ISSN 2278-3091
Volume 8, No.5, September - October 2019
International Journal of Advanced Trends in Computer Science and Engineering
Available Online at http://www.warse.org/IJATCSE/static/pdf/file/ijatcse90852019.pdf
https://doi.org/10.30534/ijatcse/2019/90852019

Social Causation of Criminalization of Cyber Crime Committed with the Use of Information Technology

Abdulgaziev R.Z.[1], Alsultanov M.R.[2], Mamichev V.N.[3], Sarukhanyan A.R.[4], Sostin D.I.[5], Sukhorukova A.N.[6]
[1] Ph.D. in Law, Associate Professor of the Department of Criminal Law and Procedure of North Caucasus Federal University; Department of Criminal Law Disciplines of Stavropol branch "MIREA-Russian Technological University", Russia, abdulgazievrz@gmail.com
[2] Senior Lecturer of the Department of Criminal Law Disciplines of Stavropol branch "MIREA-Russian Technological University", Russia, alsultanovmr@gmail.com
[3] Ph.D. in Law, Associate Professor of the Department of Criminal Law Disciplines of Stavropol branch "MIREA-Russian Technological University", Russia, mamichev-vn@gmail.com
[4] Ph.D. in Law, Associate Professor of the Department of Criminal Law Disciplines of Stavropol branch "MIREA-Russian Technological University", Russia, sarukhanyan-ar@gmail.com
[5] Ph.D. of History, Associate Professor of the Department of Criminal Law Disciplines of Stavropol branch "MIREA-Russian Technological University", Russia, sostindi@gmail.com
[6] Senior Lecturer of the Department of Criminal Law Disciplines of Stavropol branch "MIREA-Russian Technological University", Russia, sukhorukovaan@gmail.com

ABSTRACT

The work studies several specific case issues of crimes committed using IT. Cybercrime is a new line of criminal activity of Internet cybercriminals, which law enforcement agencies all over the world are fighting with varying degrees of success. Cybercrime has become so widespread that the issue was addressed by the Council of Europe [8].
The work analyzes the social causation of the criminalization of computer crimes committed using IT.
The general conclusion drawn is that Russia has been discussing the issue of improving the legislation on combating crimes threatening the security of computer information for a long time. The information security doctrine adopted back in 2000 pragmatically established the necessity to protect the rights and legitimate interests of citizens in the country's infosphere. The legislative base of the research included: the Russian Constitution [2], Criminal Code [3], Federal Laws "On Amendments to the Criminal Code of the Russian Federation and certain legislation of the Russian Federation" [4], "On Information, Information Technologies and the Information Security" [5], "On Communication" [6], "On Security" [7].The second decade of the 21st century was marked by the introduction of significant changes to Chapter 28 of the Criminal Code of the Russian Federation [3]. The legislator abandoned the term "electronic computing machine" and focused on the concept of "computer information", which is the more comprehensive taking into account the specifics of the criminal law terminology used for constructing the provisions of the Criminal Code of the Russian Federation. The very existence of articles establishing liability for crimes related to computer information is an important requirement, which is imposed by the global use of computer and telecommunication technologies in all aspects of the society's life.

Key words: cybercrime, computer crimes, Information technologies, computers, penal sanctions

1. INTRODUCTION

In the early 2000s, the Cybercrime Convention [1] was adopted in Budapest. Oddly enough, with the World Wide Web covering almost one hundred percent of the globe, to date, the Convention has been ratified only by 25 countries.
The current stage of society development is characterized by a strategic target of creating states governed by the rule of law. Many countries are experiencing radical socio-economic reforms, the democratization of all aspects of public life is progressing, which is impossible without strengthening the rule of law and order, ensuring reliable protection of the citizens' constitutional rights and freedoms [12-17].
Still, in recent years, there has been a drastic development in the criminal situation, which is currently viewed as acute and fraught with problems. A surge of criminal professionalism has been observed, and the venturesome schemes and expertly committed crimes are multiplying. With the general reduction in thefts, brigandry and robberies, the number of thefts of large sums from banks and other financial institutions, cash desks, enterprises and organizations by means of using computers and IT is increasing.
At the same time, the deployment of the scientific and technological revolution outlines not only the fundamental progressive changes in the development of a country but also determines the uprise of negative trends in the development of the criminal world, and leads to the emergence of new forms and types of criminal offense, i.a. with the use of computer and information technologies. The most alarming here is the prevalence of this type of

criminal offense associated with the use of computer equipment and information processing technologies.

Cybercrimes cause enormous damage to public safety, which predetermined the development of the legislation of many countries taking urgent responsive legal action to counter this new type of crime.

The compelling need for a comprehensive study of these problems is predetermined both by the requirement for investigative practice and the task of further improvement of the criminological theory and strengthening its influence on the efficiency of the cybercrime control.

The institution of criminal penalty as a whole has traditionally been recognized a most important means of implementing criminal law policy [9, 10, 11].

2. MATERIALS AND METHODS OF RESEARCH

The aim of the study is theoretical analysis of the criminal law and criminological characteristics of crimes related to computer information and the development of action to prevent such.

The object of the study is action to combat crimes related to computer information and committed using information technologies.

The subject of the study is public relations developing in the course of indictment and prosecution for cybercrimes, along with legal provisions establishing liability for such offense, scientific and academic works in the part covering information technology.

3. RESEARCH METHODOLOGY

The methodological basis of the study consists of such general scientific methods as analysis and synthesis, deduction and induction, and specific scientific methods: historical-legal, formal-logical, comparative-legal, etc.

4. RESULTS AND DISCUSSION

As a social phenomenon, computer crimes appeared in the late 1960s - early 1970s with the appearance of computer technology. The emergence of a new type of crime using computer technology could not go unnoticed by the state, nor by the criminal law and criminological researchers.

Despite the increased interest of law enforcement authorities and scientists to the new problem, only in 1983, through joint efforts of experts from several countries, computer crimes were first defined as any illegal or unauthorized action involving automatic processing or transmission of data (information).

Thorough research of the social phenomenon of crime using automated databases allowed to categorize computer crimes as: crime against personal rights and private secrets, financial crimes and cybercrimes against the interests of public authorities.

In our opinion, the economic interests of a country and any modern society are the most important aspects of government. Therefore, cybercrimes aimed at violating economic rights are justly considered the most dangerous type of crime committed using computer technology.

The studied group of computer crimes includes computer economic espionage, theft of information products, paralyzing the work of government authorities and significant social institutions, spear phishing and fraud, illegal possession of information for with unauthorized entry into information databases, etc.

Economic cybercrimes are usually committed with lucrative motives. Another characteristic of this category of computer crime is that such are often committed involving the employees of the aggrieved institution.

When first faced with computer crime, the criminal justice authorities tried fighting it using the traditional legal provisions on liability for theft, fraud, breach of trust, but this approach was inadequate, since many cybercrimes are not covered by traditional offense provisions. No signs of destruction or damage to property are visible, for example, in the case of the destruction of a data element of a computer system without damage to its physical element, although such actions can cause significant property damage.

The inconsistency between the criminal reality and criminal law required the new legislation, which developed in two directions:

- broader interpretation of conventional law;
- creation of special provisions on computer crimes.

In Russia, the principal document for determining the information security strategy is the Information Security Doctrine, which is a compilation of official views on the goals, objectives, principles and main trends of ensuring information security in the Russian Federation.

According to their general direction, information security threats in the Russian Federation are divided into the following types:

- threats to the constitutional rights and freedoms of man and citizen in the aspect of spiritual life and information activity, individual, group and public consciousness, spiritual revival of Russia;
- threats to the information support of the state policy of the Russian Federation;
- threats to the development of Russian information industry, including the means of informatization, telecommunications and communications; to the support of the domestic market for its products and to bringing such products to the world market; to ensuring the collection, preservation and efficient use of domestic information resources;
- threats to the security of information and telecommunication facilities and systems, both those deployed and those being created in Russia.

A society united by a global information network has become the reality of the modern world. This causes the acuteness of several problems:

- impact of the Internet on politics;
- places and roles of governments in the information network;
- destruction of the boundaries of privacy;
- formation of power and governance on the Internet.

These problems, emerging with new technical capabilities, significantly affect the security of the vital interests of citizens, states and societies, namely, their national security.

The Internet affects both global and regional politics, including the politics of individual countries.

If the efficiency of state policy cannot be guaranteed due to the transnational penetration of the Internet, it will result in violations of the law.

The Internet is a technical tool used by highly developed countries and their neighboring states for their own purposes.

It is undeniable that that still no effective protection against the use of the Internet for antisocial purposes has been found. Here, a distinction should be made between the mere personal area protected by the rule of law and the personal data available on the network anonymously.

An important task for ensuring the informational component of the national security of Russia, or any other countries, is preventing the threat of the disintegration of society into disparate, competing and situationally joint "network societies".

Computer networks and the Internet play a key role in managing the infrastructure of industrial countries. This implies the growing threat of crime pertaining to computer information. For example, a computer virus called "I love you", launched into the Internet in Asia, spread at an incredible speed around the planet, disrupting the work of government agencies, parliaments and corporations in many countries. It destroyed the programs in about 45 million computer networks. In the first five days since its launch, it inflicted material damage (Table 1) in the amount of $6.7 billion, and it was just one of such virus attacks.

Table 1: Virus and Damage

No.	Year	Virus	Damage
1.	1986	Brain	Infected over 18000 computers
2.	1988	Jerusalem	Formatted the hard drive and deleted all information from the computer, the exact number of victims is not known.
3.	1988	Morris worm	Direct indirect loss from the virus totaled about $ 100 million
4.	1992	Michelangelo	Infected over 10000 computers
5.	1999	Melissa	Total damage was later estimated at $ 100 million.
6.	2008	Conficker	While active, infected 12 million computers worldwide and was recognized as one of the most dangerous in history.
7.	2016	Petya	The virus encrypted the contents of the victim's computer and demanded a ransom of about 2 bitcoins (almost $1 million at that time)
8.	2017	WannaCry	Total damage estimated at $ 1 billion.

From the view point of law enforcement agencies, the greatest threat lies not in the vulnerability of the Network, but in the opportunities of global telecommunications it provides for the criminal world, which are extremely difficult to track.

Hence, crime involving computer information is injurious to the public and poses a real threat to both the entire world community and our country.

Along with the above factors affecting the information security of a country, there are organizational and technical factors of no less significance in Russia. Such include an underdeveloped regulatory framework governing information relations, i.a. information security; weak state regulation of the functioning and development processes of the market for informatization tools, information products and services in Russia; widespread use of imported hardware and software for data storage, processing and transmission, unprotected from information leakage, for public administration and financial sector; surge in the volume of information transmitted over open communication channels; increased number of cybercrimes.

The absence of borders in global information networks requires a certain sequence of actions to combat crime in such networks, special coordination of the efforts of the countries involved. This would move the legal regulation of fighting crime in the area of computer information from the competence of national legislators and raise it to the international, supranational level, therefore eliminating the inconsistencies in the actions of such states.

In this regard, the array of various data containing detailed information about the user, finances, physical objects turns into a demanded product. The appearance of such a product in a market which is not regulated by law may have negative consequences, including terrorism.

Given the triumphant expansion of the Internet, technology leaves the zone of democratic political influence. The dynamics of the Internet is too high to be regulated by ordinary supranational organizations, for example, the UN, which is to coordinate long-term interstate negotiation processes.

National governments and traditional international organizations are unable to govern the Internet. There is a problem of determining the scope of such regulation. Due to its technical infrastructure, the Internet has become a sort of catalyst for social, political and economic changes, which necessitates the creation of new forms of regulation.

The Internet, which has no official center, poses the threat of usurping world information resources, establishing control over the mass public consciousness.

The fragmented efforts of individual countries must be combined. This approach, given the inevitability of global coverage by computer networks, is what will reduce, and ideally, stop the "information wars". However, in the foreseeable future we can only expect their escalation.

Most European countries have chosen a second path: developing special laws on computer crimes. Russia has done the same. The legislator included Chapter 28 "Crimes pertaining to computer information" in the Criminal Code of the Russian Federation, containing three articles: Art. 272 "Unlawful access to computer information"; Art. 273 "Creation, use and distribution of malicious computer programs"; Art. 274 "Violation of the rules for the operation of means of storage, processing or transmission of computer information and information and telecommunication networks"; 274.1 "Undue influence on the critical information infrastructure of the Russian Federation". The statistics on the increased number of cybercrimes over the validity period of the applicable provisions of the Criminal Code is provided in Table 2:

Table 2 : Criminal Code

	2011	2012	2013	2014	2015	2016	2017	2018
Fraud using electronic means of payment, Art. 159.3 of the RF Criminal Code	–	85	1297	925	565	266	228	741
Crimes pertaining to computer information, Ch. 28 of the RF Criminal Code	2698	2820	2563	1739	2382	1748	1883	1233
Unlawful access to computer information, Art. 272 of the RF Criminal Code	2005	1930	1799	1151	1396	994	1079	827
Creation, use and distribution of malicious computer programs, Art. 273 of the RF Criminal Code	693	889	764	585	974	751	802	406
Violation of the rules for the operation of means of storage, processing or transmission of computer information and information and telecommunication networks, Art. 274 of the RF Criminal Code	0	1	0	3	12	3	2	0

In December 2012, the "special" elements of fraud were introduced into the Criminal Code of the Russian Federation, based on Federal Law No. 207-FZ dated November 29, 2012 "Amendments to the Criminal Code of the Russian Federation and Certain Legislation of the Russian Federation" (Article 159.6 Criminal Code of the Russian Federation "Computer Information Fraud").

The offense described in these articles are actions, which are not the mere use of computer technology as a means of committing offense. These are socially dangerous acts targeting the security of information and information processing systems using electronic computer technology. At the same time, most of such crimes are designed as material crime, they imply socially dangerous consequences in the form of damage to users of computer equipment, which generally consists in disrupting the normal functioning of computers or computer networks.

In our opinion, the economic interests of the State and any modern society are a most important government function. Therefore, cybercrime aimed at violating the economic rights are justly considered the most dangerous type of offense committed using computer technology.

The studied group of computer crimes includes computer economic espionage, theft of information products, paralyzing the work of government authorities and significant social institutions, spear phishing and fraud, illegal possession of information for with unauthorized entry into information databases, etc.

Economic cybercrimes are usually committed with lucrative motives. Another characteristic of this category of computer crime is that such are often committed involving the employees of the aggrieved institution.

The category of cybercrimes aimed at violating private rights and privacy secrets is usually committed by entering inaccurate or distorted data about users, or using the correct user data and committing unlawful acts on their behalf, as well as other abuse of the computer information obtained illegally.

5. CONCLUSION

Russia has been discussing the issue of improving the legislation on combating crimes threatening the security of computer information for a long time. The information security doctrine adopted back in 2000 pragmatically established the necessity to protect the rights and legitimate interests of citizens in the country's infosphere. One of the methods for ensuring information protection from cyber threats provided for by the indicated document is the creation and adoption of regulatory legislation establishing liability for unauthorized access to information, illegal copying, distortion and unauthorized use, intentional distribution of false information, illegal disclosure of confidential information, use of official information or information containing trade secrets for criminal and mercenary purposes. As of today, statistics show that the rate of unsolved computer crimes committed using information technology is about 30% (Table 3).

Table 3: Unsolved Cases

2017	
Investigated (closed) cases	903
Unsolved cases	790
2018	
Investigated (closed) cases	726
Unsolved cases	1031

The criminological analysis of cybercrimes committed using information technologies demonstrated that the most efficient method of preventing offense using computer information and information telecommunications is the comprehensive application of various measures to prevent cybercrime: organizational, hardware and software. For example, according to experts, to reduce the risk of viral attacks on data storage media, the following comprehensive organizational and technical measures should be taken, they can be reduced or expanded in content based on the specific situation:

1. Timely notification of all officials responsible for protecting computer information about the danger and possible damage in case of viral aggression.
2. Prohibiting establishment of personal contacts: employees should only use official means of information distribution.
3. It should be noted that today computer games are a source of greater danger to the security of computer systems. If this prohibition cannot be guaranteed, a special game site or a common game file that constantly monitored by employees can be created.
4. If third-party computer networks are to be used for the work process, special bench equipment with mandatory isolation of other equipment should be provided (workstation of a local or peripheral network). All files coming from an external computer network must be checked.
5. It is imperative to periodically check the number of files, identify them from the reference point, sometimes store them in an encrypted form or archive them with read-only option.

REFERENCES

1. **The Convention on Cybercrime (ETS N 185) (signed in Budapest on November 23, 2001) (amended on January 28, 2003) (translation into Russian provided by the State Duma of the Federal Assembly of the Russian Federation)** // *Legal reference system "Consultant Plus"*.
2. **Constitution of the Russian Federation (amended by the Russian Laws on amendments to the Constitution of the Russian Federation dated December 30, 2008 No. 6-FKZ, dated December 30, 2008 No. 7-FKZ, dated February 5, 2014 No. 2-FKZ, dated July 21, 2014 No. 11-FKZ)** // *Legal reference system "Consultant Plus"*.
3. **Criminal Code of the Russian Federation No. 63-FZ dated June 13, 1996 (as amended on April 23, 2018 and on April 25, 2018)** // *Legal reference system "Consultant Plus"*.
4. **Federal Law No. 207-FZ dated November 29, 2012 "Amendments to the Criminal Code of the Russian Federation and Certain Legislation of the Russian Federation"** // *Legal reference system "Consultant Plus"*.
5. **Federal Law No. 149-FZ dated July 27, 2006 (as amended on April 23, 2018) "On Information, Information Technologies and Information Protection"** // *Legal reference system "Consultant Plus"*.
6. **Federal Law No. 126-FZ dated July 07, 2003 "On Communication" (as amended and supplemented, in effect since June 01, 2018)** // *Legal reference system "Consultant Plus"*.
7. **Federal Law No. 196-FZ dated December 10, 1995 (as amended on July 26, 2017) "On Security"** // *Legal reference system "Consultant Plus"*.
8. **Statistics of the Judicial Department of the Supreme Court of the Russian Federation, Form 10**-3 // *Judicial Department of the Supreme Court of the Russian Federation.* Access address: http: // www. cdep.ru
9. Kibalnik A.G. **Defenses to Criminal Liability in Modern International Criminal Law** // *Criminology Journal of Baikal National University of Economics and Law*, 2013, vol. 7, no. 4, pp. 124–128.
10. Kibalnik A.G. **International Criminal Law Problems in International Thesis Researches** // *Criminology Journal of Baikal National University of Economics and Law*, 2014, vol. 8, no. 2, pp. 162–176.
11. Kibalnik A.G., Volosyuk P.V. **Russian Thesis Researches of Problems of International Criminal Law and International Criminal Justice (2010–2017)** // *Legal Science and Practice: Journal of Nizhny Novgorod Academy of the Ministry of Internal Affairs of Russia*, 2017, no. 3, pp. 72–83.
12. Gamulinskaya N.V. **Rights of employees in the event of the enterprise's bankruptcy** // *Modern Scientist.* 2018. №1. P. 105 – 108.
13. Nagoeva M.A. **Systematic in the criminal legislation of the russian federation** // *Modern Scientist.* 2018. №1. P. 113 – 116.
https://doi.org/10.17816/byusu2017131-2113-116
14. Bak E.V., Kim A.V., Gordey V.A. **On the application of information and communication technologies in the mia of russia: perspectives of improvement** // *Modern Scientist.* 2018. №2. P. 35 – 38.
15. Melnikov V.Yu., Dolgopolov K.A., Abdullayev K.F. **A full and thorough investigation of crimes as a necessary element of law enforcement activities of the state** // *Modern Scientist.* 2019. №2. P. 275 – 280.
16. S.V.R.K.Rao, M.Saritha Devi, A.R.Kishore and Praveen Kumar **Wireless sensor Network based Industrial Automation using Internet of Things (IoT)**. *International Journal of Advanced Trends in Computer Science and Engineering*. 2018. Volume 7 No. 6 (2018). Pages 82-86
https://doi.org/10.30534/ijatcse/2018/01762018
17. Ramakrishna Rath, R.Tamilkodi, K V Mishra and K Jose Cherian **Utilizing Contemporary Benchmark Protocol for Sharing Mobile Ad-hoc Network Environment.** *International Journal of Advanced Trends in Computer Science and Engineering*. 2018. Volume 7 No. 6 (2018). Pages 96-98
https://doi.org/10.30534/ijatcse/2018/04762018