CYBERCRIME AND ITS CHARACTERISTICS

Ravan Hasanov
(*ravan.hasanov@yahoo.com*)
Ph.D Candidate
(Institute of Law and Human Rights of
The National Academy of Sciences of Azerbaijan)

Abstract

The process of globalization, including the globalization of information technologies offers great prospects to make a real impact on an individual and society. One of the negative outcomes of the development of information technologies is its preconditioning the formation and development of a new type of criminality consisting of crimes occurring in the field of high technologies. In this process computers and computer networks are exposed to criminals' aggression. Also, they act as a method or means of committing crimes. The problem of cybercrime has started to acquire vitality in the period of information society.

Keywords*: cybercrime, computer, computer system, internet, information.*

In the current period computers and telecommunication systems involve all the spheres of human and state activities. Meanwhile, the global internet network is the fastest-developing sphere of telecommunication technologies. Today not only individuals, but entire states can turn into the victims of cybercrime, as the security of thousands of internet users depend on several criminals. The criminality in cyberspace grows in proportion to the number of users. For instance, one can refer to such a fact: the site (Internet Complain Centre) formed to register the victims of cyber criminality was appealed by over million people in 2007. The growing professionalism of cyber criminality and the constant improvement of information technologies generate new risks for the users of global information networks. The problem of the use of science and technology for criminal purposes is associated with one of the most urgent directions of the integrative processes. This direction constitutes the creation of the global internet network which connects millions of computers located in the most varying regions of the world. The internet offers very vast prospects for the acquisition of information and its exchange, and develops at a very high speed. In the 90s of the last century it was considered that within approximately 10-15 years the internet would embrace 1 billion computers. However, the prognoses failed. In the given period the internet already covered over 1.5 billion computers. As it is obvious, this number constituted one fourth of the world population [11]. The fast development of computer networks and their intervention into different spheres of human activities preconditioned new types of criminality. And the areas of activities intervened by computer networks depended on the appropriate time. As, in the 1960s computer networks were mainly used in military and scientific enterprises. The main risk was associated with the loss of the confidential data and unauthorized access to these data. In the 1970s already commercial criminality came to the forefront in the field of computer technologies. Such criminality can include the breakage of bank computer networks, industrial detectives, etc. In the 1980s the breakage of the software and their illegal dissemination began to spread widely. In the 1990s the appearance and

development of the internet network preconditioned the emergence of new serious problems. For instance, intervention in confidential private data, dissemination of child pornography, activities of the groups of extremist virtual networks and other similar problems can be cited [2]. In the further stage there appeared more dangerous problems sufficiently difficult to prevent. Since, the expression "infected computers" has seriously established itself in the lexicon. "Attacks" were launched against such computers whose users remained unaware. Moreover, the integration of telecommunication networks and their convergence, the presence of mobile access to the internet, etc. have enabled the use of information technologies for dangerous or criminal purposes. It should be noted that most of the crimes committed in global computer networks are characterized by a number of features which can be generalized as follows,

- Crimes can be committed quite secretly which is due to the characteristics of information space (the developed mechanisms of confidentiality, the complex nature of infrastructure, etc.)
- the objects and subjects of cybercrime can be located in the most diverse regions of the world;
- the special training of criminals, the intellectual character of criminal activity;
- the frequent renewal of methods of committing crimes, their complexity and diversity;
- the committing crimes in automated regime simultaneously in several sites and the possibility of the weaker resources of numerous individual computers turning into stronger tools of committing a crime;
- the multi-episodic nature of criminal activities;
- the victims' unawareness about their exposure to the impact of the crime;
- the committing a crime from a distance while the criminals and victims do not have any physical contacts;
- the impossibility of preventing crimes through traditional methods [4, p.109]

It should be taken into consideration that the notion "cybercrime" is most often used in parallel with the notion "computer crime". They are even applied almost as synonyms. Indeed, these notions are very close to each other. However, their usage as synonyms is not correct. It is considered that the notion "cybercrime" is broader than "computer crime". Thus, it more accurately expresses the nature of crimes committed in the information space. As, the monolingual Oxford Dictionary defines the word "cyber" as a component of a complex word. It is ascribed to information technologies, internet networks, and virtual realities [10]. Practically, Cambridge Dictionary also expresses the identical definition. As, the prefix "cyber" incorporates the usage of computers, and especially of the internet. Nevertheless, Cambridge Dictionary introduces the word "cybercrime" into the circulation [9]. Thus, cybercrime implies the crimes committed by using computers, also information technologies and global networks. Yet, computer crime implies the crimes targeted against computers or computer data. The global information space, the information mega-pace is non-material. At present with the development of information technologies, the very notion "computer" gradually grows to be vague. As, today practically all mobile phones have an access to the internet. Besides, through the development of 3G and 4G networks, the possibilities of mobile connection to the internet have considerably expanded and their quality has increased. Telecommunication infrastructures are being adapted to the exchange of the data in huge amount in a more comfortable form [3, p.18]. It is not hard to forecast that the

users of internet and mobile communication will benefit from wider potentials in near future. It is observed that the boundaries of the notions "cybercrime" and "computer crime" are distinguished at the level of international legislation as well. Since, in 2001 the Council of Europe adopted the Convention on Cybercrime. This Convention used the very notion "cybercrime". Cybercrime is a crime committed in cyberspace. From this point of view, in order to realize the essence of cybercrime more profoundly, one should elucidate the essence of the notion "cyberspace" itself. Cyberspace is a physical and non-physical space consisting of the following components:

- Computers, computer systems;
- Networks and their software;
- Computer data, content data and the action of the data;
- Users.

As the guidebook on cybercrime was developed in the frames of the UNO, when defining the goals of the criminal legislation in the appropriate field an official approach is referred to. Cybercrime is the sum of computer systems, computer networks, also the crimes committed in cyberspace through the other means allowing an access to cyberspace. This crime is relevantly committed against the computer systems, computer networks and computer data. This approach or definition is appropriate to the UN experts' instructions. Since, according to the UN experts, cybercrime involves any crime committed through the computer systems or networks in the frames of computer systems and networks against the computer systems and networks [5]. Hence one can come to such a conclusion that any crime committed in electronic environment belongs to cybercrime. Such kind of approach is ascribed to all crimes committed in the field of information and communication. In information-communication field information, information resources, information technology act both as the objects of the crimes as well as tools of committing crimes [8, p.187].

As for the issue of consistency between "cybercrime" and "computer crime" along with the above-mentioned, it should be taken into account that the UN specialists have formed a definite attitude. The notion "cybercrime" covers all kinds of crimes committed in the field of information technologies. It can involve both the crimes committed with the help of computers as well as the crimes committed against the computer's subject matter, computer networks and the information restored in them. Computer crime implies not only the illegal interventions targeted against the safe activities of computers and computer networks but also against the information produced by them [6, p.29]. So, one can conclude that computer crime is a variety of cybercrime.

Types of Cybercrime

To realize the nature of cybercrime more accurately, one should also have ideas about its types. Types of cybercrime are defined depending on the object, subject of aggression and means of committing it. Since, depending on the object of aggression, the following types of cybercrime can be distinguished: [1, p.37]

- Commercial computer crimes;
- Crimes targeted against the individual rights and integrity of individual sphere;
- Computer crimes targeted at social and state interests.

Depending on the nature of the use of computers or computer systems, three types of cybercrime can be distinguished:

- Cases when computers act as the subject matter of the crimes (possession of the data, unauthorized access to them, elimination of the files or damaging the devices);
- Cases when computers act as the tools of crimes;
- Cases when computers act as the intellectual means.

The most extensive method is defining the distinction among the crimes committed against computers through computers and computer networks. It should be noted that this classification is being used by the UNO. In reference to it, cybercrime is viewed in its broad and narrow meanings. The Convention of the Council of Europe on Cybercrime divides it into four groups (later the number of the groups was raised to five by adopting additional protocols) [7]:

The first group is defined as "computer crime" and expressed as crimes committed against confidentiality, the confidentiality and availability of electronic data and computer system, and mainly the following types of crime are ascribed to it:

- Illegal access to computer systems or its parts;
- Illegally obtaining the data not intended for the public;
- Illegal damaging, erasing, change of electronic data;
- hindering the activities of computer systems through damaging, erasing and changing the electronic data.

The crimes committed during the use of computer systems are ascribed to the second type. The crimes committed through inputting, changing, eliminating the electronic data are more precisely ascribed to such kind of crimes by the Convention. In accordance with the Convention, the fraudulence in cyberspace is the deprivation of other persons of their assets through changing, eliminating or possessing the software.

The third group includes the crimes committed in connection with the content (the content of the data). This implies child pornography. The Convention expresses the urgency of persecution of actions associated with the dissemination of child pornography. So, the crimes included in this group are associated with the content of the data placed in computer networks. Almost in all states the cybercrime associated with child pornography is punished most severely. In such crimes the persons not physically in contact with a child, but participating in the production of the pornography are also charged. The production of such pornographic materials requires the sexual exploitation of children which is of serious criminal nature.

The fourth group includes the crimes associated with the violation of copy rights and related rights. The Convention does not distinguish the types of such crimes. The national legislation of states envisages that taking actions related to such violations of rights is expressed.

The fifth group includes the crimes associated with the aggression against social security. This category includes cyber terrorism and the usage of cyberspace with aims of terror. It should be noted that the globalization of information processes has preconditioned the appearance of cyber terrorism as a new type of terrorism. Cyber terrorism can be ascribed to the technological type of terrorism. Unlike the classic terrorism, this type of terrorism makes use of the latest achievements of science and technology in the fields of computer and information technologies, radio-electronics, gene engineering.

Conclusion

Thus, it should be pointed out that cybercrime belongs to the most dangerous category of criminality of the modern period. One of the basic features characterizing cybercrime is its extent of danger grows in accordance with the development of computer and information technologies, as well as radio-electronic devices. Another dangerous feature is that there is no factor of borders for cybercrime. The subjects and objects of the crime may be located at the most varied points of the world. From this point of view, it is very hard to analyze the cybercrime or its varieties in the frames of a country or countries.

References:

1. Bekryashev A.K., Belozerov I.P. Shadow Economy and Commercial Crime. Omsk: Omsk State University. 2000, 459 p. (in Russian)

2. Bondarenko S.B. Virtual Social Networks of Deviant Activities. URL: http: // www. cyberpolitics.ru/ content/view/ 256/34/ (access date: 19.09.2018) (in Russian)

3. Kashlev Y.B. The Establishment of Global Information Community and the Place of Russia// Information. Diplomacy. Psychology. M., 2017, p.p.18-20 (in Russian)

4. Osipenko A.L. Network-based Computer Crime. Omsk, Omsk Academy of the Internal Ministry of Russia, 2009, 480 p. (in Russian)

5. Crimes Associated with the Use of Computer Network [e-resource]// The 10th UN Congress on Prevention of Crimes and Behaviour Towards to Lawbreakers//A/CONF.187/10. URL: http: // www. un.org/ russian/ topics/crime/ docs10.htm (access date: 20.09.2018) (in Russian)

6. Tropina T.L. Cybercrime. Vladivostok, Publishing House of Far-Estern University (in Russian)

7. The Convention on Cybercrime// https://rm.coe.int/1680081580 (access date: 20.09.18)

8. Shetilov A. Some Problems of the Struggle Against Cybercrime and Cyberterrrorism// Informatization and Information Security of Law Enforcement Agencies. The 11th International Conference, M.2002, p.p. 186-188 (in Russian)

9. Cambridge Advanced Learner's Dictionary [Electronic resource]. URL: http: // dictionary. cambridge. org (access date: 17.09.2018)

10. Oxford English Dictionary [Electronic recourse]. URL: http:/ /www. askoxford.com/ (access date: 17.09.2018)

11. World Internet Usage. URL: http://www. internetworldstats.com/stats.htm (access date: 19.09.2018)

Date of receipt of the article in the Editorial Office
(14.11.2018)