DOI 10.32370/IA_2019_02_12

The Global Problem of the Third Millennium: Organized Transnational Cybercrime (Historiography)

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

Bilenchuk Peter
Chairman of the Supervisory Board of the Ukrainian Committee on the Prevention and Counteraction of Corruption, PhD of Juridical Sciences, Professor, Kiev, Ukraine

Kofanova Olena
PhD of Juridical Sciences, Associate Professor of Forensic Support and Forensic Expertise of the National Academy of Internal Affairs, Kiev, Ukraine
ORCID ID 0000-0002-0919-7570 kofanova_alena@ukr.net

Abstract

During the last decade issues connected with rapid development of phenomenon known all over the world as “computer crime” have been thoroughly studied. At present this concept (rather conditionally) includes all illegal actions when electronic processing of information was an object or means of committing them. Thus the problem now embraces not only crimes directly connected with computers but also such as fraud with credit magnet cards, crimes in the telecommunications sphere (fraud with international phone conversations payment), illegal usage of electronic payments bank network, illegal software, fraud in using play slot machines and many others. Crimes connected with using evidence of computer origin when investigating traditional crimes are also referred to this group of issues. Computer crime is an international phenomenon; its level is closely connected with economic level of society development in different countries and regions. Less developed technically counties due to the activity of international law enforcement organizations have an opportunity to use experience of more developed countries for preventing and detecting computer crimes. General tendencies, criminal means and preventive measures are similar in different countries in various time periods, they are based on united technical program and methodological base of these crimes. Thus “computer crime” notion together with development of computer, telephone technologies was gradually transformed into crimes in informational technologies' sphere concept.

Features characteristic for crime in a sphere of information technologies: international character of a crime (extends the boundaries of one country); difficulties in locating a “place of crime”; weak links between chains in an evidence system; impossibility to watch and fix the evidence visually; wide usage by criminals the ways of coding the information.

Key words: computer crime, detecting and investigating computer crimes, automated systems and technologies, informatization and computerization.

Introduction Nowadays mankind goes through rapid development of automatization, informatization and computerization of all life spheres. According to the NUA Internet Surveys data the number of Internet worldwide net users increased from 80 thousand in 1988 to 400 million in the end of 2000. About 1 million of them are in Ukraine. The Decree "On Measures Concerning National Part of Global Internet Network and Providing for Wide Access to This Net in Ukraine" signed on July 31, 2000 by the President of Ukraine assists in our country efficient usage of global net possibilities for science, education, culture, and entrepreneurship activity development. This Decree, in particular, provides for central organs of executive power to create and fill with information Web-pages, to establish proper economic, legal and technical conditions for granting citizens and legal persons of all property forms wide access to the net [1]. Though spreading informational technologies also has a negative aspect: it opens way to antisocial and criminal behavior. Computer systems have new, rather advanced possibilities for violations not known before, and also for committing traditional crimes with not traditional means.

Description of the installation At Big Eight conference dedicated to cybercrime in October 2000, it was mentioned that losses from cybercrimes are up to 100 billion DM every year. USA Accounting Chamber estimates annual losses from thefts and frauds made with the help of international technologies through Internet as $5 billion [2].

Besides the fact that crimes committed under using brand new technologies cause great economic losses, society becomes more dependent on automated system work in different life spheres – beginning with administrating army, enterprises, organizations, institutions, planes and trains to medical services and national security. Sometimes even slight fault in functioning of such systems can lead to real danger for people's lives. Rapid growth of global computer and telecommunication networks, also possibility for connecting it to ordinary phone lines increase their possible usage for criminal activity. No doubt, technically developed countries mostly suffer from computer crimes (here and further it will be used as a conditional term), though there are now favorable conditions for committing such crimes in other countries with the beginning of computerization process. In particular, Internet global computer network gives a possibility for access to any world departmental computer system, including a military one. Besides, it can be done from any place in the world. In comparison with Great Britain, Germany, USA, Japan, the Ukrainian national security still much less depends on computer networks: financial credit sphere mostly suffers from computer crimes. But in near future these crimes may lead to global disasters – ecological, economical, transport, etc. Introduction of moderns system for administrating culture, education, science, medicine, aircraft's routes in air, and electronic payments system, spreading of telecommunication network, using computers in law enforcement and military activities – all that considerably widened activity sphere for all kinds of computer criminals: hackers, crackers, preachers, cyber rogues, collectors, and pirates.

The public is more interested in these issues now because every user or owner of computer, phone, radio-phone, modem, plastic card is a potential victim, he can suffer from serious consequences in a case of committing crime, especially if committed in public, commercial or industrial sector where big financial losses are probable. Computer criminals with the help of international computer networks (similar to Internet) widely spread their criminal experience, not without paying attention to state boundaries. This requires corresponding steps for cooperation from law-enforcement organs counteracting to these crimes, operative information exchange about computer crimes.

With the development of global computer and telecommunication networks the industrial espionage practice has become widespread. That is why the problems of working out protection system and keeping state, commercial and official secret acquire today special importance. Many problems arise from services' thefts, that is intrusion to phone networks, and illicit communications' services trade. Sellers of illegal software, pornography, firearms and drugs also widely use Internet for conducting business, information exchange, and coordination of actions. Computer networks besides may become an object of terrorists attack. In May 1998 "Tigers for Tamil liberation" in Sri-Lanka were first among other terrorist groups to hold cyber-attack directed against the embassies in the capital.

Starting from 1991, there is a Working group for computer crimes problems at the Interpol General Secretariat, this group studies this type of crimes in different countries, works out recommendations, helps to unify national legislation, accumulates methodological experience in investigating computer crimes.

During its existence the working group has created modern computer crimes classification, worked out unified form of notification (inquiry) about such crimes, it is working at the reference-book "Computers and Crimes", to unify methods and procedures of investigation in different countries. Every year it organizes professional training courses. Expanding activity sphere of the working group led to its renaming in 1996 into European Working Group dealing with issues of crimes in information technologies' sphere. Three major directions of working group activity were set: Internet-analysis of situations, studying legal and police issues; frauds using electronic means of payment; frauds using different kinds of communications and telecommunications. Special attention is paid to issues of international co-operation when investigating computer crimes. Many countries have created specialized detachments for fighting this kind of crime, they are at the national level engaged into detection, investigation of computer crimes and collecting other information related to this issue. Specialized national police detachments create main nuclear of counteracting international computer criminality. Such detachments have already been created and work for a long time in the United States of America, Canada, Great Britain, Germany, Sweden, Switzerland, Belgium, Portugal, Austria, Poland and many other countries [3]. Doubtless international authority in Internet safety sphere is Computer Emergency Response Team (CERT), founded by Software Engineering Institute at Carnegie Mellon University in Pittsburgh, USA. CERT workers help Internet users to expose cases of penetration to information system, work out and spread informational safety manuals.

International community reached the conclusion that organized information infrastructure safety only at national level would not be effective too. At the same time organized counteraction to criminal activity only by means of law-enforcement organs is not always effective. That is why at the beginning of 90-s FIRST organization was created – forum-incident Response and Security Teams, it unites 80 response teams from 19 countries. These teams are state, commercial, industrial and educational institutions. Information from other countries quickly and in accessible form (notification language, specific terms, crime codes, etc.) has to get to national specialized detachments (if there are none, to other organs in charge). To achieve it, and also for operative information exchange between countries, even in 1994 Interpol General Secretariat recommended all countries-organization members to create national central reference point deeding with computer crime problems, and assign certain workers to work with information about computer crimes. These points are founded as a rule at the National Interpol Bureau apparatus or at the specialized detachments that are engaged in computer criminality or economic crimes. In Ukraine at the Interpol National Central Bureau such point was established on September 17, 1996 [4].

Conclusion This gave an opportunity to accumulate material on legislative regulation and organizational experience in preventing, detecting and investigating computer crimes in different countries, to prepare a number of analytical reviews and publications on actual issues, to acquaint workers of the Ministry of Interior, the Procurator's Office, court with this new to Ukraine type of crimes, to introduce concrete propositions on improving criminal legislation of Ukraine.

References

1. The problem of the third millennium (historiography organized transnational cybercrime). URL: http://bsm.com.ua/2011-08-07-02-51-49/item/200-biznes-i-bezopasnost-3-2018
2. *Informacijne suspil'stvo: upravlinnja, pravo, tehnologiї, bezpeka*. [Information society: governance, law, technology, security.] URL: http://elar.naiau.kiev.ua/jspui/handle/123456789/4337
3. *Informacijna analityka v jurysprudencii': avtomatyzovani systemy i tehnologii*. [Information analytics in jurisprudence: automated systems and technologies.] URL: http://elar.naiau.kiev.ua/jspui/handle/123456789/4335
4. *Bezpeka informacijnoi' analityky: strategija, taktyka, mystectvo, tehnologii*. [Security of information analytics: strategy, tactics, art, technology.] URL: http://elar.naiau.kiev.ua/jspui/handle/123456789/4334