UDC: 343.98.068
Review paper
Recived: July 15, 2019.
Acceptee: August 04, 2019
Coreresponding author: Ratomir Antonović
e-mail: centardba@gmail.com

MODERN FORMS OF HIGH-TECH FRAUD IN THE FUNCTION OF MONEY LAUNDERING

Ana Matović[1] , Ratomir Antonović[2], Nataša Tošić[3]

[1]College of Economics Pec-Leposavic (CEPL), ana matovic.anna@gmail.com
[2] Faculty of Law, Security and Management Konstantin Veliki Niš, centardba@gmail.com
[3]Faculti of Law, Univerziti in Travnik, advokattosic@gmail.com

Abstract: *Modern technological resources, availability of modern technology and rapid progress in the field of high technology, have enabled its wide distribution and usability. Today almost no households exist in almost all parts of the world, where there is not even one PC, as well as other related technological equipment. Consequently, given these facts, there are more and more cases of abuse of modern technological tools, which are becoming more and more popular with criminal organizations, which recognize the advantages of this modern equipment. Technical and technological frauds, which are the subject of this paper, are used to secure unlawfully acquired material benefits, which then, through money laundering, invest in various legal affairs. Many cases of computer fraud, money theft, the abuse of plastic money, bank fraud, which resulted in huge material losses from one, and the acquisition of unlawful property gain on the other side, have been discovered. Prewar are mainly used by younger and technically literate people from the poorer parts of the world, who are highly ranked by education. Their profile is not characteristic of the perpetrator of the crime, because they have their high knowledge in the field of modern technologies materializing through computer fraud and hacking.*

Keywords: *fraud, high-tech crime, malicious use, money laundering.*

1. THE TERM CYBER CRIME

The concept of cybercrime is a form of criminal activity using modern technologies, information systems, and especially computers, which can be a means, but also the goal of this

operation. Computer technology is, in most cases, the subject of abuse, which results in the effects of traditional forms of criminal offenses, such as evasion, theft, and embezzlement, as well as new forms of criminal offenses resulting from the development of technology, such as the misuse of information systems in order to obtain unlawful material gain.

When it comes to the development of this form of criminal activity, one must take into account the fact that modern technologies do not dated for a long time at a global level. In more developed countries of the world, modern technologies have penetrated much faster than in those countries that are not developed. Thus, cybercrime began with its development in more advanced countries where modern technologies were more represented. The 1960s are considered to be the years of cyber crime, because it is heard for the first time in terms of "computer manipulation," "computer sabotage", "illegal use of the computer system" and "computer spyware". At the time, the use of modern technological devices was more than limited, and you and such isolated cases could not be under the guise of a dangerous criminal behavior. However, with massive computerization, these forms of criminal acts take on more and more important places. In the seventies of the last century, the first systematization of criminal offenses from this corpus on the criminal acts of theft and fraud in the field of telecommunication services and the transfer of electronic means. More serious cyber crime began to be spoken only at the end of the last century, with an enormous increase in personal computers and the creation of a super powerful Internet network, accessible to everyone and without any limitations.

One of the first faces convicted of cyber crime is Robert Moris of the United States, who in 1988 produced a computer virus, known as the "computer worm", which was responsible for the destruction of more than six thousand personal computers. Morris was sentenced to 400 hours of socially useful work. After him, Rus, Vladimir Ljevin, in 1994, abused modern technical devices for himself, obtained a $ 10 million unlawful property gain for himself, the Citybank system. He was deprived of liberty three years later in London and sentenced to 36 months in prison and a fine of 250 thousand dollars. The American, Kevin Mitnik was convicted in 1995 of forgery of 25 thousand payment cards. In the coming period, the authorities have met for the first time with cybercrime, which is done from a long distance, several thousand kilometers. It goes into the secret databases of very important institutions, such as vaults, banks, large companies, taking sensitive information and then abusing them in order to collect personal unlawful material gain. In support of the development of cybercrime, the expansion of the computer network, the expansion of the number of computer users and the Internet network, leads to the unstoppable expansion of this form of crime and the creation of a need for building a consistent and high-quality protection system, with the introduction of an adequate measure of legal sanctions.

In addition to these criminal acts of property and legal character, all other forms of criminal acts, created by the use of modern technologies, are all more prevalent. It first refers to the parts of the violation of copyright and related rights, then acts of pornography and child pornography, violation of privacy, blackmail, threats, fraud and so on.

2. TYPES AND FORMS OF HIGH-TECH CRIME

Given the nature and complexity of criminal offenses in this area, it is difficult to make a clear typology of cybercrime and classify it in categories. These issues were also dealt with

by the United Nations set up by two core cybercrime offices. These are: cybercrime is the treatment directed to electronic security operations of computer systems and the data they contain. It primarily refers to the production of computer viruses, hacking, piracy, computerized computing, computer spyware, theft and fraud and theft of computer services. The second definition of cybercrime offered by the United Nations is given in a somewhat broader sense, which cybercrime sees as illegal behavior in relation to the computer system and / or network, which may involve criminal offenses of illegal mediation or supply and distribution of information through computer systems and networks. This creates criminal acts of forgery, computer theft, manipulation of devices and components and abuse of payment systems.

Cyber crime can be typed based on the qualification of the crime itself, which was done using modern technologies. Thus, cybercrime can be linked to political acts, property proceeds, may consist in the production and marketing of harmful content, it may consist in manipulating prohibited products, substances and services and may be directed against the privacy rights of certain persons. In practice, manifestations of criminal offenses in this area are very diverse, with a permanent tendency to spread the spectrum of their actions and appearances. It should be noted that these works are performed by technically highly qualified people who have great ability to use modern technologies in the way they need in order to gain financial profit. Thus cybercrime can be done through so-called "spam" messages that carry a computer virus, which can literally be sent to every available email address, then through crashes into computer networks and systems for the purpose of confidential data confidentiality. Well-guarded systems of banking institutions, state institutions and other vital organs, which have large and very valuable databases, are often targeted at these incursions. Also, cybercrime also entails the theft of personal data and their abuse, and in particular the pin codes and codes for using bank cards, then the codes for accessing email or a personal computer. At the end, but not least the least, is the use of modern technologies in order to disturb security, both at the local and the global level. Thus there are cases of using computer devices for the purpose of committing terrorist acts through the sabotage of security systems, video surveillance cameras, security devices, traffic lights, especially for diversions in rail and road traffic, devices that control the supply of energy, both electricity and gas at the first place, and then other types of fuel. Also, the great diffusion of computer networks and the Internet, in particular, provides the possibility of placing various information, which can often be compromising, incriminating and tendentiously disparaging, and in particular, the spread of pornographic content, in which unfortunately more and more children are involved.

3. NIGERIAN SCAM

This special form of deception using modern technologies originated in the 1980s in Nigeria, and hence it was called a "Nigerian scam" or "fraud 419" according to the number of the Nigerian Criminal Code. The authors of this scam are Nigerian students, who needed money very much, and they did not know how to get to it. The aim of this scam is to mislead businesspeople from the West who are interested in doing business with Nigeria in the field of petroleum products trade. Due to the great success of this scam, it has gained great popularity among cyber criminals around the world, and is now represented in Africa, Asia,

Eastern Europe, Western Europe, North America and Australia.

The modus operandi for Nigerian fraud is the following. A potential victim receives an e-mail, which is so designed that he is personally sent to him. It suggests that a potential victim will be forced to take part in the distribution of certain monetary funds, but with the prior condition to make payment of a certain amount of money. Certainly, the amount claimed was drastically lower than the amount offered to the victim as a benefit that follows it. Thus, by a targeted email message, the potential victim is practically quoted to make a money transfer, for which after a while, he will receive a large percentage in the form of compensation. The amount of this final remuneration is always unknown, more precisely, it does not communicate to the potential victim, in order to keep it in uncertainty. It is only this time that suggests that this is a big reward. The authors of the messages are always falsely presented as bearers of some high-profile in Nigeria. These are usually either government members or high-ranking military officials who want to bring more money out of the country, but they cannot do so without the support of someone from abroad. He, as a counter service, is ready to share the money he gives to the one who helped him. He also insists on the secrecy of the whole job all the time, as the alleged Nigerian authorities would not find out and condemn him for the job.

The recipients of these messages are determined randomly, without any specific criteria. The content of the message is general, but with the tendency that the recipient concludes that it is exactly what he intended for himself and that this message itself is of special significance. Each response to this message introduces the victim to an ever-deeper problem, such as the disclosure of confidential personal information, user names, passwords, and payment card information. The content of these fraudulent messages is prone to changes, and they can offer a particular business offer, they can consist in seeking help to bring out a certain amount of money from Nigeria, can refer to assistance to a person at risk who needs help to come to his heir which was hampered by political opportunities in Nigeria and the like. What is immanent to every message sent with this fraudulent intention is to offer a huge tangible premium that exceeds multi-million dollar amounts, rewards in values such as gold, diamonds or securities, but with the previous obligation of the victim to pay some lower amount of money in the name "Justified costs". Often, false allegations from messages are corroborated by fake documents, which supposedly should testify truth and give a guarantee to the victim that they will not be deceived. The identities of the person in whose name they communicate with the victims are mostly stolen, and those persons with the work in question do not actually have anything.

If the victim accepts the conditions set before him and makes the payment of funds, then there is a postponement of a transaction that should enable her enormous income, and she is asked for new payments, in the name of new extraordinary expenses. Also, it creates an additional pressure of conspirators all the time, with an open threat of possible retaliation by the Nigerian authorities and police in the event of a transactional finding.

The aim of this constant delay is to deceive the victim and her guess at the impression that she is not deceived, and when she realizes the fact that it will be as soon as possible, in order for the money, paid into the accounts, has long been erected and placed securely in the hands of the deceitful. Messages of this type are mainly sent from public computers from Internet cafes or similar places, from which it is difficult to determine who and at what point in time used that computer for what purpose. For the purpose of this scam, falsified docu-

mentation is used, which looks as credible and also uses false orders on social networks, false e-mail, and so on. (Urošević, 2009)

4. CYBER ESPIONAGE AND HACKING

In addition to the above mentioned forms of fraud, which are represented throughout the world, which best illustrate how modern technological tools can be used for illegal purposes, a special emphasis should be placed on cyber spying. In general, espionage is a very dangerous form of behavior, aimed at identifying certain relevant information, which then spreads to unauthorized circles of the person. Spyware is an intelligence activity that involves the disclosure and disclosure of confidential information to another person, which may also mean another country, when it comes to inter-state spying, which is on the security plan and how it is represented. Espionage as such is incriminated and is considered a criminal offense. Spying activity takes place in various ways: by monitoring, tapping, stealing other people's letters or by penetrating other people's e-mail, through continuous monitoring of certain individuals by providing confidential data and information. Today's spies have much easier work than their predecessors in the last century. Modern technological means made their work considerably easier, since today they use modern technological tools, which indisputably point to where and who they are. Mobile phones, modern computer devices transmit their signals to the movement path, which makes espionage much easier.

Cyber Spyware is a modern form of espionage, which also aims to get to strictly guarded information without the consent of those who keep this information. It can be realized for the needs of the competition, other states, rival groups and personal enemies, all for the purpose of personal, political, economic or military benefits, which depends on what the motive of spyware is. In order to successfully conduct cyber spying, there is a need for modern technological tools and network interaction. For this purpose, specialized spyware, Trojan horses and computer viruses are used, which are designed to send their sender regularly information about the data on a computer that is unauthorized installed. (Kovačević, 2010)

The target of cyber spyware is both individuals and large companies, whose official computers remove business secrets and data of priority importance. Large companies are most often spied on by the competition, in order to be able to advance their big business step in time and prepare an adequate response to the market. In addition to individuals and companies, targets of cyber spyware are also states, state information systems and databases. State databases are considered the most valuable data repository because they contain all information from all possible areas and about every legal and natural person. Therefore, despite the strong protection systems, these databases are often subject to espionage and the information from these databases arrives to those for which they were not intended.

The statistics, which can be seen in picture one, unmistakably indicate that the largest number of cyber spying is recorded on the territory of the United States, even 49, followed by Canada with only four and Turkey with three registered cases of spyware. In other countries of the world, cases of cyber spies are negligible-

When it comes to hacking, it is characterized by a voluntary approach, because it consists in the unauthorized penetration into a carefully guarded computer system. The breakthrough into the system is carried out at a high professional and technological level, as a rule in a mysterious way, in order to further carry out acts of espionage, fraud, embezzlement,

sabotage, diffusion of computer viruses and other manipulative actions. Hackers deal with both individuals and organized groups. In addition, many hackers deal with amateurism, from hobbies, while there are also groups dealing with hacking in a highly professional manner. According to the motives, we can divide hackers into bona fide and unwanted, to those who penetrate into the alien system in the desire to read data, change them, further distribute, start and change programs without the approval of their owner, and the like. If the location is taken as a parameter, where hackers are located, we can group them into internal and external ones.

5. HARMFUL CONTENTS

Particular importance, when it comes to cyber crime, should be dedicated to the distribution and production of harmful content, which can then be easily marketed through modern technological tools, computers and the Internet. As the most vulnerable, it is necessary to highlight child pornography, which consists in the exploitation of children for the purpose of sexual exploitation. The particular weight of these works is that this sexual exploitation is publicly shown through an internet and appears to be available to broad masses that consume content interaction. Child pornography consists of porn movies and other content in which children are actors, that is, objects of sexual abuse and physical abuse.

Related to child pornography is pedophilia, which is especially developed with the development of modern technologies and the rapid spread of child pornography on the Internet. Pedophiles are persons with disturbed sexual desire, who are directed at children. It can be heterosexual and homosexual, which depends on the interest of pedophiles for the same or the opposite sex. Children are usually targeted between the age of eight and tenths of a year, while from the aspect of the law, a basophile pedophile is everywhere full-blown with a person under the age of 16. (Mančević, 2016)

In addition to these drastic forms of dissemination of harmful content through modern technologies, it is necessary to highlight the abuse by various sectarian organizations that use technology in order to recruit their followers. By doing so, members of sectarian associations, besides recruiting persons who are in some sort of hopelessness, spiritual and mental crisis, they use these people for various illegal activities and socially dangerous activities. Sects can act on the level of magic or prophesying of fate, which can be spread through the Internet. These contents are easily attracted by the cozy civic masses, who, in order to learn more about their own destiny, are willing to leave their basic information on those sites, which are then easily used for the purpose of the sect. Sects have high-quality Internet content, offering quasi-educational content, which in fact make the reader into a state of malice and bring him into a state in which he wants to approach the sects and to give her his support. In addition to the so-called educational content, sect sites allow interactive communication with potential users of the site, sending regular news and information on the work of the sect, delivering event calendars, and so on. Sect sites are enriched by leading photographs and other content that convince users of the sect's ideology. (Pastuovič, 2013)

At a time when the most valuable goods are in fact timely and accurate information, it is worth noting the abuse of modern technologies and the Internet in order to spread disinformation and false news. The state policy and well-organized state authorities work on the placement of disinformation, which is then successfully used and used for various political,

securities, economic and other purposes. Manipulation of information becomes an integral part of everyday life, which, thanks to the Internet as the current strongest medium, enables the availability of any information, at any place and at any time. Disinformation is expanding always tendentiously in order to discredit certain individuals, organizations, states, goals, ideas and so on. Today, the accuracy of information is rarely or never checked. In a plethora of information that comes in the form of a flood wave, each information finds its place in a large ether of the Internet, and usually this information is made without any consequences in case of proving their inaccuracy. Fake information is today a powerful weapon in the hands of those who want to influence public opinion and the awareness of the masses. Information, true or false, at the time of its publication, has its effect. It is accepted by the broad masses. Subsequent denials are rarely able to counteract the effect of received and processed information, which means that false information, as such, despite its denial, has nevertheless achieved its effect. Likewise, false information, except for political purposes, may be usable for marketing purposes, in order to advertise products, devices and products that attribute properties and characteristics that they do not have, in order to deceive customers. (Ilioski, 2008)

6. PERSONALITY OF CYBER CRIMINALS

One of the elementary and particularly important issues is the questions of the personality of a cyber criminal. In view of the fact that cybercrime belongs to the family of criminal acts that occurred recently, as a result of modern technological and technical evolution, it is absolutely clear that the perpetrators of cybercrime belong to a new generation of criminals, with new knowledge, abilities and skills. The cyber criminal is generally referred to as an attacker, a hacker, and a cracker. A hacker is a person who is studying modern technologies in order to gain new knowledge, while a cracker is the person who uses these knowledge and skills for the purpose of unauthorized access to the network, systems and data.

Cyber criminals can be classified into two basic categories. The first, so-called beginner category, made up of hackers with no experience, includes hacking beginners, using automated tools, such as programs and scripts, which were made by experienced hackers. Their knowledge in this field is not at a high level, and is usually unconscious about the consequences of their actions, and targets of their attack are randomly selected, starting from the available systems. The second group is made by hackers with high level of knowledge in the field of modern technologies. Hackers from this group are computer technology experts and they program their own tools, which focus on goals according to specific interests and needs. These highly skilled hackers work largely independently, but are often also professionally engaged for the needs of government agencies, large companies and international organizations. Hackers of this category are highly skilled in one particular area, and hackers join in organizations in order to be able to work more comprehensively, especially for more complex purposes.

Unlike other types of criminals, cyber criminals are characterized by atypical behavior for perpetrators of criminal offenses. They are mostly quiet people, unobtrusive, non-aggressive, often asocial and insensitive, specific appearance and behavior. They are characterized by a high level of knowledge and education in the field of modern computer technologies and a high level of persistence and persistence in solving problems from their profession.

It is mainly about people of the younger age, highly educated and intelligent people, with the characteristics of a valuable and loyal associate, ready to work as needed and constantly upgrading their knowledge and skills. These are people with a strong logical ability and possibilities for a good assessment of situations, especially those related to modern technologies and their work. (Ugren, 2012)

7. THE ATTITUDE TOWARDS CYBER CRIME

Most contemporary legal regulations in the world cyber crime treat as a criminal offense and provide for sanctions for the commission of crimes committed by the misuse of modern technologies. The Republic of Serbia stands at the position that incriminates this type of activity. Positive Criminal Code of the Republic of Serbia (Official Gazette of The Republic of Serbia) in this area provides for seven independent criminal offenses. These are: damage to computer data and programs, computer sabotage, creation and introduction of computer viruses, computer fraud, and unauthorized access to a protected computer, computer network and data processing, prevention and restriction of access to the public computer network and unauthorized use of computers and computer networks.

Unauthorized use of computers and computer networks is a criminal offense defined in Article 186a of the Criminal Code of the Republic of Serbia. The essence of this work is to damage, hide, unauthorized deletion, alteration or operation of a computer program or data unusable. This work is classified by weight in terms of the amount of material damage done by this part. In addition to prisons and cash, it is also envisaged that the equipment will be seized for the equipment that was carried out.

The criminal offense of computer sabotage consists in the destruction, deletion, concealment and the commission of computer data unusable for the purposes of electronic processing and data transfer, and the data and computer equipment belong to a state body, a public service, an institution, an enterprise or an organization.

Creating and importing computer viruses is a criminal offense that involves the creation and deliberate introduction into a computer or network of malware that is similar to harming that computer or program.

Computer fraud involves the insertion or failure to impersonate an important piece of information that conceals this information, falsely represents, and thus affects the wrong processing and data transfer, with the aim of obtaining unlawful material gain for itself or some other person, while to some other person it causes material damage.

Stopping the functioning of electronic processing and transmission of data and a computer network is a work done by a person who unauthorized access to electronic data processing or a computer network, in order to cause delays and disturbances in the functioning and processing of data.

The criminal act of unauthorized access to a protected computer or network arises from the unauthorized access to computers, networks and data that are strictly guarded. On the other hand, a separate criminal offense represents the prevention and limitation of public access to a network that is by its nature intended for the general public.

CONCLUSION

Modern technologies have greatly facilitated the lives of people and the conditions have been raised to a higher level. The exchange of information, distance communication, processing and processing of information and data has been facilitated, the work of many important state authorities and institutions has been modernized, and the ordinary life has been made easier for ordinary people.

On the other hand, in addition to these important qualities, modern technology also carries with it certain defects and defects. In fact, precision works, these defects are not the disadvantages of the technologies themselves, but people who have abused these technologies. For the sake of personal interest, a man has misused machines that have been created in order to improve his life and work, and the focus of this work is precisely on this segment. How and in what way is abused modern technology, what are the methods of abuse and what consequences it results from.

In this paper, a special emphasis is placed on contemporary forms of criminal acts, which were created by the abuse of modern technology, first of all, computers and Internet networks. These include, first of all, computer theft, sabotage, creation and placement of virus programs, unauthorized penetration into strictly protected and guarded programs, theft of strictly guarded information. Also mentioned is the famous "Nigerian scam", as an international type of cyber crime, with a large number of both the perpetrators and the injured. Also, it's about a common man, everyday user of personal computers and the Internet both in the context of the damaged party and the potential perpetrator of the crime. At the end, the personality of an average perpetrator of a criminal offense in the field of high-tech crime is highlighted, with all its character traits and characteristics that distinguish it from other perpetrators of criminal offenses from the second corps.

Most modern states have incriminated the acts of abuse of modern technologies. Modern criminal codes contain crimes that, according to their being, have the character of high-tech crime or cybercrime and contain penal provisions for perpetrators of these crimes. Given the expansive growth of these crimes at the global level, it is absolutely clear that there is a need to tighten penal policy on these criminal offenses. It is absolutely clear to everyone that the use of modern technologies cannot be limited in any way or put under control, which is not an intent, but there is certainly a need for better regulation and regulation.

LITERATURE

1. Ilioski, D. (2008) "International - Legal Aspects of the Impact of Globalization on the Right to Information", International University of Novi Pazar, Faculty of Law

2. Kovačević, Ž. (2010) "Computer Spying and Protection", University of Belgrade, Faculty of Security

3. Mančević, M. (2016) "Child pornography as a form of high-tech crime" University of Niš, Faculty of Law

4. Pastuović, D. (2013) "Sects and mental manipulation", Roto Plast, Belgrade

6. Ugren, V. (2012) "Cyber criminal", University "Singidunum", Department of Post-

graduate Studies and International Cooperation, Belgrad

7. The Criminal Code of the Republic Serbia ("Official Gazette of the Republic of Serbia" No. 85/2005, 88/2005, 107/2005, 72/2009, 111/2009, 121/2012, 104/2013, 108/2014, 94/2016 and 35/2019)