Information & Security

Published since 1998

Venelin Georgiev
vol. 43, no. 2 (2019): 145-160
https://doi.org/10.11610/isij.4313

ISSN 0861-5160 (print), ISSN 1314-2119 (online)

Research Article

Profiling Human Roles in Cybercrime

Venelin Georgiev

New Bulgarian University, www.nbu.bg

ABSTRACT:

This article presents results from a comparative analysis of the applicability of the main methods for developing cybercrime profiles. The criteria used to make the comparison take into account the specifics of the inductive and deductive profiling methods, as well as the particularities of the participants in a cybercrime and its investigation – a cybercriminal, the victim, and detection and investigation officer. The application of profiling for countering cybercrime is substantiated by appropriate profile samples selected in the review of previous studies in the same field.

ARTICLE INFO:

RECEIVED: 07 JUN 2019
REVISED: 05 SEP 2019
ONLINE: 21 SEP 2019

KEYWORDS:

cybercrime, profiling, cybercrime roles, inductive and deductive approach to creating profiles

Introduction

The spread of information technologies into business, government institutions and individual consumers is characterized by several unavoidable consequences. First of all, technology offers to users advantages, facilitates their operation, and brings them competitive advantages. This fact determines the irreversible spread of technology into the professional and private lives of people. Secondly, technology proliferation also brings consumer security threats that are exploited by a group of individuals whose actions are classified as cybercrime.

Increasing cybercrime as a number and as losses, measured in monetary value and moral consequences, raises the question of studying the tools that would ease the detection and investigation of such criminal acts. From this fact comes the motivation for carrying out the targeted study, which, apart from the actuality, is characterized by a high degree of public interest.

E-mail: vag_analitic@yahoo.com

As main components, the study includes an analysis of the strengths and weaknesses of profiling as a tool for investigating cybercrime, a comparison of the inductive and deductive approach to profile development, analysis of the specific features of developing profiles of cybercriminals, victims and low enforcement officers.

The research outcomes are addressed to researchers and practitioners dealing with counter cybercrime issues. The study also has a value for the academic community, teaching and studying cyber security programs.

A principal scheme that reflects the possible positions of human factor in the cyberspace in terms of its roles in a cybercrime is presented in Fig. 1. Obviously, from the point of view of cybercrime, the person involved may be a cyber criminal, a cybercrime victim and an investigator and law enforcement officer. In general, tackling cybercrime requires, among the other things, the knowledge of the specific features of each of these three roles. For the purposes of this study, it is appropriate to use the relevant profiling tools.

Figure 1: Human Factor's Roles in Cybercrime.

Profiling Strength

Profiling as a tool for tackling cybercrime is both a science and an art to develop descriptions of the characteristics (physical, intellectual and emotional) of criminals, victims and employees of the Investigation Services on the basis of available information on committed and reported crimes. The criminal profile can be defined as a psychological assessment made before the identity of the particular perpetrator of the offense is known. This profile includes a set of predefined characteristics that are considered typical of the perpetrator's behaviour of a type of crime. The criminal profile can be used to narrow down the circle of persons suspected of an act, as well as to assess the likelihood of that particular suspect being the perpetrator of a particular offense.

The criminal profile is a convenient tool to assist investigators in detecting the perpetrators of one or more cybercrimes. It is necessary to understand correctly that even the best-developed criminal profile gives only ideas about the general

image of the person who could be the perpetrator of the crime rather than a specific person as a criminal. The criminal profile is one of the many tools used to investigate crimes. It is not evidence, but rather a good starting point, assisting investigators in focusing on potential suspects, as well as collecting evidence of the crime.

An important issue related to cybercrime profiling is how the created profile works. For some cybercrimes' investigators, the profiling is quite exotic and one of the latest sources of information when conducting an investigation. On the other hand, the build-up of a cybercriminals profile lies on a rational basis, of information gathered and analysed along the logic path.

The profiles give an idea of the characteristics of cybercriminals based on the following indicators: [1]

- observations on specific offenders;
- Information from eyewitnesses and victims of cybercrime;
- knowledge in the field of general and criminal psychology;
- Knowing the links between behavioural patterns in different types of cybercrime.

In practice, two methods for developing cybercrime profiles are known and applied: an inductive method and a deductive method.[2] The first begins with the disclosure of specific features and ends with building a generic image (profile). The second method works the other way, i.e. it starts from the generalized image on the basis of which the specific characteristics are derived. The induction method starts with monitoring and gathering information on the basis of which a theoretical model is implemented, which is applied in practice. The deductive method starts from an assumption that is concretized into specific characteristics (see Fig. 2).

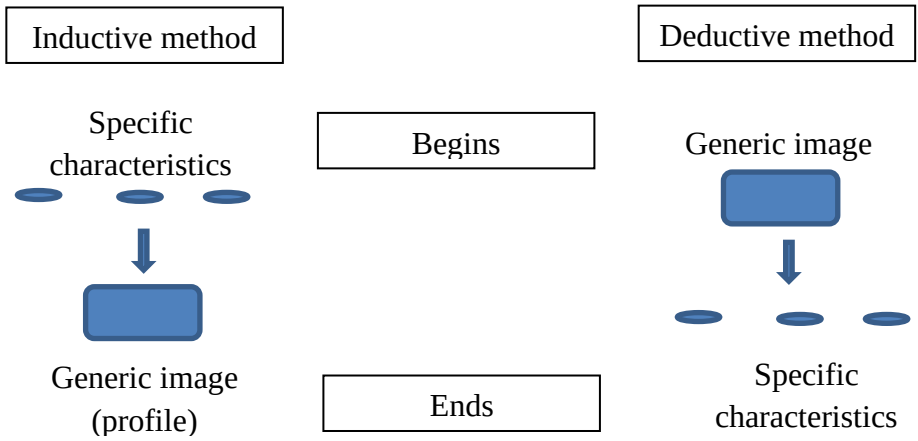

Figure 2: Differences between inductive and deductive profiling methods.

The Inductive Cybercrime profiling method relies on statistical data and benchmarking when creating the profile. Information is collected for cybercriminals who have committed a specific type of crime. This information comes from formal investigations, observing the behaviour of known criminals, clinical and other interviews with criminals, data available in different databases. By processing available data and seeking correlations, the characteristics that are considered to be common to a statistically sufficient number of criminals who have committed a particular type of crime are reached. Applying an inductive method results in characteristics that are not specific but rather generalized.

The deductive method of profiling cybercriminals relies on collected general crime information and specific conclusions about the specific characteristics of cybercriminals based on the experience, knowledge and intuition of the developers. The implementation of the method involves several steps: formulation of the problem, gathering information, formulating and testing a working hypothesis, analysing the results obtained and formulating conclusions. Hypotheses can be tested using cause and effect thinking patterns. By way of example, one can begin with the hypothesis: "The goal of hackers is not always damaging the victims." When disclosure of sufficient evidence of damage from hacker attacks, it can be concluded that the assumed hypothesis is false. The success of profiling using the deductive method depends on the developer's ability to "get into the shoes" of the criminal, to think in a similar way in order to understand the motives and to predict future action

A question of purely practical relevance is related to how cybercriminals profiles are used. It is important to understand correctly that the criminal profile itself cannot solve a particular case but can be used in several ways:

- in narrowing the circle of persons suspected of committing a crime;
- in revealing existing links and the relationship between related crimes;
- in detecting rational traces leading the crime investigation in the right direction;
- in reconsidering existing patterns of cybercrime behaviour.

The Cybercriminals' Role

A number of scientific disciplines are subordinate to creating the conditions and tools for deeper and better knowledge of criminals, including cybercriminals, and their behaviour. Examples of such disciplines include:

- Criminal psychology, studying the causes that lead people to behave illegally and deviating from the common social behaviour pattern;
- Criminology, studying the crime, effect of penalties, and influence of society on criminal behaviour and crime level;
- psychology of investigations, studying emotional and behavioural issues and patterns that assist the law enforcement, investigation and enforcement authorities.

The opponents of the theories studied in the ensuing disciplines advocate a thesis that there is no need for criminals to be understood. All that has to be done is to reveal their crimes, and to receive fair punishments themselves. In this case, the misunderstanding comes from the different content that is used in the phrase "to understand the criminal." The possible options are:

- to understand the criminal means to "get into the situation," and as a consequence to be tolerant of him;
- to understand the criminal is to study and evaluate the specifics of his or her emotions, actions, behaviour to ease the crime detection and investigation.

Obviously, this report will take into account the second option to understand the meaning of the phrase "to understand the criminal," including an understanding of the factors and motivation underlying criminal behaviour. This approach allows us to protect ourselves from criminal acts, to make them easier and more successful and ultimately to obtain a just punishment.

Developing profiles for cybercriminals brings additional benefits such as precise reassessment of existing myths about their specific characteristic.[3] Based on the images created in movies and books, hackers are perceived in some cases as misunderstood geniuses trying to save the world and in other cases as "bad" boys using technology for harming the surrounding and retrieving of personal benefits. As in most cases, the truth about hackers is somewhere in the middle.

Some of the commonly shared misconceptions about cybercriminals include the theses that they must have high IQ and remarkable technical skills, mostly men, and even more teenage boys, any computer teenager is a hacker, cybercriminals are not "Real" criminals because they do not act in the "real" world, their actions are not related to violence considering their virtual reality, they share a single profile.

The existence of such misconceptions about the image of cybercriminals is due to the use of stereotypes. The difference between profiling and building stereotypes lies in the degree of simplification and standardization of the constructed images. Criminal profile is complex and is based on collected data, while the stereotype allows the use of known facts on individual and specific situations

Here comes the question, does this feature make the stereotype always wrong. The answer is negative with the argument that if there is no truth in our beliefs over a sufficiently long period of time, they cannot turn into stereotypes. The inconvenience of using stereotypes in investigating cybercrime is that they make it hard for investigators to see and discover all existing options

As has been pointed out, one of the obsolete perceptions of the image of cybercriminals is that they all have high IQ and significant technical skills. Some cybercrimes in fact require a high level of knowledge and skills in technology, systems and networks, but others are feasible even by people with medium and even low technical literacy. Often cybercrime skills are depleted with the ability to handle e-mail or to use chat programs. Even cybercrime requiring high technical skills can be done by less-skilled hackers, known as "script kiddies," who use codes written by others for their criminal activity.

The allegation that modern cybercriminals are predominantly male, and most often teenage boys, does not meet today's characteristics. It is generally assumed that science as a whole, mathematics and information technology are traditionally a field of expression for the representatives of the strong sex. On the other hand, cybercrime statistics show that men more often commit crimes of all kinds.

In recent years, the same statistics show that gender differences in the above aspects are increasingly disappearing. The typical cybercrime profile, a male, white race, between the ages of 19 and 30, can be considered valid with a high degree of generality, but largely mistaken. In this profile, with increasing accuracy it can be assumed that those who commit cybercrime are individuals of both sexes, of each race and of each age group.

Does the theory that any computer teenager is a hacker is still relevant? In most cases, the criminal nature of young people's acts comes from downloading programs, music, and copyrighted films from the Internet. Interestingly, the idea is that cybercriminals do not use violence in their actions. In spite of both being in virtual environment and the lack of physical violence, cybercrime is a real infringement of the law. Mostly, cybercrimes involve fraud, theft and illegal access to systems and networks. There are also a lot of cases of cybercrime related to the production and distribution of pornographic materials, including child pornography, classified as violent for two reasons: violence against children who are forced to participate in the creation of the materials and a potential opportunity from occurrence of cases of violence against children, due to the influence of such materials.

False seems to be the case that all cybercriminals share a common profile. Here, it is argued that the philosophy, psychology and motivation of various cybercriminals are different.

Cybercriminals Profile Creation

Creating cybercriminals profiles is a process that goes through several steps or stages. As a first step, the formulation of some common features of cybercriminals can be established. These common features are seen as possible, not as mandatory rules. It should also be remembered that there may always be exceptions to the common rules adopted. In this line of thought, a large proportion of cybercriminals have the following characteristics: [4]

- minimal technical knowledge and skills: Many Internet users for illegal purposes are able to navigate cyberspace without any external assistance. Typically, people use tools they know well for their purposes, especially when the actions involved high risk. A typical cybercriminal cannot be defined solely as a computer genius nor as a person entering the Internet for the first time;
- disrespect for the law, a sense of being beyond or outside the scope of the law: for the most part, cybercriminals are not perceived themselves as bad people, but rather as victims of badly-written laws. Moreover, they believe that such laws must be broken. Often, their skills, intelligence, position, and the circumstances make them feel that they are above or beyond existing

laws. Some cybercriminals share the idea that laws should not be applied in cyberspace based on its virtual "unreal" character;

- people with a high risk appetite: why cybercriminals are willing to take high risk - the answer is not unambiguous. For some, this is an opportunity to do something that is forbidden and makes their lives sufficiently emotional and attractive. Others are tempted by the ability to manipulate, dominate and control third parties;
- strong, albeit radically different motivation: Generally speaking, cybercrime requires time, skills, motives and effort. Cybercriminals are highly motivated, though the sources of their motivation are quite different: from reaching their own satisfaction, entertainment, financial, political and other benefits for themselves or for the others.

Identifying the motives for committing a specific cybercrime is an essential element or step in the cybercrime profiling process. One possible answer to the question of why cybercriminals commit crimes is because they are criminals. In practice, things are not so simple, and people are violating the laws of a variety of motives. Why is the issue of motivation of criminals so important? In much of the national legislative systems, proof of guilt is sought within the triangle:

- means: related to the means of committing the crime;
- motives: expressing the reasons for committing the crime;
- opportunity: measured by being in the "right" place, in the "right" time to commit the crime.

Understanding the motivation of cybercriminals is useful for investigating cybercrime in two ways:

- when creating a criminal profile;
- when proving the guilt of the criminals.

In general, the motives for committing a cybercrime include:

- for self-expression, entertainment, pleasure;
- to obtain financial benefits for the offender or a third party;
- by emotional motivation;
- political motives;
- sexual motives;
- due to serious psychiatric illnesses.

In the category of cybercriminals, self-proclaimed and entertaining primarily include young hackers, who can be divided into several main groups:

- those who are excited and are attracted by new technologies. They have fun by studying how computer systems and networks work by the method of trial and error, and understand hacking as an opportunity to build up experience;

- hackers who have no intention of damaging computer systems and networks. They are the type of those who can hack a system or network for the sole purpose of leaving a "I was here" message;
- Researchers whose purpose is to access places to which others have failed before, or at least where they were not. Their curiosity drives them to knock nets for the sole purpose of "seeing" what is inside;
- those who view hacking as a game in which they face security systems and are motivated by the desire to overcome these systems.

One of the most widespread cybercrime motives is the extraction of financial benefits for the perpetrator or for a third party. Besides being common, this motive is also of great strength. Hacking for money can take a variety of forms – receiving money or obtaining property or services without being paid for them.

Emotional motives are also central to cybercrime motives. One part of cybercrime, and more often those associated with violence, property destruction, and so on, are driven by motives based on emotions such as anger, revanchism, etc.

Cybercrimes are also done on political motives. This group includes cybercriminals who are members of extremist or radical groups that use the Internet to propagate or attack sites of their political opponents.

The third step in the cybercrime profiling technology is related to their categorization. Except on the basis of motivation, cybercriminals can also be categorized according to the role the Internet has in their activities. This role divides cybercriminals into two major groups:

- cybercriminals who use the Internet as a means or instrument of the crime;
- cybercriminals who incidentally use the Internet for their criminal activities.

Much of the cybercrimes require the use of computer systems and networks as a crime instrument. In most cases, this does not mean that the same or similar crimes cannot be committed without the help of computers and networks. The emphasis in this case is on the fact that for these cybercrimes, computers and networks are used directly for the purposes of the crime.

The computer systems and networks can be used in various ways for criminal intentions. Most often, they are used as a tool by criminal groups in the following way:

- "white collar" crimes;
- computer fraud;
- hackers, crackers, and attacking computer networks.

"White collar crimes" is a term borrowed from the image of office workers traditionally dressed in business styles. Research has shown that this type of cybercriminals can in turn be divided into several subgroups on the basis of their motivation:

- disgruntled employees who feel deceived by the company they work for. Most often they are long-time employees who have been denied career advancement or have received negative assessments of their work, which in

their eyes seems unfair. The mindset of such employees is comparable to that of Robin Hood – they tend to harm the rich company and benefit others (most often themselves);

- employees who do not have ethical obstacles to theft. If they do not need a preliminary period to motivate, they proceed to commit the crime as soon as a convenient opportunity arises. In most cases, they have a pre-developed plan and are pursuing financial benefits. This type of "white collar" criminals are usually disciplined, careful, working with small amounts, making them hard to notice;
- white-collar criminals who commit crimes because of serious financial problems. These problems can be of different origin: medical problems, alcohol or drugs, loss of money in case of business failure, etc. White collar criminals remain traces or can be revealed on the basis of unexplained high income and standard of living, large transactions of funds, multiple bank accounts in different banks, in different currencies and in different countries, multiple businesses listed at one address and others.

The second group of cybercriminals who use the Internet as a tool for their actions are so-called computer scammers. They use different sites, emails and other services to present to selected victims of their fraud schemes. In this area, the most commonly used means include:

- Internet auctions to which buyers send the necessary amounts but do not receive the goods paid or the requirement of the fake sellers of prepayment without intending to send the purchased goods;
- credit card fraud which involves collecting information about the credit cards of victims and using them to commit fraud.

The third group of cybercriminals who use the Internet as a tool are hackers, crackers, and those who specialize in attacks on computer network security.

It is possible to create a separate profile of those cybercriminals who accidentally use computer systems and networks for criminal purposes. Examples of such criminal activity can be given: use of computer networks to find victims, use of computers and networks for recording, storing and transferring information about criminal activity, use of e-mail or chat services for correspondence with actors in the criminal activity. Even when they are not used as a crime tool, computer systems and networks can provide evidence or clues to the benefit of the investigating authorities

Cybercriminals Profiles Samples

In practice, there are various examples of cybercriminals profiles. Examples of such profiles can be: [5]

"Teenagers" have relatively low technical literacy. Motivated mainly by their own ego, they use reprogrammed scripts and their primary purpose is to defeat themselves. The more advanced among them are engaged in personal development. They can be of different age groups, but they are always out-of-the-box and

are not "up-to-date" with the latest technological capabilities. They are usually novices in the criminal world and can be traced by linking the crime to the person who has downloaded an appropriate set of software tools from a hacker website.

"Cyberpunk" hackers are members of a so-called counter-culture. They are driven and led again by their ego, and almost always aim to defeat and cross the limits of what is allowed. "Cyberpunk" hackers will commit theft or sabotage, but only for purposes that are considered legitimate by them. They are responsible for many viruses, application layers, and DOS attacks against organizations, companies, and products. "Cyberpunk" hackers are always young, computer technology professionals and at the same time social outsiders.

"Old-fashioned" hackers are probably the highest level of computer technology in the hacker community. It is typical for them that they are led by their own ego and are the last of their kind, whose only purpose is to prove their abilities by breaking the established legal frameworks with which they are particularly well acquainted. Due to the fact that they are always aware of what they are doing, they are aware of their actions and their consequences, and because their motives are relatively "soft," they can be defined, to a great extent, as non-threatening. Deleting sites is the most harmful area in which they are extremely well prepared. They are middle-aged or older, with a long personal and professional history in technology and even hacking.

"Code" wars are the first of the most dangerous and destructive profiles. In the past, they were driven entirely by ego or a desire for revenge. Nowadays, they are always guided by the desire for monetary or material benefit. As such, they are usually associated with theft and / or sabotage. Their offenses are mainly built around the use of bugs, bugs or code vulnerabilities. Typical of these are attacks at the application level and the use of Trojan horses. Just like "old-fashioned" hackers, they are professionals in the technology field with a long and rich history. It is likely that most of them have had a variety of cybercrime in the past. They may be from different age groups, but in most cases they are between 30 and 50 years of age. They may have higher education in technology, but they do not work in the sector or are unemployed. Almost always do not fit into the social system and show signs of social deviation

"Cyber-queers" are motivated by the financial gain resulting from the illegal sale of valuable information or apparent theft. Their offenses are driven by the ultimate goal and can involve any means. They use networking tools, devices, code vulnerabilities, and Trojan horses. They are extremely adaptable and are excellent in social engineering. They can be of different age groups, as in this profile the history of the branch is not compulsory. For this, these criminals may be relatively younger than those belonging to the Code of War.

The "dissatisfied inner man" profile is perhaps the most dangerous of all listed. These employees are driven by the desire for revenge or profit of money and use extortion or disclosure of company secrets for the purpose of theft or sabotage. Their goal is to steal or cause serious damage to something that is of great value to the company. They can steal information, bind destructive logic bombs or per-

form other damaging actions. A distinctive feature of this profile is the dissatisfaction with the organization or firm they are part of. They can be of any age group, at a different professional level and position. The only way to prevent this kind of criminals is to monitor employees about their discontent and their follow-up.

"Former employees" are the group of employees who were dismissed. Motivated by the desire for revenge. Their main purpose is to harm the organization they worked for. Even before they are released from their position, if they suspect that this will happen, they can place logical bombs in advance in order to put even more destructive damage. They can take advantage of knowing some sensitive inside information. They can be of any age group, at a different professional level and position.

"Cyber Travelers" are motivated by their ego and by the desire to make outbursts. Their purpose is to disrupt the personal space of people in order to learn something that is of interest to others. Most often, they use program tools to monitor and record the information entered through the keyboard, but the more advanced ones may use Trojan horses or sniffer.

"Fraudsters" are motivated by financial gain. Their purpose is fraudulent or illegal commercialization. Good in social engineering and data falsification. They perform anonymous attacks and rely on the ignorance of their victims in order not to be caught.

"Mafia Wars" is organized crime in cyberspace. Here things are very different from the rest of the categories because of the purposefulness and the high level of organization. "Mafia Wars" have the same motivation as that of their mafia "real brothers" in the real world, namely the profit of money. To achieve this goal, they are ready for theft, extortion, privacy and disregard of basic human rights and freedoms. They work together in tightly organized groups and have the best technical equipment that can be bought with money. Given the easy enrichment of cybercrime, every mafia organization in the real world is expected to move within the cyberspace.

Cybercrime Victims Profiling

The term "victim" has a Latin origin (victima) and means "an animal that has been sacrificed." Nowadays the word is used to mean someone or something that is affected by a mode of action or circumstances. In this sense, a victim of a crime is a person who has suffered damage from an illegal criminal act. Victimology in its field includes the gathering of information and profiling of the victims of crime. This information and created profiles are useful in several areas:

- assist investigating and law enforcement authorities in identifying vulnerable consumer groups and how to protect them;
- allow cybercrime investigation and disclosure bodies to better profile cybercriminals, as crime victim selection patterns are an important part of the criminal profile.

The cybercrime victims are often key witnesses and can provide important insights to the investigators.

Like cybercriminals, profiling can also be applied to cybercrime victims. In this regard, the following groups of victims can be identified: [6]

- people who have no knowledge and experience in the field of Internet technology;
- persons with a high degree of naivety, most often by nature;
- pseudo-victims reporting incidents that do not actually exist;
- people who simply had the bad luck to be in the "wrong" place at the "wrong" time.

On one hand, cybercrime victims are people who have no knowledge and experience on the Internet, but on the other hand the reason is the lack of awareness of existing threats and, the lack of knowledge of the means of achieving secure state. Another feature of this group of victims is that, because of the low level of knowledge and experience, they often do not even suspect that they have been victims of cybercrime. The enormous number of users entering the Internet for the first time increases the number of potential victims of cybercrime and the choice of cybercriminals.

In order to explain the behaviour of the so-called pseudo-victims of cybercrime can use what Sigmund Freud says: the cigar always remains a cigar, while the victim of a crime is not always just a victim. There are people who, for various reasons, report cybercrime that they invent and in which they present themselves as a victim without the truth. The motivation of so-called pseudo-victims of cybercrime may include:

- a desire to revenge someone who is charged with committing a crime;
- a desire to attract attention by allegations that the whistle-blowers have been the victims of cybercrime;
- a desire to conceal its own crime by presenting itself as a victim;
- a desire to derive (financial) benefit from funds or insurance companies that protect victims of cybercrime;
- the victim believes that a crime has been committed against her, but in fact the act is not illegal but rather unethical or immoral.

The cybercrime victims, which have happened to be in the wrong place and the wrong time, are evidence that cybercriminals do not always pre-select their victims based on their own vulnerabilities. In some cases, victims are randomly selected, by way of example, the first respondent to an emailed message.

Cybercrime Investigators Profiling

A key issue in trying to understand cybercrime investigators is whether they have the knowledge and skills of investigating common crimes or whether they need special training and preparation. Obviously, a good cybercrime investigator needs a combination of general and specific skills. The general characteristics include: [7]

- skills to monitor the environment and people's behaviour. Here one can repeat the maxim, which says that looking does not mean to see. A good investigator must capture even the smallest detail of the change in the situation;
- good memory to combine multiple clues as well as to memorize facts, dates, names, places, etc.;
- organizational skills that allow stored information to be structured in a logical manner so that existing patterns of behaviour and relationships become visible;
- skills to work with documents on which to transfer the available information, and with the help of which this information is shared with interested parties;
- objectivity, which must protect investigators from over-belief in their own assumptions and feelings that interfere with the objective analysis of the evidence;
- a wide range of knowledge in law, psychology, victimology and information technology;
- Ability to think by models inherent in cybercriminals, meaning to be able to put themselves in their "shoes," to explain and anticipate their actions;
- intellectually controlled constructive imagination to help with sufficient creativity, taking into account all the possibilities of studying the facts and formulating conclusions;
- curiosity that is inherent to the good investigators and makes them not only satisfied with the discovery of the perpetrator of the offense, but to get into the details of the motives and means of committing the offense;
- endurance, implying that the investigation of a cybercrime is a lengthy process requiring long hours of work. This puts increased demands on the physical and mental endurance of investigators;
- the patience that is made by the fact that the progress of the cybercrime investigation is slow;
- a desire to learn and accumulate knowledge that, in addition to depth, is also characterized by a wide range of areas such as crime-related facts, criminal behaviour patterns, information technology, etc.

Experts specializing in the investigation of cybercrime should also have specific skill set:

- basic knowledge in the field of computer technology, computer networks and security systems. It is true that the more this knowledge the investigator possesses, the better the results can be achieved;
- understanding the culture of hackers. As an axiom, it can be assumed that it is much easier to trace and uncover a hacker when he knows his model of thinking, strong work ethics and morale.

To summarize, both general and specific features of cybercrime investigators can be developed and developed through appropriate training and preparation.

Cybercrime investigators themselves, based on their specialization, can be divided into several groups:

- those who specialize in computer and network crime. First of all, they are investigators, and secondly, technical experts. They have highlighted the interest in technology development, they work most often on security positions in private companies or as security experts;
- computer specialists involved in cybercrime investigations. In them the leading is the IT expertise, while the secondary is the interest in conducting investigations. Most often they work as consultants for security forensics investigators;
- those who have balanced skills in the areas of information technology and crime investigation. Most often they participate in parallel training and work as independent consultants to private companies or security services;
- those who do not have special skills in investigative and information technology. Most often these are police officers who are involved in the investigation of cybercrime.

If the focus is on the problem of recruiting and preparing cybercrime investigations, the question arises as to whether the skills sought in the candidates are more of a skill or are mostly the result of talent. In principle, it can be assumed that no matter how specific the skills are given, they can be built and maintained with the help of appropriate training, while the talent is genetically (inherited) embedded in man. For example:

- in regard to skills: almost everyone who takes piano lessons can at some point play a melody and this will be an expression of the skills he has acquired;
- In terms of talent: certain people have the gift of playing "by hearing" and even without lessons manage to reproduce once heard a tune which is the proof of their presence in talent.

Cybercrime investigation is a creative process and requires skills that can be built up with training and training. Good specialists in the field, apart from skills, also have talent. They are often said to have a flair of crimes and a natural affinity for information technology. It is true, however, that it takes more just talent to achieve the desired results. In summary, good cybercrime investigator can be assumed to be sufficiently talented and at the same time ready to be trained to build and develop the required specific skills.

Profiling methods comparative analysis

Knowing the specific features of the roles form the model, shown in Figure 1, as well as the specifics of the profiling methods, shown in figure 2, a comparative analysis can be made of the applicability of the approaches to each of the three roles.

Table 1 presents the main criteria for analysis and the results.

Table 1. Results from Comparative Analysis.

Role	Access to primary sources of information	Ability to build a generic image	Applicable profiling method
Cybercriminal	Difficult to access sources	Good opportunity	Deductive
Cybercrime victim	Easily accessible sources	Very good opportunity	Inductive and deductive
Cybercrime detection and investigation officer	Easily accessible sources	Very good opportunity	Inductive and deductive

The content of Table 1 can be summarized in the following way:

- The difficulty of direct contact with cybercriminals makes it difficult to collect primary information on the specific characteristics of different cybercrimes. It is possible to determine the set of specific characteristics of the criminals and to create a generic image. Because of these two statements, we may conclude that the deductive method is more appropriate in the cybercriminals profiling;
- The possibility of direct contact with cybercrime victims helps to identify and group their specific characteristics. At the same time, it is possible to create and use a generic image of the victim of a specific type of cybercrime. In conclusion, it is argued that profiling cybercrime victim role can be done using both an inductive and deductive methods;
- Concerning the profiling the cybercrime detection and investigation officers' roles, similar conclusions can be drawn as those for cybercrime victims.

Conclusions

In conclusion, a summary can be made that profiling retains its strengths as a tool of investigation in the case of cybercrime, despite the specific characteristics of such criminal acts. The development and use of profiles alleviate the work of the employees by directing them to the potential perpetrators of the particular cybercrime bearing the corresponding profile's markings. The challenge remains the accumulation of relevant information and practical experience to ensure the development of adequate profiles that meet the characteristics of different cybercriminals groups. The analytical and applied side of profiling as a tool to counteract cybercrime confirms the need for it to be taught by students teaching cybersecurity programs.

References

1 Marco Gercke, "Understanding Cybercrime: A Guide for Developing Countries," International Telecommunication Union (2012).

2 Tennakoon Hemamali, "A Comprehensive Methodology for Profiling Cyber-criminals," Asia Pacific Institute of Information Technology (2012).

3 Cameron S.D. Brown, "Investigating and Prosecuting Cyber Crime: Forensic Dependencies and Barriers to Justice," *International Journal of Cyber Criminology* 9, no. 1 (2015): 55-119.

4 Nick Nykodym, Robert Taylor, and Julia Vilela, "Criminal Profiling and Insider Cyber Crime," *Digital Investigation* 2, no. 4 (December 2005): 261-267.

5 "Profiles of Cyber-Criminals and Cyber-Attackers," project funded by the European Commission, Seventh Framework Programme, University of Cagliari, 2015.

6 Jason R.C. Nurse, Oliver Buckley, Philip A. Legg, Michael Goldsmith, Sadie Creese, Gordon R.T. Wright, and Monica Whitty, "Understanding Insider Threat: A Framework for Characterising Attacks," 2014 IEEE Security and Privacy Workshops, San Jose, CA, USA, 2014, pp. 214-228.

7 Okechukwu Wori, "Computer Crimes: Factors of Cybercriminal Activities," *International Journal of Advanced Computer Science and Information Technology* 3, no. 1 (2014): 51-67.

8 Marcus K. Rogers, "A Two-dimensional Circumplex Approach to the Development of a Hacker Taxonomy," *Digital Investigation* 3, no. 2, (June 2006): 97-102.

9 Venelin Georgiev, *The Human Factor in Cybersecurity* (Sofia: Avangard, 2018). – in Bulgarian.

About the Author

Dr. Venelin **Georgiev** is a professor in the National and International Security Department at the New Bulgarian University. Lecturer in bachelor and master degree programs in the areas of security and defence policy and strategy, security and defence risk management, critical infrastructure protection, public-private partnership, cybersecurity, etc. Associate member of the Security and Defence Management Centre in the Institute of ICT at the Bulgarian Academy of Sciences, member of the Athens Institute for Education and Research; member of the Editorial Board of "Defence Management" journal and the series "IT4Sec Reports." Author of books for risk management, critical infrastructure protection and cybersecurity. Participant in research projects funded by the EU and national programs.