Methods for Cybercrime Fighting Improvement in Developed Countries

Olzhas B. Murashbekov
B. Beisenov Karagandy Academy of the Ministry of Internal Affairs of the Republic of Kazakhstan 124 Yermekova St., Karaganda city, Republic of Kazakhstan, 100021, Tel: 7471250-48-20; E-mail: murashbekov@mail.ru

ABSTRACT

The paper submitted covers advanced methods of cybercrime fighting in developed countries and opportunities of their use for law enforcement in Republic of Kazakhstan. Economic opportunities of computer technologies make them attractive for criminals. Cybercrime is promoted by IT in everyday life and Internet. Technical methods of protection from criminal offense committed with the use of computer technologies are studied together with organizational and criminal law methods enabling efficient investigation of cybercrimes, correct classification of crime components and fair punishment. Feasibility of further criminalization of acts accounting for lucri causa and crime commitment method in cybercrimes is substantiated. The conducted research enabled the author to classify the advanced contemporary methods in connection with fighting cybercrime and come to the conclusion on their comprehensive use. Some exact steps were submitted for improvement of criminal regulations of Republic of Kazakhstan accounting for lucri causa and crime commitment method (using computer technologies in a number of classified components of crimes against property).

Keywords: Cyber-threat; Cybercrime; Computer technologies; Computer information

© Olzhas B. Murashbekov, 2015
INTRODUCTION

Currently, large-scale establishment of global information society is going on, when information security issue is in the lead. Today it is impossible to imagine financial and economic activity without the use of information and communication technologies developing greatly in XXI century. At present time, such technologies are widely used in business including banking (Internet banking), electronic auctions/trade, etc. Meantime, their wide implementation created such a negative phenomenon as computer crimes or cybercrimes, threatening their safe use.

Meanwhile, law enforcement offices need qualified and timely protection from criminal offense in digital sphere. Cybercriminals threaten Kazakhstan’s economic development and prevent the establishment of information society. As evidenced by the statistics, IT crime growth rate is still high. In Kazakhstan, the number of threats is continuously growing and last year the share of unique users suffering Internet attacks exceeded 50% [1].


The global trend evidences that about 70% of crimes committed in hi-tech are those where computers and other electronic devices are used as means for theft and offender’s fraudulent intent is aimed at seizure of other person’s property [3].

State crime fighting policy including that in connection with transnational organizational forms (also, in cyberspace) has undergone great changes within the latest decade. The results of efforts in connection with cybercrime fighting do not satisfy the information society establishing in Kazakhstan. Active search for optimal organizational and legal forms of fighting economic and organized, transnational crime is going on. Kazakhstan’s Ministry of internal affairs is timely responding to the developing new cyber safety threats taking active part in fighting cybercrime.

Yet the time is relentless and is going on very quickly. Today, offenders are using new criminal methods more often, like electronic methods and means, for instance, mobile communications, Internet banking. At the contemporary stage it is crucial and notational to continuously improve the methods ensuring successful prevention, clearing and investigation of cybercrimes, providing unavoidability of punishment. It should be noted that recently a number of scholar schools has been emerging in cybercrime fighting, including the Russian scholar school [4,5] focused mainly in criminal law aspects of fighting cybercrime. Those researches are as a rule the basis for traditional methods of cybercrime fighting like criminalization and decriminalization of cybercrimes. The western scholars [6,7] pay the most attention to the criminological aspects, classifying cybercrimes or types of cybercriminals. Such research is aimed at the establishment of general public methods for fighting cybercrimes and technical protection. Not arguing the significance of the above scholars it should be said that today it is feasible to use the advanced methods applicable in the countries fighting cybercrime long and successfully. Mainly, those
are the Western countries, the EU, the USA, but recently Russia has also demonstrated success in fighting cybercrime. The study of the methods enabling to reach certain success in fighting cybercrime is the objective of this paper. Use of the methods not yet used by Kazakhstan’s law enforcement offices will let them always be a step ahead preventing acts of cybercriminals of all kinds.

**METHODOLOGY OF RESEARCH**

The main research method of this paper is dialectic cognition, related general philosophical methods (systems approach, analytical, synthetic, syntax methods) and particular scientific methods of cognition, namely formal logical, historical, comparative legal, exact sociological, system structural and statistical methods of research.

**RESULTS**

According to Convention on Cybercrime (Budapest), effective since July 1, 2004 (hereinafter referred to as Convention), cybercrimes are acts against confidentiality, entirety and accessibility of computer systems, networks and computer data and abuse of such systems, networks and data. Article 12 provides for corporate liability which contradicts to the effective Russian criminal regulations. As reasonably stated by Arbuzov and Kubantsev [8] current provisions on criminal corporate liability in Russia are rather shallow, ignore the existing criminal law doctrine and in the event of their realization are able to disorganize the criminal proceedings system becoming an extra source of law enforcement offices and other governmental institutions corruption [8].

Due to the urgent need for cybercrime fighting, on June 1, 2001 in Minsk, Agreement of the CIS countries on cooperation in cybercrime fighting was concluded, article 1 stating that a cybercrime is a criminally punished act where the subject of violence is computer information.

Accounting that the above international regulations on cybercrime are rather contradictory including contradictions in determination of cybercrime it may cause criminal liability avoidance only due to the fact that the state where a cybercrime was committed and the state where the guilty person was apprehended are oriented at different international treaties on cybercrime.

As assessed by Europol, annual damage from cybercrime in the world is assessed at EUR 290 billion. Only last year, the EU citizens suffered direct damage EUR 1.5 billion worth. It makes cybercrime more profitable that marijuana, heroin and cocaine trade all together [9].

According to the Europol’s report The EU Serious and Organized Crime Threat Assessment (SOCTA) [10], only in the EU territory 3,600 of criminal groups were liquidated, committing crimes in Internet with the objective of personal financial profit and break of economic stability. Europol’s experts have to state that currently only 30% of all cybercrimes are detected and therefore growth of criminal acts in that sphere is predicted, connecting the growth of cybercrime with the growth of Internet’s significance in personal life. Also, the said experts state that growing significance of
mobile devices as the main means of Internet access may cause wider use of those devices by criminals [10].

It should be also stated that not all the countries criminalized cybercrime. Cybercrime is not criminally prosecuted in some countries which creates unpunished professional cybercriminals.

To commit cybercrimes it is enough to buy a means of satellite communication. The time for commitment of this kind of crimes may take less than a minute and a criminal is not limited in choosing the country in which territory he/she will use it. Law enforcers as a rule need a lot of time to find and call liable such a person, enabling a criminal to cover up traces of crime which will make it impossible to call such a cybercriminal liable. In that situation, only combining efforts of all law enforcers from all countries makes efficient prevention of that category of transnational crimes possible.

Due to open Internet access, most cybercrimes are committed via Internet as it is rather hard to find the person who committed a crime. One of the factors for growth of those crimes in Kazakhstan is the lack of needed cooperation of law enforcers in investigation of those kinds of crimes. In that connection, the need for professional development of law enforcement officers in investigation of those crimes is of special importance.

As reasonably noted by Kostin [11], cybercrimes are seldom separate, they are as a rule accompanied by other antisocial deeds and are non-binding. This is conditioned by the fact that the use of computer technology as the means for committing another crime becomes the subject of antisocial deed.

Great problems are experienced by law enforcers in fighting computer fraud. At the opening of IV International conference, High-tech fraud fighting AntiFraud Russia [12] the head of Bureau for special technical measures of Ministry of internal affairs of the Russian Federation (hereinafter referred to as BSTM MIA RF) Major-general of police Moshkov stated that every year the complexity of Internet fraudulence is growing bringing special requirements to the qualification of staff engaged in cybercrime investigation. In the first 9 months of 2013, the number of criminal cases sent to court by K Department grew by 12.6% [12].

There is some national and foreign experience in solution of the problems of informational and analytical support of fighting cybercrime, especially organized. Some time ago in the Russian Federation various systems of decision making and database management systems were used (DBMS KRONOS, Binar, Laguna using entity-relationship information model) together with the specifics of informational and analytical work of law enforcers in fighting organized crime [13].

In publications on that topic, there are some methods including association matrixes of network of ties between organizations (stable ties between various independent organized groups), other objects of study like man-car. A man can own a car, drive it by P/A, security driver may drive it – ties may be different. Even a tie itself has own view – business, corrupted, criminal, etc.
For instance, a tie between any two people may be found on the fifth or sixth level [14]. Recently, Moscow Institute of MIA of Russia which was established for the interests of law enforcers in fighting organized crime and was training competent specialists for them has had a special course Analytical Reconnaissance. That covers anything related to open information sources, economic, competitive or business reconnaissance and cyber safety. Practical studies included elective course practice in computer class and finding various ties.

There are some analytical experts trying to synthesize the view of scattered data (if some data is missing, there are some statistical methods for working with lost data), anticipating optimal solution. When we include a certain analyst in decision making, he/she should have good command of the professional area. But unfortunately it is not taught in law colleges.

When information model is mentioned, information data model is meant like statistical data on cybercrime. In reality we have something different - information system. The situation may be represented by a mathematical model as well. Crowd behavior in case of massive rivalry or public order offense is described by differential equations system.

The above systems (DBMS) were good for detecting chains of ties but did not solve the lot of analytical problems and could not give probable structure of crime group (including cybergroup), while structure is the most important feature of a criminal organization [13].

There is a methodology of preventive measures, like prevention of IT crimes via distribution of booklets K Department warns and notes on webpages. Those initiatives were met with interest by the web community. We are helping regular users to assess the risks in connection with IT and obtain a command of information security basics. Those simple yet efficient measures ensure great contribution in cyber safety, stated Moshkov, head of BSTM of MIA RF [12].

It should be noted that BSTM MIA of Russia did a number of successful actions to eliminate the activities of organized criminal groups engaged in bank deposit theft from individuals and entities. Besides, some persons were identified engaged in creation and use of malware for secret copying of access details in connection with bank deposits of individuals and entities. In total, K Department staff prevented theft of 1 billion rubles from individual deposits [12]. It should be noted that for a long time many scientists were offering to add a separate clause in the Russian criminal regulations providing for computer fraud liability which was however made in 2012 only.

Let us see some examples of successful use of other methods by law enforcers from other countries. There is a well-known example of using hacker methods by secret services.

FBI of the USA has been using for a couple of years at least one of the most sophisticated crack methods to get into users’ computers which try to hide their Internet surfing, as reported by Wired [15].
In particular, there is a method called drive-by download. It allows to install on user’s computer a malware code without any need to install anything manually. For infection it is enough to visit a web page with code placed by hackers (FBI in that case).

FBI used hacker methods to fight the criminals using Tor network. It does not allow to see which computer was used for Internet access and helps to conceal the location of web page’s server.

The technology which Tor is based on was developed by R&D laboratory of the US Navy in the 1990’s to protect governmental communication channels and later became available to public as a private life protection means. However the networks became popular among criminals engaged in child porn distribution, sale of drugs, arms, etc.

In 2011, FBI and the police of Netherlands began the operation called Torpedo, to catch the criminal engaged in child porn distribution via Tor network. The policemen regularly visited the criminal’s site and once found that he left his administrator account open for any visitor. Access to control panel allowed the policemen to find the IP address from which the criminal was surfing Internet and identify his personality. It was a US citizen Aaron McGrath [15].

But instead of arresting McGrath, FBI started watching him for a year. Upon court permission, secret services modified Tor code by placing ID tool for IP- and MAC-addresses of all visitors of the porn page. After that the authorities applied to Internet providers and obtained real addresses of users. In April, 2013, after 5 months since the code installation, law enforcers started coordinated arrests of offenders all over the country.

Christopher Soghoian, a technologist of American Civil Liberties Union (ACLU) opines that the use of hacker methods in catching criminals may be illegal. He points that there were no words like crack, malware or exploit in FBI’s requests for court orders which as he opines could attract judge’s attention.

It was previously known that FBI does not reject hacker methods in catching criminals. In 2007, FBI, using a spyware, was able to identify a young terrorist who informed of a bomb put in school.

In 2013, the authorities arrested owner of Freedom Hosting Company Eric Eoin Marques, accusing him of child porn distribution. As investigators found, Freedom Hosting servers were used for Tor sites. It became known upon placement of the code in the system to reveal the users of the anonymous network [15].

Tor cracking is also interesting for MIA of Russia. In July, the authority announced closed competition with prize fund i3.9 million worth. Those funds are promised to the person who will help to crack Tor technology and find the way to disclose information about its anonymous users.

We add that the government of the USA is the main source of funding support and development of Tor Project. In 2013, the governmental funding grew by 47%.
Is it justified to use their methods for counteractions? Many think that for war any means are good. However, the civilized world should not stay on one step with criminals. Even in fighting absolute evil like terrorism we should be discriminating the means. The most productive weapon in fighting cybercriminals is official [16].

DISCUSSION

Establishment of a uniform system in fighting virus software and interstate legal policy is one of the conditions for efficient counteraction in connection with that kind of crimes.

Technical and technological approach alone for information safety in informatization conditions including for prevention of cybercrimes is not a great success [17].

Cybercrime analysis predicts complication of fighting it as cybercrime methods are getting more sophisticated and hard to detect. That problem should be solved comprehensively.

Professionals specify the following elements of law enforcement in global information networks: study and assessment of situations in networks; optimal distribution of resources; cooperation; management, planning and control; coordination of law enforcers [4].

An important element of cybercrime fighting is prevention or precaution. Most foreign specialists state that to prevent a cybercrime is much simpler and easier than investigate it.

Commonly, three prevention measure groups are specified: legal, organizational and technical, criminalistic, totally making up an aggregate system of fighting that antisocial phenomenon [18].

As reasonably reported by European commissioner on implementation of new technologies N. Kroes at World Economic Forum in Davos, 2013, the most serious mistake is interpretation of cyber safety as a technical task only, as the main subject should be government. A strategic task is cyber safety improvement on all governmental levels [19].

Crime components of hi-tech fraudulence are contained in German regulations (paragraph 263a of the Criminal Code of the FRG), Japan (article 246-2 of the Criminal Code of Japan), Austria (article 148a of the Criminal Code of Austria), Poland (article 287 of the Criminal Code of Poland), France, Canada (article 2061e of the Criminal Code of Canada) etc.

Thus, criminal regulations of a number of countries provide for liability for fraudulence in hi-tech. Those crimes, although not related to cybercrime, are committed using computers.

What can the regulations of RK move against the above threats? Only recently, there was just one article 227 of the Criminal Code of RK [20], containing two simple crime components and two aggravations, and now there is a whole chapter (Chapter 7 of
Special part of the Criminal Code of RK, 2014 [21], containing 9 articles (205-213), each of them contains besides simple crime components one or two aggravations. Besides, two aggravations were included in the chapter on crimes against property providing for liability for acts using information systems and networks (Theft, article 188 of Criminal Code of RK, part 2, clause 4, via illegal access to information system or changing information transmitted via information communication network, and Fraudulence, article 190 of Criminal Code of RK, part 2, clause 4, by fraudulent conduct or abuse of user’s confidence of information system user). It is seen that in that case the regulator made liability for cybercrime more detailed which quite complies with the contemporary trends of criminal regulations. The following should be noted herewith. Criminals using computer technologies are rather sophisticated and in future, some theft schemes may be developed not including access or change of information systems or networks. Therefore we opine that the RK legislators should borrow from their Russian colleagues the legal notion of computer technologies applicable in construction of criminal components under article 159.6 of the Criminal Code of the RF [22], Fraudulence using computer technologies.

Currently, not only cybercrime regulations are improved but automatic cybercrime detecting software is developed. New Jersey government (the USA) sponsored a new anti-hacker project and funded some USD 2.6 million.

There are some more examples of serious cybercrime fighting. Since January, 2013 European cybercrime center commenced working (EC-3, hereinafter referred to as Center), a structural division of Europol. That entity should become the main instrument of cybercrime fighting in the EU. EC-3 will be engaged in creation of operational and analytical facilities to ensure fast response to cybercrime and organization of cooperation of official authorities of the EU and member countries with international partners.

Center’s mandate includes fighting the following kinds of cybercrime:

Crimes committed by organized criminal groups to receive illegal incomes like credit card or banking fraudulence;

Crimes with material damage to victims like debauchery of youth and unlawful transaction with minors;

Crimes bringing damage to critically important infrastructure and information systems in the EU.

Besides, Center will be engaged in collection and processing of data, informational, technical and criminalistics support to relevant divisions of law enforcers of the EU member countries, coordination of joint investigations, training and preparing specialists (cooperating with CEPOL). Center will cooperate in doing the required research and R&D, assess and analyze the existing and potential threats and issue timely warnings. Center will also assist judges and public prosecutors [5].

Time goes on, and in XXI century everything should develop in compliance with Charter on global information society (Okinawa) while the present state of information and analysis work in law enforcement offices, security divisions of
governmental and commercial organizations in Republic of Kazakhstan is virtually on the same level.

CONCLUSION

The paper covers on advanced methods ensuring efficient cybercrime fighting, namely timely preventing offences, detecting and investigating crimes committed, punishing criminals fairly. The research specifies the four methods the use of which ensures great improvement of cybercrime fighting system:

Technical methods for protection of software and equipment applied by computer safety specialists in all economic spheres using computers and information software;

Technical and criminalistics methods applied by IT specialists of law enforcers in crime investigation and searching criminals;

Organizational methods providing for establishment of special divisions and arrangement of inter-authority cooperation in cybercrime fighting;

Legal methods with the main method of criminalization of acts not only committed but probable in future.

The above methods are used by law enforcers and security specialists. Meantime, the opportunities of a great number of private users of information technologies so called the Internet community. A special method employing civil activeness of the Internet community is the information exchange method implemented today. For instance, Anti-Phishing Working Group announced public software for cybercrime alert aimed to speed up the collecting of data on cybercrime and its communication to information security companies, investigators and antivirus companies. The software called APWG Accredited Reporter Data Submission Program allows to obtain information about cybercrime first hand, to maximize inter-sector data exchange about the events required for prevention, record and investigation of cybercrime attacks on the first defense line [23].

In cybercrime fighting, it is impossible to use some methods and refuse from or ignore others. Only comprehensive approach as a general method will ensure successful solution of cybercrime fighting tasks and its decrease. Surely, a number of contemporary and efficient methods are not covered in this paper which enforces the authors to deepen and widen the research of cybercrime fighting methods in future works.
REFERENCES

15. To fight users of Tor (2015) FBI infects their computers.