Organized Transnational Crime and Combating Crimes in the Field of Information Technologies (Past and Present)

Pavlovska Nataliia  
*PhD of Juridical Sciences, Associate Professor, Associate Professor of Theory and History of Law, Kyiv National Economic University, Kiev, Ukraine*  
ORCID ID 0000-0003-3311-0364  
wwwpav@gmail.com

Patyk Lesia  
*associate professor, Forensic Science and Medicine Department National Academy of Internal Affairs, PhD in Law, associate professor*  
ORCID ID 0000-0002-3698-4799  
Lesya_rob@ukr.net

Erhard Nataliia  
*PhD, Associate Professor, Associate Professor of the Department of Forensic Medicine and Medical Law of the Bogomolets National Medical University, Lawyer, Kyiv, Ukraine*  
ORCID ID 0000-0002-6002-0463  
ergard2017@ukr.net

Kofanov Andrii  
*PhD of Juridical Sciences, Associate Professor, Professor of Department of Forensic Support and Forensic Expertise of the National Academy of Internal Affairs, Kiev, Ukraine*  
ORCID ID 0000-0002-5242-2518  
kofanov_andrey@ukr.net

Kobylianskyi Oleg  
*PhD of Juridical Sciences, Associate Professor, Professor of Department of Civil and criminal law of the State University of Infrastructure and Technologies, Kiev, Ukraine*  
ORCID ID 0000-0002-1842-1810  
pronter@ukr.net

Abstract

The article deals with the issue of criminal law aspects of organized crime. The author's vision of the foundations of the concept of organizational and tactical elements of the Ministry of Internal Affairs of Ukraine is presented. Recommendations on prevention and counteraction of transnational computer crimes are provided.

**Key words:** transnational organized crime, organized transnational cybercrime, transnational crime; criminalistics analysis.
Introduction Organized crime is a complicated transcontinental antisocial phenomenon that endangers the development of the mankind. Its specificity is that it penetrates into all life spheres causing destabilization of political, social, economic activities, creating real threat to safety of all countries. The tendency in growth of organized crime, it’s extending the separate states’ boundaries, increasing the influence on politics, economy, and also rapid growth of its financial base lead to the situation when a problem of fighting organized crime has become interstate, required coordination in actions, working out united approaches to solving it. The UNO World Conference on transnational organized crime (Naples, 1994) underlining its global character, arose a question about corresponding the national legislation to demands of fighting different forms of organized crime, and working out leading principles, standards of this struggle.

According to international treaties, conventions most countries brought in special laws on fighting organized crime, put amendments to law codes related to increasing the responsibility for crimes committed by organized groups. These laws invariably excreted such indications on organized crime as high level of unity, organizing, substantial, economic base, huge budget, wish to take roots in power and administration organs, relations with shadow economy, serious safety system, etc.

Scientific definitions of this term underline the same features of organized crime. Undoubtedly, all these features are really the criteria for determining organized crime as antisocial phenomenon, which worsen criminal situation in all countries. But one should not forget that organized crime (as any other one, though), is not only social but also complicated law phenomenon, which has a specific criminal-law meaning.

Criminal-law essence of organized crime including common for criminal activity traits has two specific (inherent only for it) features: a) special character and danger of committing crimes; b) the most dangerous forms of group crime. The unity of these two features must determine both the classification of crimes committed by organized groups and limits of responsibility for these crimes, in other words, be a legal basis for the strictest criminal responsibility for them.

The analysis of crimes which make a nuclear of organized crime reflects the aim. Transnational direction of its activity shows that there are the international character crimes, «infringing normal relations between states, causing losses to peaceful cooperation in different
fields’ of relations (economic, social-cultural, material etc.) and also to organizations and citizens».

Importance of the objects, danger in means of committing crimes, especially big damage, motives, aims define extreme danger of these crimes that allows to refer them to grave and especially grave crimes category. In this connection with it is very important to research the issue of classifying crimes according to their gravity.

Although the analysis of current legislations in different countries allows to draw the following conclusions: a) in some states there are no special provisions on classifying crimes according to their gravity; b) in states whose legislation has such provisions, there is no unique approach and criteria to classify the gravity of crimes. That is why the common understanding of grave or especially grave crime is absent. This shows an absence of unique legal base for mutual efforts in fighting organized crime: its special danger for all world community do not find adequate reflection in national legislation concerning the gravity of the most dangerous crimes.

The problem of classifying crimes according to their gravity despite its fundamentalism for solving all problems of criminal responsibility is not thoroughly studied in science. The significance of such a classification is recognized by not only science, but lawmakers though. Thus, the Criminal Code of New York State in Section A, paragraph 1.05 one of general purposes for its provision defines such objective as “to establish the difference on reasonable basis between serious and petty infringements and fix adequate punishment for them”. 2 The necessity in this classification has been evident lately in a process of working out new criminal codes in several countries, in Ukraine, Spain. It is necessary to note that criteria for such characteristic are the society danger level (maximum criterion), and type, kind of punishment (formal criterion). These are the criteria for defining grave or especially grave crimes as one of standards for unifying transnational organized criminality notion. As an example, we may use Article 12, Part 4 and 5, the Criminal Code of Ukraine.

Second standard in unifying definition of organized crime in national legislation must be separation of group criminality forms, which are typical for it, and reflect its special danger. We think such forms of complicity should be organized group and criminal organization, distinguishing by too high a unity level, stable relations of its members, strict role distribution. National legislation firstly, should have definitions of these forms as it has been done in new
Criminal Code of Ukraine, secondly, to define their most severe legal consequences. As such consequences the CC of Ukraine of 2001 defines an independent crime - “creating a criminal organization for committing grave or especially grave crimes, also being in charge of such group or participation in it” (Article 230), and as a result in most grave and especially grave crimes committing them by an organized group or criminal organization is a special qualifying circumstance [1-4].

Like other similar revolutionary technologies, Internet brings huge potential as for progress as for abuses, attacks in the net, fraud, software pirates, industrial espionage, children pornography trade - they are only some crimes committed in the global net.

Initial investigating actions related to detecting transnational computer crimes (cybercrimes), cause special difficulties, that relates to many problems.

The results and analysis of conducted research of law enforcement organs practical activity concerning investigating computer crimes testify that computer equipment study SHOULD be carried out in criminalistic laboratory conditions when professionals with necessary training will do this work.

Let us consider some typical mistakes that are often made while carrying out inquiry actions related to computer information and computers themselves. Several rules of working with computers, expropriated when investigating crimes in computer information sphere, can be distinguished, we also can propose general recommendations which may be useful when processing computer evidence in DOS or Windows operational systems.

Error #1. Erroneous work with a computer. First and general rule that to be mandatory implemented is never and under any conditions not to work on the seized computer. This rule considers an seized computer as an object for professionals’ studying. That is why one should not even turn it on until transferring to experts, as it is absolutely prohibited to run any programs on such a computer without using necessary safety measures (e.g., protection from modification or creating backup files). If computer has a protection on run up system (e.g. — password), then turning the computer on can cause destroying the information on hard disk. Turning such computer on, using its own operational system is not allowed. This is explained simple enough: a criminal has no difficulty in installing a program for wiping the information off on hard or floppy disk, recording such “traps” by operational system modification. For example, simple DIR command used for displaying disk’s catalogue can be changed to format hard disk. Then
the data and the destroying program itself are deleted nobody can tell for sure whether the “suspected” computer was specially equipped with these programs, or this was a result of negligence in handling computer evidence [5, 7].

Error #2. Letting access of computer owner or user to computer. Admitting an owner of computer that is being studied for helping in its work is a serious mistake. Many foreign sources describe cases when suspected on a questioning, concerning computer evidence was granted an access to seized computer. Later, they told their friends as they coded files in the policemen’s presence and policemen did not even suspect anything. Considering these consequences, quite quickly computer specialists started to create back up files of computer information before granting access to it [6, 7].

Error #3. Absence of computer scanning for viruses and macro-viruses. To scan a computer for viruses and macro-viruses, it is necessary to load a computer not from operational system in it, but from prepared in advance floppy disk, or from experts’ hard disk. All information carriers - floppy disk, hard disk, some others are subjected to check up. Specialist attracted to inquiry actions using special software should do this work.

It is necessary not to allow the court to accuse the investigator: in special virus’s infection of a computer, or in incompetence when carrying out inquiry actions or just in negligence, because it is hardly possible to prove that the virus existed in the computer before its examining, such an accusation will doubt the expert’s work and probability his conclusions. These are the most typical errors when examining computer in investigating computer crimes. But described list does not include all mistakes that are possible in the process of extracting and studying computer in-formation. This is easily explained: lack of experience in investigating similar cases in our country. At the same time Western Europe countries, the USA especially, have rich experience in investigating complicated computer crimes. This experience should be more thoroughly studied to avoid many mistakes [7].

Conclusions To prevent errors in carrying out the inquiry actions at the first investigation stage which can cause losing or destroying computer information one should keep to some preventive measures as:

First, one should make a reserve copy of information. When searching and seized computer, magnet carriers (hard disk, floppy disk), and information there are some common problems connected with specific character of seized technical means. It is necessary to foresee
safety measures, which criminal takes to destroy computer information. For example, he can use special equipment, which under special conditions create strong magnetic field and thus delete magnet records. During the search all electronic evidence in computer or computer system should be collected so that later the court would admit them. World practice testifies that in many cases under the pressure of defense lawyers in court electronic evidence are not considered. To guarantee their recognition as evidence, one should strictly keep to criminal-procedural legislation requirements standard methods of extracting them. As a rule, computer evidence is kept creating an exact copy from original (primary evidence) before somehow analyzing it. But it is not enough to make computer files copies using only standard programs of reserve copying. Physical evidence can exist as deleted or hidden files, and data, connected with these files, can be saved only with the help of special software, they can be Safe Back type programs, for floppy disks DOS Disk copy may be enough. Magnetic carries which are intended for copying the information, should be prepared in advance (you should be sure they do not contain any information). Carriers should be kept in special wrapping or wrapped in clean paper. You should remember that information could be completely spoilt by humidity, temperature or electrostatic (magnetic) fields. Find and copy temporary files. Many text editors and databases software create temporary files as software normal work by-product. Most computer users do not realize the importance of creating such files, as the program in the end of work usually deletes them. But the data inside these deleted files may be most useful. Files could be recovered especially if an output file was coded, or a document was typed [5-7].

Check Swap File. Microsoft Windows popularity brought some additional means for studying computer information. Swap File works as disk memory or huge database, many different temporary information pieces or even all the document text may be found in this Swap File.

Compare duplicates of text documents. Duplicates of text files may often be found on hard disk or floppy disk. These may be slightly changed version of one document that may have value as evidence. These divergences can be easily identified with the help of modern text editors.

Check and analyze computer network. Computers may be linked with each at other in computer network (e.g. local network), that in its turn may be linked to global computer networks (e.g. Internet). That is why there is possible that certain information (which can be
used as evidence) can be transferred through the net to another place. This place can be situated abroad or on the territory of several countries [5-7].

References


Translation of references into native language

1. Кривоченко Л.М. До питання про кримінально-правовий зміст організованої злочинності. Materials of the final conference of the Ukrainian-American scientific and
academic programs of the Academy of Legal Sciences of Ukraine and the National Institute of Justice for the US Justice Department. Kharkiv, Ukraine. 2001, pp. 3-5.


