Julia Czajka
Academic Center For Strategic Analysis
ORCID: 0009-0000-6596-7069
j.czajka@akademia.mil.pl

Computer crime in the information society

Abstract

The development of new forms of communication and information exchange which use electronic and digital devices makes the problem of computer crime grow in importance. The advances in technology and electronics have made devices like computers, cellular phones, and the Internet available to the population. Although ICT (information communication technology) devices make everyday life easier, their operation generates a number of risks.

This paper focuses on computer crime in the face of the development of the information society. The main objective of the study discussed here was to determine the impact of computer crime on the information society. The classification and forms of computer crime, the methods used as a tool to prevent computer crime, and the strategies used to combat computer crime at international level were among the issues identified for the problem under study.

Key words

computer crime, information society, cyber threats, cybercrime, data protection and security

Introduction

The development of social and economic life depends on the ability to communicate and exchange information[1]. The second half of the twentieth

1 J. Radzimirski, *Społeczeństwo informacyjne*, [in:] *Informatyka ekonomiczna: podręcznik akademicki,* eds. S. Wrycza, Warszawa 2010, p. 470.

century saw the rise of importance of computer devices as communication media. They brought about a qualitative change as a new type of society emerged: a society based on information, where information is among the most valuable commodities; it affects economies and is decisive to their competitiveness. This new society based on information and its exchange is called the information society. Coined after the 1950s, the concept of information society identifies the advances in engineering, especially electronics and information communication technologies as key development drivers of the information society[2]. The first theoretical works from the USA and Japan concerning the information society were written in the 1960s and 1970s; the first ones from Europe, including Poland, appeared in the 1990s.

The official term "information society" was adopted at the 2005 World Summit on the Information Society (WSIS) in Tunis. According to the definition of information society, it has been established that it is a type of society in which everyone is allowed free access to create, receive, share and use information and knowledge, which contributes to economic, social, political and cultural development[3]. The foundation which the information society needs to function on are modern telecommunication networks, which should reach all citizens and be publicly available.

The development and sophistication of ICT is accompanied by a wide range of potential vulnerabilities that may imply security breaches of data or IT systems and infrastructure. One of the risks to users of ICT devices and systems is *computer crime*, which the International Criminal Police Organisation "INTERPOL" defines as "[...] criminal acts against computer systems and criminal acts committed using computers as crime tools"[4]. In turn, some researchers define „computer crime" as „any criminal activity in which the computer is either a tool or an object of attack"[5] or „a phenomenon of forensic science involving any criminal behaviour relevant to the functioning

2 Ibidem, p. 473.
3 Ibidem, p. 471.
4 *Charakterystyka przestępczości komputerowej*, http://przestepstwo-komputerowe.eprace.edu.pl/1081,Charakterystyka_przestepczosci_komputerowej.html#google_vignette [access: 26.12.2024].
5 K.J. Jakubski, *Przestępczość komputerowa – podział i definicja,* „Przegląd Kryminalistyki" 1997, no. 2, p. 31.

of electronic data processing, which directly harms the processed information, its carrier and circulation in computers and entire computer connection systems, as well as the computer hardware itself and the right to computer programs"[6]. Approaches to computer crime equally include a narrow and broad range of understanding; all of the definitions cited above apply to and include criminal acts using a computer as a tool or object of attack. When considering the problem of computer crime, it is worth mentioning its purpose, which is "the theft of data, unauthorised disclosure of information, sabotage of an IT system or other legally prohibited actions against the IT infrastructure of an organisation, company, individual, institution or an entire state"[7]. Note that it is not only individuals who can fall victim to computer crime; the victims can be groups, such as commercial companies, which can pose a threat to the national economy.

Research methods

The problem outlined above was decisive to this author's undertaking the research aimed to identify the key determinants of computer crime in the information society. The main problem was formulated as the following research question: 'How does computer crime affect the functioning of the information society?' Specific problems were formulated as the following questions to address the main problem:

1. What is the classification and forms of computer crime?
2. What are the methods of computer crime prevention?
3. What strategies exist to combat computer crime at the international level?

The subject of computer crime is important and worth addressing for several reasons. Firstly, the fundamental problem concerns the correlation between computer crime and the information society. In an age of evolving information and communication technologies, society is increasingly reliant on digital infrastructures in various spheres of daily functioning, both private and professional. This phenomenon provides benefits while generating

6 Ibidem, s. 31.

7 D. Filipek, *Co to jest przestępczość komputerowa?*, https://itcenter.pl/2023/10/31/co-to-jest-przestepczosc-komputerowa/ [access: 26.12.2024].

new risks related to computer crime. Awareness and understanding of this phenomenon and its consequences is essential to safe functioning in cyberspace. Secondly, computer crime is a serious threat to state security. Attacks on critical infrastructure, including financial and energy systems, can paralyse the entire state and stir public chaos. These arguments are the basis for justifying the high importance of the problem being addressed. It remains relevant in this day and essential to understand and counter one of the greatest modern challenges. Investigating computer crime in today's information society can contribute to structuring knowledge on the subject being addressed here. It can also raise awareness of the risks involved in the use of electronic or digital devices, as well as promote ethical and safe use of the latest technologies.

The research objective was achieved by applying a research method such as content analysis. This method builds on existing material that is the body of knowledge on a given issue, reflecting existing beliefs and opinions. Publications, scientific papers and content from selected websites and web portals were used in this paper.

Discussion and findings

Classification and forms of computer crime

Computer crime is a type of crime which the Polish criminal law qualifies as a typical economic crime[8]. As A. Adamski points out, "[...] being one of the latest types of criminal activity, it [computer crime] challenges the traditional criminal law system"[9]. The official website of the Podlaskie Province Police Command details the classification and types of computer crime (fraud) committed online (on the Internet), which are specified in the Polish Criminal Code of 1997[10]:

8 A. Adamski, *Prawo karne komputerowe*, Warszawa 2000, p. 115.
9 Ibidem, s. 115.
10 Ustawa z dnia 6 czerwca 1997 r. – Kodeks karny, Dz. U. 1997, no. 88, ited 553, art. 267, 268, 268a, 269, 269a, 269b, 286, 287.

– illegal acquisition of information (hacking);
– covert computer monitoring and data capturing (sniffing);
– computer sabotage;
– computer espionage;
– malicious software (malware) distribution and software cracking;
– hacking tools;
– phishing[11].

Illegal acquisition of information, known as *hacking*, is the use of remote techniques and tools to gain unauthorised access to computer systems, networks or data. The activity means hacking into someone else's computer or mobile device (a phone or tablet) to steal data. Its fixture is to include manipulation or exploitation of gaps in systems to steal data, interrupt services, or initiate other actions. The most often motivation behind hacking is financial, political, social or educational. Its consequences include the possibility of corrupting or deleting information stored in the memory of a device or making it difficult for authorised personnel to access the data[12].

Covert computer monitoring and data capturing (sniffing) is defined as "illegal monitoring and data capturing by means of technical facilities, monitoring of networks with the intent of stealing data, spying on network activity and collecting information about users"[13]. Initially, sniffing was a tool used by network administrators to diagnose and analyse online link performance issues, but hackers quickly recognised the potential of this technique and began using it for illegal ends[14]. This type of activity uses special computer software to capture and analyse data. The objective of criminals committing sniffing is to extract confidential data for a financial gain or, by

11 *Rodzaje i kwalifikacja przestępstw komputerowych*, https://podlaska.policja.gov.pl/pod/policja-podlas/dzialania/przestepczosc-gospodar/struktura-wydzialu/zespol-iii/rodzaje-i-kwalifikacja/28410,Rodzaje-i-kwalifikacja-przestepstw-komputerowych.html [access: 26.12.2024].

12 *Hacking*, https://www.comcert.pl/slownik/hacking/ [access: 26.12.2024]; *Czym jest hacking?*, https://conselion.pl/czym-jest-hacking-komputerowy/ [access: 26.12.2024].

13 *Kształtowanie się cyberprzestępczości*, https://gazeta.policja.pl/997/numery-specjalne/specjalne-gazeta-policy/gazeta-policyjna-nr-2-s/212264,Ksztaltowanie-sie-cyberprzestepczosci.html [access: 26.12.2024].

14 *Podsłuch komputerowy*, https://cyberprzestepczosc.info/podsluch-komputerowy/ [access: 26.12.2024].

tracking a user's online activity, to act against individuals, violating the human right to privacy.

Computer sabotage is an action with the objective of disrupting or blocking the operation of a computer system. The main subject of protection in this criminal act is IT data of major importance for state defence; it can be, for example, operational data of the Armed Forces, information concerning critical infrastructure, or data concerning citizens, like personal data. Computer sabotage consists of modifying data without authorization, violating the integrity of the attacked system, destroying, corrupting, deleting or altering computer data of major importance to national defence, communication security, or the functioning of the government, another state agency or a central or local government institution. The methods most often used by criminals carrying out computer sabotage include: computer viruses, worms, logic bombs, denial of service attacks, unauthorised modification of information, scanning of information or unauthorised access to or use of information[15].

Computer espionage is a form of intelligence operations that is based on the acquisition of confidential data and its transmission to a specific intelligence service via computer networks. This presupposes, first and foremost, that computer espionage is an action in favour of another country[16]. Computer espionage is similar to traditional espionage in many ways. It is characterised by the secrecy of the operation (masking the spy as effectively and for as long as possible), operating in conspiracy (under the pretext of legitimate activity), acquisition of classified information and transmitting it in various forms through computer networks.

Distribution of malware (malicious software) and cracking are crimes which consist in breaching or defeating security features of the exploited software. There is distinction between network cracking (defeating the security features of computer systems) and software cracking (bypassing or removing exploited software-based barriers)[17]. When a device is infected with malware,

15 A. Warchoł, *Sabotaż komputerowy*, https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/12/sabotaz-komputerowy/ [access: 26.12.2024].

16 *Szpiegostwo komputerowe*, http://pandf.wex.pl/szpiegostwo.html [access: 26.12.2024].

17 *Przestępstwa komputerowe*, https://informaticalegis.com/uslugi/przestepstwa-komputerowe/ [access: 26.12.2024].

unauthorised access, data attacks or device freezing are possible. The intent of criminals who commit cracking is to profit from acquired credentials, for example by cracking banking services, to collect personal data for sale or to extort money.

Delving into computer crime, the typical hacking tools used by cyber criminals are worth mentioning. They help to exploit security gaps in systems and networks. These tools include Nmap (for network mapping), Wireshark, Metasploit, John the Ripper, Burp Suite, Aircrack-ng or Kali Linux[18]. While they can be used by criminals, they are common and ethical tools of security professionals, for example, to close security gaps in their own systems.

The final category of computer crime is phishing, a type of attack based on email or cellular text messages (SMS). The latest data from a report by NASK's CSIRT (Cyber-Security Incident Response Team) reveals that the organisation received nearly 96,000 reports of phishing on Polish networks during 2023[19]. The perpetrators of phishing attacks usually want to deceive the victim or cause the victim to take action as the criminals intended. The most common way this happens is by impersonating parcel couriers, government agencies, telecom operators or even friends in an attempt to phish for login details, social media credentials or even bank account credentials. As pointed out on the Polish government's official website, gov.pl, fraudsters have been increasingly operating via instant messaging and social networks, where an example is the "BLIK scam"[20]. Phishing messages are characterised by a high degree of authenticity. Cyber criminals are careful to prepare such messages with precision, so that they appear to be as real as possible, while they are actually fake and pose a high risk (through infected links they can feature, for example).

An increasingly popular type of computer crime is spoofing[21]. This is a type of attack in which a criminal can impersonate a bank, a government agency

18 *Najpopularniejsze narzędzia hakerskie*, https://akademiawywiadu.pl/najpopularniejsze-narzedzia-hakerskie/ [access: 26.12.2024].

19 *Raport roczny z działalności CERT Polska 2023*, https://cert.pl/uploads/docs/Raport_CP_2023.pdf#page=87 [access: 26.12.2024].

20 *Czym jest PHISHING i jak nie dać się nabrać na podejrzane wiadomości e-mail oraz SMS-y?*, https://www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y [access: 26.12.2024].

21 *Czym jest spoofing? Jak go rozpoznać i nie dać się nabrać?*, https://www.gov.pl/web/baza-wiedzy/czym-jest-spoofing-jak-go-rozpoznac-i-nie-dac-sie-nabrac [access: 26.12.2024].

or official, or even another individual, in order to obtain the victim's data or money by deception. Fraudsters can impersonate not only an email address or phone number, but also an IP address (the address of the device connected to a computer network).

The catalogue of risks discussed here refers to attacks with the intent of stealing data; these activities are often financially motivated. Computer crimes also include attacks on infrastructure and cyberspace. These include cryptojacking (the unauthorised use of another person's computer to mine cryptocurrencies), hybrid attacks (particularly dangerous attacks that target state security and involve threats to critical infrastructure, public agencies or economic institutions), or DoS (Denial of Service) and DDoS. (Distributed Denial of Service) attacks that overload a system, network or website by generating large volumes of network traffic, which make the attacked systems or services unavailable to users.

Computer crime, due to its dynamic evolution and multifaceted nature, represents a significant challenge for modern users, entire states and systems. The classification discussed here includes hacking, sniffing, computer sabotage and espionage, cracking, phishing, and spoofing. Although each of the listed crimes is characterised by different methods of action, they share the same overall goal, which is to steal data and gain unauthorised access to information. The increase in the number of attacks, such as phishing and spoofing, suggests a growing threat to data security and privacy, especially in the context of the increasingly popular use of new technologies and instant messaging. Computer crime requires continuous prevention and the application of systemic solutions adapted to the changing realities of the digital world.

Methods of computer crime prevention

Digital attacks are on the rise and can affect any computer user. According to projections by the Council of the European Union, as many as 41 billion devices worldwide will be connected to the Internet of Things in 2025 and, as a consequence, cyber attacks and cybercrime will become more frequent

– and more sophisticated[22]. It is likely that the scale of the problem will grow, which is why awareness of the risks, possible prevention and vigilance, as well as knowledge of methods to prevent computer crime, is so important.

According to a model proposed by cybercrime prevention specialists, methods to prevent digital attacks include four stages:

1) prevention;
2) preparation;
3) response;
4) recovery[23].

The first two stages (prevention and preparation) mean preparing the IT infrastructure in such a way as to make a potential attack as difficult as possible. They include the secure connection of users' computers, including the use of anti-virus software and dedicated platforms that counter potential threats in real time. Response means decisions made in the face of an actual attack, including the victim's response to e.g. the issue of ransom. The last stage (recovery) is a kind of test for the performance of backup solutions and the recovery of the systems' infrastructure to a state of continued operability[24].

The main axis of protection against cybercriminal activity proposed by some experts is the development and implementation of IT security policies and procedures for information system management. An effective solution to prevent loss of access to information is to make regular backups (they are data backups)[25]. Continued education and awareness-raising of users on IT security also remains important.

Concerning individual methods of protection against computer crime, some sources stress the importance of cyber maturity[26]. Cyber maturity is about extreme caution and vigilance during use of digital devices and the Internet. It is recommended to avoid suspicious websites that can intercept

22 *Cyberbezpieczeństwo: jak UE radzi sobie z cyberzagrożeniami*, https://www.consilium.europa.eu/pl/policies/cybersecurity/ [access: 26.12.2024].
23 A. Kostrzewa, *Zapobieganie cyberprzestępczości*, https://mitsmr.pl/b/zapobieganie-cyberprzestepczosci/PLZjzYpX3 [access: 26.12.2024].
24 Ibidem.
25 D. Filipek, op. cit.
26 A. Kostrzewa, op. cit.

data, to secure accounts with strong passwords or use additional (multi-factor) verification methods, and to use anti-virus and firewall software[27].

Strategies of combating computer crime at the international level

As mentioned, cybercrime, including computer crime, is a growing problem in an increasingly digital world. In addition to improving self-awareness about the risks of cybercrime, states and international institutions like the European Union are constantly working at national and international levels to increase the safety on the Internet and of computer use. Processes are underway at European level to strengthen EU-wide resilience to illegal cyber operations. European cybersecurity measures implemented by the European Union Cyber-Security Agency and CERT-EU (Computer Emergency Response Team for EU institutions, offices and agencies) include tracking malicious activities and ensuring education and awareness among citizens and businesses about computer threats and incidents[28]. The institutions of the European Union financially support efforts to ensure and enhance online security, given the important role of the security of networked systems and services in society.

In addition to the measures taken at the European level, regulations and papers on cybercrime exist on the international tier that have been adopted by members of the United Nations. They include the UN Convention against Transnational Organised Crime (UNTOC) of 15 November 2000, the pages of which specify standards for combating organised crime, including criminal acts committed using computer and telecommunications networks[29]. The UNTOC and other UN resolutions on cybercrime are legal instruments in the international system that can help fighting computer crime and foster a coherent approach among the UN member states.

27 M. Budka, C*zym jest cyberprzestępczość i jak się przed nią bronić?*, https://www.money.pl/gospodarka/czym-jest-cyberprzestepczosc-i-jak-sie-przed-nia-bronic-6743245515295296a.html [access: 26.12.2024].

28 *Jak chronić się przed cyberprzestępczością*, https://www.europarl.europa.eu/topics/pl/article/20200327STO76003/jak-chronic-sie-przed-cyberprzestepczoscia [access: 26.12.2024].

29 J. Wrona, *Cyberprzestrzeń a prawo międzynarodowe: status quo i perspektywy*, Białystok 2017, p. 159–160.

Conclusion

A review of publications and sources on computer crime reveals that it represents one of the most serious challenges of the information society and has a significant impact on it. With humans operating in an environment based on modern information communication technologies and systems, the catalogue of risks entailed by their use is obviously expanding. The evolution of increasingly sophisticated forms of online attacks spurs a growing awareness of the landscape of cyber risks and the opportunities to prevent and combat them. As indicated in this work, computer attacks such as hacking, phishing or sniffing share the common goal of gaining unauthorised access to data or information resources, which can lead to financial losses, breach of privacy and even threats to the critical infrastructure of entire countries. Methods of computer crime prevention from the standpoint of the individual user were indicated, stressing the role of education, public awareness and systemic solutions in the fight against cyber threats; European strategies to combat computer crime were identified. The conclusions of this work can contribute to raising awareness of the risks and promoting responsible and ethical use of technology.

Bibliography

Adamski A., *Prawo karne komputerowe*, Warszawa 2000.

Budka M., C*zym jest cyberprzestępczość i jak się przed nią bronić?*, https://www.money.pl/gospodarka/czym-jest-cyberprzestepczosc-i-jak-sie-przed-nia-bronic-6743245515295296a.html [access: 26.12.2024].

Charakterystyka przestępczości komputerowej, http://przestepstwo-komputerowe.eprace.edu.pl/1081,Charakterystyka_przestepczosci_komputerowej.html#google_vignette [access: 26.12.2024].

Cyberbezpieczeństwo: jak UE radzi sobie z cyberzagrożeniami, https://www.consilium.europa.eu/pl/policies/cybersecurity/ [access: 26.12.2024].

Cyberbezpieczeństwo: jak UE radzi sobie z cyberzagrożeniami, https://www.consilium.europa.eu/pl/policies/cybersecurity/ [access: 26.12.2024].

Czym jest hacking?, https://conselion.pl/czym-jest-hacking-komputerowy/ [access: 26.12.2024].

Czym jest PHISHING i jak nie dać się nabrać na podejrzane wiadomości e-mail oraz SMS-y?, https://www.gov.pl/web/baza-wiedzy/czym-jest-phishing-i-jak-nie-dac-sie-nabrac-na-podejrzane-widomosci-e-mail-oraz-sms-y [access: 26.12.2024].

Czym jest spoofing? Jak go rozpoznać i nie dać się nabrać?, https://www.gov.pl/web/baza-wiedzy/czym-jest-spoofing-jak-go-rozpoznac-i-nie-dac-sie-nabrac [access: 26.12.2024].

Filipek D., *Co to jest przestępczość komputerowa?*, https://itcenter.pl/2023/10/31/co-to-jest-przestepczosc-komputerowa/ [access: 26.12.2024].

Hacking, https://www.comcert.pl/slownik/hacking/ [access: 26.12.2024].

Jak chronić się przed cyberprzestępczością, https://www.europarl.europa.eu/topics/pl/article/20200327STO76003/jak-chronic-sie-przed-cyberprzestepczoscia [access: 26.12.2024].

Jakubski K.J., *Przestępczość komputerowa – podział i definicja,* „Przegląd Kryminalistyki" 1997, no. 2.

Kostrzewa A., *Zapobieganie cyberprzestępczości*, https://mitsmr.pl/b/zapobieganie-cyberprzestepczosci/PLZjzYpX3 [access: 26.12.2024].

Kształtowanie się cyberprzestępczości, https://gazeta.policja.pl/997/numery-specjalne/specjalne-gazeta-policy/gazeta-policyjna-nr-2-s/212264,Ksztaltowanie-sie-cyberprzestepczosci.html [access: 26.12.2024].

Najpopularniejsze narzędzia hakerskie, https://akademiawywiadu.pl/najpopularniejsze-narzedzia-hakerskie/ [access: 26.12.2024].

Podsłuch komputerowy, https://cyberprzestepczosc.info/podsluch-komputerowy/ [access: 26.12.2024].

Przestępstwa komputerowe, https://informaticalegis.com/uslugi/przestepstwa-komputerowe/ [access: 26.12.2024].

Radzimirski J., *Społeczeństwo informacyjne*, [in:] *Informatyka ekonomiczna: podręcznik akademicki*, eds. S. Wrycza, Warszawa 2010.

Raport roczny z działalności CERT Polska 2023, https://cert.pl/uploads/docs/Raport_CP_2023.pdf#page=87 [access: 26.12.2024].

Rodzaje i kwalifikacja przestępstw komputerowych, https://podlaska.policja.gov.pl/pod/policja-podlas/dzialania/przestepczosc-gospodar/struktura-wydzialu/zespol-iii/rodzaje-i-kwalifikacja/28410,Rodzaje-i-kwalifikacja-przestepstw-komputerowych.html [access: 26.12.2024].

Szpiegostwo komputerowe, http://pandf.wex.pl/szpiegostwo.html [access: 26.12.2024].

Warchoł A., *Sabotaż komputerowy*, https://vademecumbezpieczenstwainformacyjnego.uken.krakow.pl/2020/03/12/sabotaz-komputerowy/ [access: 26.12.2024].

Wrona J., *Cyberprzestrzeń a prawo międzynarodowe: status quo i perspektywy*, Białystok 2017.