Access to Justice in Eastern Europe
ISSN 2663-0575 (Print) ISSN 2663-0583 (Online)

Journal homepage http://ajee-journal.com

Case Note

SOME TYPES OF COMPUTER CRIME AND CYBERCRIME IN UKRAINE

Vasyl Stratonov, Dmitro Slinko and Sergey Slinko

Summary: 1. Introduction. – 2. Types of Computer Crime on the Internet and Finding Ways of Fight against Them. – 3. oncluding Remarks.

To cite this note: *V Stratonov, D Slinko, S Slinko,* 'Some Types of Computer Crime and Cybercrime in Ukraine' 2021 3(11) *Access to Justice in Eastern Europe 191–197*. DOI: 10.33327/AJEE-18-4.3-n000078

To link to this note: https://doi.org/10.33327/AJEE-18-4.3-n000078

Submitted on 11 Jan 2021 / Revised 28 Feb 2021 / Revised 13 Jul 2021 / Approved 26 Jul 2021 / Published online: 02 Aug 2021 View data

Submit your article to Access to Justice in Eastern Europe

ACKNOWLEDGEMENTS

The authors would like to express their gratitude to the reviewers and editors of the journal for their remarks and suggestions, which allowed them to improve this contribution substantially.

CONFLICTS OF INTEREST

The authors declare no conflict of interest of relevance to this topic.

CONTRIBUTORSHIP

Vasyl Stratonov is responsible for the intellectual discussion underlying this paper, Dmitro Slinko and Sergey Slinko are responsible for literature review and writing. All the co-authors fully accept responsibility for the content and interpretation. The content of the note was translated with the participation of third parties under the authors' responsibility.

SOME TYPES OF COMPUTER CRIME AND CYBERCRIME IN UKRAINE

Stratonov Vasyl,
Dr.Sc., Full Professor of the Department of Branch Law, Faculty of Business and Law,
Kherson State University, Ukraine
stratonov@ksu.ks.ua
https://orcid.org/0000-0002-7548-0630

Slinko Dmitro,
Dr.Sc., Associate Professor of the Department of Criminal Law Disciplines,
V. N. Karazin Kharkiv National University, Ukraine
d.s.slinko@karazin.ua
https://orcid.org/0000-0001-7793-3667

Slinko Sergey,
Dr.Sc, Full Professor of the Department of Criminal Procedure, Criminology and Expertology
Kharkiv National University of Internal Affairs, Ukraine
s.slinko743@knuia.ua
https://orcid.org/ 0000-0002-2182-1436

Abstract *In this note, the most frequent types of computer crime on the Internet in Ukraine are analysed. It is suggested that international experience in computer crime investigation should be used to combat this because cybercrime has become an international problem, causing enormous damage to governments, commercial entities, and computer systems of individual users. Governments and commercial entities spend significant funds to prevent losing information and ensure its protection. Cybercrime is based on technical knowledge, which is difficult to detect or prevent. This type of criminal activity has a high latency because of the difficulty of determining the qualification of a criminal offence.*

Keywords: *computer crime, cybercrime, types of computer crime*

1 INTRODUCTION

The constant growth of computer crimes demands the definition of new provisions in the fight against this criminal phenomenon. Informatisation, like any social phenomenon with the positive benefits, unfortunately, has negative effects as well, namely, the possibility of using computer technology to commit offences, including crimes. Thus, it is fundamentally important to study ways of committing crimes in the field of information technology.

The Centre for Cybercrime Research, referring to global statistics, indicates the growing use of the Internet and the number of cybercrimes.[1] Only in Ukraine has the level of this

1 LJ Freeh, 'Statement for the Record of Louis J. Freeh, Director of the Federal Bureau of Investigation Cybercrime for the Senate Committee Judiciary Subcommittee for the Technology, Terrorism, and Government Information Washington, DC' (28 March 2000) < https://www.nti.org/analysis/articles/statement-louis-j-freeh/ > accessed 13 July 2021.

type of crime increased by around 100%.[2] Analysis of the practice of pre-trial investigation of criminal proceedings shows that the reason for the increasing numbers of this type of crime is the savings of financial institutions on cybersecurity and, in some cases, the victim's distrust of criminal justice.

Forensic theory does not fully define the characteristics of committing computer crimes or their specific names and classifications. This problem is under theoretical and practical development.[3] Firstly, scientific development in this sphere began after the large-scale application of computer technology in practice. Secondly, based on the analysis of practice, the theory of criminology began to develop counteraction to computer crimes in the early 90s, while European researchers began in the late 70s.[4] European and American studies have produced theoretical developments and a lot of practical material, which is used in the analysis and resolution of emerging issues in the pre-trial investigation of criminal offences.

Our purpose is to analyse the methods and techniques of committing criminal offences based on the use of computer technology on the Internet and propose legal instruments for the detection, cessation, and prevention of crimes committed using computer technology.

2 TYPES OF COMPUTER CRIMES ON THE INTERNET AND FINDING WAYS OF FIGHT AGAINST THEM

Scholars have determined that the digital age provides criminals with new ways of committing crimes and provides an opportunity to establish cybercrime behaviour.[5] Generally, people are unaware of the individual threats posed by criminals on the Internet. They do not use the opportunity to prevent the actual risks that arise while on the Internet. These shortcomings lead to people becoming victims of crime. One example may be a criminal offence disclosure mechanism that is based on 'garbage collection'. This method of committing a crime consists of the illegal use by a criminal of technical waste of the information process left by the user after work on computer equipment. It is carried out in two forms: physical and electronic. In the first case, the search for waste is consists of careful inspection, and technological waste is removed. The electronic version requires the review and sometimes subsequent study of the data stored in the computer's memory. It is based on some technological features.

2 V Stratonov, '"Computer crime" features and characteristics' (2020) 2 Scientific Bulletin of Dnipropetrovsk State University of Internal Affairs 134-141.

3 See, for instance, JB Hill, NE Marion, *Introduction to Cybercrime. Computer Crimes, Laws, and Policing in the 21st Century* (CA Praeger 2016); H Jacobson, R Green, 'Computer Crimes' (2002) 39 Am Crim L Rev 273; AJ Carter IV, A Perry, 'Computer Crimes' (2004) 41 Am Crim L Rev 313, 327; A Galicki, D Havens, A Pelker, 'Annual Survey of White Collar Crime' (2014) 51 Am Crim L Rev 875; C Fehr, 'Computer Crimes' (2016) 53 Am Crim L Rev 977, 1011-12; M Trujillo, 'Annual Survey of White Collar Crime' (2019) 56 Am Crim L Rev 615.

4 See also D Icove, K Seger, W Von Sorsh, *Computer Crim: A Crime fighter's Handbook* (O'Reylli & Associates Inc 1995); H Chu, DJ Deng, H Chao, 'Potential cyberterrorism via a multimedia smart phone based on a web 2.0 application via ubiquitous Wi-Fi access points and the corresponding digital forensics' (2011) 17 Multimedia Systems 341–349; P Wang, J Li, B Ji, 'Online fraud detection model based on social network analysis' (2015) 12 (7) Journal of Information and Computational Science 2553-2562. DOI: 10.12733 / jics20105690; S Leman-Langlois, *Technocrime: Technology, crime and social control* (Wilan 2008) DOI: 10.4324 / 9781843925378; A Al-Nemrat, H Jahankhani, D Preston, 'Cybercrime victimization / criminalization and punishment' (2010) 92 CCIS 55-62. DOI: 10.1007 / 978-3-642-15717-2_7; Centre for Computer Crime Research <https://www.crime-research.ru/library/terror3.htm> accessed 13 July 2021.

5 Al-Nemrat et al (n 4) 55-62.

Depending on the various ways in which computer crimes are committed, certain actions can be taken to obtain unauthorised access to computer equipment. The first, most common means is to enter the computer using the owner's data. Characterising this typical situation and methods of physical penetration, we can identify the main methods that are now known to employees of units engaged in operational and investigative activities. Basically, the option of the criminal's intrusion into the premises and the computer is designed based on the low vigilance of security officers. The criminal has internal elements of the psychological approach and counts on deception and fraud concerning security officers.

One of the elements includes entering the premises with the help of the institution's uniform (organisation) or using the uniform of epidemiological, sanitary, fire, medical service. Typically, a person holds items related to this role, fraudulently manipulates special professional terms that beat security guards, or exerts moral pressure so that security guards are allowed to enter the room where the computer equipment is located. By disguising his/her illegal actions, the offender is allowed to enter the premises and has unauthorised access to the object of encroachment. In this case, the security guards themselves escort the criminal to the room where the computer equipment is located. The person can then simply enter the room and commit their illegal actions. He/she may even ask a security guard to help bring the alleged devices to work on the computer.

The second method is the most common. In this case, a criminal uses the uniform of the post or food delivery, municipal service, etc. With the help of a fake ID, a person can penetrate the premises with computers.

According to the practice of criminal proceedings and their analysis (1,400 criminal proceedings), during the commission of a criminal offence, in 85% of cases, the offender entered the premises without hindrance. In one case, a person called the security post on behalf of the institution's staff and entered the premises without security guards even accompanying him. The criminal then removed the information from the computer and left the office.

A common type of crime is when the criminal 'falls on the tail of the victim'. This mechanism for accessing the computer and retrieving information includes the following types. In the first type, a criminal connects to a user's line of communication using computer communication and waits for a signal that marks the end of work, intercepts it, and then, when the user finishes an active mode, carries out access to the system. The second type is called 'computer boarding'. In this case, the crime is carried out via the random selection of the subscribed number of the computer system of the injured party using a telephone. Sometimes, to achieve the goal, the offender calls the victim, simulates the provision of information, and identifies his/her data in the computer. After receiving any information, the criminal uses an automatic password search program. The algorithm for setting the password is to use high-speed modern computer devices to go through all possible combinations of letters, numbers, and special characters installed on a standard PC keyboard. Once the character combination matches the original, the specified subscribers are automatically connected.

It should be noted that there are many programs that a person can use to 'hack' any computer. These programs become ineffective in computer systems because software products developed by owners of Intel computer systems protect computer ports.

Recently, criminals have begun to use the 'intellectual search' method, selecting the expected password based on predetermined thematic groups of affiliation. In this case, the program 'cracker' transmits some initial data about the identity of the author of the password.

Numerous experiments show that 42% of passwords are manually revealed using the 'smart search' method. For example, last names, first names, dates of birth, and other personal details of the victim allow a criminal to choose a password that works about 55% of the time.

Commonly chosen passwords include dates of birth, zodiac signs of users, names of their close relatives, their place of residence, street, house number, mobile phone number, etc. But most often, it is just a sequence of PC keys.

New forms of intervention involve 'slow choice'. The criminal achieves unauthorized access to the computer system by identifying vulnerabilities in its protection. This method is usually used for those who do not pay due attention to the recommendations of their security system use; for example, the user does not update anti-virus programs, etc.

Unlike 'slow choice', when using another method of penetration, the offender finds weaknesses in protecting the computer system and identifies errors in the logic of the software. Weaknesses detected in this way can be used repeatedly until they are detected. This method is used because programmers sometimes make mistakes when developing software products.

Sometimes a criminal enters a computer system posing as an authorised user. Computer security systems that do not have authentic identification functions, such as fingerprints, retina scans, voice recognition, etc., are vulnerable to this method. The easiest way to penetrate such systems is to obtain codes and other identifying cyphers of legitimate users. This can be done by purchasing a list of users with all the necessary information by bribery, extortion, or other illegal actions against persons who have access to this document.

The next group of methods of committing computer crimes includes those related to data manipulation methods and control teams of computer equipment. These methods are most often used by criminals to commit various illegal acts and are quite well known to law enforcement officers. The most widely used are methods of 'data substitution'. This is a simple and, therefore, very common way of committing a crime. The actions of criminals aim to change or enter new data, which is usually carried out during the input-output of information. In particular, this method is used to attribute the account to 'foreign' history, i.e., the modification of data in the automated system of banking operations, which leads to the appearance in the system of amounts that are not actually credited to this account.

A 'trojan horse' is the secret introduction into someone else's software of specially created programs, which, once they are part of the information and computer systems, pretend to be well-known service programs and begin to perform new, unplanned actions, after which computer software ceases to work and, in some cases, no information remains. With this method, criminals usually transfer funds during banking operations to a different account. A 'Trojan horse' program can be detected with great difficulty and only by qualified programmers.[6]

Examples of investigative practice testify to the use of the 'Trojan horse'. Security services used personal computer software to set up teams that did not print a cash flow statement. These amounts circulated only in the information environment of the computer. Having stolen forms for issuing money, the criminal filled them in with the code and then included certain sums of money. Relevant transactions for their issuance were also not printed and could not be documented.

The 'salami' method of committing computer crime became possible only through computer technology in accounting. It is based on transferring a trifling amount to a fictitious account, which, in professional accounting language, is called 'salami'. From the point of view of criminals, this is one of the simplest methods used in embezzlement in accounting transactions in which fractional (less than one unit of currency) amounts of money are

6 See A Manoilo, A Petrenko, D Frolov, *State information policy in the conditions of information - psychological war* (Telekom 2006).

deducted from each transaction because in these cases, the amounts are always rounded to the established integer values. The bet that criminals make is that the victim loses so little that it is practically not recorded in each transaction.

Sometimes, it is easiest to commit embezzlement for tactical reasons by establishing a set of actions that will occur at a specific time. Criminals use the 'logic bomb' method of committing a crime, based on secretly making changes to the victim's program with a set of commands that must work when certain circumstances occur after a specific period. Then the algorithm of the 'Trojan horse' program is included. The 'logic bomb' is a kind of 'time bomb' triggered at a certain point in time.

Computer crime is characterised by the use of computer simulations. Thus, to avoid taxation, the criminal begins to use so-called 'black' or 'double' accounting, which is based on the existence of two simultaneously working programs of automated accounting with common control data. One of them operates legally and the other illegally to conduct illegal accounting transactions.

3 CONCLUDING REMARKS

Cybercrime, especially its transnational component, has become one of the biggest international problems due to the widespread introduction of global information networks that connect all the countries in the world. They cause huge losses to users, forcing them to spend significant funds on developing and implementing software, hardware, and other means of protection against unauthorised access to information.

Computer crimes have a high latency because governments and commercial entities that have been attacked, especially in banking, do not have much confidence in the possibility of identifying a suspect who has committed a criminal offence. Some problems arise at the stage of pre-trial investigation due to the difficulty of determining the qualification of a criminal offence and the specifics of individual investigative actions. The third aspect is the small number of computer technicians who have the knowledge to detect, prevent, and combat such crimes.

REFERENCES

1. Stratonov V, '"Computer crime" features and characteristics' (2020) 2 Scientific Bulletin of Dnipropetrovsk State University of Internal Affairs 134-141.
2. Hill JB, Marion NE, *Introduction to Cybercrime. Computer Crimes, Laws, and Policing in the 21st Century* (CA Praeger 2016).
3. Jacobson H, Green R, 'Computer Crimes' (2002) 39 Am Crim L Rev 273.
4. Carter AJ, Perry A, 'Computer Crimes' (2004) 41 Am Crim L Rev 313, 327.
5. Galicki A, Havens D, A Pelker, 'Annual Survey of White Collar Crime' (2014) 51 Am Crim L Rev 875.
6. Fehr C, 'Computer Crimes' (2016) 53 Am Crim L Rev 977, 1011-12.
7. Trujillo M, 'Annual Survey of White Collar Crime' (2019) 56 Am Crim L Rev 615.
8. Icove D, Seger K, Von Sorsh W, *Computer Crime: A Crime fighter's Handbook* (O'Reylli & Associates Inc 1995).

9. Chu H, Deng DJ, Chao H, 'Potential cyberterrorism via a multimedia smart phone based on a web 2.0 application via ubiquitous Wi-Fi access points and the corresponding digital forensics' (2011) 17 Multimedia Systems 341–349.
10. Wang P, Li J, Ji B, 'Online fraud detection model based on social network analysis' (2015) 12 (7) Journal of Information and Computational Science 2553-2562. DOI: 10.12733 / jics20105690.
11. Leman-Langlois S, *Technocrime: Technology, crime and social control* (Wilan 2008) DOI: 10.4324 / 9781843925378.
12. Al-Nemrat A, Jahankhani H, Preston D, 'Cybercrime victimization / criminalization and punishment' (2010) 92 CCIS 55-62. DOI: 10.1007 / 978-3-642-15717-2_7.
13. Manoilo A, Petrenko A, Frolov D, *State information policy in the conditions of information - psychological war* (Telekom 2006).