Meaning of profiling of cybercriminals in the security context

Aldona Kipane

Rīga Stradiņš University, Riga, Latvia

Abstract. In this article, the author analyzes the criminological aspects of profiling of cybercriminals. The development and trends of crime are affected by both the globalization process and the development of information technology. All over the world, crime, disorder and riots are causing more and more troubles and worries for people. Nowadays, cybercrime or criminal offenses committed in the Internet environment take a stable position in the overall mass of criminal offenses. Cyberspace is easy to use to harm an individual, a group of people, or a country as a whole. The role of profiling cybercriminals is determined by the tasks of law enforcement authorities. The profile of cybercriminal combines the personal traits of cybercriminal, behavioural patterns, and demographic data based on cybercrime characteristics.

Key words: cybercrime, criminality, cybercriminal, criminal profiling, profiling cybercriminal.

1 Introduction

Vulnerability of people and threats in the virtual environment are growing, the public is concerned about security on the Internet. Cybercrime is a particularly harmful offense that manifests itself in various areas of society and has a serious impact on it in a number of forms – social disorganization, economic loss and psychological disorder. Cybercrime as a legal, practical and political problem is a direct threat to human rights, entrepreneurship, the state and the global world as a whole. Cybercriminals can disrupt or destabilize, hurt, others seek empowerment, others get data or identity, socially most dangerous persons led by political targets attack state infrastructures (electricity networks etc.).

At present, cybercrimes are the fastest – growing criminal offence compared to others. The situation is made more complex by increasing of the transnational character of crime [1]. According to experts' forecasts, cybercrime will exceed the entire drug market in 2021 and the damage is going to be six trillion all over the world. An Indian criminologist, professor Karuppannan Jaishankar reasonably points out that cybercrimes are no longer simply a hacker attack or an attack on the system, but it is an attack on people [2]. The data of Global Cyber Risk Perception Survey 2018 showed that nearly two-thirds of respondents rated cyber risk as one of the five highest risks in their organization [3]. Data from the Eurobarometer report on cyber security show that most respondents in Latvia and among European citizens are concerned about Internet offenses. The main fears of citizens are about online transactions and the use of online banking. For example, 65% of respondents in Latvia admitted that they generally feel poorly informed about the risks of cybercrime, while in countries where most Internet users feel well informed, confidence in online insecurity and inability to protect themselves is increasing [4]. The problem of cybercrime is determined by the rapid development, implementation and use of information technologies, as well as the use of these

technologies for criminal purposes. For example, the rapid development of cloud computing technologies also opens up a favourable environment for cybercriminals. The criminological aspect of modern technologies is diverse.

Cybercrime is a specific, complex set of criminal offences, which, like crime phenomenon, can be assessed not only by its type, methods of committing them, harmfulness, social danger, harmful consequences, but also by the personality of a criminal. Indian advocate and Legal Scholar, Dr. Debarati Halder and Indian criminologist, professor Karuppannan Jaishankar define Cybercrimes as "offences that are committed against individuals or groups of individuals with a criminal motive to intentionally harm the reputation of the victim or cause physical or mental harm to the victim directly or indirectly, using modern telecommunication networks such as Internet (Chat rooms, emails, notice boards and groups) and mobile phones (SMS/MMS)" [5]. Thus, it can be pointed out that cybercrime is a specific, complex set of offences, and a new branch of criminology – Cyber criminology – has been developed to study it.

Since criminologists consider cybercrime as a new type of criminal activity in the cyberspace, the causes of cybercrime, the characterization of a criminal, the victimological aspects have been studied, and new theories have been raised. Cybercrime, like traditional crimes, consists of **action, action – victim/purpose – modus operandi – criminal – harm, and loss.** From a criminological point of view, cybercrime is a socially legal phenomenon, which also consists of specific elements such as an automated data processing system, cyberspace, an individual, criminal action or inaction. A cybercriminal disputes the values developed by the society. A cybercrime is being committed because of the excessive increase of the cybercriminal's need for expression in an unacceptable way for the public. In addition, it should be borne in mind that in different situations a cybercriminal has more or less possibilities to commit a crime and that there are circumstances that create a high or low level of risk. That is why cybercriminals are the biggest problem of the global web today.

Modern criminologists and law enforcement officers use criminal profiling to describe an investigative approach, which is based on analysis of behavioural and psychological patterns to predict the characteristics of a person, who probably has committed a crime. Profiling leads to the identification and interpretation of criminal behaviour or actions to identify a criminal's personality, his/her modus operandi, and possibly the motivation of a criminal offense. The purpose of profiling is not only to obtain information about character of a criminal, but also to mark a preventive measure to prevent a repeat of a similar criminal offence [6]. There are two parts of the detection of any cybercrime, both technical and legal. Both the legal and technical circumstances of the offense should be identified during the investigation of criminal offences of these categories. Depending on the circumstances of a particular offense, different traces of the offense may occur on a case-by-case basis, which helps to identify the criminal's profile. Thus, recruitment of specialists such as a criminalist, IT specialist, psychologist etc. is essential.

Professor of criminology and sociology, Ph.D. Scott A. Bonn points out that criminal profiling is a cross between law enforcement and psychology. It is still a relatively new field with few set boundaries or definitions [7]. In the last 30 years, the frequency of study of a criminal's profile has increased, the volume of literature has been growing, as well as the method of criminal profiling used in investigation is a common practice worldwide. Criminal profiling is a sub-discipline of forensic criminology. It is, therefore, a discipline within criminology, rooted in the behavioural science and forensic sciences alike [8]. Forensic criminology is currently multidisciplinary in nature [9]. Forensic criminology is a discipline characterized by an integration of material from many sub-disciplines including medicine, psychiatry, psychology; penology, anthropology, mathematics and statistics, forensic science,

criminal investigation, criminology, forensic psychology, victimology, crime reconstruction, criminal event analysis, history, philosophy, practical experience, geography and more.

2 Aim

Aim is to describe the criminological aspects of the criminal profile of a cybercriminal. Profiling of a cybercriminal is a relatively new cross-disciplinary field that is in continuous development and its practical meaning is rising rapidly within the criminology.

3 Material and methods

Analysis of scientific literature and analysis of researches made before. Mainly the following scientific methods were used: analytical, comparative; historical, systemic, publications and analysis of resources.

4 Criminal profiling or profiling a criminal in the context of law enforcement authorities

Criminal profiling or profiling a criminal is a popular investigative technique where psychological achievements are also used. Criminal profiling is often reflected in detective films – by analyzing the features of a criminal offense, the investigator assumes about what a potential criminal might be. For example, a murderer is a man, perhaps a young, powerful, utterly cruel, living one, and so on. Criminal profile is a set of basic features of a person's character.

The informal process of criminal profiling has a long history. The various sources show different indications, such as the reference to the 15th century, but others that the method was already used in 1880 to make predictions about a serial killer. While some experts are discussing the effectiveness of this method, it has been used successfully in law enforcement practices for more than a century. At the end of the 20th century and in the 21st century, the method of criminal profiling was successfully applied by law enforcement authorities. Criminal profiling is typically used in crimes where the offender's identity is unknown. Nowadays there are two types of criminal profiling: the deductive and inductive approaches.

Professor of International Law and Human Rights Martin Scheinin defines profiling as "systemic linking of physical, behavioural, or psychological characteristics to specific offenses and their use as a basis for taking law enforcement decisions. Profiling in the context of law enforcement can generally be a legitimate method of investigation. Profiles can be descriptive and predictive" [10].

There is no common definition in the special literature. There are diverse interpretations of criminal profiling and different terms are used: criminal profiling; offender profiling, criminal profiling, psychological profiling, criminal investigative analysis, crime scene analysis, behavioural profiling, criminal personality profiling, socio-psychological profiling and criminological profiling, more recently, investigative psychology [6]. Generally speaking, criminal profiling involves making inferences about the physical, habitual, emotional, psychological, and even vocation characteristics of criminals [6].

The term "offender profiling" was introduced in the 1970s, linked to the activities of the FIB analysis unit, to describe their criminal investigative analysis work. Initially, criminal profiling was used for serial murders, but the boundaries of research expanded over time. Nowadays, it is linked to various criminal offenses (rape, torture, murder, terrorism, cybercrime, etc.). This includes– criminal profiling – refers to identifying and describing

essential information about a suspect. Psychological profiling refers to a behavioural sketch of an individual who may or may not be a suspected offender [11].

Criminal offense has a biological, social and legal nature. Crime is a diverse, complex phenomenon and explaining many of its aspects are a real challenge [12]. It must be admitted that "criminal offense is the shadow of civilization". Similar findings are provided by David Canter, professor of psychology, who believes that profiling a criminal is a "criminal shadow". He points out that the criminal "leaves psychological traces, behavioural alarm tells that indicate personality. From the crime scene and the testimony of the witnesses, these traces are much vaguer and subtler than those examined by a biologist or physicist. They cannot be studied in a laboratory or under a microscope. They are more like shadows, which are undoubtedly related to the criminal who leave them, but they are flashing and changing, and it is not always clear where they come from [13].

For comparison, the author will refer to a number of wordings of this concept in the special literature to show the features they contain. Emeritus Professor of the University of Sheffield Peter B. Ainsworth points out that "profiling is a process where all available information about a criminal offense, the place of the crime, and the victim is used to create a (yet) unknown perpetrator's profile" [14].

Anne Davies, a specialist from the UK, writes: "Offender profiling (more technically known as Criminal Investigative Analysis) is the name given to a variety of techniques, whereby information gathered at a crime scene, including reports of an offender's behaviour, is used both to infer motivation for an offence and to produce a description of the type of person likely to be responsible" [15].

Forensic scientist and Criminal Profiler Brent Turvey, basing on behavioural evidence defines it as "the process of inferring the personality characteristics of individuals responsible for committing criminal acts [8].

Retired Lieutenant Commander of the New York City Police Department Vernon J. Geberth understands profiling as "an educated attempt to provide investigative agencies with specific information as to the type of individual who may have committed a certain crime" [16].

Latvian specialist Evija Strika writes that criminal profiling is the identification process of traits, behavioural tendencies and demographic data basing on characteristics of a criminal offence [17].

Some scientists define it as a forensic technique used by forensic investigators and law enforcement agencies to understand why criminals are committing crime, to classify criminal behaviour and to solve crimes that have already been committed [18].

Basing on the peculiarities of the research data, conclusions about the personality of a criminal are drawn and the description of a wanted person is made. This means that the main purpose of criminal profiling is to narrow the range of people, where a potential criminal has been searched for – to identify a set of information about individual peculiarities of a criminal, which are expressed as circumstances of criminal activities and traces. It is reasonable to point out that criminal profiling is a form of prediction, which helps to establish a hypothesis in order to identify a person or persons who might be liable for the crime committed. It allows dividing potential criminals into particular categories, based on particular peculiarities being observed, in order to derive other characteristics that cannot be observed [19].

Profiling is a technique or approach for solving crime. In essence, criminal profiling is primarily based on the assertion that the format in which the offender committed the offence reflects his or her behaviour and personality [18].

Summarizing it, the author acknowledges that these formulations do not differ greatly in substance. The author points out that profiling is not only a process, but also the result

of analysis and research (the result of a process) – a set of features of an alleged criminal (profile). It is the method of identification of a person, who has committed a criminal offence. The criminal profile is the result of the observation and conclusion process. This is based on the analysis of evidence resulting from the criminal investigation. The author explains the profiling of a criminal **as the result of research and analysis based on the features of a criminal offense, identifying the personality traits, behavioural tendencies and demographic data of an alleged criminal.**

Criminal profiling is usually used in investigation of difficult-to-detect crimes (especially when there are indications that an offence, or a series of offences were committed by a person having a mental disorder). Criminal profiling can also be used in cases where there are several suspects; more intensive search is done for the person who corresponds to the established profile. At the general level, profiling is the classification of individuals according to their characteristics, i.e. whether they are "constant" (such as gender, age, ethnic origin, and height) or "variable" (such as habits, choice and other behavioural elements). Profiling can be a legitimate tool to apprehend suspected offenders after a criminal offense has been committed. Profiling can also be based on deliberate assumptions derived from experience and training, focusing on behaviour rather than racial, ethnic or religious characteristics. For example, police officers can work with profiles that contain instructions to search for people who repeatedly visit certain sites, that behave unpredictably or nervously, or who repeatedly make large purchases using only cash [20].

Although profiling is a popular method, there are specialists who point out that there are factors that determine its shortcomings: 1. It is wrong to think that human behaviour is constant in time and space, i.e. unchanged in different situations. 2. It is wrong to believe that specific hints and traces can always be obtained at the crime scene, enabling the psychological characteristics of the offender to be provided. However, it should be taken into account that profiling is also a means of forecasting. Based on crime scene information and the behavioural patterns or habits of the offender, the profiler tries to "predict" who the offender or offenders might be and where and how the next crime may occur [11]. In addition, it should be noted that profiling can be used to combat previously committed offenses or prevent future offenses to be committed. Two approaches can be used in the profiling process. One is prospective (related to future prospects, attempting to create a certain template/pattern), which is based on data on the characteristics of previously detained offenders. The other is retrospective approach (focused on the past, an overview of past events), which is based on the study of personality and his/her behaviour, made through the analysis of the crime scene, facts and circumstances of the criminal offense.

5 Criminological profile of a cybercriminal

Criminological research of a criminal personality is carried out in order to identify and evaluate the individual peculiarities, which lead to the commitment of a criminal offence. Criminals, including cybercriminals, have several sharpened personality traits: impulsiveness, aggressiveness (high level of aggression), difficulty predicting the consequences of their actions, rigidity, lies, selfishness, egocentricity, affluently saturated feelings, peculiar orientations and judgments, hard-to-predict behaviour, abstinence from social reality, inability to internalize moral and legal norms, hostility [21].

Personality traits play a key role in personality behaviour. A man has both inherent and typical traits. The personality of an offender is a set of negative personal traits that are specific to the type of criminals and individual criminals. A cybercriminal is not only a person with a certain status, who has rights, duties, responsibilities, but an individual as a complex system

with several structures: 1) needs – interests – abilities; 2) emotions – thinking – will; 3) temperament – nature – value orientation.

The commitment of a criminal offense can be determined by a system of needs, peculiarities of temperament and nature, basic orientation of value orientation and other circumstances. The personality of a criminal, like the formation of a personality of any individual, is determined by three factors - heredity, socialization and self-actualization [22]:

1. Heredity is the succession of organism properties with genetic determination in generational shifts. Biological effects and genetic factors have been demonstrated in various studies, for example, the nature of genetics has been identified in a meta-analysis of individual traits and inheritance characteristics. Summarizing data from over 14 million twin pairs in the 50-year period in 39 countries worldwide, it is concluded that all features are heritable; they are not featuring with less impact.
2. Socialization – mastering the norms of behaviour in a particular social environment consisting of a unit of three subsystems: micro environment, macro environment and the social environment as a whole. For example, the analysis of multi-factor research on the development of criminal behaviour shows that mental health, family stability and home conditions are the decisive criteria for children aged 8−10 to experience a full adult life;
3. Self-actualization (nature, intelligence, values of life) – the interaction of personality-forming factors focuses on self-actualization, which directly forms the basis of criminogenic motivation. However, the criminogenic motivation milestone – the cause of the criminal offense – links these factors to the circumstances conducive to a particular criminal offense.

6 Criminal profiling of cybercriminal

Unlike majority of society, criminals are not able to adopt norms adequately because of diversions in the process of their socialization or they accept “the special forms” of criminal environment. It is affected by various factors: heredity, education, culture, lifestyle and socio-economic factors. A cybercriminal denies the values developed by society. In addition, it should be taken into consideration that in different situation a cybercriminal has more or less possibilities to commit a crime and that there are circumstances that present a low or high risk.

Specific common features and traits are identified in criminal profiling of cybercriminal. One has to agree that profiling is more powerful in multiple than single crime case [23]. There are traditionally distinguished three approaches of criminal profiling: 1) a criminal investigative approach; 2) a clinical practitioner approach; 3) a scientific statistical approach [24]. Each of these approaches has a discrepancy in knowledge field, based on which it is assumed to explain the criminal behaviour.

According to the criminal investigative view, it can be argued that offender profiling relies heavily on a mix of tacit and evidence-based expert knowledge. Arguably, this may make a profiler’s advice more susceptible to cognitive biases and faulty decision-making [25]. Criminal profiling is reactive via the examination of behaviours exhibited at crime scenes. Offender profiling in the interring of an offender’s characteristics from his or her crime scene behaviours. For example, a profiler might try to infer a criminal’s age, gender or employment history from the way he or she has behaved during a crime.

Clinical profilers draw up their conclusions on the offender’s traits from their clinical experience, which is obtained while working with detained offenders.

The aim of the statistical approach working with statistical data, databases is to find the relationship between the information recorded in the statistical reports and the features of the offender, using data on similar crimes and detected criminal offenses.

It is reasonable to point out that criminal profiling of cybercriminal has multidisciplinary nature. The different types of offender profiling can be broken down broadly into two types: geographical profiling[1] and the profiling of an offender's personal characteristics. The latter is what people most commonly associate with the term offender profiling [26].

The aim of geographical profiling is the reverse. Using the locations of an offender's crime as his or her starting point, the geographical profiler tries to predict the area in which the offender lives. Geographical profiling is not simply the consideration of the meaning of a dot on a map. The location has to be understood in the context of as many other aspects of the crimes as can be harnessed to the inference process [27]. Routine Activities Theory and Pattern Theory are relevant to geographical profiling. This suggests that criminals will offend in an area with which they are familiar.

One of the directions of profiling is the psychological evaluation of certain properties and traits. The profile of cybercriminal combines the description of an individual's behaviour and qualities that are created without knowing the criminal's identity. Criminal profiling involves the identification of an unknown criminal by using several techniques:

1. Analysis of the crime scene;
2. Determination of the peculiarities of criminal offence;
3. Characterization of the personality of a criminal [28].

Crime scene analysis (behaviour configuration) plays a significant research role. The analysis of the scene (also known as crime scene) is the inspection of the particular place and the objects contained therein, if it is made after receiving information about the committed criminal offense and if there is sufficient reason to believe that a crime has been committed there or continued in this place [29]. Its purpose is to find and seize traces that indicate the commission of a criminal offense, as well as to restore the mechanism of committing a criminal offense. Already in 1925, professor of Moscow State University Ivan Yakimov (Иван Николаевич Якимов) wrote that "the following stages can be distinguished in the restoration of the crime: the detection of a criminal offense, the obtaining and evaluating evidence, investigating the alleged perpetrator [30].

Nowadays, in the case of cybercrime, the investigator has to recognize a huge amount of evidence in electronic or digital form. The crime scene, contrary to the physical scene, contains computer systems or computer networks. A set of scene conditions and other investigation data can provide information about the personality, motivation, and characteristics of the offender. Taking into account the diversity of cybercrime and profiling approaches - the forensic aspect, the psychological aspect, the technical aspect, – the joint work of multidisciplinary specialists is essential. A psychologist plays an important role. The forms of cooperation may vary during the investigation. Professor Laurence Alison of the University of Liverpool has suggested a number of ways in which the expertise of a psychologist could aid the police and support the work that they do. It is important to appreciate that the ways in which psychologists can contribute extends well beyond the process of profiling offenders. Indeed, the apprehension of the offender would be assisted by enhancing police decision-making and leadership skills, improving

[1] Geographical profiling has its history in environmental criminology.

methods of interviewing witnesses and victims, developing accurate methods of recording, collating and analyzing data on pre-convictions of offenders, developing suspect prioritization systems based on empirical research and enhancing intelligence-led policing and the use of informants [31].

When predicting and profiling an individual's behaviour, his/her most significant psychological features – a system of values, an emotional state, and demographic indicators (biological parents, ethnicity etc.) are described. At the same time, the analysis of the kind of criminal activity (*modus operandi*) and action type, as well as the analysis of the crime scene are made [32]. Modus operandi reflects the nature of cybercriminal [33]. The reconstruction of modus operandi of a cybercriminal is identified from the assumption that criminal behaviour is the set of several aspects, which form a criminal's criminal experience, life experience and influential life changing events, professional skills and the level of development of intellect.

Several experts point out that this method is the most useful on the initial stage of investigation because it can help them plan and lead the process of further investigation. For example, the results of the survey carried out show that 46% of 184 cases criminal profiling specialists were invited to the initial stage of an investigation (Annon 1995; Douglas et al. 1986). The author agrees with this view and points out that by the developing modern technologies and the increasing use of them the importance of rapid and high-quality activities in the detection of a criminal offense (especially cybercrime) in the early stages of the investigation is dramatically increasing, because a timely undetected and not apprehended criminal continues his/her criminal activities. Thus, the fear of cybercrime is expanding.

The criminal profiling of an unknown cybercriminal involves three stages: the first, a law enforcement officer collects data obtained from the crime scene and transmits them to the profiler; the second, the profiler analyzes the data and the third, the profiler provides the predictions of the nature of a potential criminal. The processes that profilers use in analyzing crime scene data can be classified as either "clinical" or "statistical" in nature. Clinically oriented techniques incorporate aspects of the profilers' intuition, knowledge, experience, and training to generate predictions [34].

A profile of cybercriminal can be described by including such key elements as:

1. Personality characteristics/traits, which are specific to a particular person, and which predispose a person to commit a cybercrime. Personality traits are defined as a broad individual psychological dimension that describes the interpersonal, stable and common individual differences of the individual's behaviour, thoughts and feelings. Traits appear in individual activities in different situations and at different timescales [35]. There is a high level of legal nihilism among cybercriminals. The cybercriminal has deviations in legal consciousness; the deformation in legal consciousness is determined by the inability of a particular individual to live according to legal norms. In the author's view, it is in close connection with the enhanced internal necessity to risk in violation of the law, and with such behaviour to achieve some personal benefit or to gain material benefit, profit. The impact of the micro environment is important. For example, family factors that negatively affect personality formation, thereby increasing cybercrimes include: deficiencies in the process of bringing up children (lack of parents, lack of support and understanding), relationship of deformation in the family (neglecting children, etc.), unfavourable families (problems of addiction, financial problems) and / or social problems).
2. Criminal professionalism – it means the personality traits that contribute to the safe and effective commitment of cybercrime. It includes four mandatory features: specific

personal qualities; knowledge and skills; fearlessness, courage and self-confidence; effectiveness and viability of action; commission of a criminal offence and achieving a specific aim [36]. For example, some financially motivated cybercriminals generally have two main purposes – input data and user identity to gain access to finances through the identity they have acquired.

3. Technical knowledge related to specialized knowledge and technical skills in dealing with complex programs and devices that enable cybercrime. The Cybercrime Survey concludes that technical execution of 65% of all illegal activities is relatively simple, 13% – required medium-level technical skills, and 22% – complex technical skills. The most common cybercriminals were university students or students of other educational institutions. It is generally recognized that the level of education among cybercriminals may be higher than among other categories of criminals [37]. If a cybercriminal has the highest technical education, knowledge and skills that can be used for committing a cybercrime, then the social danger of the offense will not only increase, but increase progressively. In this case, intelligence is the main element of a cybercriminal. It must be acknowledged that a person with criminal skills based on the knowledge, skills and abilities acquired, implementing criminal behaviour, causes more harm both in everyday situations and in changed situations [36].
4. Social characteristics are demographic features, socio-economic status, socio-psychological and moral qualities. The basic elements are gender, age, nationality, socio-economic status, for example, the features of a typical fraudster are: a middle-aged man with higher education and substantial work experience in his company (almost half had six or more years of experience, almost a third – three to five years of experience).
5. Characteristics of motivation. In criminology, motivation is understood as a set of motives of action in which each of the motives determines the element of motivation and exists in both the consciousness and the subconscious. The motives are developed and formed under the influence of human emotions and feelings. The motives are internal - chosen by the person and external – driven by others. Research has shown that human behaviour is driven by a number of motives – different internal and external factors [38]. The motive is the leading and facilitating function of the activity (internal psychic encouragement), which, when creating the subject of the activity, directs the human activity. The motivation of the action is formed by a separate motive or motives. Certain types of activity can contribute to a certain motivation and different motives can contribute to a certain type of activity [22]. Juvenile offenders have their own stereotypical way of thinking – "if anyone can do it, why not me". This is one of the motives of commission of a criminal offense, the same as self-affirmation; a desire to be independent and lack of material provision in the family. The behaviour of minors has their own characteristics: insufficient experience of life, low self-criticism, superficial evaluation of circumstances, increased sensitivity, increased mobility and verbal activity, they are easy to impress, imitation, imbalance, increased sense of independence, striving for recognition by the referent group. Hackers also have the possibility of hacking for the sake of their ego, for proving a self that is different from the selves of others. Perpetrators in this category are usually frustrated in social competition elsewhere and seek an opportunity to compensate by employing their computer techniques [39].

The author points out that cybercriminals do not form homogenous group of criminals. A cybercriminal can be both a woman, a man of any age, economic status, race, religion or nationality. In addition, it should be noted that a cybercriminal has several advantages

over a criminal who committed the offense in the traditional way: 1) Global accessibility; 2) Anonymity; 3) Disproportion between the perpetrator's actions and the victim's protection – the attacker chooses the time, place, type and method to offend the victim. There is no direct contact between criminals and victims, no physical use of the weapon; 4) Distance and mobility – there is no need to flee from the crime scene, low risk, but potentially great material gains or profit.

Most cybercrimes are by nature serial in that the offender habituates their behaviour and commit multiple offenses. From this, signature and modus operandi can be drawn. For example, analysis of indicators of the attack's "digital crime scene" can determine the computer hacker's intrusion activity and provide them with an insight. As such, it is an important method when it comes to classifying criminal investigations [40].

The criminal profile of a cybercriminal includes a data set of inductive and deductive profiles of a criminal. Inductive profile of a cybercriminal combines: collection of statistical data related to certain behavioural patterns; – the demographic characteristics of a criminal. Deductive profile of a cybercriminal includes the following range of data – set of the evidence obtained; evidence found on the crime scene and traces; victimological aspects; description of a criminal's personality [8].

The author supports the view that the process of profiling of cybercriminal consists of four interrelated and successive stages:

1) Victimological aspect. The current procedure within criminal profiling is the study of victimological aspects – the role and behaviour of a victim before the cybercrime, during and after it. They reveal new information; allow to study reasons and consequences in details, and to assess the risk weight of a potential victim's actions. The virtual space creates a greater chance of facing a socially dangerous person and more often than in the real world. The content entered on the Internet is eternal, providing long-term content of information, repetitious victimization of a victim, which can last for many years, often a victim not knowing about that. The researches show that a majority of the Internet users lack the experience, skills to identify, assess risk, identify and prevent harmful effects. For example, the activity of a neglected child in the cyberspace (disclosure of personal information, contact with a foreigner etc.) is of high risk. Cybercrime can harm an individual, enterprise or organization. The victimological aspects of cybercrime can be described by using Routine activity theory (RAT) and General Theory of crime and victimization (known as a general theoretical perspective).

According to the RAT guidelines, crime occurs when three elements interact in time and space: a motivated cybercriminal, a suitable victim (a suitable target) and a lack of an active, capable defender. Thus, cybercrime happens when there is a motivated cybercriminal and a suitable victim, and there is no one who might prevent a cybercrime.

In accordance with the General Theory of crime and victimization the main individual factor, which causes a criminal offence and deviance, is the low self-control of an individual. Self-control is explained as the inability by an individual to exercise personal restraint in the face of tempting immediate and easy gratification both in the short and long-term [41].The founders of this theory Michael Gottfredson and Travis Hirschiclaim that a person's self-control level is already set at an early stage, aged 8 and 10. This is a consequence of ineffective parenting and it has a variety of features that occur throughout the life cycle (bullying, bad marks, delinquency, school leaving, divorce, alcoholism, obesity, crime and unemployment). For example, the study of American specialist Fawn T. Ngo and Raymond Paternoster showed that low levels of self-control were significantly related to the likelihood of experiencing three of the five forms of cybercrime victimization – unauthorized access to one's computer, having

information added, deleted or changed on one's computer without knowledge or permission, and online harassment [42].

2) Clarifying the motives of a criminal. Within the framework of criminology, several motives of cybercrime can be distinguished.

Motive of financial gain (money, financial resources): According to the data of Global Report "The State of Industrial Cyber security 2017", the average annual cumulative reported financial loss for a business affected by an ICS cyber security breach was $347,603 including the actual consequences of the incident and costs for software upgrades, staff and training [43]. According to the UK survey, 67% of hackers admitted that money is the main incentive for criminal activity. It is estimated that one cybercriminal manages to gain more than 20,000 pounds a year on average, an average of 8,600 pounds in each attack [44].

Emotional motive: Often, cybercrime is based on emotions – anger, rage, hatred, revenge, love or despair, hopelessness. The motivation spectrum for fraud is broad – greed, expression of power, vengeance, adventurousness, desire to taste the "forbidden fruit", gain satisfaction, self-affirm, gain respect, cause harm. It can also be a revenge of an unsatisfied employee by joining an employer's computer system.

A motive of self-affirmation or self-respect: It should be noted that an activity of a cybercriminal as a human being is determined by his/her cooperation with the environment. This process takes place in two basic forms: the need for self-fulfilment (self-affirmation) and the need for self-respect. The need of a cybercriminal for self-affirmation is a testimony of one's abilities, knowledge, as well as its importance and needs, such as the desire to succeed. In turn, the need for self-respect is the desire to gain recognition, appreciation and feedback from other (surrounding) people. Thus, it is an attempt to succeed, to gain appreciations, praises, which strengthens his/her self-respect.

Sexual impulses and desires: Sexual motivation or libido develops throughout the individual's life. For sexually easily excitable persons with weaker will and insufficient or improper social upbringing, the desire to satisfy one's libido frequently becomes prevalent, overwhelming many other tendencies and interests, and drives these people to violate the basic standards of people's mutual relationships, ethics and rights [45]. The results of the Cybercrime Comparative Study [37] show that: 1) The offenders, who committed crimes referring to child pornography, are between 15 and 73 years old (average age – 49 years); 2) 60% of criminals not only stored, but also distributed these materials; 3) one fifth of these criminals did not work (was retired, unemployed or received a benefit), others worked or studied; 4) 42% of criminals lived with a partner and/ or child; 5) 4% of all criminals had mental health problems; 6) all the criminals identified in the study carefully hid their activities from their relatives; 7) the registered duration of the offense – from six months to 30 years.

Political, ideological and religious motives: Hacktivism – cyber-attacks in the form of political or social protest – is the most common form of politically motivated harm. Hactivists are particularly active in the context of political events.

"Just for fun" motive is usually typical for adolescents or children [46]. The data collected from the survey "Mobile phone and Internet usage habits among children and young people" show that only 4% of parents know that their child has emotionally humiliated, hurt another child via a mobile phone, and 3% know that a child has threatened someone using a mobile phone. In turn, 12% of children admitted that they had performed above mentioned activities. Parents do not know about such activities of their children: 23% of parents do not know about emotional humiliation, 18% – about threatening by using a mobile phone [47].

3) Identification of features/properties. Inductive criminal profiles are developed by studying statistical data involving known behavioural patterns and demographic

characteristics shared by criminals. Deductive profiling uses a range of data including forensic evidence, crime scene evidence, victimology, offender characteristics etc, using such techniques seems possible in the physical world. However, in the cyber-world, their applicability might be questionable [48].

4) Digital behavioural analysis (digital evidence). Today, the field of digital forensics is rapidly advancing, a sign of encouragement to the cyber-criminal profiler. Technical ability, for the purposes of profiling, consists of a subject's expertise with digital technologies, as opposed to other technical skills (e.g., engine repair). There are two distinct subareas that are of interest in the investigative profile – general expertise and the adoption of new technologies [49]. Digital behavioural analysis is a relatively new field that applies the concepts of traditional behavioural analysis to the digital footprints of criminals. The importance of digital forensics is apparent since it is the only means of tracing the perpetrator in the absence of physical evidence. Digital evidence information of value to a criminal case that is stored or transmitted in digital form [50]. The digital evidence can indicate what category of a victim is to be searched for, where a criminal could have contacted the victims [8].

Cybercriminal behaviour is influenced by the interaction between numbers of factors. Such behaviour is a result of mutual interaction, which covers individual, social, environmental factors and conflicts between individual and society. It is influenced by various factors: heredity, education, culture, lifestyle and socio-economic conditions. Author admit that cybercrime is often caused by a person's expression of frustration and bitterness against the social structure and person's position in it.

7 Conclusions

1. Profiling of a cybercriminal is legal (criminal procedural, forensic, criminological) psychological method, which used to determine the behavioural tendencies of a criminal, personal traits and demographic peculiarities, as we as to predict the criminal's further activities.
2. Profiling of a cybercriminal shows the character of a personality of a typical cybercriminal:
   a. Technical knowledge;
   b. The degree of legal nihilism;
   c. High tolerance to risk and needs to risk;
   d. Commitment to self-assertion;
   e. A desire to manipulate or beat others;
   f. A description of motivation, which reveals the reason for committing a crime.
3. Profiling of a cybercriminal may include several criminological and criminal-law-based key elements:
   1) personal characteristics/traits that are specific to a particular person and which predispose a person to commit a cybercrime;
   2) criminal professionalism – by understanding the personality traits that contribute to the safe and effective cybercrime;
   3) social characteristics – demographic features, socio-economic status, socio-psychological and moral qualities;
   4) motivation characteristics – a system of human activity orientation that prompts people to act;
   5) the activity type of a cybercriminal (modus operandi);
   6) the way a cybercriminal has identified or contacted the victim.

References

[1] K. Jaishankar (2011) *Cyber Criminology: Exploring Internet Crimes and Criminal Behavior* (Boca Raton, FL, USA: CRC Press, Taylor and Francis Group, 2011)
[2] V. Tumalavičius, J. Ivančiks, O. Karpishchenko (2016) Issues of society security: public safety under globalization conditions in Lithuania, *Journal of Security and Sustainability Issues* **4**(9): 545–573. https://doi.org/10.9770/jssi.2016.5.4(9)
[3] *Global Cyber Risk Perception Survey 2018*. By the Numbers: Global Cyber Risk Perception Survey. Available on: https://www.marshmma.com/blog/2018-cyber-and-data-security-risk-survey-report
[4] *Special Eurobarometr 390 Cyber Security. Report. 2012.* Available on: http://ec.europa.eu/commfrontoffice/publicopinion/archives/ebs/ebs_390_en.pdf
[5] D. Halder & K. Jaishankar (2011) Cybercrime and the victimization of women: laws, rights and regulations. Information Science Reference
[6] *Criminal Profiling: International Theory, Research, and Practice* (2007), edited by Richard N. Kocsis (Human Press Inc, Totowa, New Jersey)
[7] S.A. Bonn, Criminal Profiling: The Original Mind Hunters. Available on: https://www.psychologytoday.com/intl/blog/wicked-deeds/201712/criminal-profiling-the-original-mind-hunters
[8] B.E. Turney (2012) Criminal Profiling: An Introduction to Behavior Evidence Analysis. Fourth Edition (Elsevier, Oxford)
[9] Forensic Criminology (2010) / edited by Wayne Petherick, Brent E. Turvey, Claire E. Ferguson (Elsver Academic Press)
[10] M. Scheinin, Report of the Special Rapporteur on the promotion and protection of human rights while countering terrorism', UN Doc. A/HRC/4/26, 29 January 2007. Available on: https://unispal.un.org/DPA/DPR/unispal.nsf/1ce874ab1832a53e852570bb006dfaf6/813e9af0b820e2e58525730800513beb?OpenDocument
[11] C.R. Bartol, A.M. Bartol (2011) Introduction to Forensic Psychology: Research and Application (SAGE Publications)
[12] R.J. Lilly, F.T. Cullen, R.A. Ball (2015) Criminological Theory. Context and Consequences. Sage Publication, Inc., 2015
[13] D. Canter (1994) Criminal Shadows: Inside the mind of the serial killer (Endeavour Media)
[14] P.B. Ainsworth (2001) Offender Profiling and Crime Analysis **7** (2001)
[15] A. Davies (2002) Rapists Behaviour: A three Aspect Model as a Basis for Analysis and Identification of a Serial Crime, Forensic Science International, **173**
[16] V.J. Geberth (1996) Practical Homicide Investigations: Tactics, Procedures, and Forensic Techniques, 4th edition
[17] E. Strika. Kriminālā profilēšana (2015) / Psiholoìija 3. Lietišiās jomas. Zvaigzne ABC (In Latvian)
[18] R. Saroha (2014) Profiling a Cyber Criminal. Int. J. Inf. Comput. Technol. **4**(3), 253–258
[19] J.-M. Dinant, C. Lazaro, Y. Poullet, N. Lefever and A. Rouvroy (2008) Application of Convention 108 to the Profiling Mechanism – Some ideas for the future work of the consultative committee. Available on: *http://www.coe.int/t/e/legal_aff airs/legal_co-operation/data_protection/ documents/*

[20] Uz pamattiesībām balstīta policijas darbinieku apmācība. Rokasgrāmata policijas darbinieku apmācītājiem (2018) Eiropas Savienības Publikāciju birojs (In Latvian)
[21] D.A. Andrews, J. Bonta (1998) *The Psychology of Criminal Conduct* (New York: Matthew Bender & Company, Inc.)
[22] I. Vedins (2008) *Zinātne un patiesība*. Rīga: Avots (In Latvian)
[23] K. Rossmo (2000) Geographic profiling (CRS Press LLC)
[24] D.A. Muller (2000) Criminal profiling: Real science or just wishful thinking? Homicide Studies **4**(3), 234–264
[25] D. Kahneman, P. Slovic, A. Tversky (1982) Judgment under uncertainty: Heuristics and biases (New York: Cambridge University Press)
[26] R. Bull, C. Cooke, R. Hatcher, J. Woodhams, C. Bilby, T. Grant (2006) Criminal psychology: A Beginner's Guide (Oneworld Publications, Oxford, England)
[27] D. Canter, D. Youngs (2008) *Principles of Geographical Offender Profiling* (New York: Toylor & Francis Group)
[28] R.N. Kocsis (2006) Criminal Profiling: Principles and Practice (Totowa NJ: Humana Press Inc.)
[29] Krimināprocesa likums: Latvijas Republikas likums. Latvijas Vēstnesis Nr. 74 (3232), 11.05.2005 (In Latvian)
[30] I. Jakimov (2003) *Kriminalistika. Rukovodstvo po ugolovnoj tehnike i taktike*. Novoje izdanije perepechatonoe s izdanii 1925, Moskva: LeksEst(Якимов, И. Н. (2003) Криминалистика. Руководство по уголовной технике и тактике. Новое издание, перепечатанное с издания 1925 г. Москва: ЛексЭст) (In Rusian)
[31] L.J. Alison (2005) *The forensic psychologist's casebook: Psychological profiling and criminal investigation* (Cullompton, UK: Willan)
[32] R. Knight, J. Warren, R. Reboussin, B. Soley (1998) Predicting rapist type from crime scene variables. Criminal Justice and Behavior **25**, 46
[33] J. Lieckiewicz (2011) Cybercrime psychology – propsal of an ofender psychological profil. Problems of Forensic Sciences, Vol. **LXXXVII**: 239–252. Avalable on: `http://www.forensicscience.pl/pfs/87_Lickiewicz.pdf`
[34] B. Snook, J. Eastwodd, P. Gebdreau, C. Coggin, R.M. Cullen (2007) Taking stock of criminal profiling: A narative review and meta-analysis. Criminal Justice and Behavior **34**, 437–453
[35] S. Omārova, (2002) *Cilvēks runā ar cilvēku*. Rīga: Kamene (In Latvian)
[36] V.V. Tulegenov (2014) Kiberprestupnost kak forma virazheniia kriminalnogo professionalizma. *Kriminologiia: vchera, segodnia, zavtra*. **2**(33) (Тулегенов В. В. (2014) Киберпреступность как форма выражения криминального профессионализма. *Криминология*: *вчера*, *сегодня*, *завтра* № 2 (33) (In Russian)
[37] *Comprehensive Study on Cybercrime* (2013) New York: United Nations. Available on: `https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/CYBERCRIMESTUDY_210213.pdf`
[38] N. Ksheti (2010) *The Global Cybercrime Industry: Economic, Institutional and Strategic Perspectives* (New York: Springer)
[39] X. Li (2017) A Review of Motivations of Illegal Cyber Activities. Criminology & Social Integration Journal **25**(1), 110–126
[40] F. A. Zuhri, The Profile of a Cybercriminal. Digital Forensic Magazine. Available on: `http://digitalforensicsmagazine.com/blogs/wp-content/uploads/2017/05/The-Profile-of-Cybercriminal.pdf`

[41] T. Hirschi (2004). Self-control and crime. In R.F. Baumeister & K.D. Vohs (Eds.), Handbook of self-regulation: Research, theory and applications (New York: Guilford Press), pp. 537–555

[42] F.T. Ngo, R. Paternoster (2011) Cybercrime Victimization: An examination of Individual and Situational level factors. International Journal of Cyber Criminology **5**(1) (January – July), 773

[43] Global Report "*The State of Industrial Cybersecurity 2017*". Available on: `https://go.kaspersky.com/rs/802-IJN-240/images/ICS%20WHITE%20PAPER.pdf`

[44] S. Simkin, L. Ponemon, (2016) *Flipping the Economics of Attacks.* No: *Ponemon Institute*. Available on: http://www.polyscope.ch/site/assets/files/42688/06_16_53.pdf

[45] *Crime Investigation (Investigation features of the most frequently encountered crimes*) (2003) /edited by professor Anrijs Kavalieris. Riga: The Police Academy of Latvia

[46] D. Shinder (2010) Profiling and categorizing cybercriminals. Available on: `http://www.techrepublic.com/blog/it-security/profiling-and-categorizing-cybercriminals/`

[47] Aptauja "*Mobilo telefonu un interneta izmantošanas paradumi bērnu un jauniešu vidū*" (2012). Available on: `http://www.drossinternets.lv/upload/materiali/petijumi/mob-tel_interneta_izmantosana_2012.pdf`
(In Latvian)

[48] H. Tennakoon, The need for a comprehensive methodology for profiling cyber-criminals. Available on: http://www.newsecuritylearning.com/index.php/archive/150-the-need-for-a-comprehensive-methodology-for-profiling-cyber-criminals

[49] C.M. Steel, Idiographic digital profiling: behavioral analysus based in digital forensics. Journal of Digital Forensics, Security and Law **9**(1), 7–18

[50] Scene of the Cybercrime: Computer Forensics Handbook (2002) 1st Edition (Syngress Publishing, Inc.)