COMPUTER CRIME AND ITS PROSPECTS

Joanna Piotrowicz-Dębicka[1]

Abstract

The primary objective of the paper is a closer examination of the issue of cybercrime and its perspectives. The author analyzed sources of crime, its types and effectiveness as well as the means to fight against computer crime.

Key words: computer crime, Internet crime, cybercrime

Introduction

The late twentieth and early twenty-first century probably can be called a stage of history of rapid progress of civilization. This period has caused many political, social and cultural changes, but first of all it has introduced many transformations in the areas of new technologies, computerization and digitization.

In today's civilized world, the Internet plays the role of one of the most influential, opinion-forming and global medium. However, information technology has become not only the convenience of everyday life, but it poses in many cases a risk for the financial sector, national security, national infrastructure, business, and finally personal safety.

Sources of the phenomenon of cybercrime

Influence of information technology on all areas of human functioning is increasing with their development. The integration of computer technology often changes the face of the world, thereby providing new patterns of behaviour.[2]

---

[1] The Jan Kochanowski University in Kielce, Poland.

[2] See: P. Sienkiewicz, H. Świeboda, *Bezpieczeństwo informacyjne jako czynnik jakości życia*, „Zeszyty Naukowe Akademii Obrony Narodowej", no 2(71), p. 14.

The first computer – ENIAC – was built in 1946, what started the "era" of large computers used mainly by various institutions. In the eighties of the twentieth century new versions of microcomputers such as the ZX Spectrum, and then PCs began to emerge, what led to home-use computers and their use in everyday business activity.[3]

Putting aside the development of computers, progress of the Internet should be also noted. The beginning of the Internet dates back to 1965. At the beginning, however, network access remained restricted only for scientific and governmental purposes. Wider dissemination of the Internet occurred in the late eighties, initially in the United States and further in other countries.[4]

Polish access to the Internet was achieved in 1991, but initially it was limited only to research activities in the universities. In subsequent years, individual access has become widespread, what resulted in use of the Internet for commercial purposes.[5]

Among the main sources of the phenomenon of cybercrime, we can mention the desire for profit. However, we should also remember about the people for whom the main incentive to commit a crime online is to achieve the ideological objectives. They are called hactivists. A lot of people in the net have also a need for an escalation of their negative emotions through mockery or psychological harassment.

Sources of crime must be sought in such activities as slander and insult, discriminatory offense and pornography. This is due to the fact that over time these acts gained importance as computer crime, which entailed the introduction in a type of act signs inter alia, of the possibility of committing these acts via the Internet, or they are committed mainly through a computer network. Moreover, they gained the attention of international bodies aiming to put their widespread criminality. The character of Internet should be mentioned here.[6] Users regard it as a bastion of freedom of speech, realized by the ability to freely present and promote the most diverse opinions, networking and obtaining access to information.[7] In popular publications we can meet the definition of the Internet as a "wonderful world of communication and information, in which no one tells us to do anything, but we can do everything we want",[8] or an advice directed to the reader:

---

[3] See: A. Adamski, *Prawo karne komputerowe,* Warszawa 2000, p. 1.

[4] K. Conner-Sax, E. Krol, *Internet. Następne pokolenie*, Warszawa 2000, p. 4.

[5] P. Fajgielski, *Internet dla prawników, mały przewodnik*, Lublin 2001, p. 15.

[6] J. Sobczak, *Wolność słowa a zjawisko inwigilacji przekazu internetowego* [in:] *Oblicza Internetu. Architektura komunikacyjna sieci,* ed. M. Sokołowski, Elbląg 2007, p. 71-72.

[7] Y. Benkler, *Bogactwo sieci. Jak produkcja społeczna zmienia rynki i wolność*, Warszawa 2008, p. 159.

[8] J. Hofmokl, *Internet jako nowe dobro wspólne*, Warszawa 2009, p. 153.

"You can, for example, say what you want or offer the world any information. Remember, however, that others have the same freedom – if something wrong happens to you in the net or someone offends you, you will not have anyone to complain to."[9] This approach to the possibilities offered by the Internet, and the initial lack of interest of law enforcement institutions and the difficulty in prosecuting the perpetrators have made the Internet a global Hyde Park – where anyone can at any time get a word in. This served the spread of discriminatory crimes and pornography on the broader scale than previously encountered.[10]

The essence of computer crime

The term "computer crime" is not defined in the science of law unambiguously approved by all or most of the representatives of the science of law. The various methods and criteria of defining depend on the aims of the authors of specific publications. Attempts to define this concept sometimes come down to list various types of activities, and sometimes they are doubtful because of their generality.

Certainly, this concept is vague. The research shows that it should be regarded more as a headword than a concrete indication of the criminal act. Both in literature and in regulations developed by European or international organizations, there is no universal agreement on the clear definition of the concept, under which generally accepted group of offences involving the violation of legally protected goods with the use of an electronic system for processing information should be understood.[11]

In the eighties U. Sieber defined computer crime as unethical, unauthorized and unlawful activities relating to the processing and / or transmission of data. He also claimed that there is no unambiguous definition of computer crime.[12]

On the other hand, K. Jakubski is of the view that currently a computer can be used by the perpetrators of many crimes, and therefore there is no uniform computer crime, and due to the imprecision of the term, it should be regarded only as a certain headword. Finally, K. Jakubski defines computer crime as a criminology phenomenon, containing any criminal

---

[9] H. Hahn, *Internet. Wykłady Harleya Hahna*, Poznań 2001, p. 12.

[10] J. Barta, R. Markiewicz, *Główne problemy prawa komputerowego*, Warszawa 1993, p. 30.

[11] M. Siwicki, *Podział i definicje cyberprzestępstwa*, „Prokuratura i Prawo" 2012, no 7–8, p. 10.

[12] U. Sieber, *Przestępczość komputerowa a prawo karne informatyczne w międzynarodowym społeczeństwie informacji i ryzyka*, „Przegląd Policyjny" 1995, no 3, p. 15.

activity related to electronic data processing, directly detrimental to the processed information, the medium and circulation in the computer and in the computer connection system, as well as to the hardware and the copyright of the computer program.[13]

B. Fischer cites in his work an extensive list of various definitions of this concept and classifications of the phenomenon, developed, among others, by the Committee of Experts of the Council of Europe or the International Criminal Police Organization "Interpol" – confirming the absence of a uniform understanding of the term "computer crime".[14] The ambiguities in the definition are noted also by H. Cornwall, who states that the more publications and articles relating to computer crime have appeared, the less accurate became the boundaries of the issue.[15] Therefore, a term computer crime could be attributed, in the narrowest sense, only to acts which required from perpetrator exceptional programming skills, and in the broadest sense – all acts related with the use of the computer. As a computer crime we can thus call a crime which was enabled or at least facilitated by the use of the computer. In other words, computer crime is a crime, for which the computer was used as a tool.[16]

It seems noteworthy to distinguish between two acts of computer crime.[17] First, with the use of information technology, when acts that traditionally are considered a crime are committed and computers only confer new opportunities to commit them. Another, related to the development of computer technology and their popularization, what generates new categories of offenses. K. Jakubski additionally indicates within the computer crime: acts committed with the use of electronic data processing systems and acts against such systems.[18]

This division is wider discussed by A. Adamski, who in substantive aspect of computer crime distinguishes between two types of attacks: attacks against systems, data and computer programs (calling this a computer crime) and attacks involving the use of electronic data processing systems in order to violate the legal rights traditionally protected by the criminal law, calling it a computer fraud.[19]

---

[13] K. J. Jakubski, *Przestępczość komputerowa – zarys problematyki,* „Prokuratura i Prawo" 1996, no 12, p. 34.

[14] P. Fischer, *Przestępstwa komputerowe i ochrona informacji,* Kraków 2000, p. 23.

[15] H. Cornwall, *Datatheft. Computer Fraud, Industrial, Espionage and Information Crime,* London 1990, p. 53.

[16] Supreme Court judgment on 11 April 1984. RNW 4/84, OSNKW 1984/11–12/113.

[17] J. Barta, R. Markiewicz, *Internet a prawo,* Kraków 1989, p. 311.

[18] K. Jakubski, *Przestępczość komputerowa...*, op. cit., p. 34.

[19] A. Adamski, *Prawo karne...*, op. cit., p. 30.

H. Cornwall introduces a more detailed classification of computer crime, highlighting the following types: a crime having a special relation with computers, a crime not possible to commit outside the computer environment, crime facilitated by computers (eg. forgeries), a crime in which the computer plays a passive role, a crime in which perpetrators use the computer as an auxiliary, without a close relation with a deed.[20]

Types and effectiveness of computer crime

The aforementioned Interpol lists in its work the following types of computer crime: violation of access rights to resources, which include, in particular hacking, data capture, theft of time, modification of resources using logic bomb, computer worm, Trojan horse or virus, fraud using computer (fraud related to payments, eg. by ATMs), counterfeiting of input or output devices (eg. for magnetic stripe card), fraud with false identity data, fraud relating to sales systems, fraud in telecommunication systems, copying programs (in particular: computer games, computer software, topographies of integrated circuits), sabotage including computer hardware and software, offenses committed with the use of BBS[21] possession of materials prohibited by law, generally understood crime on the Internet.

Analyzing types of cybercrime it is worth to note that computer crime is in the area of interest of both organized crime groups that use the Internet and computer systems as a new instrument for carrying out illegal activities, as well as individual cybercriminals.

According to a report on cybercrime prepared by Beyond the Breach, the most common type of cybercrime globally are attacks by viruses and malicious programs. The following places in the ranking fill: fraud, theft and cyberbullying.[22]

It is worth to note that the current police statistics record more often several prevailing trends in crimes related to the content of information, eg. crime against honor, dissemination of pornography and crime against public order.[23]

---

[20] H. Cornwall, *Datatheft...*, op. cit., p. 53.

[21] BBS (Bulletin Board System): a system that allows users of dial-up modems to exchange information on an e-mail account base, http://www.gimklucze.pl/strony/slownik_komp.html, [01.08.2016].

[22] http://www.structum.pl/_Beyond_the_Breach_raport_o_cyberprzestepczosci_w_2013_roku-2-49249-15_37.html, [30.07.2016].

[23] http://www.policja.pl/pol/kgp/bwik/bsk/cyberprzestepczosc/74203,Byc-swiadomym-i-bezpiecznym-uzytkownikiem-Internetu.html, [08.08.2016].

Research on the scale of Internet crimes are also carried out by non-governmental organizations, among others, by CERT Polska, which is a team operating within the Research and Academic Computer Network, active since 1996. CERT Polska is a member of FIRST – the largest organization in the world uniting computer emergency response teams from the entire world.[24]

In its reports, CERT Polska lists the following main types of incidents: publication of unwanted and abusive content, distribution of spyware and malware, processing and dissemination of false data, hacking attempts, unauthorized logging, intrusion to accounts, sabotage associated with encoding, decoding content without the permission of administrators, changing information or production of false messages, copyright infringement, impersonation of a "third parties".[25].

It should be noted that computer crime is much less absorbing in many cases than traditional crimes. It is also a crime much more difficult to detect. Moreover, the Internet gives the opportunity to reach a much larger group of potential victims and creates new opportunities for making a wide range of fraud, eg. "false trade" through web portals.[26] Certainly, occurrence and dissemination these crimes remain in correlation with the socio-economic changes and general enlargement of material goods possessed in the society.

A particular problem is also a software piracy. The losses it causes originate not only from the economic value of computer programs that are the target of the attack, but also from lost benefits.[27]

Illegal downloading via the Internet raises huge loss for the artists every year. Probably only one-tenth of games or multimedia program is sold legally, the rest are pirated copies. The total value of the pirated software was estimated at more than $63 billion globally and $618 million in Poland.[28]

---

[24] https://www.cert.pl/, [11.08.2016].

[25] *Realne zagrożenia i trendy na podstawie raportów CERT, http://docplayer.pl/1687129-Realne-zagrozenia-i-trendy-na-podstawie-raportow-cert-polska-cert-polska-nask.html,* [10.08.2016].

[26] D. McQuail, *Teoria komunikowania masowego*, Warszawa 2007, p. 166.

[27] According to Polish law, the owner of the entity that use illegal software could be fined three times the market price of this application and as far as criminal liability is concerned a piracy is punishable by up to 5 years imprisonment. Despite the possibility of the punishment, every second Pole admits that he/she illegally acquired software that gives the fifth place in the ranking of EU countries with the highest piracy rates. Ahead of Poland in the ranking there are only Latvia and Lithuania (54 percent.), Greece (61 percent.), Romania (63 percent.) and Bulgaria (64 percent.).

[28] http://www.wsr.webd.pl/index.php/referaty-z-informatyki/99-piractwo-komputerowe, [08.08.2016].

Prevention of computer crime

According to M. Siwicki, measures to prevent cybercrime can be classified into three groups.[29] The first group includes the development and application of methods and procedures for preventing the possibility of making an attempt on certain legal interests. Protection of computer systems and processed information focuses primarily on technical provisions built into the operating system and based on access control. In addition to the above mentioned methods, additional solutions, primarily software protecting computing resources, are also used. Mainly we can include: firewalls based on the appropriate software that filters and controls network activity, antivirus software used to protect the computer system from malware, anti-spyware and adblock software to detect and remove spyware, anti-spam software designed to reduce the number of unwanted commercial information received by a user.

In the quest to protect information processed electronically a variety of solutions are used for identification and authentication of an authorized entity (eg. passwords and access codes), filtering content (eg. parental control systems), encryption and information authentication using cryptographic and biometric methods. Today, security packages become more and more popular. They have a form of integrated software, combining several security parameters (eg. anti-virus software, firewall, anti-spam software).[30]

In order to prevent computer crime a number of actions aimed at blocking or restricting access to illegal and harmful content on the Internet are also undertaken. In this area, the systems of classification and quality marks in combination with filtering technologies are considered as the most effective. An example of such a system is PICS – the Platform for Internet Content Selection, created by ICRA – the Internet Content Rating Organization. This platform enables parents to control the content their children can access. The effectiveness of this system depends on number of web pages put in the appropriate classification.[31]

According to the opinion of M. Siwicki, above indicated systems are conducive to control web content, but it seems that their real meaning may be highly questionable. The sense of freedom prevailing on the Internet causes that a lot of content filters are not functioning properly today and the top-down imposition of standards on the Internet is perceived as an attack on freedom.[32]

---

[29] M. Siwicki, *Cyberprzestępczość,* Warszawa 2013, p. 19.

[30] A. Adamski, *Prawo karne...*, op. cit., p. 25-28.

[31] https://www.w3.org/PICS/iacwcv2.htm, [01.08.2016].

[32] M. Siwicki, *Nielegalna i szkodliwa...*, op. cit., p. 258.

The second method of preventing cybercrime is to promote the safe use of modern technologies. This method is based primarily on the development of self-help or legal actions which are designed to increase user awareness of the existing threats. Non-governmental organizations are particularly active in this area.[33]

The third method of preventing computer crime focus attention on developing and improving cooperation between law enforcement agencies, the private sector and end users. Such cooperation is, in particular: operational support between national and international law enforcement agencies, taking actions in cooperation with other countries to prevent and fight coordinated cyber attacks,[34] exchange of information on technical methods to fight computer crime, the establishment and development of special reporting offices, intervention centers (ie. hot-lines) through which users can report a computer crime.

The establishment of the European Cybercrime Centre by the European Commission on 28 March 2012 is of special importance. The Centre, set up within the Europol (European Police Office), aims to protect European citizens and businesses from Internet threats. It was designed to be the main European tool to fight against computer crime and focus on illegal online activities carried out by organized crime groups (eg. Internet fraud with the use of payment cards and passwords to access bank accounts).[35]

Prevention of computer crime is undoubtedly a difficult task. This is due to a general lack of understanding of the importance of the problem and the essence of security and the lack of awareness of how to deal with emerging threats on the Internet. The escalation of the commercialization of cyberspace, the differences in the cyber policy of various countries, the diversity of rules and practices in the field of combating and preventing computer crime entail difficulties in enforcing the law at the international level. Attacks in cyberspace make that the responsibility of law enforcement agencies and national security institutions begins to blur, thereby causing the need to develop new forms of cooperation. Increasing level of threat posed by the frequent use of computers and network for computer crime, clearly poses new challenges for national law enforcement authorities and international organizations.

---

[33] J. Kulesza, *Ius internet. Między prawem a etyką*, Warszawa 2012, p. 56.

[34] D. E. Denning, *Wojna informacyjna i bezpieczeństwo informacji*. Warszawa 2002, p. 294.

[35] M. Siwicki, *Cyberprzestępczość...*, op. cit., p. 21.

Conclusions

Undoubtedly, the development of modern technology also has its "dark side", which is reflected in the development of computer crime. Due to the severe consequences that could result from cybercrime, it seems necessary to undertake actions on the creation of a more appropriate legal framework to effectively combat this phenomenon. Equally important should be preventive actions to protect against attacks in cyberspace.

References

Adamski A., *Prawo karne komputerowe,* Warszawa 2000.
Barta J., Markiewicz R., *Internet a prawo,* Kraków 1989.
Barta J., Markiewicz R., *Główne problemy prawa komputerowego,* Warszawa 1993.
Benkler Y., *Bogactwo sieci. Jak produkcja społeczna zmienia rynki i wolność,* Warszawa 2008.
Conner-Sax K., Krol E., *Internet. Następne pokolenie,* Warszawa 2000.
Cornwall H., *Datatheft. Computer Fraud, Industrial, Espionage and Information Crime,* London 1990.
Denning D. E., *Wojna informacyjna i bezpieczeństwo informacji.* Warszawa 2002.
Fajgielski P., *Internet dla prawników, mały przewodnik,* Lublin 2001.
Fischer P., *Przestępstwa komputerowe i ochrona informacji,* Kraków 2000.
Golata R., *Internet – aspekty prawne,* Warszawa 2003.
Hahn H., *Internet. Wykłady Harleya Hahna,* Poznań 2001.
Hofmokl J., *Internet jako nowe dobro wspólne,* Warszawa 2009.
Jakubski K. J., *Przestępczość komputerowa – zarys problematyki,* „Prokuratura i Prawo" 1996, no 12.
Kulesza J., *Ius internet. Między prawem a etyką,* Warszawa 2012.
McQuail D., *Teoria komunikowania masowego,* Warszawa 2007.
Sieber U., *Przestępczość komputerowa a prawo karne informatyczne w międzynarodowym społeczeństwie informacji i ryzyka,* „Przegląd Policyjny" 1995, no 3.
Sienkiewicz P., Świeboda H., *Bezpieczeństwo informacyjne jako czynnik jakości życia,* „Zeszyty Naukowe Akademii Obrony Narodowej", no 2(71).
Siwicki M., *Nielegalna i szkodliwa treść w Internecie. Aspekty prawnokarne,* Warszawa 2011.
Siwicki M., *Cyberprzestępczość,* Warszawa 2013.
Siwicki M., Podział i definicje cyberprzestępstwa, „Prokuratura i Prawo" 2012.
Sobczak J., *Wolność słowa a zjawisko inwigilacji przekazu internetowego* [in:] *Oblicza Internetu. Architektura komunikacyjna sieci,* ed. M. Sokołowski, Elbląg 2007.