BIOSCIENCES BIOTECHNOLOGY RESEARCH ASIA, November 2014. Vol. **11**(Spl. Edn. 1), p. 381-385

Cybercrime: Criminal Law and Criminological Aspects

Baimagambetov Tannur Meiramovich

The academy of financial police, Republic of Kazakhstan, Akmola region, Tselinograd district, Kosshy Settlement, 010000, Republic of Kazakhstan, Astana, Central post office, Post off. box 53

doi: http://dx.doi.org/10.13005/bbra/1490

(Received: 27 September 2014; accepted: 10 October 2014)

The present article shows the increase in cybercrime, as well as the impact of cyber threats to national security. Economic opportunities of using computer technology make them very attractive for criminals. Extensive penetration of information technologies into the everyday life and creation on their basis of the global Internet network foster the spread of cybercrime. The article presents the study of issues related to qualification and classification of cybercrime in terms of criminal law and criminology that stipulate the need to improve the criminal law of the Republic of Kazakhstan (RK). Author justifies the feasibility of using a larger number of crime target features for definition of the cybercrime components.

Key words: Cyber threats, Cybercrime, Telecommunication technology, Computer information.

Today, in the context of the creation of the information society on the basis of widespread use of telecommunication technologies, mankind is faced with a new threat, namely cybercrime.

Due to the constant rise in cybercrime and the scale of the damage that it causes to natural persons and legal entities, such crimes are a serious threat to society. Therefore anti-criminal warfare becomes a major concern for law enforcement agencies, particularly in respect to the operational establishment of intruders, verification of the very fact and the place of crime, and hence, the jurisdiction[1].

* To whom all correspondence should be addressed.

According to JSC "Kaspersky Lab", every day about 125 thousand malicious objects (files) emerge in the global networks, and attackers are becoming more sophisticated. In recent years, about 90% of Russian companies recorded incidents in the field of IT-security. At that, more than half of surveyed experts acknowledged the loss of data due to infection by malicious software. Most often IT-specialists are faced with viruses. The up-to-date list of threats includes also spam, phishing, network attacks on businesses infrastructure, including DDoS-attacks (Distributed Denial-of-Service attack). Most often, incidents in the field of IT-security lead to loss of data relating to payments (13%), intellectual property (13%), client databases (12%), and employee information (12%)[2].

According to the Norton Cybercrime Report, in 2011 about 341 million people became victims of cybercrime. About 69% of adult Internet

users at least once faced with the manifestations of fraud on the network, and at least 10% of individuals, using mobile phones and smartphones, were suffered by telephone fakers. Total loss (total damage), caused by IT-offenders over the last year amounted to about 388 billion USD. Moreover, during this year computer trespassers received about 114 billion USD. The cost of works needed to restore infrastructure security after cyber attacks is about 247 million USD [3].

Note that the threat of spreading cybercrime is becoming increasingly important for the Republic of Kazakhstan, not lagging behind the global trends in the development of telecommunications computer technology.

Kazakhstan's economy possesses high potential: the country has a lot of large industrial enterprises and developed banking system. A number of Internet users are growing rapidly. All this create in Kazakhstan the conditions that promote to the revitalization of cybercriminals, focused primarily at financial gain.

In Kazakhstan, a number of cyber threats is gradually growing. At the end of last year, the proportion of users, who were exposed to online Internet attacks, has exceeded 50% [4].

The statistics on increase in a number of committed cybercrimes is as follows: in 2004 there were 26 computer-related crimes, whereas in 2005 – 713, in 2006 – 1437, in 2008 – 1622, in 2009 - 2196, and in 2010 - 2423[5]. Such a trend is explained by a rapid growth in a number of Internet users.

For years Kazakhstan gets into the top of the countries, leading in terms of a number of servers that attack users[6].

All of the above causes the close attention of researchers in the field of criminal law, criminal law developers and criminologists to the phenomenon of cybercrime.

Historically, the concept of "cybercrime" arose spontaneously under the influence of the representatives of not only legal science, but also information security professionals, who borrowed conceptualization from their Western colleagues. It is known that the term "cybercrime" began to appear in the Western press in the 60s of the 20th century, when first crimes, related to the use of computers, were solved. Development of scientific and technological progress, particularly in the field of computer technology and the Internet, with the advent of electronic payments, has led to the fact that a number of professionals with good knowledge in the field of IT-technologies, in an effort to enrich themselves, began to invent different ways of unlawful withdrawal (transfer) of money funds from foreign accounts. This has contributed to the emergence of a special category of offenders called "hackers".

"Hacker" is the attacker, who uses knowledge of computers and software, as well as the capabilities of the Internet, to carry out unauthorized activity, including injurious actions on computer networks, in particular, for the hacking of computer systems and the data stored by developing and distributing for this purpose of malware (computer viruses, worms, and Trojan horses)[7].

In criminology, the basic issues for typification of criminal's personality are relationships between the operational features of the mentioned persons and certain types of their criminal activity.

Within this framework, the scope of cybercrime is not an exception. Nevertheless a number of aspects show certain specificity. This specificity is stipulated by a number of circumstances, including not only the variety of subjects and methods of criminal attacks, but the availability of obvious distinctive features relating to the identity of the cybercrime committer. Apparently, it is impossible not to draw attention to the presence of a particular feature of the criminal groups that are created for the commission of the crimes. For example, this refers to the specific mindset, as well as subculture, etc.

Such a specificity of "cybercrime" perpetrator and related criminal conspiracies, reflecting through the methods, mechanisms and types of crimes committed, has a negative impact on the effectiveness of law enforcement by the internal affairs bodies. The latters are extremely slow in adapting to the new conditions of the fighting crime.

According to experts, the most common reasons and conditions for the crimes, commissioning in the field of computer information are the follows:

a) increase in the number of computers and, as a consequence, increase in the amount of computer processed and stored information;
b) lack of measures to protect computers, computing systems and computer networks;
c) insufficient software protection;
d) increase of information exchange through the global information networks;
e) deviation from the technological modes of information processing;
f) lack, imperfection or deviation from the operating rules in respect to the computer codes, databases, and hardware ensuring network technologies;
g) lack or inconsistency of information security solutions for the labeled output;
h) violation of the rules on processing legally protected computer information;
i) low level of specialized training of law enforcement officials, who must prevent, detect and investigate crimes in the computer information field;
j) lack of a state policy in the sphere of information security[8].

American researchers Debarati Halder and K. Jaishankar define cybercrime as endeavor against a person or a group with direct or indirect criminal intent to cause damage to reputation, physical or mental health of the victim through the use of communication computer systems or mobile communication systems[9]. They note that cybercrime poses a serious threat to national security and the national economy[10].

It should be noted that this type of crime is most widely defined in the Council of Europe Convention on Cybercrime, where it appears as any kind of property damage caused by the wrongful manipulation of computer information[11]. A similar approach has been implemented in the legislation of the United States, providing for four components of deceitful practices using computer technology[12].

Russian researcher I.G. Chekunov offers noteworthy classification of cybercrime on the basis of various special criminological features. At that, it should be emphasized that:

a) targets of cybercriminals are achieved by the unlawful use of information and communication technologies (ICT), especially the Internet, as well as mobile tools and communication systems;
b) the use of contemporary information and communication technologies to commit crimes creates specific problems in terms of establishing the attacker, proving the very fact of commissioning wrongful act and determining its geographical location, because information and communication resources, used for the offense, may be located not only in one or two countries, but in many countries (this circumstance causes high latency of the crime);
c) evidences, related to such crimes, may be kept and transmitted, as a rule, only through electronic networks (this raises the complexity when collecting and securing evidence and conducting procedural actions; the problem of latency becomes even more complicated);
d) as mentioned above, crimes are often committed in order to achieve self-serving financial goals, though goals may be also both political and economic, as well as terroristic;
e) tendency to organized nature of cybercrime, as well as gang offences increases and becomes stable; at that, the cooperation of intruders occurs on a voluntary basis; thus, today it can be asserted that the epoch of "individualists" filed as a history.

Based on the above-described characteristic features of cybercrime, I.G. Chekunov gives a detailed concept of this type of criminal act. Cybercrime is a deliberate criminal act, committed in the virtual space using telecommunication means and methods. At that, computers, software, the Internet or the means of the mobile communication network are either tools or objects of endeavor. It should be noted that according to European Convention on Cybercrime, the latter includes also unlawful acts, associated with the matter of content (localization and distribution of pornography in cyberspace), as well as crimes related to the exploitation of information and communication technologies with regard to infringement of copyright and related rights[13].

It should be noted that the responsibility for cybercrime under the laws of the United States ranges from a fine and a few months in prison, for

crimes of minor severity (Class A), to 15 years in prison (Class C)[14].

What can be opposed to above cyber threats by the criminal law of the Republic of Kazakhstan? Today it is the only Article 227 of the Criminal Code of the RK, which provides liability for unauthorized access to computer information, protected by law, violation of the operation rules of computers, computer systems or their networks by persons, having access to a computer, if this deed led to the destruction, blocking, modification or copying of information, disruption of computer operation; as well as creating computer codes or making changes to existing codes, knowingly leading to unauthorized destruction, blocking, modification or copying of information, disruption of the computer operation, use or distribution of such codes or computer hardware with such codes. The article includes two ordinary and two qualified component elements of a crime. It seems that in this case the legislator admits over-simplification in the management of responsibility for cybercrime, which is hardly consistent with today's trends in the development of criminal law. For comparison, consider the criminal liability for cybercrime, established by criminal codes of the CIS countries. First of all, note that the Model Criminal Code for Member Nations of the CIS includes Chapter 30 "Crimes against information security" with following seven components of crime: "Unauthorized access to computer information", "Modification of computer information", "Computer sabotage", "Misappropriation of computer information", "Manufacture and sale of special means for non-legitimate access to a computer system or network", "Malicious software development, use and distribution", "Improper operation of a computer system or a network". The Criminal Code of Ukraine provides six articles stipulating responsibility for various violations in the field of computers, computer operating systems and treatment of computer information. The Criminal Code of the Russian Federation includes a separate Chapter 28 "Crimes in the sphere of computer information" including three articles 272, 273 and 274. Chapter 30 of the Criminal Code of Azerbaijan includes three corresponding articles with five preferred components, providing for liability for unlawful activities in the field of computer information. Within this framework, the proposal of the General Prosecutor's Office of Kazakhstan is of undoubted interest. It concerns the introduction of Chapter 7, "Crimes and offences against the security of information technology" into the new edition of the Criminal Code of the Republic of Kazakhstan[15].

In the original version of Chapter 7, the authors provided ten components of cybercrime: Art. 220: "Violation of the operation rules of information systems, electronic information resources or information and communication networks"; Art. 221: "Unauthorized access to information"; Art. 222: "Illegal modification of information"; Art. 223: "Computer sabotage"; Art. 224: "Illegal abstraction of information"; Art: 225 "Coercion for information transfer"; Art. 226: "Creation, use, or dissemination of malicious computer codes and software products"; Art. 227: "Unauthorized dissemination of electronic information resources, falling within the resources of restricted distribution"; Art. 228: "Provision of hosting services of Internet-resources for unlawful purposes"; and Art. 229: "Unauthorized change of the identification code of the user terminal of cellular communication, the user identification device, as well as the creation, use and dissemination of software to change the identification code of the user terminal".

The comparative analysis has shown that among all above mentioned crimes there are those indicated in the Cooperation Agreement of the CIS Member Nations devoted to the fighting crimes in the computer information sphere (Minsk, June 1, 2001). Thus, the draft conception of the Criminal Code of the Republic of Kazakhstan includes virtually all cybercrimes that are recognized by regional international community. However, these articles were implemented under a different title of a chapter of Special Part of the Criminal Code, namely "Crimes and offences against the security of information technology", instead of a title of Chapter 30 of the Model Criminal Code of the CIS Member Nations. This approach was endorsed by several Kazakh researchers, in view of the fact that information security is a broad concept that includes not only crimes in the field of information technology, but also crimes committed with the use of computer technology[16]. It should be noted that the provisions of the Draft Criminal Code meet generic object-based classification, whose features

are specified as "Crimes and offences against the security of information technology". Thus, public relations, which are harmed due to the commission of computer crime, are formed regarding "information that is processed by electronic computers, systems or computer networks". Generic object-based classification is a backbone factor for the whole Criminal Code of the Republic of Kazakhstan. In addition to expanding a number of object attributes, an important way to improve the Criminal Code of the Republic of Kazakhstan is the differentiation and further tightening of responsibility for committing cybercrimes on the background of the transformation of social relations and the emergence of new threats posed by cybercrime, in order to provide a decent protection of individuals, society and the state.

In addition to the above, besides criminal justice response, counter efforts to cybercrime should also include a number of preventive measures of general social character, as well as special criminological and individual nature[17].

Key objectives of preventing and combating this type of crime are the development of an optimal mechanism of social control over the crimes committed with the use of computer technology, as well as establishing control in the field of high technology and providing information security of both society as a whole and an individual. Along with the control, the organization of counter efforts must provide a clear process of interaction and exchange of information between law enforcement bodies and other relevant ministries and agencies of the Republic of Kazakhstan, as well as between national agencies and their foreign colleagues. Here it is necessary to prepare guidelines on the identification, prevention, and detection of crimes in the sphere of high technologies, to establish subdivisions, as part of forensic institutions, providing expert examination in criminal matters in the field of high technology, as well as to carry out training of the qualified staff to meet the challenges of combating crime in the high technology sphere, and to assist law enforcement agencies in other countries.

REFERENCES

1. Chekunov, I.G., Cybercrime: concept and classification. *Russian investigator*, 2012; **2**: 37-44.
2. www.kaspersky.ru/downloads/pdf/kaspersky_security_network.pdf.
3. www.nozsoft.com/819-ocenen-globalnyy-uscherb-ot-kiberprestupleniy.html.
4. Mambetov, S. Kazakhstan attracts many cybercriminals. Date Views 16.06.2014 www.kursiv.kz/freshkursiv/details/hitech-weekly.
5. www.kzinform.com›ru/press/20110919/03087.html.
6. Crimes of hackers in Kazakhstan, Date Views 16.06.2014 www.iport.kz/blog/kaznet/1194.html.
7. Kozlov, V.E. Theory and practice of fighting computer crime. Date Views 20.06.2014. www.twirpx.com/file/370870.
8. Sizov, A.V., Causes and circumstances of the crimes in the computer information sphere. Information Law, 2008; 2.
9. Halder, D. and K. Jaishankar, Cyber Crime and the Victimization of Women: Laws, Rights, and Regulations. Hershey, USA: IGI Global, 2011.
10. Jaishankar, K., Cyber Criminology: Exploring Internet Crimes and Criminal Behavior. Boca Raton, USA: CRC Press, *Taylor and Francis Group*, 2011.
11. Csonka, P., Internet Crime; the Draft Council of Europe Convention on Cybercrime: A response to the challenge of crime in the age of the internet. *Computer Law and Security Report*, 2000; **16** (5).
12. Balkin, J., J. Grimmelmann, E. Katz, N. Kozlovski, S. Wagman and T. Zarsky, Cybercrime: Digital Cops in a Networked Environment, New York University Press, New York, 2006.
13. Chekunov, I.G., Criminological and criminal aspects of the cybercrime prevention. *Russian investigator*, 2013; **3**: 36 - 43.
14. Computer fraud charges in New York, New York computer fraud lawyer. Bukh Law Firm, New York, 2011.
15. Kazakhstan offers criminal sanctions for cybercrime. www.tengrinews.kz/kazakhstan_news/v-kazahstane-predlojili-ugolovno-nakazyivat-za-kiberprestupnost-223903.
16. Samaldykov, M.K. Cybercrime in the Concept of the Draft Criminal Code of the Republic of Kazakhstan. G-Global Project, Date Views 25.07.2014. www.group-global.org/ru/publication/view/6230.
17. Gulian, A.R., The main directions of fighting computer crime in the Russian Federation. *Russian Investigator*, 2009; 5.