DR RAFAŁ WIELKI
University of Opole | DOI: 10.32041/9788367149761/10

Chapter 10. Crime Analysis Against the Challenges of Cybercrime

10.1. Introduction

Cybercrime is currently one of the biggest threats occurring in the public space, causing huge economic and social costs. At the same time, law enforcement agencies are constantly looking for new ways to combat criminals who take advantage of new technologies and their constant development to remain elusive.

Several main goals can be recognise in this study. One of them is to identify the characteristics of cybercrime, whereby the priority is not to create definitions, typologies or theoretical classifications, but to identify such characteristics of crimes committed in connection with new technologies that may be of great practical importance for law enforcement agencies. In addition, I would like to propose, on the basis of the characteristics developed, methods of combating cybercrime can be useful in investigations, and which are based on information analysis. Hence, the tools of information analysis as an investigative method will be discussed along with the most appropriate analytical techniques. Legal issues that relate to the problem of data retention are also an important element in the work, since without having the right data sets, investigators will not be able to effectively use the proposed solutions and thus the fight against cybercrime will be even more difficult.

In view of such stated goals of the work, several research problems can be posed. It is necessary to obtain an answer to the question

of whether cybercrime has any characteristics that distinguish it from "traditional" crime, and whether the actions of perpetrators may differ in some way. In addition, it is necessary to examine which information analysis tools can be most effective in terms of combating cybercrime.

10.2. Characteristics of Cybercrime

Without citing the historical background of cybercrime, which seems irrelevant to the considerations carried out in this article, it can be stated without controversy that cybercrime is one of the greatest contemporary threats to public security.

Early in the field, the dominant term for the misuse of information technology was "computer crime", or "crime by computer". Over time, the prefix "cyber" began to disappear to refer to everyday activities, while only the negative connotations referring to harmful or negative activities (e.g., cybercrime, cyberbullying, cyberterrorism, cyberstalking) remained in use.[1]

It is also not the purpose of this article to provide an overview of the definition, typology, or taxonomy of cybercrime, but primarily to try to identify and describe the common characteristics specific to cybercrime *in gremio*. It is difficult, moreover, to come up with any single, universally accepted definition of cybercrime, as the phenomenon is very broad and at the same time constantly and dynamically changing. Nonetheless, for the sake of order in the deliberations to be carried out, we will look at a few universal approaches to accompany the ongoing discussions.

Cybercrime is an act that violates the law, which is perpetrated using information and communication technology (ICT) to either target networks, systems, data, websites and/or technology or facilitate a crime. Such a view can be found in the reports of a professional

[1] K. Philips, J. Davidson, R. Farr, C. Burkhardt, S. Canappele, M.P. Aiken, *Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies,* "Forensic Sciences" 2022, No. 2, p. 381.

organisation, where it is indicated, however, it is not so important from the point of view of practice.[2]

According to another, similar, straightforward definition of the problem:

> Cybercrime involves the use of the Internet, computers, and related technologies in the commission of a crime. It includes technologically specific crimes that would not be possible without the use of computer technology as well as traditional crimes committed with the assistance of a computer.[3]

We can encounter a division of cybercrimes into: cyber-dependent crimes and cyber-enabled crimes. Cyber-dependent crime can be defined as any crime that can only be committed using computers, computer networks or other forms of information communication technology (ICT). In essence, without the Internet, criminals could not commit these crimes. Cyber-dependent crime includes such activity as the creation and spread of malware, hacking to steal sensitive personal or industry data, and denial of service attacks to cause financial and/or reputational damage.[4] Cyber-enabled crimes are traditional crimes facilitated by the Internet and digital technologies. The key distinction between these categories of cybercrime is the role of ICT in the offence – whether it is the target of the offence or part of the *modus operandi*.[5]

It is worth referring to a study adopted by the UK Crown Prosecution Service on the basis of the British cyber security strategy,

---

[2] International Telecommunication Union, *Understanding Cybercrime: Phenomena, Challenges and Legal Response*, ITU, Geneva 2012, p. 11–12.

[3] M.-H. Maras, *Computer Forensics: Cybercriminals, Law, and Evidence,* Burlington 2015, p. 2.

[4] Europol, *Organised Crime Threat Assessment 2018,* European Union Agency for Law Enforcement Cooperation, Hague 2018, p. 15.

[5] United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime. Draft-February 2013*, United Nations, New York 2013, p. 15.

which clarifies the distinctions made with the following definitions and exemplifications.[6]

Cyber-dependent crimes are crimes that can only be committed through the use of ICT devices, where the devices are both the tool for committing the crime and the target of the crime (e.g., developing and propagating malware for financial gain, hacking to steal, damage, distort or destroy data and/or network or activity). Cyber-dependent crimes fall broadly into two main categories: Illicit intrusions into computer networks, such as hacking and the disruption or downgrading of computer functionality and network space, such as malware and Denial of Service (DOS) or Distributed Denial of Service (DDOS) attacks. Cyber-dependent crimes are committed for many different reasons by individuals, groups and even sovereign states. For example:

- Highly skilled individuals or groups who can code and disseminate software to attack computer networks and systems, either to commit crime or facilitate others to do so.
- Individuals or groups with high skill levels but low criminal intent, for example protest hacktivists.
- Individuals or groups with low skill levels but the ability to use cyber tools developed by others.
- Organised criminal groups.
- Cyber-terrorists who intend to cause maximum disruption and impact.
- Other states and state sponsored groups launching cyber-attacks with the aim of collecting information on or compromising UK government, defence, economic and industrial assets.
- Insiders or employees with privileged access to computers and networks.

Cyber-enabled crimes are traditional crimes which can be increased in scale or reach by the use of computers, computer networks or other forms of ICT (such as cyber-enabled fraud and

[6] See: HM Government, *National Cyber Security Strategy 2016–2021*, United Kingdom 2021; The Crown Prosecution Service, *Cybercrime – Prosecution Guidance*, https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance (accessed on: 07.07.2023).

data theft). These are crimes which do not depend on computers or networks but have been transformed in scale or form by the use of the internet and communications technology. They fall into the following categories, for example:

- Economic related cybercrime, including fraud intellectual property crime - piracy, counterfeiting and forgery.
- Online marketplaces for illegal items.
- Malicious and offensive communications, including communications sent via social media.
- Cyber bullying/trolling.
- Virtual mobbing – Offences that specifically target individuals, including cyber-enabled violence against women and girls like disclosing private sexual images without consent, cyber stalking and harassment, coercion and control. Also child sexual offences and indecent images of children, including: child sexual abuse, online grooming, prohibited and indecent images of children.
- Extreme pornography, obscene publications and prohibited images.

The definitions presented related to cybercrime are very universal in nature and practical due to the inclusion of exemplification, so let's adopt them for the purpose of this work. It is worth adding that in the case of cybercrime, defining with the use of examples is a very useful and correct move, since these phenomena are dynamically subject to change, and with the development of new technologies, new acts are and will constantly appear. Hence, resorting to typologies loses its meaning, while the proposed approach allows us to understand the essence of individual acts.

It may also be that in the future we will cease to distinguish between cyber-dependent crimes and cyber-enabled crimes, as the line between individual acts is gradually blurring, and more and more "traditional" crimes are being committed with the support of new technologies, and many cases involve electronic evidence, even if the perpetrator did not use new technologies to commit the crime at all. However, it is possible that during the commission of the crime he was carrying a cell phone, smartwatch or any other

device that – for example – is able to prove his location at a specific time, which is crucial for clarifying the circumstances of the act.

Let's look at the characteristics specific to cybercrime, as well as the motivation of the perpetrators of this type of crime, as this is crucial in terms of combating crime and adapting law enforcement's tools to fight it.

To better understand how the Internet has become a channel for criminal activity, it is important to look at the key elements of Internet technologies and distributed systems. These include:

- globalisation and "glocalization",
- distributed networks and grid technologies,
- synopticism and panopticism,
- asymmetric rather than symmetric relationships,
- data trails (data doubling, data trails, and the disappearance of disappearance),
- changes in the organisation of criminal activities.

Globalisation has expanded the reach of criminals across cultures and legal systems beyond traditional boundaries, reshaping the relationship between the global and the local, thus influencing law enforcement efforts. Distributed networks and grid technologies are creating new forms of commercial and emotional relationships between individuals that create new opportunities for victimisation. Unfortunately, these same features also generate flows of multiple information that cannot be easily captured to create consistent summaries of deviant behavior and identify new forms of risk. The simultaneous synoptic and panoptic features of Internet technologies generate new forms of victimisation. Criminals can observe their victims and commit crimes from afar. However, these same features also provide significant potential for identifying crime patterns, as well as individual criminals. The relationship between criminals and victims and the justice processes resulting from changes in the organisation of criminal activity have profound implications for the justice process. For example, the problem of multiple low-impact victims scattered across jurisdictions collectively represents

significant criminal activity, but individually does not justify the expenditure of resources to investigate or prosecute.[7]

The creation and retention of data traffic on the Internet means that we are increasingly experiencing "disappearing disappearances". Every time an electronic transaction takes place, a person leaves behind a trail of data traffic. On the one hand, this helps law enforcement; on the other hand, it combines with the requirement of access technology to recreate the "duplicate data" of an individual's identity in cyberspace, and a threat to privacy and human rights is created. Moreover, the concept of "double data" is also beginning to change the relationship between the self and the state by creating new forms of subordination to maintain levels of access and privilege. Because of the desirability (and value) of access to limited resources, data doubling generates new opportunities for identity theft. Additionally, just as there have been fairly profound changes in the nature of criminal opportunities, there have also been some interesting transformations in the organisation of criminal behavior on the Internet.[8]

Another problem is that unlike traditional crime, which is committed in one geographic location, cybercrime is committed online and is often not clearly linked to any geographic location. Therefore, a coordinated global response to the problem of cybercrime is necessary. This is largely due to the fact that there are a number of issues that pose obstacles to effectively combating cybercrime. Many criminological perspectives define crime based on social, cultural and material characteristics, and view crime as taking place in a specific geographic location. This definition of crime has made it possible to characterise it and then tailor crime prevention, mapping and measurement methods to a specific target group. However, this characterisation is not transferable to cybercrime because the environment in which cybercrime is committed often cannot

[7] D.S. Wall, *The Internet as a Conduit for Criminals*, [in:] A. Pattavina (ed.), *Information Technology and the Criminal Justice System,* Thousand Oaks 2010, pp. 78–79.

[8] Ibid, p. 79.

be attributed to a geographic location or to distinctive social or cultural groups.[9]

In addition to the obvious problem of identifying the places where cybercrimes are committed, we can also talk about the specific characteristics of cybercrime victimisation. Victims do not disclose that they have experienced a crime or simply do not realise that they have been victimised. Many victims of online crime remain anonymous until law enforcement discovers their photos or images during an investigation. The supposed anonymity of online activities often provides a false sense of security and secrecy for both the perpetrator and the victim. Cybercrimes have increasingly serious consequences as they become more widespread and sophisticated, and have a more severe economic impact than many conventional crimes. The structural uniqueness of cybercrimes is also pointed out, as they use new technologies and require high levels of skill; have a higher degree of globalisation than conventional crimes; and are relatively new. Law enforcement agencies, such as the police, lack experience in these new forms of crime. In fact, local police forces in most countries are not prepared to deal with the global nature of cybercrimes. There is no denying that these crimes are rarely reported by victims, which in turn affects their already low detection rate.[10]

Other peculiarities of cybercrime include the problem of criminals' expertise. To commit a cybercrime a person needs to have a good knowledge about the computers and the Internet. In many instances cybercrime is committed by very educated people, as they have accurate knowledge of the technology and its use, and it becomes very hard to trace them.[11] However, some maintain that the majority of cyber criminals have relatively low skills levels, but their attacks are increasingly enabled by the growing online criminal marketplace, which provides easy access to sophisticated

[9] H. Jahankhani, A. Al-Nemrat, A. Hosseinian-Far, *Cybercrime Classification and Characteristics*, [in:] B. Akhgar, A. Staniforth, F. Bosco (eds.), *Cyber Crime and Cyber Terrorism Ivestigator's Handbook*, Waltham 2014, p. 152.

[10] D. Miglani, *Characteristics of Cyber Crime,* https://deepakmiglani.com/characteristics-of-cyber-crime/ (accessed on: 02.07.2023).

[11] N. Sindhu, *Cyber Crime in India: Features, Cause and Elements of Cyber Crime,* https://www.ejusticeindia.com/cyber-crime-in-india/ (accessed on: 02.07.2023).

and bespoke tools and expertise, allowing these less skilled cybercriminals to exploit a wide range of vulnerabilities.[12]

Cybercrime is also characteristic in terms of evidence, as every action generates the creation of many digital traces of activity. However, the collecting of evidence is problematic. Virtually every modern electronic device generates a mass of digital traces that can be useful in explaining a case, but it's difficult to collect them, as is matching them to specific perpetrators, acts, etc., hence the need for law enforcement to use analytical tools to facilitate the interpretation of large data sets, as will be discussed later.

One can also consider whether cybercrime is specific in terms of the motivation of perpetrators and whether the factors leading to involvement in criminal activity differ in some way from those in 'traditional' crime. Undoubtedly, this is an intriguing question. New technologies are attractive to cybercriminals, especially in the case of various types of cyberattacks, is the massive effect their actions can have. For example, by infecting hundreds of thousands of computers with a Trojan, it is possible to launch attacks with really serious consequences at the same time. Therefore, the most daunting task in such cases is the subsequent investigation of the origin of these incidents, since it is very difficult to get to the real cause of the damage: the attacks come from thousands of infected computers from different countries, whose owners may not even be aware that they were part of the infrastructure used to carry out the attacks. This fact makes it extremely difficult to identify the true author of the attacks, so these authors can achieve attractive anonymity.[13]

It is worth noting in this context the research conducted into the motivation of cyber criminals based on interviews they gave, although it should be remembered that it only concerned hackers, therefore a narrow group of cyber criminals. Nevertheless, the authors concluded that most of them are motivated by the desire for profit, which corresponds to the most common motivation

[12] HM Government, *National …*, *op. cit.,* p. 43.

[13] J.C. Fernández-Rodríguez, F. Miralles-Muñoz, *Psychological Characteristics of Cybercrime*, [in:] J.M. Ramirez, L.A. Garcia-Segura (eds.), *Cybersprace, Advanced Sciences, and Technologies for Security Applications*, Cham 2017, p. 188.

among 'traditional' criminals, but there are also noticeable issues of interest in information, privacy, technology, or even with motives indicating a desire to change the world.[14]

A very interesting look at the motivation of cyber criminals is provided by a study prepared by researchers who reviewed the literature on the profile of cyber criminals. The scientific articles reviewed show that the most common motivations are varied, such as:

- the desire to make a profit,
- malice,
- revenge,
- ideological grounds,
- commercial sabotage or espionage,
- participation in hostilities,
- entertainment,
- curiosity,
- undertaking an intellectual challenge,
- desire for publicity, fame or recognition,
- mental health disorders,
- escape from physical life,
- vandalism,
- addictions.[15]

Unfortunately, the exact distributions of motivations in the population of criminals are not currently studied, hence the exact quantitative data are not known, although the information gathered is able to guide investigators in terms of preparing strategic programs to combat cybercrime, including using the tools of crime analysis, which will be discussed later.

To conclude the considerations related to the characteristics of cybercrime, it is worth citing how a typical cybercriminal is perceived. Criminal profiling is an extremely complex activity that is constantly undergoing scientific evaluation, so the data

[14] G. Pogrebna, M. Skilton, *Navigating New Cyber Risks. How Businesses Can Plan, Build and Manage Safe Spaces in the Digital Age*, Cham 2019, pp. 32–33.

[15] M. Martineau, E. Spiridon, M. Aiken, *A Comprehensive Framework for Cyber Behavioral Analysis Based on a Systematic Review of Cyber Profiling Literature*, "Forensic Sciences" 2023, No 3, pp. 462–463.

presented below should be treated with great caution. A viable profile of the cybercriminal will be possible to determine in the future, when data retention issues can be resolved internationally and international cooperation between police services and prosecutors' offices is strengthened.

Nevertheless, a study prepared by the University of North Dakota indicates that the typical cybercriminal is a male between the ages of 29 and 49, from the Asia-Pacific region (mainly China and Indonesia), who may work alone or in a group of about six members, or working in organised groups with a defined hierarchy of executives, managers, and workers.[16] This is very modest information, but it is worthwhile to strive in science to develop criminal profiling in the field of cybercrime that will determine the characteristics of the perpetrators, but it seems that the key here is to obtain a lot of successes by the prosecution service, which will result in the dismantling of networks of cybercriminals operating internationally, and after successfully bringing the perpetrators to justice, in the future we will be able to have more data on the basis of files research.

In conclusion, it seems that an attempt can be made to characterise cybercrime in terms of its most important specific features:

- Cybercrime is characterised by a relatively high degree of anonymity of the perpetrators, but also of the victims, making detection efforts much more difficult.
- Cybercrimes are cross-border in nature, they can be committed from almost anywhere in the world, and the virtual movement of the perpetrator can occur very quickly in time. This makes it very difficult for investigations to determine the exact place and time of the crime, which is crucial from a criminal law perspective.
- Relationships are very fuzzy among perpetrators acting in a group, we often have criminals acting together, in the same interest, but the perpetrators may not even know each other

[16] University of North Dakota, *Decrypting Cyber Crime and Profiling Cyber Masterminds,* https://onlinedegrees.und.edu/blog/decrypting-cyber-crime-and-profiling-cyber-masterminds/ (accessed on: 15.07.2023).

in the real world, which makes hierarchical structures in organised crime groups less visible. Nevertheless, the digital traces left behind can help establish relationships between perpetrators or crimes.

- Cybercriminals are generally characterised by a high degree of expertise and are adept at finding their way in the world of new technologies. However, it is likely that a not inconsiderable percentage of perpetrators – especially cyber-dependent crimes – are not at all great computer scientists, but rather are people who know how to use new technologies and take advantage of ignorance in this area on the part of the victims.
- Cybercrimes do not generate many physical traces, although they leave a great deal of intangible traces that can be analysed, but a rational analysis of the evidence must take into account the need to work with large data sets that require connecting the dots to recognise the whole picture of the criminal act.
- The motivation of cybercriminals resembles that of 'traditional' perpetrators, but it is likely that in this case a larger percentage may be those who commit criminal acts for ideological motives or to gain publicity, since the Internet significantly facilitates quick and inexpensive access to a wide audience.

The presented characteristics of cybercrime can provide important information in terms of planning investigative activities using crime analysis, the essence of which is presented in the next part of the discussion.

10.3. Crime Analysis in Cybercrime Cases

The aim of this part is to show how crime analysis – as an investigative tool – can be useful in the light of the challenges posed by cybercrime. Changes in human behaviour, through shifting means of communication, supposedly forces a change in the techniques used by analysts. Researching this problem is also important for the effectiveness of investigations. Cybercrime is characterised by multiple links, a lack of information as to where the crime

was committed, and multiple actors involved in criminal cases. Crime analysis can be an effective tool in the fight against cybercrime, but a change in the techniques used may be required.

Crime analysis is closely related to the use of criminal intelligence, which in law enforcement we can call an information management system. Criminal intelligence is the process of collecting and analysing data and information, carried out in a systematic, methodical manner, in order to identify critical problems in combating crime, determine the characteristics of these problems, and provide guidance for conducting police operations at the strategic, tactical and operational levels.

Often associated with criminal intelligence is the concept of the intelligence cycle, which is an approximation of the activities undertaken by law enforcement agencies and provides an understanding of the various cognitive processes. We should add that it is sometimes presented in many forms, so it is difficult to speak of its universal character. It was adapted for the needs of law enforcement agencies from the achievements of the military.[17] We can characterise the elements of the intelligence cycle as follows:

a) determining a course of action – when information gaps appear, it is necessary to take steps to exclude them;
b) gathering information – this is the stage for obtaining information from various sources;
c) evaluation of information – when the missing information is obtained, it is necessary to make an assessment as to its relevance, reliability, probability, etc.;
d) information processing – is associated with placing the evaluated information in the relevant databases and giving it the form necessary for further use;
e) analysis and communication of results to the recipient – this is the process of formulating conclusions from the processed information and communicating decision proposals to the final recipient. If the results are satisfactory to the recipient,

[17] J. Buckley, *Managing Intelligence: A Guide for Law Enforcement Professionals*, Boca Raton 2013, pp. 184–186.

the cycle is completed – otherwise the recipient formulates further expectations and the cycle continues.

The intelligence cycle, traditionally viewed in this way, is sometimes criticised nowadays for not taking into account part of the real intelligence work, especially in the area of defining the main concepts related to decision-making in intelligence activities. On the other hand, its usefulness is recognised in terms of training and the objectives of conceptualising strategic operations.[18]

In police science, a different paradigm has begun to emerge over time to interpret phenomena in the criminal environment and the circumstances surrounding specific acts. This model is strongly oriented toward the use of the work of crime analysts, who rely on multiple sources of information, both internal (within a particular police department or other investigative organisation) and external. The information obtained should be passed on to the relevant cells that influence criminal environments, which in turn requires intelligence units to have the right attitudes in the realm of problem identification and decision-making. Decision-makers, in turn, should take such steps as to reduce crime and positively influence criminal environments, which can be understood as the implementation of two-pronged measures aimed at both investigating a specific case and implementing preventive policies.[19] Such a concept is known as the 3-i model, which takes into account three important elements: interpret, influence, and impact.

Over time, the 3-i model mentioned above has evolved and is cited today as the 4-i model: intent, interpret, influence, and impact. Today, this is probably the most up-to-date concept of police work using analysts. The model emphasises the relationship between crime analysts and decision-makers. Decision-makers assign tasks, direct, advise and guide the analysts or crime intelligence teams. They must be sure that their intentions are clear and clarified.

[18] See: A.S. Hulnick, *What's wrong with the Intelligence Cycle,* "Intelligence and National Security" 2006, Vol. 21, No. 6, pp. 959–979; J. Ratcliffe, *The structure of Strategic Thinking*, [in:] J. Ratcliffe (ed.), *Strategic Thinking in Criminal Intelligence,* Sydney 2009, p. 9.

[19] J.H. Ratcliffe, *Intelligence-Led Policing*, "Trends and Issues in Crime and Criminal Justice" 2003, No. 248, p. 3.

With respect to the 3-i model, it is these intentions that are emphasised in the 4-i model. Analysts then interpret facts related to criminal environments and influence decision-makers with the results of crime analysis. Based on these findings, decision-makers translate the criminal environments through strategic management, the creation of action plans, investigations and operations.[20]

It seems important to mention the analysts themselves, as skilled professionals who undertake the effort to fight crime while being responsible for proper communication and for the transfer of information and analysis to decision-makers. The tasks faced by analysts are not easy, moreover, they need a certain competence to perform the tasks. Technological development has led many branches of the private and public sectors to consolidate the position of analysts. One can see a growing demand for people engaged in information analysis.

The work of an analyst is characterised by adding value to the work of others (e.g., the client or the decision maker). The multidimensional approach of analysts makes this value lie in the potential of a specific way of reasoning. This characteristic is special because of internal factors in the analyst's thinking. To put it another way, the added value in an analyst's thinking is its intriguing nature, and this becomes an important argument to emphasise its importance as a separate profession.[21] Moreover, analysts are often involved in developing data collection requirements, reorganising data collection activities, or confirming and evaluating intelligence information.[22]

Predispositions and competencies play a large role, and among the most important are high self-motivation and a constantly unsatisfied curiosity about the world, hence those toiling in this profession tend to read and observe, which leads to the discovery of new information about any objects. A separate and important issue is the definition of the relationship between the analyst and the recipient

[20] J. Ratcliffe, *Intelligence-Led Policing,* Routledge, New York 2016, p. 83.

[21] N. Hendrickson, *Reasoning for Intelligence Analysts: A Multidimensional Approach of Traits, Techniques, and Targets*, Lanham 2018, p. 68.

[22] J.B. Bruce, R.G. George, *Intelligence Analysis – The Emerge of a Discipline*, [in:] J.B. Bruce, R.G. George (eds.), *Analyzing Intelligence: Origins, Obstacles, and Innovations*, Washington 2008, p. 8.

of the content of his work (usually the decision-maker). Analysts actively collect information from colleagues, taking into account the needs of investigators, including those in contact with secret sources. A certain challenge for analysts can be the fact that many decision-makers are not involved in the case from the outset, if only as principals, and it is not uncommon for decision-makers to even be from outside the police service community. In addition, it sometimes happens that there are more recipients of the analysis than one might expect, a fact that is completely beyond the analyst's knowledge at the beginning of the effort, hence it is crucial to clearly establish between the decision-maker and the analyst the tasks. The final stage requires analysts to influence the thinking of decision makers.

It is worth noting that the responsibility of an analyst is high, the competencies required to perform this profession are high, and very often we have a situation where the analyst is not properly paid, so that in the Polish reality there is a shortage of people willing to take on this type of task. We may think that the current system of recruiting candidates, as well as opportunities for professional development, should be subjected to deeper reflection.

At this point, it is already necessary to address the question of the essence of crime analysis, in order to clarify what it is and its usefulness in the conduct of criminal cases. We can trace the genesis of the use of the activity we today call crime analysis to the early 20th century. The chief of police in Berkeley, California (USA) adapted the English technique of systematically classifying the modus operandi of known perpetrators on American soil. There was developed the technique of examining recorded calls for service to perform beat analyses and was instrumental in promoting the use of "pin" or "spot" maps for visually identifying areas where crime and calls were concentrated. On the assumption of regularity of crime and similar occurrences, it is possible to tabulate these occurrences within a city and thus determine the points which have the greatest danger of such crimes and what points have the least danger.[23]

[23] S. Gottlieb, S. Arenberg, edited by S. Busack, *Crime Analysis: From Concept to Reality*, Office of Criminal Justice Planning Edition, U.S. Department of Justice, Washington 1992, p. 6.

The next stage of development took place in the Chicago Police Department, which had a section that examined daily reports of serious crimes to determine location, time, special features, and similarities with other recorded acts to help identify the perpetrator or pattern of criminal activity (modus operandi).[24] Of course, similar practices have been introduced in law enforcement practice before, but they have not been systematised or described in the form of scientific textbooks that would prove the effectiveness of this tool. Therefore, it can be concluded that this is an investigative tool that is relatively young in forensic science, at the same time it is constantly being developed, and in many places – for example, in Poland – it is still not developed enough for investigators to benefit from its entire potential. It is worth noting that the need for the development of modern crime analysis can be seen in three factors. First, there has been a need to relieve the operational staff of the police and intelligence services from dealing with the processing of the information obtained and determining the direction of its acquisition. On the other hand, the author notes that there is a not-insignificant need to improve the flow of information between cooperating services and their units. Finally, one recognises the potential of information technology, which provides more opportunities than ever to process information.[25]

Thus, we can consider that the breakthrough times for crime analysis occurred in the 1990s due to widespread computerisation and access to the Internet, while today's breakthrough can be considered as equipping crime analysis tools with solutions using artificial intelligence.

In general, crime analysis is the collection and processing of crime-related information and data and the discovery of existing patterns in order to predict, understand and empirically explain crime and delinquency, as well as to carry out evaluations of law enforcement activities or to create tactics and human resource management strategies in the broader criminal law. Although crime analysis is used by

[24] O.W. Wilson, *Police Administration*, New York 1963, p. 103.

[25] A. Ibek, *Teoretyczne podstawy analizy kryminalnej*, "Przegląd Policyjny" 2011, t. 103, nr 3, pp. 24–26.

police services, constant development shows that its potential can have wider application in the social sciences or criminology. We can speak of four main goals of crime analysis: understanding and predicting crime; creating strategic assumptions and rationalising police resources; conducting evaluations of police resource allocation efficiency; conducting evaluations of police personnel performance.[26]

In addition, crime analysis is a systematic study of crime and public disorder problems, as well as other police matters, including sociodemographic, spatial and temporal factors that can help the police fight crime, reduce public disorder and prevent crime and evaluate activities.[27]

10.4. Techniques of Crime Analysis

According to the International Criminal Police Organization (hereinafter INTERPOL), in a rapidly evolving environment, threat actors (both individual and collective) have proven to be nimble in overcoming obstacles and seeking opportunities for criminal activity. In this context, law enforcement agencies must be able to quickly detect and decipher the complex dynamics of ever-evolving criminal markets and networks in order to develop and implement the most effective strategies to prevent and combat crime. Access to accurate crime analysis is a key element in obtaining this information. This is particularly important as today's threats are related to digitalisation, which is influencing the growth of cybercrime, but also financial crime, illegal trafficking, terrorism and organised crime.[28]

Within the framework of crime analysis, its four forms can be distinguished:

1. Tactical crime analysis is the daily identification and analysis of emerging or existing patterns of criminal behavior.

[26] C.M. Lum, *Crime Analysis*, [in:] J.R. Greene (ed.), *The Encyclopedia of Police Science*, New York 2007, p. 283.

[27] R. Boba, *Crime Analysis and Crime Mapping*, Thousand Oaks 2005, p. 6.

[28] INTERPOL, *2022 INTERPOL Global Crime Trend Summary Report,* Lyon 2022, p. 3.

In addition, it is an in-depth study of recent incidents and criminal activity by examining how, when and where crime occurs, as well as how patterns, trends and potential perpetrators develop. This can also be applied to the analysis of individual cases.

2. Strategic crime analysis is treated as a study of data processing to better understand long-term crime trends.
3. Administrative crime analysis is a study related to crime research and analysis of legal, political and practical concerns to inform public administration and citizens.
4. Police operations analysis is the study of police policies and practices in order to effectively dispose of personnel assignments, funds, equipment and other resources.[29]

At this point it is worth discussing the issue of techniques that are used in the framework of crime analysis. While it is certainly not a closed catalog, the most important techniques of crime analysis include the following:

- link analysis,
- flow analysis,
- event charting,
- phone call analysis,[30]
- repeat offender and victim analysis,
- criminal history analysis,
- social media analysis,
- crime pattern analysis,
- repeat incident analysis,
- linking known offenders to past crimes,[31]
- social network analysis,
- crime mapping.

[29] G. Grana, J. Windell, *Crime and Intelligence Analysis. An Integrated Real-Time Approach*, Boca Raton 2017, pp. 219–220.

[30] See: United Nations Office on Drugs and Crime, *Criminal Intelligence: Manual for Analysts,* New York 2011, pp. 35–64.

[31] See: International Association of Crime Analysts, *Definition and Types of Crime Analysis [White Paper 2014-02]*, KS: Author, Overland Park 2014, pp. 3–4.

From the point of view of combating cybercrime, due to its characteristics, several techniques may be key. First, let's turn our attention to link analysis. The basic problem for analysts is to group information in a structured way to make it easier to extract meaning from it. Link analysis makes it possible to graphically represent information about the relationships linking objects, such as people, organisations, places, phone numbers, addresses, web domains, etc. In turn, clarifying link information by presenting it in context will help in formulating conclusions. Linkage analysis can be applied to objects that, in light of the analysed findings, are connected by mutual relationships.[32] In the case of link analysis, information is most often visualised in the form of graphs or diagrams, which should serve to simplify perception so that it is easier to understand the relationships between the various data.

There are four elements most commonly found in visualisations:

- objects (e.g.: persons, companies, organisations, places, events, means of transportation),
- relationships (connected objects, which can be family, relate to legal obligations, define roles in companies, roles in criminal organisations, etc.), and
- directions (schemas of relationship flows, indicate the side of information flow, etc.),
- strength (this is a subjective assessment of the interactions occurring within the analysed data).[33]

Linkage analysis can be a very useful tool in terms of visualising the various pieces of information gathered in a case to create a kind of map of the crime in terms of objects and the connections between them. It is a practical, very useful tool, facilitating the assimilation of large data sets in the form of diagrams, and in principle – if prosecutors had unlimited resources of analysts – this type of visualisation could be presented in every case presented before the court. At the initial stage of the investigation there may be problems with having a small set of information or the problem of lack of order, but practice shows that often from simple, inconspicuous information

[32] United Nations Office on Drugs and Crime, *Criminal…*, *op. cit.*, p. 35.
[33] Ibid., pp. 45–46.

(e.g., personal data) it is possible to build quite a sizable network of facts and links between them using open-source intelligence alone. Of course, such 'connecting the dots' requires time to search the data on the Internet to an advanced degree, but with an increase in the staffing of analytical teams in law enforcement agencies, at least in the most relevant cases, it is possible to use this technique more often.

Flow analysis can be considered a modification of this technique, but it's a tool used mainly in terms of analysing the means and benefits gained from criminal activity, e.g., money, drugs, goods, cryptocurrencies. This makes it possible to gain knowledge of who the largest amount of funds ultimately goes to, as well as what the flow of funds says about the relationships within an organised group, often also indicating the hierarchy of its members.[34]

The classic approach here is to use data retained in banking systems regarding accounts, transfers, and individuals that can be linked to particular transactions. Of course, due to the smaller number of traces left during transactions in the criminal world, handling cash will still be popular. In the case of cybercrime, we often have to deal with cryptocurrency trading. Here, much depends on the specific cryptocurrency, but in the case of the most common, Bitcoin, in general, transactions between different wallets are public and anyone can observe them online. Of course, it remains a problem to determine what specific person is the user of an anonymous cryptocurrency wallet and then obtain the wallet's password, although law enforcement success stories are known here.

Event charting generally presents a chronology of an individual's or group's activities in graphic form. In other words, it is simply a timeline that offers investigators a way to focus on individual incidents to develop an overall graphical overview of the crime. In this sense, event charting answers the question of what were the actions of that person leading up to the crime in relation to time. It is worth adding that the preparation of such charts often reveals obvious discrepancies in witness testimony or in their estimates

[34] Ibid, pp. 54.

of when the incident occurred, and often reveals potentially fruitful avenues of investigation.[35]

It is generally an organising technique rather than a strictly analytical one, but it is very useful, since in cybercrime cases the problem is generally one of attributing particular acts or movements of criminals to time and place. Nonetheless, with more data collected, it can support other techniques and allow linking of individual facts gathered in a case.

Phone call analysis is one of the most widespread techniques that can produce valuable results. It can be separated into quantitative or statistical analysis and linkage analysis. The purpose of quantitative analysis is to determine patterns in a data set based on the numerical parameters of a phone call: date, time, duration. Linkage analysis uses the results of statistical analysis and linkage diagrams to formulate hypotheses about the purpose and content of calls (i.e., the relationship and purpose for which the figureheads contact each other). The data customarily collected by telecommunications operators in the course of their ordinary business can be accessed relatively easily and with minimal resources. Perhaps the most salient feature of this type of information is that it is voluntarily (and hence usually in good faith) provided by the customer and that it can be obtained from the operators without direct contact with the subscriber. With phone call analysis, it is possible to determine the numbers dialed by the suspect's phone, identify behavioral patterns and frequently dialed numbers, gain knowledge of call frequency, call duration with date and time, locate phones based on the location of base transceiver station (BTS), and obtain any other personal information managed by the subscriber's operator.[36]

We would add that phone call analysis is crucial for obtaining basic information about the interrelationships and communications between criminals, as well as for fruitful investigation. Examining the flow of telephone information makes it possible to identify individuals who play a key role within a criminal organisation

[35] M. Sparrow, *The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects*, "Social Networks" 1991, No. 13, p. 258.

[36] United Nations Office on Drugs and Crime, *Criminal…*, *op. cit.*, pp. 59–60.

or connect different subgroups. An even broader picture can be provided by correctly interpreted statistical data, if one takes into account the amount of information and its distribution over time for a given crime. At the same time, it is difficult to disagree with the statement that the analysis of cell phone network traffic for investigative and forensic activities aimed at uncovering relational dynamics between actors is a complex task.[37]

It is perhaps the most widely used forensic analysis technique in Polish investigative practice, but one that relies mainly on data obtained from mobile network operators. On the one hand, it is hardly surprising, since the slowly-building theoretical paradigm in forensic science assumes that most people carry an electronic device generating digital traces, which is most often a cell phone, which we now refer to as a smartphone. This includes criminals who use such devices, even while committing a crime (knowingly or unknowingly).

However, I would like to point out that the way cell phone users communicate is changing, and they are – it seems we can assume so theoretically – increasingly less likely to use technologies based on the infrastructure of mobile networks, moving to cloud-based services. To illustrate, let's give a simple example: Users are increasingly sending messages via instant messaging and social media, and are increasingly having real-time conversations in this way, which allow not only voice transmission, but also simultaneous voice or video. This means that mobile network operators have very modest data, which at most can relate to network traffic, but because instant messaging and social networking applications encrypt data, it is rather impossible for services to obtain information that is typically subjected to analysis. Paradoxically, it is possible that the obligation to register SIM cards, which was supposed to limit the communications of offenders, has encouraged criminals to use instant messaging. The problem is that obtaining data from service providers is unregulated by law and very complicated in practice, and in the event that the communication took place in the mobile network, it would be

[37] S. Catanese, E. Ferrara, G. Fiurama, *Forensic Analysis of Phone Call Networks,* "Social Network Analysis and Mining" 2013, No. 3, p. 33.

much easier to obtain data from operators. The problem of data retention will be discussed later in the paper.

Social network analysis in the field of forensic science supports analytical processes concerning organised crime groups or complex social relationships of actors involved in criminal procedures. A characteristic feature of cybercrime is the so-called fuzzy connections, which make it difficult to understand the role of individual objects. The analysis of social networks allows to broaden the interpretation of the information held, and also helps to determine the roles of individual people involved in the criminal network. Among other things, it is possible to determine who is the main decision-maker in the organisation, who interacts with whom and what kind of interactions they are, whether there are different subgroups in the organisation, who is the source of linkage of different groups in the network, etc.

Social Network Analysis is an analytical tool that examines the social relationships that exist within social entities, such as a criminal network. In addition, it is able to identify the overall structure of the network, how information flows between members of the networks, important individuals and potential targets. These capabilities have led to increased interest in the method because of its potential for use by law enforcement agencies.[38]

This is the analytical tool that offers the greatest potential in terms of interpreting large data sets containing various entities and relationships between them, although it requires the use of quite sophisticated software and more thorough training of analysts. No less, it is definitely worth investing in retrofitting analysts with the skills to use social network analysis, as this technique provides answers to the greatest number of questions, thanks to the fact that it uses advanced mathematical models.

In view of the presented characteristics of cybercrime, it seems that crime, together with the presented techniques, can be an effective tool against criminals. It is a tool with great, still massively underutilised potential that can significantly contribute to

[38] M. Burcher, *Social Network Analysis and Law Enforcement. Applications for Intelligence Analysis*, Cham 2020, p. 2.

the clarification of both individual criminal cases and can be useful in planning strategic actions to combat cybercrime in some area. The key thing to remember, however, is that analytical teams need to be more numerous and present in every prosecutor's office as well as in many police units, not just at the provincial and higher levels. It is also worth bearing in mind that an analyst's salary must match his or her skills, since in the private sector analysts are regarded as one of the better-paid groups of employees, which cannot be said of the public sector. However, the effective use of crime analysis capabilities requires a wealth of data, and this in many respects can present legal challenges due to the problem of regulating data retention.

10.5. Conclusions

The research I conducted as part of the Polish-Hungarian Research Platform 2023 aimed to address three main issues related to cybercrime problems. One group of problems related to the issue of what cybercrime looks like, what characterises the acts as well as their perpetrators. The second group of problems related to the issue of investigative methods that can be useful in fighting cybercrime, and what techniques should be used to address the specific challenges posed by perpetrators. The third group of problems related to the legal issues of acquiring the data necessary to effectively fight cybercrime. The conducted research made it possible to make some – it seems – cognitively and usefully interesting observations, and at the same time contributed to the formulation of final conclusions.

First of all, it is possible to identify the characteristics of cybercrime. Cybercrimes are characterised by relatively high anonymity of the perpetrators, but also of the victims; they are cross-border in nature and can be committed from almost anywhere in the world, and the virtual movement of the perpetrator can occur very quickly in time. Cybercrimes are also characterised by fuzzy relationships and less frequent hierarchical structures in the case of organised crime groups. In addition, while cybercriminals generally have a great deal of expertise, many are simply effective in committing

crimes by exploiting their advantage in knowledge and skill in handling the virtual world over and against unwitting victims. Cybercrimes leave a great many digital footprints, but obtaining this data can be very difficult and is often not regulated by any laws. Finally, it is worth noting that there may be motivation among cybercriminals from ideological and political motives or a desire to gain publicity, which is very quickly and cheaply possible through the Internet.

In view of the above conclusions, it is necessary to propose solutions in the area of lawmaking. Among the *de lege ferenda* proposals, it is suggested that international cooperation in the prosecution of cybercrimes be tightened in general, and that as many procedures as possible be regulated in a similar manner, so that laws are not mutually exclusive in different countries. It is also worth bearing in mind that the provisions of substantive criminal law similarly define individual acts, and that the sanctions provided for are similar to each other. The development of the Council of Europe's Convention on Cybercrime was an example of effective action of this kind, but its casus shows that in the case of cybercrime there are problems with the ratification of individual specific solutions, although it is good that the general idea of a common view of criminal problems in this area has been realised. Given that cybercrime enables the rapid spread of information and the possibility of large-scale attacks, including for ideological and political motives, it seems worth considering the issue of punishment. It seems that a mass attack by means of electronic communication, even if it is only a fraud, where the victims lose a relatively small amount of money, but there are many victims, should be considered a more serious act, subject to an increase in the upper penalty limit.

It has also been shown that forensic analysis can and even should be used as one of the investigative methods against the problem of cybercrime. However, it is necessary to select the right techniques to be able to establish the basic facts, the actors in the case, and the relationships between them in scattered and multi-threaded cybercrimes. Forensic analysis can also help unravel the difficulties of determining where and when a crime was committed, especially if the electronic data left behind is subjected to additional examination. Much attention, however, should be paid to the use

of phone call analysis, as one of the most widely used analytical techniques. Nowadays, criminals are turning more often to instant messaging to communicate with each other, while at the same time the tools of communication via cell phone networks are gradually being consigned to oblivion. This fact poses a very serious challenge in the form of the lack of access to network traffic data of suspected users, as currently the retention of data collected by social media and instant messaging is not regulated either by national law or international law.

REFERENCES

Boba, R., *Crime Analysis and Crime Mapping*, Sage, Thousand Oaks 2005.

Bruce, J.B., George, R.G., *Intelligence Analysis – The Emerge of a Discipline*, [in:] Bruce, J.B., George, R.G. (eds.), *Analyzing Intelligence: Origins, Obstacles, and Innovations*, Georgetown University Press, Washington 2008.

Buckley, J., *Managing Intelligence: A Guide for Law Enforcement Professionals*, Boca Raton 2013.

Burcher, M., *Social Network Analysis and Law Enforcement. Applications for Intelligence Analysis,* Cham 2020.

Catanese, S., Ferrara, E., Fiurama, G., *Forensic Analysis of Phone Call Networks,* "Social Network Analysis and Mining" 2013, No. 3.

Europol, *Organised Crime Threat Assessment 2018,* European Union Agency for Law Enforcement Cooperation, Hague 2018.

Fernández-Rodríguez, J.C., Miralles-Muñoz, F., *Psychological Characteristics of Cybercrime*, [in:] Ramirez, J.M., Garcia-Segura, L.A. (eds.), *Cybersprace, Advanced Sciences, and Technologies for Security Applications,* Cham 2017.

Gottlieb, S., Arenberg, S., edited by Busack, S., *Crime Analysis: From Concept to Reality*, Office of Criminal Justice Planning Edition, U.S. Department of Justice, Washington 1992.

Hendrickson, N., *Reasoning for Intelligence Analysts: A Multidimensional Approach of Traits, Techniques, and Targets,* Lanham 2018.

HM Government, *National Cyber Security Strategy 2016–2021,* United Kingdom 2021.

Hulnick, A.S., *What's wrong with the Intelligence Cycle*, "Intelligence and National Security" 2006, Vol. 21, No. 6, pp. 959–979.

Ibek, A., *Teoretyczne podstawy analizy kryminalnej*, "Przegląd Policyjny" 2011, t. 103, nr 3.

International Association of Crime Analysts, *Definition and Types of Crime Analysis [White Paper 2014-02]*, KS: Author, Overland Park 2014.

International Telecommunication Union, *Understanding Cybercrime: Phenomena, Challenges and Legal Response,* ITU, Geneva 2012.

INTERPOL, *2022 INTERPOL Global Crime Trend Summary Report,* Lyon 2022.

Jahankhani, H., Al-Nemrat, A., Hosseinian-Far, A., *Cybercrime Classification and Characteristics,* [in:] Akhgar, B., Staniforth, A., Bosco, F. (eds.), *Cyber Crime and Cyber Terrorism Investigator's Handbook*, Waltham 2014.

Lum, C.M., *Crime Analysis*, [in:] Greene, J.R. (ed.), *The Encyclopedia of Police Science,* New York 2007.

Maras, M.-H., *Computer Forensics: Cybercriminals, Law, and Evidence*, Burlington 2015.

Martineau, M., Spiridon, E., Aiken, M., *A Comprehensive Framework for Cyber Behavioral Analysis Based on a Systematic Review of Cyber Profiling Literature*, "Forensic Sciences" 2023, No 3.

Miglani, D., *Characteristics of Cyber Crime*, https://deepakmiglani.com/characteristics-of-cyber-crime/ (accessed on: 02.07.2023).

Philips, K., Davidson, J., Farr, R., Burkhardt, C., Canappele, S., Aiken, M.P., *Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies,* "Forensic Sciences" 2022, No. 2.

Pogrebna, G., Skilton, M., *Navigating New Cyber Risks. How Businesses Can Plan, Build and Manage Safe Spaces in the Digital Age*, Cham 2019.

Ratcliffe, J., *Intelligence-Led Policing*, "Trends and Issues in Crime and Criminal Justice" 2003, No. 248.

Ratcliffe, J., *Intelligence-Led Policing,* Routledge, New York 2016.

Ratcliffe, J., *The structure of Strategic Thinking*, [in:] Ratcliffe J. (ed.), *Strategic Thinking in Criminal Intelligence,* Sydney 2009.

Sindhu, N., *Cyber Crime in India: Features, Cause and Elements of Cyber Crime*, https://www.ejusticeindia.com/cyber-crime-in-india/ (accessed on: 02.07.2023).

Sparrow, M., *The Application of Network Analysis to Criminal Intelligence: An Assessment of the Prospects*, "Social Networks" 1991, No. 13.

The Crown Prosecution Service, *Cybercrime – Prosecution Guidance*, https://www.cps.gov.uk/legal-guidance/cybercrime-prosecution-guidance (accessed on: 07.07.2023).

United Nations Office on Drugs and Crime, *Comprehensive Study on Cybercrime. Draft-February 2013*, New York 2013.

United Nations Office on Drugs and Crime, *Criminal Intelligence: Manual for Analysts*, New York 2011.

University of North Dakota, *Decrypting Cyber Crime and Profiling Cyber Masterminds,* https://onlinedegrees.und.edu/blog/decrypting-cyber-crime-and-profiling-cyber-masterminds/ (accessed on: 15.07.2023).

Wall, D.S., *The Internet as a Conduit for Criminals*, [in:] Pattavina, A. (ed.), *Information Technology and the Criminal Justice System*, Thousand Oaks 2010.

Wilson, O.W., *Police Administration*, New York 1963.