https://doi.org/10.26552/com.C.2005.3.24-28

kamUnikácie
COMMUNICATIONS

Jozef Meteňko *

INFORMATION AND COMMUNICATION CRIME

In this paper the author tries to shortly characterize the content and scope of crime connected with information and communication technologies. He analyses the (known) possibilities to commit crime connected with abuse of information and communication systems. These are registered in the uncovering and clarifying activities performed by police officers. He demonstrates ground conditions under which such crime arise, as well as their specialities. The author points out some possibilities within the crime control, as a practical analysis on the basis of police sciences, law, criminology and criminalistics.

Key words: *crime, information and communication crime, crime connected to information and communication technologies, information and communication system, conditions for origin of crime, possibilities of crime control*

Introduction to an issue

Development of human society is perhaps the most significantly characterized by the development of new technologies. Automated data and information processing have been developing and penetrating into all spheres of social life. The same significance is put as well on their transmission, mainly as a tool of directing complex processes for different, particularly technical areas of life. Fast development of information and communication technology has an impact on all spheres of present-day society. An integration of telecommunication and information system enables the speeding and improves the reliability of information processing, storage and transmission. It is the matter regardless the distance and the way of communication, thus opening a wide spectrum of possibilities in positive or negative directions.

In its positive direction, this development causes and backs up huge economic and social changes in the Slovak Republic, too. Technics and technology are, in general, created to serve the people. Development of information and communication technologies (ICT – Information and Communication Technology) is very fast. Efficiency of technics and technology is growing, but the areas where they are used are also spreading. At present time one may not find any branch of human activity where he would not meet the electronics and its application. Close future will be typical for a larger and deeper integration of information and communication technologies with other ordinary household and office equipment (television set, telephone, refrigerator etc.). We will be encircled by technologies on our every step and still in a larger extent. [13]

Jobs and free time performances depend, each day to a larger extent, on the right, reliable and unstoppable work of complex computer and communication systems. Information and communication technologies started to create a *new form of conduct of individual subjects in economic and management spheres*. These technologies have a significant influence on our everyday life. Development is so fast that observing new information is a need; otherwise a huge gap between reality and knowledge arises. Information technologies *expand very fast even into ordinary life* and at the same time a fast development in the area of technologies themselves is in the process.

We may claim that the phenomenon of crime has social features, and is directly connected to the development of society, people. Without any doubts we may claim that as the development of human civilization reaches different levels in different societies, as well crime development has its drawbacks and peculiarities and its development is not directly connected to a human progress. Knowledge of criminology and crime development in Slovakia shows that democratization trends within social relations lead to their clearance but simultaneously to the increase of crime [4]. Consequently, the safety is being worsened and investments into protection and safety are significantly growing, logically by the use of modern technologies and technics. We dare to state our third premise on the issue of mutual contingency of the progress of human society and its structure towards "development of crime technologies". It is so because technologies and technics in every human activity are used not only in a positive sense, but also fully naturally for negative and condemnation worth goals. Neither technics nor technologies do have the possibility to choose the result and the way of how to reach it. Such feature is typical only for a man as a creator and at the same time abuser of stated "tools for improvement of life".

Criminogenic factors

Technology and technics are and will remain *the subject and tools* of interests, which overcome the boundaries of allowed and belong to the area of their misuse. Certainly, to deal with it, it is not always necessary to be it the matter of crime. On the other hand, new and not used or unknown technologies as a tool or means of activities cause the doubts whether the act is criminal or due to various reasons able to be recourse-able or still allowed. It

* **Jozef Meteňko**
Department of Criminalogy and Forensic Science, Police Academy Bratislava, E-mail: metenko@minv.sk

is *non-existence of relevant regulations* within Criminal Code that causes and may cause doubts about a criminal act, or – namely in the area of protection of social and ethic norms, about a need and possibility to bring other sanctions for such activity.

Regardless other human activities, *expanding development of communication and information technologies* has its shadow side, too. This is featured by new forms of crime as well as by traditional crime committed via new technologies. Technological expansion causes the fact that the consequences of criminal or other anti-social activity are hardly recourse-able.

Among the *reasons of its non-recourse-ability* and conditions for the development of such crime belongs mainly the fact that national borders do not geographically limit crime. Current cases of fast spreading computer viruses in the world confirm the fact. One of the main reasons of Internet crime is the feeling of anonymity. Basically, Internet offers anonymity *to everyone*. Also this is the reason why one of the main directions of the development of information and communication crime is Internet crime.

For the development of information technologies, software is the most important form of creative work, usually done with the use of computer. Programs represent one of the most remarkable features of intellectual creative work. Protection of creativity in this area is the goal of international organizations and its legislators' interests are gradually increasing. Simultaneously there prevails a bigger power and higher pressure on *misuse or non-exercising* copyrights for these products. On one hand development is negative – loss of respect to law and work of others, on the other hand it has been over 30 year's journey of intensive impulses on communication and information technologies development.

Existence of new information technologies, computer networks and updated technical achievements enable to reveal crime more effectively, but at the same time they provide, in many cases, space for *non-recourse-able crime*. As a rule offenders are usually *one step ahead of repressive apparatus*. Such statement is the matter of the police in its full extent. Reasons are several. First of all it is *a qualitative and quantitative level of software and hardware equipment*. Furthermore it is the lack of *qualified* experts. Unfortunately it is true that the police does not stand on the same level with the offenders, it is far behind.

Our goal is to *keep such distance to its minimum*. In case of information technologies it is very true. The present puts heavy demands on the police and we may say they will grow. Communication and information crime will grow all the time. Not far is the period when, like today we are afraid of stealing our vehicle or afraid of burglary, we will be afraid of unauthorized gain of data from our personal computer or making our lives unpleasant which is more and more dependable on information technologies, not speaking about personal data security.

New technologies bring new features, functionality and consequently, an added value for a final user. These modern technologies behave at the same time as tools and goals of incorrect use of even abuse what may be in its final form reflected in crime. *Breaking and abuse of ownership rights of owners and holders of license for technologies* in private sector represent diverse and actual form of communication and information abuse. In their working hours, working staff is involved also in other activity than the ones set by the agreement, making use of the employer's technology and thus causing him direct or indirect loss. In these cases law is broken, sometimes only internal regulations are broken. Area of war applications is a separate chapter where information technologies might act as a goal and tools of information war.[1)] [12]

Change of content and scope of notions

In the last decade everyday speech, but mainly police language has been using the notion of *cyber crime* [9]. Specialized literature still lacks any theoretical elaboration of traces caused by ICT such as analysis of their classification in the theory of criminalistic traces, what has a tradition in the Slovak and Czech criminalistics. Often we talk about cyber crime and cyber torts but we do not specify them, we do not study their features, ways of their detecting, specifics of their seizing, documentation, analysis and evaluation in details [14]. There is still absence of attempts to sum up all knowledge with an aim to reveal and prove this type of crime and at the same time to have a successful control over it and prevent its further spreading.

The notion of cyber crime appeared at the times of mainframe computers and this area has been fully developed. Nowadays other technologies and means seem to be common and they connect or are suitable complements to information possibilities with communication in various forms. They have a common platform in a digitalization of everything around us.

Every day we use mobile phones, wireless data transmissions from our personal electronic devices (WiFi, Bluetooth), electronic diaries, handlers (personal computers to our palms in a size of cigarette packet), audio digital record devices, digital videocameras and cameras, video and DVDs, credit and identification cards, various record media (CD, DVD, USB keys, digital memories of videocameras and cameras, optic media etc.), rich extras of different types of peripheries to all these devices. There are also coparts of other technologies – board computers of cars, planes, ships; different safety and monitoring devices, electronic identification of objects, goods, etc. All these and many other objects may be the subject, object and goal of criminal acts.

From the viewpoint of criminalistic and forensic research all these devices leave traces of their activities having general and individual features and which are usable in practice. After our

[1)] Murdza, K.: ISBN 80-8054-325-9. s. 110-111. unlike Jašek, R.: Bratislava: Akadémia PZ 2004. ISBN 80-8054-325-9, 104-108. alike Cuľba, M., Felcan, M., Gýmerská, J.: Bratislava: Akadémia PZ 2004. ISBN 80-8054-325-9, p. 135.

attempt to analyze the problem in criminalistics, we have introduced the notion of *digital trace* [8].

There is a legal *tendency to subsume* specific activities – namely objective side, attack and goals, motive and specific conditions, under already existing merits of the case. However it is logical, it is not sufficient any more.

Police sciences and their applicable practice are forced to find new *ways of how to control* of specific activities showing evidence on their trots substance. They deal with this problem from the viewpoint of existing merits and from the viewpoint of methods of revealing, documentation and verification valid up today. Preventive and curative effect is almost completely minimized for this case, since there no power, time or finances are left. Despite that this effect is the most suitable from the economic viewpoint.

From the stated above it is clear that the meaning of a legal content of the notion "cyber crime" is much wider than in the past. In that time cyber crime was correctly and logically perceived only in relation to computer. Nothing else was comparable or existed.

How shall we classify today's crime connected to credit or identification cards, which contain magnetic or other data media, altering of unprotected data during their wireless transmission etc.? Most technological devices, despite not being the means or goal of crime, contain a large number of various data. In the course of investigation of other crime, act or completely other activity not linked to this one, in the initial phase they have a classical character of a criminalistic trace and in the final phase, in ideal case, they obtain a character of forensic evidence.

All these traces are useful in verification of investigation versions of a case, in gathering evidence against perpetrator or on the other hand in confirmation of alibi of the innocent. In the trial traces become direct or indirect evidence. Data medium may contain records of computer user's activity, mobile phone may contain a list of last calls of victim, video record of a department store or bank checkpoint may contain a view of customers in that particular time, car board computer may contain identification numbers (VIN), which offender might have forgotten to alter or he did not know how to do it while performing mechanical falsification of other vehicle numbers, telephone exchange may contain a list of all calls, GPS systems may contain objects grids (for instance car) in a concrete time etc.

All these questions are related to *information and communication technologies* and their possible misuse and control as well as revealing and investigating of this crime. Sometimes other type of crime, not directly linked to these technologies, but impossible to be realized without these technologies is investigated.

Content of information and communication crime

European Agreement on cyber crime is a core document for analyses of a wider notion of crime related to information and communication technologies. Slovakia has not signed the Agreement yet and thus it is not legally binding. According to unofficial statements of relevant authorities, Slovakia has been waiting for re-codification. Other countries face the same problems along with its ratification and implementation into legal order [2]. Practically all-new EU countries except Slovakia and Czech Republic have ratified it[2)] [8]. Unfortunately the proposal has not settled yet by its submitter and thus the legal framework remains as it has been realized under valid Criminal Code.[3)]

EU committees recommend using such classification of cyber crime, which would unite the legislation of European countries in order to ensure a unified criminal policy in prosecuting criminal acts within cyber crime.

On the basis of the stated analyses we have tried to work out a notion that would meet the needs of all four cooperating branches. We define *information and communication crime as an illegal and unauthorized act, in some cases connected to immoral behavior, which include misuse or unwarranted change of data obtained, elaborated, stored and distributed via information and communication technics and information and communication technologies.*

In the last 3 years in the Slovak Republic communication and information (ICT) crime has been committed in the following forms:

- Computer programs theft
- Theft of data stored in memory media of computer or server disc
- Different forms of non-cash payment misuse
- Unauthorized use of the means of communication and information technics, most often PC service theft
- Damage of data stored in memory media
- Computer viruses and their distribution
- Damaging or placing banned pages on servers[4)]
- Non-warranted advertising – ad spam.

Nevertheless, even in this case as well as when defining cyber crime, it is inevitable to divide content of this crime. On the one hand, from the viewpoint of the means and tools, on the other hand, from the viewpoint of offenders and the way of committing crime, it is divided into close ICT crime and crime committed by the use of communication and information technologies.[5)] [8].

[2)] Meteňko, J. et al: ISBN 80-8054-336-4, EAN 9788080543365, p. 24.

[3)] the problem is related from the viewpoint of crime and its recourse with Criminal Code, but as well as from the viewpoint of its revealing and modernization and speeding up the work of the court predominantly by the use of electronic documents and digitalization of criminalistic and investigation documents, see [10] Meteňko, J.: New trends in criminalistic documentation, 2005, CD.

[4)] whose content covers the merits of different crimes in compliance with Criminal Code.

[5)] Meteňko, J. et al. ISBN 80-8054-336-4, EAN 9788080543365, p. 126 and next

Prevention possibilities in the field of communication and information crime

Generally speaking, crime prevention is a special area of prevention enforcement. Its aim is to prevent crime and the protection against crime. From the social and practical viewpoint, crime prevention represents scientifically reasonable, aimed, comprehensive, planned and coordinated impact on reasons and conditions of crime. The aim is to remove them or by a suitable selection of forms and methods of the impact to at least partly eliminate or to restrict their negative features and at the same time to support the creation of anti-criminogenic conditions. [6]

Repression of crime is a complementary notion to a notion of crime prevention. Its meaning covers the suppression of this phenomenon by the use of violent but legal means. Mutual relation of prevention and repression may be demonstrated by their functions in relation to legitimacy. Prevention measures shall create difficulties for possible crime and make offenders aware of the fact that crime is not worth. If despite this the law is broken, repression comes. Effective prevention decreases repression needs, and repression influences prevention backwards. Both parts take part in crime control.

Social prevention is a general prevention of all social and pathological phenomena. In might also be a specific crime prevention without which crime prevention would not be complete. Social prevention is a part of social policy. In our conditions, i.e. while examining the reasons and conditions of communication and information crime, social prevention means the widest context of prevention performance. In particular, it is important to create suitable social conditions in various areas of every-day life, building of social consciousness in the area of computer and communication technologies. Not less important task is performed by family, school and after-school activities, by cooperation of the police and organization and companies dealing with information technics and schools etc.

Unlike social prevention, situational prevention is specifically aimed at concrete type of crime. It follows the fact that particular types of crime occur in particular time, on particular places, under particular circumstances and are committed by particular offenders. Communication and information crime are typical for time discontinuance, i.e. this crime may be committed practically without interruption in extraordinary short time and also in any daytime. It is pretty hard to localize this crime since current mobile technics enables offenders to perform their illegal activity almost from any part of the Earth. On the other hand we must drop a few words about offenders. These are mostly highly qualified, erudite people, often-technical university graduates (electrotechnics, information science, cybernetics etc.). According to statistical data from abroad, mainly from USA, it is clear, that the age of offenders vary from 16 to 40. But most of them study at secondary schools and universities or are young employees of firms and businesses dealing with information or telecommunication technics.

Situational prevention makes use of several forms in this area. The main forms are:

1. Classical protection
   It covers mechanical preventive tools. They are used for hardware, peripheral equipment of computer systems and also for separate objects in which the equipment is placed. In particular we talk about so called hardware keys that prevent direct physical access to equipment such as hard disc, sluts, buses, and internal and external communication. Other tools of classical protection are lock systems of premises, door security systems, bars, security covers of mobile data media etc.

2. Technical protection
   Besides classical technical protection such as electronic safe signalizations, closed-up TV circuit etc. there is also so called software protection, which is important in the area of communication and information crime. By it we understand software equipment of the systems and peripheral devices in order to provide signalization and to prevent unauthorized access into system with a particular procedure (e.g. while an unauthorized person tries to access data file, the content of the file is automatically erased so the offender does not have any chance to have a look into a file).

3. Physical protection
   It is provided mainly by security guards, private security services, but in some case also by the police or army.

4. Regime protection
   It covers predominantly administration and organizational measures, which shall provide good running of the whole safe system. Within this area it is inevitable to make use of safety regime. It means to determine regime access for authorized persons to data and information and communication system, to ensure key and password regime, multilevel cipher protection measures, authorized access and exit from the system or premises where the system is placed etc. [7]

In connection to crime prevention, the notion of victim prevention has occurred. Such prevention is specifically oriented with the aim to prevent man from being a victim. In today's fast development of information and communication technics, man as an owner and user of this achievement of 20th and 21st century becomes a potential victim of communication and information crime practically from the time he encounters it for the first time. Obviously it is quite an open understanding of this problem.

The most endangered are the firms and organizations, which make use of this technics for storage and elaboration of huge amount of data of strategic character. And these are later the subjects of interest of offenders involved in this type of crime. We cannot forget about spreading electronic business and Internet banking. Bank and financial institutions are directly endangered, but within a wider context, consequences of possible crime (illegal bank transfers, data thefts from bank clients) affect clients of these organizations as well.

Victim prevention may be performed on a general level, in relation to all people, their education, informing them about crime danger, their training in preventive behavior, advertising technical possibilities of protection against crime, conferences and lectures given by experts in a field etc.

The second aspect of crime prevention complexity is the fact that social, situational as well as victim prevention might be realized as primary, secondary and tertiary prevention from the viewpoint of crime development.

Primary prevention has an impact on wide public, which might not be affected with this crime. It approaches mass or groups of people and presents responsible methods of education.

Secondary prevention deals with risk groups or individuals that are probable to become offenders or victims. Moreover it deals with elimination of criminogenic factors. Methods of information distribution are in fact likewise, circle of people is closed-up. Substantial change is linked to elimination of criminogenic factors – as mentioned above, what requires besides already known methods and distribution ways, to use predominantly new – technologies and methods and applications responding to a social situation.

Tertiary prevention concentrates on groups or individuals that have already been involved in crime or have become its victims. In fact it is relapse prevention. It is very interesting that people once involved in committing this type of crime are becoming the best experts for protection of information and communication systems [11].

Conclusion

Every society is accompanied with a certain level and scope of crime as a feature of non-conform interests of individuals or groups. In our opinion, modern technologies do not bring any changes into this situation. However, it seems that information and communication technologies cause the negative development of crime; this fact is influenced more or less by a quality and scope of communication and exchange of information. The bigger problem is that relevant social structures of the society are not well prepared to make use of digital communication and information technics and technology in their jobs, and particularly to use them in the course of control of homogeneous and heterogeneous types of crime.

References

[1] CUĽBA, M., FELCAN, M., GÝMERSKÁ, J.: *Definition of terrorism and significance of knowing its notion spectrum,* In. Threats of present-day international terrorism and possibilities to fight against it. Bratislava: Academy of PF. ISBN 80-8054-325-9. p. 135.
[2] DLOUHÝ, M.: *Convention on cyber crime.* In. Reports from criminalistics, 2/20004, volume XLVIII. p. 37–38.
[3] GELETA, M.: *Tasks of criminal police in prevention and revealing some types of cyber crime:* Conclusion / Jozef Meteňko. – Bratislava: Academy of PF, 2001. (78p) p. 55–59.
[4] CHALKA, R., HOLCR, K., HOLOMEK, J.: *Criminal scene of the Slovak Republic: Prognosis up to the year 2000 with the view up to the year 2010.* – Bratislava: Academy of PF, 1998. 84p.
[5] JAŠEK, R.: *Defense against socio-technical manipulation,* In. Threats of present-day international terrorism and possibilities to fight against it. Bratislava: Academy of PF. ISBN 80-8054-325-9. p 104–108.
[6] KLOKNEROVÁ, M.: *Some possibilities of how to apply education in the work of criminal police in the course of crime prevention.* In. Police theory and practice 4/2003. p. 79–88.
[7] LÁTAL, I.: *Cyber crime as a crisis phenomenon and its prevention via administration proceeding.* Reports of expert studies from the seminar Criminalistic problems in revealing, investigation and prevention of software piracy. PA CR, Prague, 1999, p. 336
[8] METEŇKO, J. et al: *Criminalistic methods and possibilities of sophisticated crime control.* Bratislava 2004. Academy of PF of SR in Bratislava. ISBN 80-8054-336-4, EAN 9788080543365. p. 356
[9] METEŇKO, J.: *International seminar on cyber crime.* In. Police theory and practice. Volume 6, no. 4 (1998), p. 122–123.
[10] METEŇKO, J.: *New trends in criminalistic documentation,* In.: Reports from the seminar organized by FSI PF on 9th – 10th March 2005, "Criminalistics in practice". Bratislava 2005. FSI PF Bratislava, CD.
[11] METEŇKO, J.: *Penetration into information systems and criminalistic knowledge.* In.: Reports from international conference Internet and competitive strength of the business. UTB Zlín, 2005.
[12] MURDZA, K.: *Sociological analysis of terrorism,* In. Threats of present-day international terrorism and possibilities to fight against it. Bratislava: Academy of PF. ISBN 80-8054-325-9. p. 110–111,
[13] RAK, R.: *Information science in criminalistic and security practice.* Prague, Police Presidium CR, 2000. (471)
[14] RAK, R.: *Cybernetic crime and cybernetically related crime,* In. Reports from scientific conference "Advances in criminalistics", Police Academy, Prague, 2004.