Prof. JUDr. Jaroslav Klátik, PhD.
Director, Department of Penal Law, Criminology, Criminalistics and Forensic Sciences, Faculty of Law, Matej Bel University, Banská Bystrica, Slovakia
E-mail: jaroslav.klatik@gmail.com

JUDr. Milada Raďašová
External PhD. student, Department of Penal Law, Criminology, Criminalistics and Forensic Sciences, Faculty of Law, Matej Bel University, Banská Bystrica, Slovakia
E-mail: milada.radas@gmail.com

DOI:
Review paper
Received: February 28, 2025
Accepted: April 4, 2025

CYBERCRIME: MODERN THREAT IN CONTEMPORARY SOCIETY

Abstract: *The content of the paper deals primarily with the issue of cybercrime, emphasizing the European Cybercrime Centre. It presents an impartial view on the issue of cybercrime and the activities of the European Union in this area. It introduces the basic concepts related to cybercrime, including cyber security, cyber threats, and types of cyber attacks. It examines the legal regulation of cybercrime, emphasizing the gradual development of transnational legal instruments. The paper mentions the historical context of cybercrime and the various major cyber attacks in selected European Union Member States.*

Keywords: *cybercrime, cyberspace, cyber threat, cyber attack*

Introduction

Today, we live in a modern age influenced by the latest technological advances. It is no exception that everything around us is connected to the Internet, and what in the past was only a passive part of our homes is no exception. However, few people realize that what we usually consider an advantage today and a simplification of our lives is an opportunity for someone else to threaten or rob us.

Threats are literally around every corner in the online space, and you never know if opening a message from an unknown sender will open the gates to your computer wide open. In addition, various organizations face similar threats, including banks, hospitals, government organizations, and even states. To defend against such cyber-attacks, all sorts of organizations have been set up that operate at national, international and even global levels.

One such organization is the European Cybercrime Centre, which operates within the European Union as part of Europol. The European Cybercrime Centre is the focus of this paper.

We consider the issue of cybercrime and cybercrime to be particularly important today. The activities carried out not only by the European Union protect us and our property from illegal threats from the Internet environment. However, the activities carried out in this area are only minimally discussed among the general public. This was one of the main reasons why we decided to define such an important organization as the European Cybercrime Centre in this paper.

1 Cybercrime

Based on the constantly developing and growing use of information technology globally, it is practically possible to trace that the use of computers and the Internet is now ubiquitous. With the growing trend in the use of these technologies, the possibility of using these modern technologies also increases to misuse them to commit criminal activities. Therefore, information technology inherently creates a platform that practically enables the development of existing crime or even the creation of entirely new crimes that have not yet been classified. Cybercrime, as we know it today, dates back to around the 60s -70s, when the first use of information technology to commit crime was recorded (Ivor, 2013). However, we must state that cybercrime is a much more serious problem today, as the sophistication of the perpetrators' actions has increased considerably, and the technologies used for criminal activity are at a completely different level. The variety of individual crimes has also increased significantly. To better understand cybercrime, it is helpful to become more familiar with the terms crime and cyberspace, in which cybercrime occurs (Dianiska, 2016).

By crime, we can conceive of intentional activity that is inherently unlawful, punishable, and punishable by law (Lubelcová, 2003). The definition of this concept has

changed only minimally in the historical context. In contrast, the very criteria of what is considered a crime have changed over time in parallel with changes in social norms and territorial location, which is decisive in developing measures to combat cybercrime, among other things. Within the European Union, for example, the creation of several international organizations such as Europol has now made it possible to coordinate measures taken against cyber criminals. Some states in other parts of the world, such as India or some African states, which are currently struggling with an increasing number of cybercrimes, have largely inadequate legislation in place, and we can still encounter states in which such legislation does not exist (Andrasko, Mesarčík, Sokol, 2022).

One of the earliest uses of the word cyberspace was recorded in the 1984 novel Neuromancer, by William Gibson. Although this definition has remarkably little to do with the word's current meaning, it is realistic to paraphrase it and define cyberspace as an abstract environment used to represent the data on which computers operate (Anisa, 2016).

The US National Institute of Standards and Technology (NIST) defines cyberspace as a global domain within the information environment that consists of an interconnected network of infrastructures and information systems, including the Internet, telecommunications networks, computer systems, and embedded processors and controllers. However, cyberspace is also defined as an electronic system that allows computers worldwide to communicate and retrieve information (Cambridge Dictionary, 2022). Based on these definitions, it is apparent that there is simply no clear and precise definition of what cyberspace is at this time. However, it can be stated that it is an abstract space, primarily an Internet environment made up of a computer network that is separate from the physical world.

2 Historical context

We deem it appropriate to delineate at least a brief history and development of cybercrime. We have included this section primarily to understand better the individual criminals who have shaped the crime sector we are studying today. Since the history of cybercrime itself, which can realistically be traced over the past 40 years or so, is extremely rich, in this section of the paper, we will summarize those crimes that were pioneers within their category or significant to the extent that they changed the course of development and the very view of cybercrime (Matějka, 2002).

Even though we can practically state that the history of cybercrime itself began around the 1960s, the fact remains that at that time, the term was not yet defined as we know it today. If we look at things from this perspective, the history of cybercrime itself only began to be written during the 1980s, when the first genuinely significant cyber incidents were recorded, which, in essence, fit into the current understanding of the term (Freed, 1996).

3 The origins of cybercrime

For the origins of cybercrime, the phase of the invention of the mobile phone from 1976 to 1981 is significant. The invention of the mobile phone is considered necessary in this context, mainly because it is regarded as the first means of electronic communication (Matejka, 2002). Associated with this first period is the emergence of cybercrime, aimed at perpetrating damage to the material component of computers or, in later times, to the data stored on them. The first personal computer was put on the market on 12.08.1981, and in this period, the first interconnections of computers at the network level occurred (Jirovský, 2007).

It was characteristic of the 1980s that computers were becoming more and more accessible to ordinary users. However, it was also typical of this period that data protection was only minimally developed and even less applied, which allowed for real vulnerabilities in the systems of the time. However, this vulnerability was overlooked primarily because it was not realistically expected to be exploited to cause difficulties for users at the time. There were no known cyber attacks yet that would affect higher numbers of users or systems. The protection of user data was significantly underestimated, making it relatively easy to spread the first malicious programs. This software is generally considered to be the first documented computer worm (Whiteside, 1978).

In November 1988, a computer program called the Morris worm saw the light of day. This name was derived from its creator, Robert Tappan Morris. The spread of this worm led those responsible to change the perception of computer security, both among the developers themselves and among end users. Several reasons for creating this program are known, but it is impossible to identify its primary purpose. It could have been to overwhelm the OSUNIX devices or some of the by-products (Draper, 2018).

If we take a closer look at the Morris worm, the program itself was not malicious, as it had only one function, namely replication on the infected device, which led to a rapid

slowdown of the infected computer. The truth remains, however, that Morris created a self-replicating program, which effectively made him the first documented case and the first person to be convicted of creating a malicious program (Erickson, 2008).

Another first was recorded in 1989. This incident was already much more damaging than the one before. It was in this year that the emergence of the first Randomware, commonly known as AIDS, was recorded. As such, the virus spread through floppy disks that were given out to patients who were infected with the AIDS virus. The workings of this program were based on the fact that when a floppy disk was inserted into a computer, the number of times the operating system was booted was monitored. When the number reached ninety, all data on the device was encrypted. The ransomware then prompted victims whose devices were unusable in this state to send a ransom note, after which the data was decrypted again. Although this design is relatively primitive by today's standards, it laid the groundwork for concepts still in use today (Kosseff, 2018).

Even during 1999, computer viruses were still relatively unknown. With the development of computer networks, technology misuse has evolved into cybercrime as we know it today. The ineffectiveness of security techniques at the time encouraged the rapid spread of the virus known as Melissa. This virus, once infected, took control of the user's MS Word program, spreading via emails. Upon opening an enticingly named email attachment, the message was sent to the first fifteen contacts in the user's address book, through which the virus spread relatively quickly. Derivations of this solution are still being used today, particularly in the case of social engineering and spam messages.

4 Global incidents over the past decades

In line with the increasing digitalization of society and the common everyday use of information technology, the last decade has brought significant changes in malware applications. These are becoming increasingly sophisticated and sought after by organized groups, individuals, and possibly government departments. The targets of individual attacks have also changed. They are now not attacks on individuals but targets of international or global significance (Elisan, 2015).

Malware is becoming a target for pursuing political or state objectives, and humanity has entered a new era of the severity and scale of cyber-attacks. In 1999, an incident virtually made it possible to define a new field of cyber incidents, namely the cyber weapon or cyber weapon.

Stuxnet is a specific worm that appeared in an Iranian computer. Its primary function was targeting systems, obtaining information, and controlling surveillance devices. Based on the fact that it definitely takes human resources to create such a program and also considerable funds, and also based on the fact that it was discovered in the system of the Iranian nuclear program, it can be assumed that the origin of this malware goes back to the United States of America in cooperation with Israel. This solution can be described as a cyber weapon based on its characteristics. Its discovery has led to a failure to rethink the perception of cyber-security at the state level (Fruhlinger, 2022).

Indeed, the massive spread of digitization among end-users allows more manageable and more efficient access to information, but it also opens the way for the subtle exploitation of malware. The profile of many malware solutions has changed significantly over the last decade. It was also during this period that the most serious attack by such software to date was recorded. WannaCry was the first known ransomware to operate as a worm, i.e., replicate itself as it was distributed, allowing it to spread rapidly. The software exploited a vulnerability in the older Windows OS, which was heavily exploited. The biggest problem arose in the US, where the healthcare sector was significantly affected (Kolouch, 2016).

It is on the basis of the incidents described above, their scale, and severity, it can be stated that cybercrime has an increasing tendency with time, not only concerning the number of attacks but also their severity and scale.

5 Cyber Incidents in Europe

With the development of technologies that support the anonymity of users and devices in the Internet environment in the form of virtual private networks (VPNs), it is becoming increasingly difficult to identify the originator of malware and the source from which the software originates. Against this background, the demands for international cooperation in cybercrime investigation are growing exponentially. Even though it is challenging to identify the source and author of malware, it is possible to determine at least the approximate location of a cybercrime by quickly locating the victim. Similarly, based on the number of victims of each attack, it is also possible to determine the number of victims in a country or a more significant representation of countries.

An example of an incident recorded in this way was the one in 2007, which targeted Estonia. The incident took place over three months when Estonia's server system was

attacked by DDoS attacks that crippled its operations. DDoS is a type of attack that has as its primary goal to completely cripple or at least slow down the attacked server or service as much as possible. Even though, based on the situation at the time, this attack was attributed to Russia, it is impossible to say who was behind it. Similarly, this attack has been classified as a cyber-weapon attack (EC-Council, 2009).

Hand in hand with the increasing number of cyber-attacks, and given their decentralization and the growing problems associated with the prosecution and conviction of the perpetrators of these attacks, the response coming from the European Union has been the creation of coordination and security groups under the umbrella of existing security forces. These new groups aim to monitor, coordinate, and, where appropriate, assist in the active resolution of cybercrimes carried out within the European Union. Establishing these groups has led to a turnaround in the detection of cybercrimes and the identification of victims.

An example of how the fight against cybercrime works is detecting and dismantling an organized group that carried out targeted attacks on ATMs. This group was referred to by the security services as ATM Black Bo. Essentially, this was a type of attack through an unauthorized device (laptop) connection that sent cash withdrawal orders directly to the ATM to withdraw cash from the ATM and convince the ATM that a legitimate user was interacting with it. In most cases, users gained access to the ATM by drilling holes or melting the main panel to attach the device. Once the device was connected to the wiring, it sent commands that caused the ATM to dispense all the cash. In this case, there was an internationally organized group, which in particular led to the execution of arrest warrants in some Member States of the European Union. The perpetrators were prosecuted for their actions (Jirovský, 2007).

Another example that could be mentioned was the elimination of one of the longest-running malware families, Andromeda. Malicious code based on this family of viruses formed a network of bootlets. Andromeda's primary goal was to distribute malware. The possibility of cooperation available, made possible by the cooperation of the security services and adequate legislation, made it possible to coordinate the attacks on the servers distributing Andromeda, which led to the cessation of its activities (NEC Security blog, online).

According to Europol, the Emotet malware, which primarily targeted the banking system, was considered the most significant threat in Europe. An organized group was

behind this malware, suggesting changes in how cyber attacks are understood and carried out. In this case, the primary task was to infect a device that would make the server available to other malware. Its secondary function was to be able to collaborate with different groups and install other types of malware on the already infected device. This malware was stopped in 2021 with the cooperation of several European Union Member States (Germany, the Netherlands, Lithuania, Britain, and France) and the USA, Canada, and Ukraine (EUROPOL, online).

It is necessary to highlight a cyber attack recorded within the Slovak Republic. The Office of Geodesy, Cartography, and Cadastre of the Slovak Republic has been the victim of a ransomware cyber-attack. This type of malware blocks a computer system or encrypts data written on it and demands a ransom from the victim to restore access. This cyber-attack paralyzed the information system of individual cadastral departments and is considered the most extensive intervention ever in state organizations within the Slovak Republic. This cyber-attack blocked the functioning of individual cadastral departments and the downstream activities of other bodies, e.g., in the performance of tax administration etc. (Legalis, 2025).

However, cyber-attacks expose weaknesses in the internal security of individual states. Thus, there is a constant shift in the field of cyber-security, especially concerning foreign cyber-attacks.

6 Cybersecurity

The evolution of global trade and communication has increased global interconnectedness, where states are now connected through many complex networks (Rothery, 2019). Cybersecurity is one of the newest areas of state security policies that is becoming increasingly important in the security sectors of states in Europe. Given the rate of innovation, policymakers and others are continuously seeking to understand the range of modern technologies, techniques, and their application. This situation requires rapid and comprehensive development of new legal and political frameworks (Milenkovic, 2023).

Looking around our neighborhood, we find that people of all ages and genders constantly stare at mobile phone screens, laptops, or tablets. Whether we are more or less aware of it, virtual reality has become a regular part of our everyday lives. It is certainly worth mentioning that cyberspace is now officially recognized as the fifth military space for a possible encounter with the enemy (Ivančík, Baričičová, 2019).

In professional circles, we read, among other things, that cyberspace is essentially a space for business and education, i.e., a space for storing and retrieving information and, from the point of view of the majority of the population, a space for entertainment. Cyberspace holds incredible possibilities that most of the population has no idea about. At the same time, however, this space is also open to hackers, crackers, atavistic groups, and, unfortunately, terrorist groups. For this reason, it certainly makes sense to look at the security of cyberspace. On the one hand, thanks to the acceleration of digitization, information is being exchanged more and more efficiently, and everyday concerns are being simplified. On the other, however, we are constantly under the negative influence of cyberspace, which makes us weaker and weaker (Andraško, 2022).

Digital technologies have become the backbone of all the world's advanced economies, especially in recent years. It could be said that a complex system is built on them, which keeps the economy running, medical facilities, energy supply or transport systems, and so on. Many companies base their business primarily on permanent access to the Internet and the smooth functioning of information and communication technologies (Koffeff, 2018).

Cybersecurity incidents (hacking or terrorist attacks) or accidental incidents (earthquakes or incidents caused by human error) that disrupt standard space have a negative impact not only on the economy but also on human conscience or human lives (power outages in hospitals or airports can have fatal consequences). All of us have probably encountered some form of attack, which in most cases has been associated with data loss. However, few people give real thought to the kind of attacks that state institutions, ministries, or critical infrastructure entities may face in practice outside our awareness. Security in cyberspace is essential for all actors, from the lowest to the highest level.

Cyber threats have expanded from targeting and harming computers, networks, and smartphones — to people, cars, railways, planes, power grids, and anything with a heartbeat or an electronic pulse. Many of these things are connected to corporate networks in some fashion, further complicating cybersecurity (Morgan, 2020).

While the Internet provides economic benefits to individuals and institutions, the accessible, unrestricted, and unlimited access to the Internet exposes the space to both criminal actors and users, giving room for myriads of cyber-criminal activities, including

hacking, phishing, ransomware, identity theft, cyberstalking, etc. These activities have led to considerable costs to individuals, organizations, and world nations (Onwuadiamu, 2025).

7 Information Revolution

It is often said that the current century is the century of the Internet and information technology. Due to the speed of development of new technologies and the almost instantaneous transmission of data and information anywhere in the world, information is becoming a desirable commodity with immense strategic value. To ensure security for all actors, securing a particular competitive advantage in information is essential. Today's war is not based on who has the greatest access to human resources, capital, or advanced technologies; it is primarily about who has the best information about the enemy and the battlefield.

The information revolution transcends real and perceived boundaries, transforming world politics so governments lose their dominant position as the leading players. Individuals are now capable of moving and influencing global events. For example, Edward Snowden, a former employee of the National Security Agency, leaked information about the massive surveillance of electronic communications and the interception of telephone conversations. Various organizations are also influencing global events, and we could include, for example, the world-famous Wikileaks as a media company publishing long-classified information. The information revolution fosters the growth of a global network that allows individual actors to communicate, consult, coordinate, and work together regardless of distance. However, this also creates a significant threat source (Andress, 2019).

Conclusion

Defining the term security itself is, in our opinion, easiest through its negative definition. Thus, security is a state in which the subject is not threatened. We must state that this state is still a utopia at present. Even a seemingly secure Europe is facing terrorist attacks. Where there is virtually no open armed conflict, we have terrorist attacks, murders, and ambushes. On the positive definition of security, we could note that it refers to a specific object, thing, person, state, or security community. The most secure subject is the

one that is assured of its survival and the possibility of further development. Thus, a secure entity is not under any direct or urgent threat or reliably protected from such threats.

Traditional forms of crime appear to be committed to a lesser extent nowadays, but crime has increased through modern technology. Computer crime is a growing problem, causing enormous damage every year.

The field of cyber security or cybercrime has gained the attention of experts and researchers who focus on research aimed at increasing cyber resilience, introducing the latest cyber security technologies to strengthen research and innovation in the field of cyber security.

The paper also pointed to specific cyber-attacks, in which it can be noted that cybercrime is emerging even in the most advanced countries. Therefore, looking for innovative solutions that will protect against the latest, cutting-edge cyber threats is essential. As today's society increasingly uses and relies on modern technology, states are spending considerable resources to prevent cyber-attacks from being perpetrated.

References

1. Andraško, J. et al. (2022) Právo kybernetickej bezpečnosti. Bratislava: Univerzita Komenského v Bratislave, Právnická fakulta 2022. 544 s. ISBN: 978-80-8168-905-5.
2. Andress, J. (2019) Foundations of information security: A straightforward Introduction, No Starch Press. 248 s. ISBN: 978- 17-1850-004-4.
3. Cambridge dictionary. [Online]. https://dictionary.cambridge.org/dictionary/english/cyberspace.
4. Convention on cybercrime. [Online]. https://rm.coe.int/1680081561.
5. Dianiška, G. et. al. (2016) Kriminológia. 3 vydanie. Plzeň: vydavatelství a nakladatelství Aleš Čenek s.r.o. 405 s. ISBN: 978-80-7380-620-0.
6. Draper, J.T. et. al. (2018) Beyond the little blue box. Friesen Press. 263 s. ISBN: 978-15-2550-570-6.
7. Directive (EU) 2016/1148 of the European Parliament and of the Council of July 6 2016 concerning measures for a high common level of security of network and information systems across the Union.
8. Elisan, Ch. C. (2015) Advanced Malware Analysis. 1 st ed. Mc Graw – Hill Education. 544 s. ISBN: 978-00-7181-974-9.
9. Enisa: Definition of cybersecurity – Gaps and overlaps in standardisation. [Online]. https://www.enisa.europa.eu/publications/definition-of-cybersecurity.
10. Erickson, J. (2008) Hacking: The Art of exploitation. 2 ed. San Fransicso: No Starch Press. 488 s. ISBN: 978-15-9327-144-2.
11. Freed, R.N. (1996) Computer Fraud – a management trap: Risks are legal, economic, professional. In Business Horizons. ISSN: 0007-6813, vol. 12, no 3.
12. Fruhlinger, J. Stuxnet explained: The first known cyberweapon. [Online]. https://www.csoonline.com/article/562691/stuxnet-explained-the-first-known cyberweapon.html.
13. Ivančík, R. Baričičová, Ľ. (2019) Kybernetické hrozby ako súčasť asymetrických bezpečnostných hrozieb v 21. Storočí. In Aktuálne výzvy kybernetickej bezpečnosti (v podmienkach bezpečnostných zložiek). Zborník príspevkov. Bratislava: akadémia Policajného zboru v Bratislave. s. 35-47. ISBN: 978-80-8054-819-3.
14. Ivor, I. (2013) Trestné právo Európskej únie. Bratislava: Eurokódex. 888 s. ISBN: 987-80-8155-017-1.

15. Jirovský, V. (2007) Kybernetická kriminalita: nejen o hackingu, crackingu, virech a trojských koních bez tajemství. Praha: Grada. ISBN: 978-80-247-1561-2.
16. Regulation (EU) 2019/881 of the European Parliament and of the Council of April 17 2019 on ENISA (the European Union Agency for Cybersecurity) and on information and communications technology cybersecurity certification and repealing Regulation (EU) No 526/2013 (Cybersecurity Act).
17. Rothery, C. (2019) Time for a national security strategy. In: National Security Journal, Volume 1, Issue 1, ISSN: 2703-1934.
18. Kosseff, J. (2018) Defining Cybersecurity Law. In Iowa Law review. vol. 109. no 985. p. 1010.
19. Lubelcová, G. (2003) Kriminalita: koncepcie, trendy, dôsledky. In: Slovensko v devätdesiatych rokoch: osem pohľadov. Bratislava: Univerzita Komenského. s. 181-228. ISBN: 80-223-1732-2.
20. Matějka, M. (2002) Počítačová kriminalita. Praha: Computer Press. 106 s. ISBN: 978-80-7226-419-3.
21. Morgan S. (2020) Cybercrime to cost the world $10.5 trillion annually by 2025. In: Cybercrime magazine. [Online]: https://cybersecurityventures.com/cybercrime-damage-costs-10-trillion-by-2025.
22. Milenkovic, D. (2023) Cyber security and data collection. In: Security Science Journal. Vol. 4. No. 1. [Online]: http://www.securityscience.edu.rs/index.php/journal-security-science/article/view/98/68.
23. Onwuadiamu, G. (2025) Cybercrime in criminology, a systematic review of criminological theories, methods, and concepts. In: Journal of economic criminology. [Online]: https://doi.org/10.1016/j.jeconc.2025.100136.
24. Slatalla, M. (1995) The masters of deception: The gang that ruled cyberspace. New York: Harper Collins. 240 s. ISBN: 978-0-06-092694-6.
25. Whiteside, T. (1978) Computer Capers: Tales of electronic thievery, Ebmezzlement and Fraud. 1 ed. New York: Ty Crowell Co. 173 s. ISBN: 978-06-9001-743-4.
26. https://www.europol.europa.eu/media-press/newsroom/news/world%E2%80%99s-most-dangerous-malware-emotet-disrupted-through-global-action
27. https://www.legalis.sk/sk/aktuality/kyberneticky-utok-na-kataster-bezpecnostna-rada-sr-zasadne-v-piatok.a-1101.html
28. https://www.nec.com/en/global/solutions/cybersecurity/blog/240823/index.html