, namely: computer forensics, mobile forensics, network forensics, database forensics, and data analysis forensics.

One of the main priorities of the Republic of North Macedonia, as well as of other national entities, is to stimulate and guarantee cyber security in the future. In this research, a special focus has been given to the statistical aspect of computer crime, as well as measures to reduce the impact of computer crime and the ethical and legal aspects of RNM. Based on theoretical approaches and empirical literature on the impact of computer crime in local society, individual assumptions have been formulated. First, assumptions are made about average computer crime rates by cities and the Department of the Interior, starting with the state capital and other cities. The analysis continues with assumptions of means and variances by gender and age and analysis of age in a cumulative manner. From the comprehensive approach of digital forensics, the research aims to examine the statistical evidence of computer crime in the Republic of North Macedonia.

ETHICAL AND LEGAL ASPECTS IN COMPUTER FORENSICS

According to Gogolin (2021), technological developments in digital forensics occur at a high speed, where private sector digital forensics investigators must contact law enforcement and develop a collaboration because sooner or later the two paths will intertwine. Digital forensics systems collect, filter, process, store, and distribute data to facilitate the investigative-organizational decision-making process. These specialized systems are used to locate and understand the specifics of electronic incidents. Because it is a new discipline, other contributing factors must be considered because these systems violate and challenge many norms that have become acceptable to both individuals and organizations (Balogun & Zuva, 2017). Digital forensics investigations potentially have an ethical effect on any decision made. This means that the digital investigator has the option to decide which evidence to investigate, validate, and decide on the depth of analysis in any particular situation, but it must be remembered that the investigator has an obligation, and if neglects such a duty, they may face the possibility of taking legal action against them (Ironis & Konstadopoulou, 2007).

Some of the legal issues surrounding attribution are discussed, and it is argued that well-defined international cyberspace laws together with strong cooperation between governments are needed to find and punish cybercriminals. Ethics, according to Nelson, et al. (2019) are the rules we adhere to and use to measure our performance; standards that others apply to us, rules (codes) of conduct, or professional responsibilities. Most criminologists work in forensic science laboratories associated with law enforcement or other government agencies that have codes of ethics developed specifically for their organizations, whereas codes of ethics developed for prosecutorial agencies address those areas of professional conduct that are important to most people (Barnett, 2001). The Council of the European Commission is the first institution that develop the ethical certification of hackers (C|EH program), where the purpose of this program is to learn the methodologies, tools, and techniques used by hackers, using the collective knowledge of hundreds of subject matter experts. The program has quickly gained popularity across the globe and is now offered in more than 70 countries by more than 450 authorized training centers, and more than 60,000 information practitioners have been trained in this context (EC-Council, 2010).

The analysis can predict legislative and political controversies that will weigh citizens' rights to privacy and autonomy against the state's needs for national security and public safety (Losavio et al., 2018). Current issues arising from the development and implementation of digital forensics systems direct future research to focus on addressing the concerns they present for the well-being of a society, such as fear of unpredictability, breach of privacy, exploitation of tools, commercial motives, and of market segmentation, standardization of practices and inadequate education and training outcomes (Balogun & Zuva, 2017).

DIGITAL FORENSIC AND CODE OF ETHICS

The responsibility of the digital forensics professional regulation is left into the hands of various certification entities or professional digital forensic societies (Sharevski 2015). Starting from this point of view according to Nelson, et al. (2019) the International Society of Computer Forensic Examiners (ISFCE) code of ethics and professional responsibility guides its members, while the International Association of Computer Forensic Specialists (IACIS) has a well-defined and simple guide to the expected behavior of forensic experts.

According to Sharevski (2015), organizations related to the practice of digital forensics codes of ethics are the American Academy of Forensics (AAFS); American Board of Criminal Investigation (ABC); American Society for Digital Forensics and e-Discovery (ASDFD);

California Association of Criminalists (CAC); Consortium of Digital Forensics Specialists (CDFS); Cyber Security Institute (CI); Digital Forensics Certification Board (DFCB); EC Council (ECC); High Technology Crime Investigation Association (HTCIA); International Association of Computer Investigation Specialists (IACIS); The SANS Institute (SANS) and the International Society of Computer Forensic Examiners (ISFCE). Forensic experts must be careful of the basic rules of professional conduct that they must follow. They must still follow the model code of professional responsibility and model rules of professional conduct which are the basic codes of ethics of digital forensics (Nelson, et al., 2019).

EU laws focus on the common issues of protecting privacy and ensuring the reliability of evidence and results, while on the other hand, the Fourth Amendment of the US Constitution prohibits unreasonable searches or seizures of the state that are contrary to law when without any probable cause of a crime, violates the privacy of citizens (Losavio et al., 2018). Pfleeger (2015) points out that with greater power comes greater responsibility. This concept also applies to today's times, where new technologies, governments, and regulatory bodies can intervene to impose structure, guidelines, standards, or penalties on safety practices. However, interventions that sound perfect in theory do not always work well in practice.

METHODOLOGY

Statistical data on criminal offenses from computer crimes in the Republic of North Macedonia (RNM) have been provided by the database of the Ministry of Internal Affairs (MIA), for the period from 2011 to 2020. In the following table (Tab. 1) the types of computer crime in the country in compliance with the relevant "articles" from the Criminal Code (CC) of the Republic of North Macedonia have been introduced.

Table 1: Map of computer crimes

LEGAL CRIMINATION FROM THE CRIMINAL CODE OF THE REPUBLIC OF NORTH MACEDONIA	
Articles	Types of Computer Crimes
article. 144, p.4	Security risk
article. 149, p.2	Abuse of personal data
article. 157, p.2	Violation of copyright and related rights
article. 157-a	Violation of the distributor's right
article. 157-b	Audiovisual piracy
article. 157-v	Pirate phonogram
article. 193	Display of child pornography
article. 193-a	Production and distribution of child pornography through a computer system
article. 193-b	Reduction of sexual harassment of children under the age of 14
article. 251	Damage and unauthorized access to a computer system
article. 251-a	Creating and importing a computer virus

article. 251-b	Computer fraud
article. 271, p.3	Creating, receiving, or alienating counterfeit funds
article. 394-g	Distribution of racist and xenophobic material through a computer system
article. 274-b	Making and using a false payment card
article. 379-a	Computer forgery

Source: Ministry of Internal Affairs (MIA) of the Republic of North Macedonia

Criminal offenses from computer crimes for the year 2011 in RNM according to the Criminal Procedure Law (CPL) are articles: 251, 251-b, and 379-a, while in 2011 no criminal offense was found according to article 274-b of the Criminal Procedure Law. For the year 2012, there is data on computer criminal offenses for articles of the criminal law: 251, 251-b, and 274-b, while for article 379-a, namely computer forgery, no data of the corresponding criminal offense was found. The following criminal offenses were registered in 2013 for the relevant articles according to (LCP): 251, 251-b, 274-b, and 379-a. For the same articles according to the Criminal Procedure Law, legal violations have been registered, but the same data provided to the Ministry of Internal Affairs are structured according to the Internal Affairs Sectors (IAS) and according to the following criteria: the number of perpetrators, the number of offenses recorded criminal, gender and age. According to the (IAS) and the above criteria, data were also provided for the year 2015. For the year 2016, data were provided for the perpetrators and criminal offenses according to the (IAS) articles: 251, 251-b, 193-a, 149, 271, and 274-b. During the years 2017 to 2020, the data of all the relevant articles of the (IAS) have been secured from the map of computer crimes.

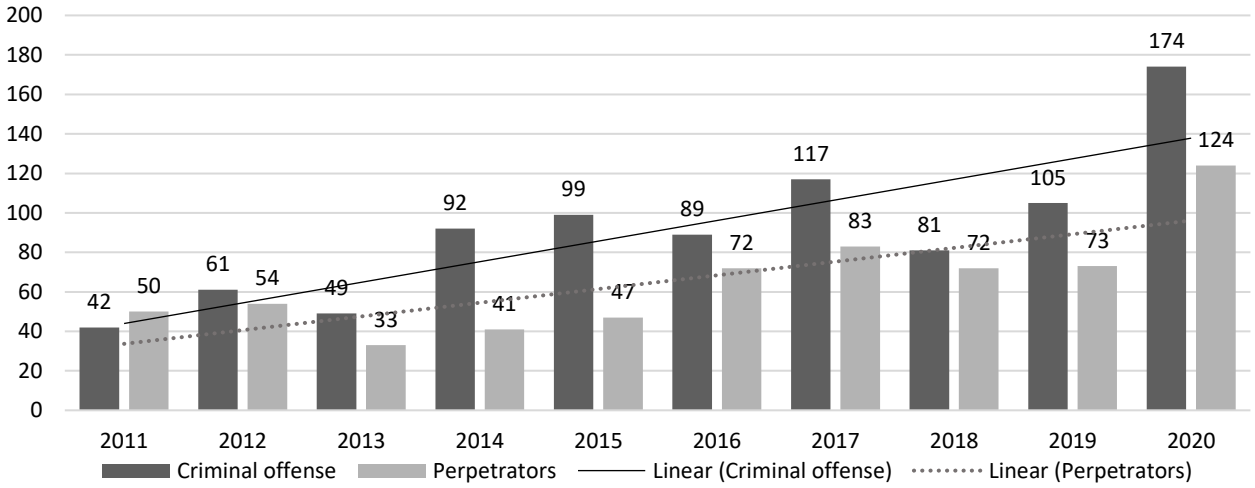
The structure of the analysis is based on the analogy of the perpetrators of computer crimes and criminal offenses for the period 2011-2020. The analysis continues with the structuring of criminal offenses and perpetrators according to the legal basis and is differentiated into two detailed tables according to the available data on criminal offenses and perpetrators over the years. In continuity, the average of criminal offenses by city (Sectors for Internal Affairs) has been analyzed and the ANOVA test has been used. The last analysis is subjected to research also using the ANOVA test analyzing the means and variances according to gender and age and approaching the analysis with a summary in the form of a cumulative synthesis. Some of the results can be viewed in detail in the appendix of this research paper.

FINDINGS AND DISCUSSION

Below is an analogy and flow of the trend between criminal offenses and perpetrators during the years 2011-2020 in RNM. It is characteristic that during the years of research, the

total number of perpetrators was lower than the total number of criminal offenses. On the other hand, the highest number of criminal offenses (174) and perpetrators (124) was recorded in 2020, while the lowest cumulative number was recorded in 2013, in total 82. A special feature is that a linear trend is observed during the years of the research, also that the flow of the movement of the positive trend of criminal offenses is higher than the flow of the positive trend of perpetrators of computer crimes in RNM (Chart 1).

Chart 1: Criminal offenses and perpetrators for the period 2011-2020



Source: Ministry of Internal Affairs (MIA) of the Republic of North Macedonia

The causes of the increase in criminal offenses and perpetrators of computer crimes in the country vary. The main factor is technological development, while another determinant is the growth of internet users in RNM during this period. According to data from the World Bank (2021), the number of Internet users (expressed as % of the population) has an increasing trend in RNM, namely starting with (52%) in 2010, (68%) in 2014 and the latest data are for 2018 with (79%).

In the following, a comparison is presented between the criminal offenses of computer crime and the perpetrators according to the legal basis (Chart 2). A greater number of criminal offenses (267) and perpetrators (182) were identified according to Article 251 of the Criminal Procedure Law, namely "damage and unauthorized access to a computer system".

The second legal basis with fewer criminal offenses and perpetrators of computer crimes is according to the legal criterion "reduction of sexual harassment of children under the age of 14", with 230 criminal offenses and 83 persons appearing as perpetrators. The third legal basis is the "distribution of racist and xenophobic material through a computer system" with 112 criminal offenses during the period 2011-2020, with 134 persons being registered as perpetrators. In total, according to criminal offenses and perpetrators of 107 legal violations

and commissions, they were registered under the legal bases “security risk” and “computer fraud”. While 102 criminal offenses and the commission of computer crimes were recorded for the legal criteria: “creating and importing a computer virus” and “making and using a fake payment card”. On the other hand, with fewer legal violations and several perpetrators (with less than 36 registrations), for the years of the research, they were registered according to the legal basis: “production and distribution of child pornography through a computer system”, “abuse of personal data”, “displaying child pornography”, “creating and receiving or alienating counterfeit funds”, and “computer forgery”. “Violation of distributor's right” and “audiovisual piracy” are presented with each (1) criminal offense and the number of the perpetrator. With regard to the “violation of copyright and related rights” on the one hand and “pirated phonogram” on the other hand, no legal violations have been officially registered.

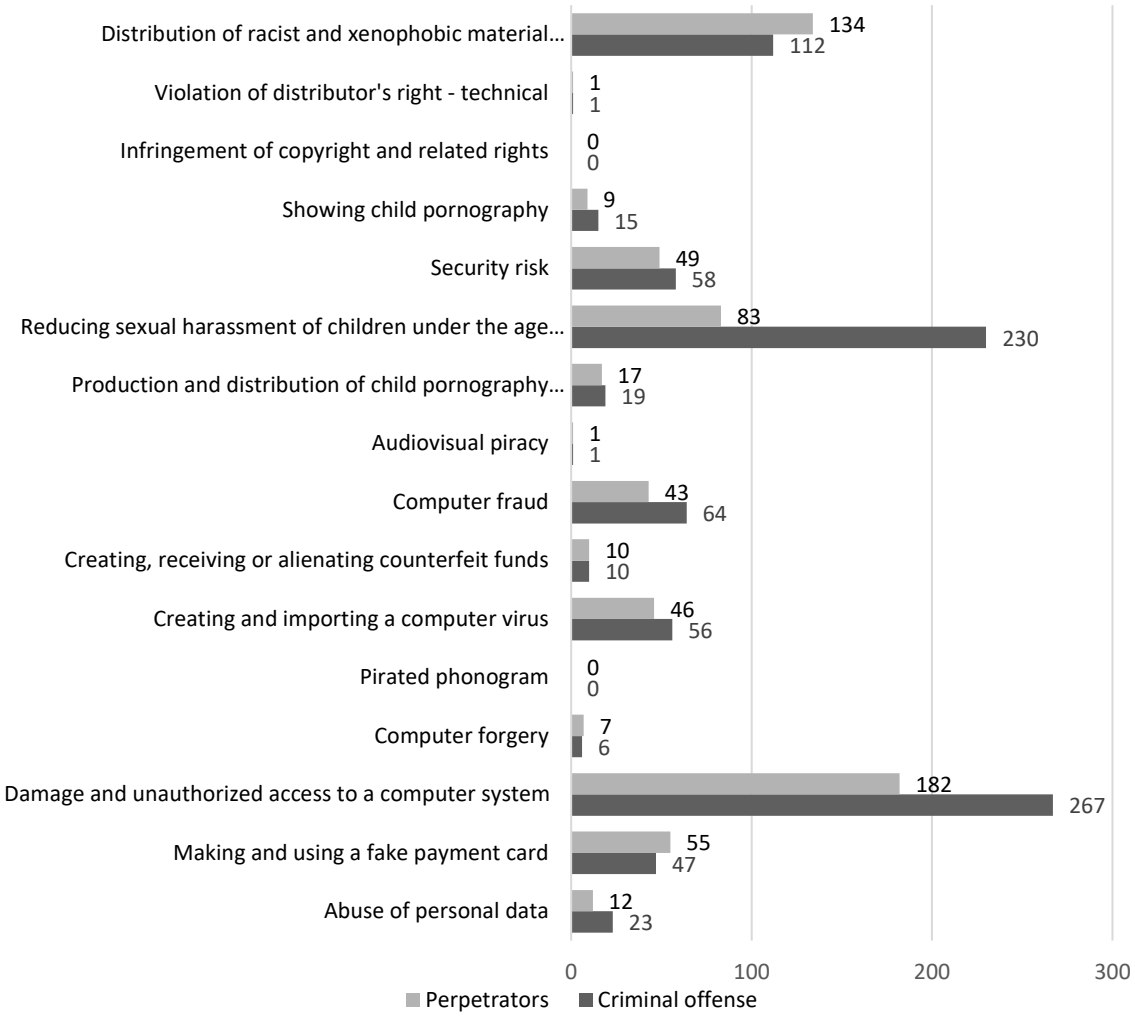
In the detailed analysis of the types of computer crimes in RNM during the period 2011-2020, it is characteristic that the period from 2011 to 2016 witnessed less crimes compared to the period from 2017 to 2020. For that reason, the analysis is decomposed into two analyses for the aforementioned periods. The second factor of such disintegration is also the main determinant that for a large number of types of computer crimes there is no data for the period from 2011 to 2016. The reason for not having data for the years 2011-2016, include: endangering security, abuse of personal data, violation of copyright and related rights, violation of distributor's right, audiovisual piracy, pirated phonogram, display of child pornography and distribution of child pornography through a computer system (Annex, Tab. 2). Other types in the relevant table have low values of computer crimes compared to crimes of their type in the following years (from 2017 to 2020). Except for sexual activities with a child under 14 years of age, in particular, high criminal offenses and the commission of such computer crimes were recorded during the years 2014 and 2015. The second exception during the years 2011-2016 is the distribution of racist and xenophobic material through a computer system which is characterized by an average registration of 21.75 criminal offenses and computer crimes during the years 2015-2016.

Further on (Annex, Tab. 3), it can be noted that the most frequent types of computer crimes in RNM during the period from 2017 to 2020 were:

- Jeopardizing security, with a record of criminal offenses and perpetrators during the years 2019-2020, with an average of about 24 computer crimes per year;
- The abuse of personal data as the most common computer crime appeared in 2020 with 19 criminal offenses;

- Child pornography whose highest incidence was recorded in 2017 with 6 offenses and 9 criminal offenses;
- Production and distribution of child pornography through a computer system - on average, about 6 criminal offenses were registered during the years 2017-2018 and 2020;
- Damage and unauthorized access to a computer system during the period 2017 to 2020 follows an average of about 46 unauthorized violations during a year;
- Computer frauds that were registered during the years 2017-2020 are with an average of about 11 criminal offenses and perpetrators during a year;
- Making and using a false payment card is registered as a criminal offense of the highest level during the years 2017-2018 with an average of about 16 false uses of a payment card during these two years;
- Distribution of racist and xenophobic material through a computer system, with a higher registration during 2020 with an average of around 27 criminal offenses.

Chart 2: Criminal offenses and perpetrators according to legal basis, years 2011-2020



Source: Ministry of Internal Affairs (MIA) of the Republic of North Macedonia

In (Annex, Chart 3) presents the average values of crimes by cities, while in (Annex, Tab. 4) presents criminal offenses according to Internal Affairs Sectors (IAS) during the period 2011-2015.

During the research period, 211 computer crimes were registered in Skopje, a city with the densest population and a population of about 30% of the total national population, and with criminal offenses of computer crime of about 62%. In (IAS)-Skopje, the most ferquent crime is “damage and unauthorized access to a computer system”, for which an average of about 35 crimes were recorded during the research period. The city of Bitola follows, for the 4 years investigated, with 33 computer crimes and 10% of registered criminal offenses; also, the most frequent crime is “damage and unauthorized access to a computer system” with 5 crimes committed. The data on computer crime recorded by the Department of Internal Affairs of the city of Shtip ranks it in third place with 30 recorded crimes and 9% of crimes, with an average

of 4.2 crimes and the most common is "damage and unauthorized access to a computer system." In the city of Strumica, the number of computer crimes is 25 crimes in the 4 years under research, and 7% of registered criminal offenses, also on average about 3.2 unauthorized access to a computer system as the most potentized crime. (IAS)-Ohrid records 18 crimes and 5% of criminal offenses from the total of criminal offenses according to the criterion of diversification by cities. In the city of Ohrid, the crime "damage and unauthorized access to a computer system" occurs on average about 2.2 times in 4 years. (IAS)-Kumanovo is characterized by 12 computer crimes, 4% criminal offenses, and an average of 1.5 unauthorized accesses to a computer system, as well as an average of 1 fraudulent use of a payment card. (IAS)-Veles records 10 crimes, 3% of criminal offenses, and an average of 2 unauthorized accesses to a computer system. (IAS)-Tetovo registers only 1 computer crime, namely the registered crime is “damage and unauthorized access to a computer system”.

To examine whether there are statistically significant differences between the Internal Affairs Sectors in the average number of crimes committed in the period from 2011 to 2015, the ANOVA test is used. The F-Statistics of this test is 6.35 and as such represents statistically significant data, with a significance level of 0.05 (p-value is 0.000). If (IAS)-Skopje is excluded from the analysis, as a sector with the highest average rate of crimes committed, the F-statistic is 2.23 and is again statistically significant at the same level of significance (p-value is 0.044).

From the total number of persons reported in the period 2011-2015, 88% (or 215 persons) are male and 12% (or 28 persons) are female (Annex, Tab. 5 & Chart 4). The participation of computer crimes committed by men of the opposite sex is in a ratio of 3 to 1, although this does not correspond to the natural structure of the number of the opposite sex during the years 2011-2020 in RNM. According to the reports of the World Bank (2021) during the years 2011-2020 in RNM, the average female population was 1,038,607 inhabitants, while the male population amounted to 1,039,376 inhabitants, whereupon it can be seen that the natural ratio is equal while regarding the reports of computer crimes, males predominate three times more than females in RNM during the research period.

Regarding age, the majority of people registered in the mentioned period are between 25 and 29 years old, followed by persons aged 18-24 years (Annex, Tab. 6 and Chart 5). The most common computer crimes committed by people between the ages of 25-29 are damaging and unauthorized access to a computer system, with 14 crimes committed during 2011, and using a fake payment card - 10 crimes during 2012. People aged 18 - 24-year-olds committed

at most 12 damage and unauthorized access to a computer system during 2012 and 10 crimes of using a fake payment card in 2014.

If we observe the cumulative percentages (Annex, Tab. 7), slightly more than 58% of the persons reported in the observation period are under 30 years old. In the third place, according to the average percentage of a participant in computer crimes is the age group of 30-40 years, with participation of (15.2%) which is characteristic because, with the preliminary cumulative of ages under 30 years old, they make up approximately 73% of the total of computer crimes in RNM for the research period. The differences in the average values of the number of registered persons according to gender and age are statistically significant at the significance level of 0.05. The F-statistics of the ANOVA test performed are 13.66 and 5.98, respectively for gender and age, where the p-value in both cases is equal to zero.

CONCLUSIONS

Based on the conducted research, it can be concluded that the highest number of criminal offenses (174) was recorded in 2020, while a special characteristic is that a positive linear trend can be observed during the last decade. In addition, the largest number of computer crimes according to the Criminal Procedure Law are: “damage and unauthorized access to a computer system” with 267 criminal offenses, and “sexual harassment of a child under 14 years old”, with 230 criminal offenses.

The most frequent types of computer crimes in RNM during the period from 2017 to 2020 were: endangering security; abuse of personal data; damage and unauthorized access to a computer system, which during the period from 2017 to 2020 follows an average of about 46 unauthorized violations during a year, as well as computer fraud that has been recorded has an average of about 11 criminal offenses during a year.

During the period 2011-2015, 211 computer crimes were registered in Skopje, where the most expressed crime is “damage and unauthorized access to a computer system”, as well in all cities in RNM. As for the reports of computer crimes, males predominate three times more than females during the research period in RNM. In terms of age, the majority of persons registered in the mentioned period is between 25 and 29 years old, followed by persons aged 18-24 years. According to cumulative percentages, slightly more than 58% of persons reported in the observation period are under 30 years old.

It is nearly impossible to estimate the amount of cybercrime that occurs in most nations around the world due to the lack of standardized legal definitions for these crimes and few valid

and reliable official statistics (Holt & Bossler, 2016). According to the Global Cyber Security Index in Europe (2017), which presents an analysis of cybersecurity for the European region, RNM ranks at the average level. of the index in question includes the following pillars: Legal Measures: based on the existence of legal institutions and frameworks dealing with cyber security and cybercrime (low level); Technical Measures: based on the existence of technical institutions and frameworks dealing with cyber security (low level); Organizational Measures: based on the existence of policy and strategy coordination institutions for the development of cyber security at the national level (medium level); Capacity building: based on the existence of research and development, educational and training programs, certified professionals and public sector agencies promoting capacity building (high level), and Cooperation: based on the existence of partnerships, cooperative frameworks, and information exchange networks (high level).

REFERENCE

1. Arnes, A. (2018). Digital Forensics. John Wiley & Sons Inc.
2. Balogun, A. M., & Zuva, T. (2017). Open Ethical Issues In Digital Forensic Systems. International Journal of eBusiness and eGovernment Studies. Vol 9, No 1.
3. Barnett, P. D. (2001). Ethics in Forensic Science: Professional Standards for the Practice of Criminalistics. Boca Raton, FL: CRC Press.
4. ccdcoe.org. (2021), 06 22). ict4peace.org, ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf. Accessed 06 22, 2021 [Online] Available at: https://ict4peace.org/wp-content/uploads/2012/08/Eneken-GGE-2012-Brief.pdf
5. EC-Council. (2010). Investigating Data and Image Files. Cengage Learning.
6. Gogolin, G. (2021). Digital Forensics Explained. CRC Press.
7. Hassan, N. A. (2019). Digital Forensics Basic. New York: Apress.
8. Horsman, G., Laing, C., & Vickers, P. (2012). A case-based reasoning framework for improving the trustworthiness of digital Forensic Investigations. 11th International Conference on Trust, Security, and Privacy in Computing and Communications. IEEE.
9. Internet Live Stat. (2021). Live Stat. Accessed 06 21, 2022 [Online] Available at: https://www.internetlivestats.com/internet-users/#trend
10. Ironis, A. D., & Konstadopoulou, A. (2007). Professionalism In Digital Forensics. EC2ND 2006, Springer. London.
11. Losavio, M. M., Chow, K. P., Koltay, A., & James, J. (2018). The Internet of Things and the Smart City: Legal Challenges with Digital Forensics, Privacy, and Security. Special Issue Article, Security and Privacy.
12. Nelson, B., Phillips, A., & Steuart, C. (2019). Guide to Computer Forensics and Investigations: Processing Digital Evidence. 2019, 2016 Cengage Learning, Inc.
13. Sammons, J. (2012). Forensics, The Basics of Digital: the primer for getting started in digital forensics. Syngress is an imprint of Elsevier.
14. Sharevski, F. (2015). Rules of professional responsibility in digital forensics: A comparative analysis. Journal of Digital Forensics, Security and Law, Vol. 10, No. 2. Article 3.
15. United Nations. (2021). United Nations. Accessed 06 22, 2021 [Online] Available at: https://ccdcoe.org/organisations/un/
16. Zakaras, M. (2001). Revue internationale de droit pénal. International computer crimes. General report, 3(3-4), 813-829.
17. Pfleeger, S. L. (2015). Spider-Man, Hubris, and the Future of Security and Privacy. IEEE Computer and Reliability Societies.

18. World Bank. (2021). worldbank.org. Accessed 03 19, 2021 [Online] Available at: https://data.worldbank.org/country/MK

19. Holt, T. J., & Bossler, A. M. (2016). Cybercrime in Progress: Theory and Prevention of Technology-Enabled Offenses. New York: Routledge.

20. Global Cyber Security Index in Europe. (2017). itu. int. itu.int/en/ITU-D/Cybersecurity/Documents/EUR_GCIv2_report.pdf. Accessed 03 22, 2021 [Online] Available at: https://www.itu.int/en/ITU-D/Cybersecurity/Documents/EUR_GCIv2_report.pdf

ANNEX

Table 2: Types of computer crimes in the period 2011-2016

Legal basis	2011		2012		2013		2014		2015		2016		**TOTAL**	
	Criminal offense	Perpetrators	Criminal offense	Perpetrators	Criminal offense	Perpetrators	Criminal offense	Perpetrators	Criminal offense	Perpetrators	Criminal offense	Perpetrators	Criminal offense	Perpetrators
Reducing sexual harassment of children under the age of 14	0	0	47	29	31	14	74	16	76	22	0	0	**228**	**81**
Damage and unauthorized access to a computer system	36	43	0	0	0	0	0	0	0	0	0	0	**36**	**43**
Creating and importing a computer virus	0	0	1	2	7	5	4	1	4	5	40	33	**56**	**46**
Computer fraud	5	6	0	0	0	0	0	0	0	0	8	3	**13**	**9**
Creating, receiving, or alienating counterfeit funds	0	0	0	0	0	0	0	0	0	0	7	7	**7**	**7**
Making and using a fake payment card	0	0	0	0	1	1	1	0	1	0	7	6	**10**	**7**
Computer forgery	1	1	0	0	0	0	0	0	0	0	1	0	**2**	**1**
Distribution of racist and xenophobic material through a computer system	0	0	13	23	10	13	13	24	18	20	26	23	**80**	**103**
TOTAL	**42**	**50**	**61**	**54**	**49**	**33**	**92**	**41**	**99**	**47**	**89**	**72**	**432**	**297**

Table 3: Types of computer crimes in the period 2017-2020

Legal basis	2017		2018		2019		2020		**TOTAL**	
	Criminal offense	Perpetrators	Criminal offense	Perpetrators	Criminal offense	Perpetrators	Criminal offense	Perpetrators	Criminal offense	Perpetrators
Security risk	3	1	5	2	21	22	29	24	**58**	**49**
Abuse of personal data	1	1	1	1	2	0	19	10	**23**	**12**
Infringement of copyright and related rights	0	0	0	0	0	0	0	0	**0**	**0**
Violation of distributor's right - technical	0	0	0	0	1	1	0	0	**1**	**1**
Audiovisual piracy	0	0	0	0	0	0	1	1	**1**	**1**
Pirate phonogram	0	0	0	0	0	0	0	0	**0**	**0**
Showing child pornography	9	6	0	0	2	1	4	2	**15**	**9**
Production and distribution of child pornography through a computer system	7	5	4	6	2	1	6	5	**19**	**17**
Reducing sexual harassment of children under the age of 14	0	0	2	2	0	0	0	0	**230**	**83**
Damage and unauthorized access to a computer system	70	40	43	34	53	28	65	37	**267**	**182**
Creating and importing a computer virus	0	0	0	0	0	0	0	0	**56**	**46**
Computer fraud	12	3	13	12	14	10	12	9	**64**	**43**
Creating, receiving, or alienating counterfeit funds	2	2	1	1	0	0	0	0	**10**	**10**
Making and using a fake payment card	13	25	12	14	4	2	8	7	**47**	**55**
Computer forgery	0	0	0	0	1	3	3	3	**6**	**7**
Distribution of racist and xenophobic material through a computer system	0	0	0	0	5	5	27	26	**112**	**134**
TOTAL	**117**	**83**	**81**	**72**	**105**	**73**	**174**	**124**	**909**	**649**

Chart 3: Criminal offenses by city

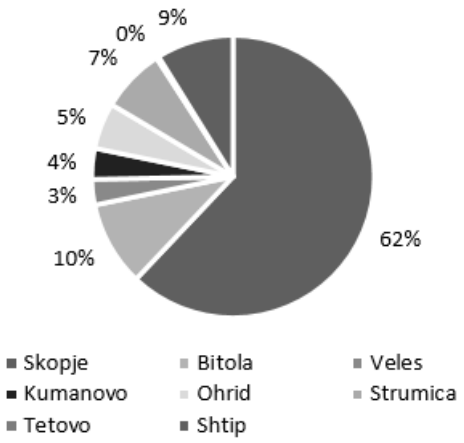


Table 4: Average number of crimes by Internal Affairs Sector, 2011-2015

Groups	*Sum*	*Average*	*Variance*
Skopje	211	10.6	278.1
Bitola	33	1.7	4.8
Veles	10	0.5	1.0
Kumanovo	12	0.6	0.8
Ohrid	18	0.9	1.5
Strumica	25	1.3	6.9
Tetovo	1	0.1	0.1
Shtip	30	1.5	6.1

Chart 4: Participation of reported persons by gender

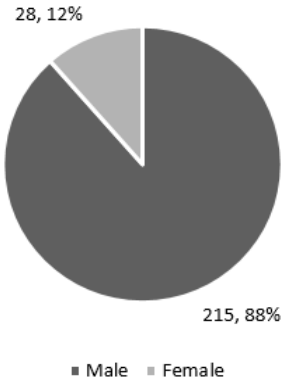


Table 5: Persons reported by gender

Groups	*Sum*	*Average*	*Variance*
Male	215	10.8	124.0
Female	28	1.4	4.0

Table 6: Persons reported according to age

Groups	*Sum*	*Average*	*Variance*
minors	13	0.65	2.03
from 18-24 years old	55	2.75	11.25
from 25-29 years old	59	2.95	15.00
from 30-34 years old	37	1.85	6.13
from 35-39 years old	24	1.2	3.54
from 40-44 years old	16	0.8	2.17
from 45-49 years old	11	0.55	1.63
from 50-54 years old	8	0.4	0.67
from 55-59 years old	3	0.15	0.13
from 60-64 years old	4	0.2	0.17
over 65 years old	0	0	0.00

Chart 5: Participation of persons reported by age

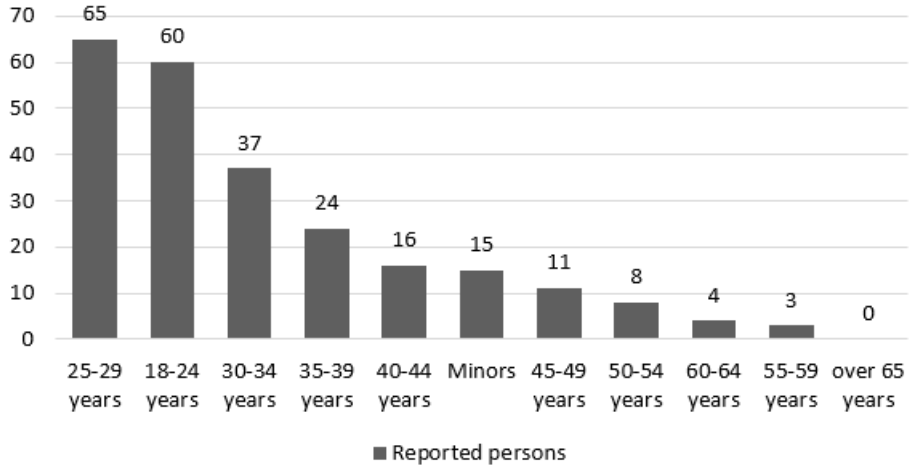


Table 7: Persons reported by age (%-cumulative)

Age	*%*	*%-cumulative*
Minors	6.2	6.2
18-24 years	24.7	30.9
25-29 years	26.7	57.6
30-34 years	15.2	72.8
35-39 years	9.9	82.7
40-44 years	6.6	89.3
45-49 years	4.5	93.8
50-54 years	3.3	97.1
55-59 years	1.2	98.4
60-64 years	1.6	100.0
over 65 years	0.0	100.0