WEB OF SYNERGY:
International Interdisciplinary Research Journal
Volume 2 Issue 2, Year 2023 ISSN: 2835-3013
https://univerpubl.com/index.php/synergy

Methodology of Cybercrime Investigation

Jumaev Bekzod Bakhtiyarovich
Republic of Uzbekistan, Academy of the General Prosecutor's Office, Independent researcher

Article Information

Received: December 18, 2022
Accepted: January 19, 2023
Published: February 20, 2023

Keywords: *cyber security, security, right, obligation, data protection, internet, information, cybercrime, backup, copy.*

ABSTRACT

the article describes the rights and obligations, content and characteristics of cyber security, as well as the basics of state regulation of cyber security, data backup.

Computers are a part of our daily lives, it can be even said that sometimes they are a necessity. On the one hand, they represent a communication tool connecting the whole world with unbeatable speed, they represent an invaluable helper in the duties of everyday life, an ideal means of spending free time, or a common work tool. On the other hand, they can be a tool through which its user can harm another, for example by committing a crime; alternatively, the user can make already existing crime easier for himself/herself, which is simpler, more effective and more anonymous with the help of a computer (and the Internet)[1].

Cybercrime is now a common concept, which is analysed in many respects and it is possible to find several relevant sources of information that analyse this issue from a criminological, technical, legal, social, or general and summarizing point of view[2]. The beginnings of cybercrime (computer) crime date back to the 60s and 70s of the last century, taking into account the differences between contemporary computers and current computers. At present, it is one of the fastest growing types of crime and at the same time it is a highly sophisticated crime[3].

Cybercrime is causing increasing social and economic damage, which affects the fundamental rights of individuals and poses a threat to the rule of law and the stability of democratic societies in cyberspace, and is a growing problem in EU Member States. Cybercrime is gaining in intensity, complexity and scale, to the extent that in some EU countries it is more widespread than traditional forms of crime, extending to other areas of crime, such as trafficking in human beings. The use of encryption and anonymisation tools for criminal purposes and attacks through so-called ransomware are more common than the usual threats in the form of malware, such as

[1] L. Klimek, Základy trestného práva Európskej únie, Bratislava 2017, p. 101
[2] V. Porada a kol., Kriminalistika. Technické, forenzní a kybernetické aspekty. 2. aktualizované a rozšířené vydání, Plzeň 2019, p. 706.
[3] L. Klimek, op. cit., p. 101.

Trojan horses. Malware (such as bank Trojan horses) is still at the centre of cyberattacks, but there has also been an increase in the number and consequences of attacks on industrial control systems and networks aimed at destroying critical infrastructure and economic structures, as well as destabilizing companies[4].

Cyber/computer crime (also known by the acronym "cybercrime") can be defined as the commission of a crime in which a computer interacts in some way as a collection of hardware and software, including data, or just some of its components, or a number of stand-alone computers or connected to a computer network, either as the subject of this criminal activity (with the exception of the criminal activity involving the described facilities as movable property) or as an instrument of a crime commission. From the forensic point of view, cybercrime also means a group of criminal offenses (anti-social behaviour) committed by means of computer technology in the conditions of electronic communications networks, ICT systems, software and databases in the means of computer technology[5].

The boundaries between cybercrime, cyber espionage, cyber warfare, cyber sabotage, and cyber terrorism are becoming increasingly blurred; as cybercrime can target individuals, public or private entities and can cover a wide range of crimes, including invasions of privacy, sexual abuse of children online, public incitement to violence or hatred, sabotage, espionage, financial crime and fraud, such as payment fraud, theft and identity theft, as well as illegal interference with the system. A significant number of cybercrime remain unprosecuted and unpunished[6].

It is precisely children who use the Internet at an ever younger age and are particularly vulnerable, so they can become victims of so-called grooming and other forms of sexual abuse on the Internet (cyberbullying, sexual abuse, sexual coercion and extortion), misuse of personal data, as well as dangerous challenges aimed at promoting various forms of self-harm (the case of Blue whale game) and therefore need special protection; as Internet perpetrators can find and deceive victims more quickly through chat forums, e-mails, online games and social networks, and as hidden peer-to-peer (P2P) networks remain the main platforms for access, communication for child sex offenders, storing and exchanging material depicting the sexual exploitation of children and tracking new victims without being detected[7].

It is man who is the one who can most endanger the security of himself/ herself or others in cyberspace, and that is by acting or failing to act. The basic technical causes of cybercrime, such as obsolescence and non-updating of the software used, non-use of anti-virus programs, insufficient security settings, relative availability of sophisticated technical means that can be used for attacks and the like, must also be adequately taken into account. Smartphones, for example, are relatively easy to exploit, and users often have no idea about them. It is clear that the human factor plays a key role in committing cybercrime; the human factor is undoubtedly generally considered to be the greatest safety risk[8].

The typical perpetrator of computer crimes is most often an employee of the injured organization. Literature sources indicate that, for example, in the United States, only 6% of offenders were employees of other companies, 24% of offenders were directly employed in the computer centre of the injured company, and 70% were recruited from end users of the injured company's computers. The situation in the Slovak Republic and the Czech Republic seems to be similar[9].

The perpetrator's personality is dominated by more than a high IQ, greed or desire for power,

[4] European Parliament Resolution No. 2017/2068 (INI) of 3 October 2017 on the fight against cybercrime.
[5] V. Porada a kol., op. cit., p. 960.
[6] European Parliament Resolution No. 2017/2068 (INI)…
[7] Ibidem.
[8] V. Porada a kol., Bezpečnostní vědy, Plzeň 2019, p. 161
[9] Idem, Kriminalistika. Technické, forenzní a kybernetické aspekty…, p. 965.

perseverance and ruthlessness. Many perpetrators are neurotics who are clumsy in social contacts, often with sexual problems. Perpetrators of cybercrime often do not feel guilty and do not see anything wrong with their actions. Of importance is the specific position of the typical perpetrator of this illegal activity, which may be that:

- ✓ is authorized to perform certain computer operations,
- ✓ is familiar with the sequence of operations required, including details of the behaviour of the automated system,
- ✓ is able to misuse his/her knowledge without the risk of immediately signalling the system to the unauthorized operation of the operation, or without the risk of recording the operation in a "log" or "audit trail" type, etc.,
- ✓ knows in detail the functions of individual programs, – has access to the workplace software,
- ✓ has access to files intended for the transmission of data to the headquarters or to other organizations,
- ✓ can create or abuse non-standard situations that are handled operationally without standardized procedures.

The most common motives of these perpetrators are in particular greedy motives, motives arising from conflicts in interpersonal relationships, desire to gain power or sovereignty, desire to demonstrate their intellectual superiority, desire to overcome the feeling of underestimation of their abilities, cover motives to conceal the pursuit of another criminal activities, political motives and others. Knowing the motive of a computer crime is significantly important, especially for identifying the probable perpetrator of a crime from a predefined circle of suspects - mostly current or former employees of the injured company. Finding out the motive is closely linked to resolving the question of who benefits or can benefit from the consequences of an anti-social act. Last but not least, it is important to know the motive for the correct criminal qualification of the unlawful conduct and for determining the degree of social harm of this proceeding. Knowing the motive of a computer crime is significantly important, especially for identifying the probable perpetrator of a crime from a predefined circle of suspects – mostly current or former employees of the injured company. Finding out the motive is closely linked to resolving the question of who benefits or can benefit from the consequences of an anti-social act. Last but not least, it is important to know the motive for the correct criminal qualification of the unlawful conduct and for determining the degree of social harm of this behaviour.

Given technical developments and the exploitation of its results in relation to crime commission, computer data are a valuable source of evidence for bodies active in criminal procedure and the courts. The commission of crimes by means of computer systems, the transmission of information on planned, committed or already committed criminal offenses through them and the storage of information relevant to criminal proceedings by means of computer systems require that these bodies have a legitimate impact on computer data, whether in order to obtain evidence or removal of computer data with defective content from the computer system. Criminal law at both international and national levels had to respond to this need and technical progress[10].

From a practical point of view, in investigating cybercrime by bodies active in criminal procedure, relatively effectively are used for example, institutes of storage and issuance of computer data (Section 90 of the Criminal Procedure Code) and the discovery and reporting of data on telecommunications operation performed (Section 116 of the Criminal Procedure Code), which are subject to telecommunications secret, or covered by the protection of personal data

[10] R. Kubička, O. Kubička, Počítačové údaje v trestnom konaní, [in:] Aktuálne výzvy prevencie počítačovej kriminality. Zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou, Akadémia Policajného zboru v Bratislave, Bratislava 2018, p. 83.

which are necessary to clarify facts relevant to criminal procedure. The criminally relevant facts thus established may subsequently serve as evidence in criminal proceedings[11].

Forensics is an independent scientific discipline that examines and clarifies the laws of origin, extinction, search, seizure, investigation and use of forensic traces, other forensic evidence and forensically relevant information. On this basis, it develops methods, means, procedures, operations and recommendations for forensic practical activities, regardless of the formal conditions of their use in the practice of various police forces[12].

Since its inception, forensics has been classified (together with criminology, penology, criminal science and various forensic sciences) into a group of scientific disciplines dealing with the negative social phenomenon – crime[13].

Cybercrime can also be described as one of the modern types of crime, which, no doubt, is also dealt with by forensics. Its origins date back to the 60s and 70s of the last century and it is currently one of the fastest growing types of crime and at the same time it is a highly sophisticated crime. The theory, but also practice, distinguishes several methods of committing this so-called computer crime, whether it is unauthorized interference with input data, unauthorized changes in stored data, unauthorized intrusion into computer systems and their databases and the like, and these methods of cybercrime can constitute certain offences stipulated by the Criminal Code. In the process of investigating cybercrime, it is possible to encounter a number of forensic traces, some of which are typical for cybercrime, especially material traces, digital, computer traces, documents and factual evidence, and memory traces. Given these highly specific forensic traces, the investigating authority must adapt not only the process of securing these traces, but also the process of cybercrime investigation itself so that the individual evidence is legally secured so that the perpetrators of the crime can be identified and fairly punished in the subsequent process. However, the fight against cybercrime should be primarily about protecting and strengthening critical infrastructure and other network facilities, and not just about taking repressive measures[14].

References

1. Dražová P., Zákonnosť a prípustnosť elektronických dôkazov, [in:] Zákonnosť a prípustnosť dôkazov v trestnom konaní. Zborník príspevkov z medzinárodnej vedeckej konferencie Bratislavské právnické fórum 2019, Univerzita Komenského v Bratislave, Právnická fakulta, Bratislava 2019.
2. Klimek L., Základy trestného práva Európskej únie, Wolters Kluwer, Bratislava 2017.
3. Kubička R., Kubička O., Počítačové údaje v trestnom konaní, [in:] Aktuálne výzvy prevencie počítačovej kriminality. Zborník príspevkov z vedeckej konferencie s medzinárodnou účasťou, Akadémia Policajného zboru v Bratislave, Bratislava 2018.
4. Musil J., Kriminalistika, vybrané problémy teorie a metodologie, PA ČR, Praha 2001. Polák P., Kubala J., Repetitórium kriminalistiky, druhé, prepracované a doplnené (aktualizované) vydanie, Wolters Kluwer, Bratislava 2017.
5. Polčák R. a kol., Elektronické důkazy v trestním řízení, 1. vyd., Masarykova univerzita,

[11] Pursuant to Section 63 para. 1 of Act no. 351/211 Coll. on electronic communications, subject to telecommunication secrecy is a) the content of transmitted messages, b) related data of communicating parties, which are the telephone number, business name and registered office of a legal entity, or business name and place of business of a natural person - entrepreneur or personal data name, surname, title and address of permanent residence; the subject of telecommunication secret is not the data published in the telephone directory, c) operational data and d) location data.
[12] J. Musil, Kriminalistika, vybrané problémy teorie a metodologie, Praha 2001, p. 18
[13] V. Porada a kol., Kriminalistika. Technické, forenzní a kybernetické aspekty…, p. 29.
[14] European Parliament Resolution No. 2017/2068 (INI)…

Právnická fakulta, Brno 2015.

6. Porada V. a kol., Bezpečnostní vědy, Aleš Čeněk, Plzeň 2019.
7. Porada V. a kol., Kriminalistika. Technické, forenzní a kybernetické aspekty, 2. aktualizované a rozšířené vydání, Aleš Čeněk s.r.o., Plzeň 2019.
8. Smejkal V., Kybernetická kriminalita, 2. vyd., Aleš Čeněk, Plzeň 2018.