European Proceedings of
Social and Behavioural Sciences
EpSBS

www.europeanproceedings.com
e-ISSN: 2357-1330

DOI: 10.15405/epsbs.2021.06.03.77

AMURCON 2020
International Scientific Conference

THE PHENOMENON OF CYBER CRIME IN THE FOCUS OF CONCEPTUAL LEGAL ANALYSIS

Dmitriy V. Lobach (a)*, Sergey S. Shestopal (b), Nina L. Smirnova (c)
*Corresponding author

(a) Vladivostok State University of Economics and Service, 41 Gogolya St., Vladivostok, Russia, dimaved85@mail.ru
(b) Vladivostok State University of Economics and Service, 41 Gogolya St., Vladivostok, Russia,ss.shestopal@ya.ru
(c) Far Eastern Federal University, FEFU Campus, 10 Ajax Bay, Russky Island, Vladivostok, Russia, ta_kamen@inbox.ru

Abstract

The paper explores the phenomenon of cybercrime in the modern conditions of digital transformation of social relations. Based on the analysis of five regional conventions (the Council of Europe Convention “On Crime in the Field of Computer Information”, 2001; African Union Convention “On Cybersecurity and Personal Data Protection”, 2014; State Cooperation Agreement- the Members of the Commonwealth of Independent States in the fight against crimes in the field of computer information, 2001; League of Arab States Convention "On the fight against crimes in the field of information technology", 2010; Agreement between Governments of States- members of the Shanghai Cooperation Organization on cooperation in the field of ensuring international information security, 2009.) and generalization of theoretical ideas about this phenomenon, there is a conclusion that the concept of "cybercrime" is relevant, since in international practice of countering socially dangerous acts committed through the use of information and communication technologies, there is no unified and a comprehensive list of cybercrimes. The article provides a conceptual and legal definition of cybercrime, by which it is proposed to understand a historically changeable social and criminal-legal negative phenomenon, representing the entire set of crimes committed through the use of information and communication technologies that infringing on the security of information systems and threatening confidentiality, integrity and availability of computer data and systems, public health and public morality, as well as public relations emerging in connection with the owner’s powers and in the field of the implementation of copyright and related rights.

Keywords: Social transformation of social relations, digitalization, cybercrime, cyberthreats

https://doi.org/10.15405/epsbs.2021.06.03.77
Corresponding Author: Dmitriy V. Lobach
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

1. Introduction

In the context of the intensive development of cross-cutting (disruptive) information and communication technologies (hereinafter referred to ICT) and their broad integration in various areas of society, a qualitative change in social relations is taking place, which is accompanied by the emergence of new and emerging threats to life, health, subjective rights and freedoms, honor and dignity of a person, property, public security and order, public interests of society and the government (Kenney, 2015; Lawson, 2013), which also actualizes the problem of erosion of sovereign borders in the context of ensuring national security (Yakoviyk et al., 2018). One of these threats, actualized in the conditions of the fourth industrial revolution, is cybercrime. The high social danger of this threat is evidenced by the following representative picture of cybercrime of 2019, based on the basis of open information sources.

For the period from 2009 to 2018 there has been an exponential increase in the number of malware infections. So, if in 2009 there were registered 12.4 million incidents, then 29.97 million incidents already in 2010, in 2011 - 48.17 million incidents, in 2012 - 82.62 million incidents, in 2013 - 165.81 million, in 2014 - 308.96 million, in 2015 - 452.93 million, in 2016 - 580.40 million, in 2017 - 702.06 million, and there were registered 812.67 million in 2018 corresponding infection facts (The Ultimate List Of Cyber Security Statistics For 2019…, 2020). In general, the growth rate for the indicated ten-year period was about 6553%.

2. Problem Statement

The current situation in the field of cybersecurity, characterized by quantitative (in terms of the increasing the total number of attacks) (Internet crime report, 2019) and qualitative factors (in terms of evolving hacker tools) threatening the security of information systems, suggests the formulation of a task associated with the need to develop an acceptable definition of cybercrime that would adequately meet the modern realities of the digital transformation of social relations. The solution to this problem is necessary due to the fact that the conceptual characteristics of this phenomenon will contribute to the correct identification and assessment of the scale of the threat (in a relevant focus), which is carried by this phenomenon, and also the ways and tendencies of its probable development (if the trends and patterns of scientific technical progress are taken into account). Besides, the concept of "cybercrime" should be unambiguously defined as an object of promising political and legal impact at the level of interstate cooperation.

3. Research Questions

Raising the question regarding the concept of "cybercrime" assumes highlighting two points that are connected, firstly, with the international legal regulation of liability for socially dangerous acts committed in the digital environment of the virtual space (in cyberspace), and, secondly, with theoretical perception this phenomenon in the science of the criminological cycle.

The international legal regulation of responsibility for socially dangerous acts committed using information and communication technologies (socially dangerous acts committed in the digital environment

https://doi.org/10.15405/epsbs.2021.06.03.77
Corresponding Author: Dmitriy V. Lobach
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

of the virtual space; cybercrimes; computer crimes; information crimes), in the modern conditions of the development of international law enforcement, is envisaged in five regional conventions acts: the Council of Europe Convention "On Crime in the Field of Computer Information" (ETS N 185), 2001 (hereinafter referred to the Council of Europe Convention); The Agreement on Cooperation of the Member States of the Commonwealth of Independent States in the Fight against Crimes in the Area of Computer Information, 2001 (hereinafter referred to the CIS Agreement); The Arab League Convention on “Combating Crimes in the Field of Information Technology”, 2010 (hereinafter referred to the Arab League Convention); The African Union Convention on “Cybersecurity and Personal Data Protection”, 2014 (hereinafter referred to the African Union Convention); Agreement between the Governments of the Shanghai Cooperation Organization member states on cooperation in the field of ensuring international information security, 2009 (hereinafter referred to the SCO Agreement).

The analysis of these documents allows to state the normative and legal dynamics of the criminalization of acts as cybercrimes, since these conventions reflect the list of criminal acts in different ways. For example, Council of Europe Convention from 2001 contains 7 elements of such crimes, CIS Agreement from 2001 includes 4 corpus delicti of computer crimes, League of Arab States Convention from 2010 includes 13 offences, and The African Union Convention from 2014 classifies 4 groups of crimes to cybercrimes, covering 24 criminal acts.

In the science of the criminological cycle, a conceptual and legal uncertainty of this phenomenon is observed, owing to the relevant approaches to the content side of this phenomenon. Despite the fact that most researchers consider cybercrime in the context of the use of information technology, there is still no definitive definition of this phenomenon. This situation is explained, firstly, by the fact that in the modern conditions of the digital transformation of social relations there is still no unified understanding of what information technology is, and, secondly, in the academic field, controversy continues regarding the list of criminal acts that make up the concept “cybercrime ". In the conceptual and legal aspect, the situation is more complicated by the fact that in the scientific environment there is a mixture of dissimilar concepts to the level of uniform understanding or complete identification. For example, cybercrime is often revealed through concepts such as computer crimes, crimes in the information environment, crimes in the virtual space, crimes in the digital environment (Agapov, 2014; McQuade, 2006; Nomokonov & Tropina, 2012; Okutan & Çebi, 2019).

4. Purpose of the Study

The purpose of the study is to analyse the regional convention mechanism governing countering socially dangerous acts committed through the use of information and communication technologies, and also to the study of theoretical insights regarding the concept of "cybercrime", with the subsequent proposal of a conceptual and legal definition of this phenomenon in the capacity as actual threat in modern digital transformation conditions of social relations.

https://doi.org/10.15405/epsbs.2021.06.03.77
Corresponding Author: Dmitriy V. Lobach
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

5. Research Methods

In this article there are used methods such as analysis (with respect to a differentiated consideration of the phenomenon of cybercrime through the provisions of individual regional documents), synthesis (the method is reflected in the generation of a general definition of cybercrime), deduction (the method is used in terms of specifying the types of cybercrime), and also a formal legal method that allowed to analyze the normative provisions of five regional documents which are regulating the relations in the field of cybersecurity, a statistical method that allowed to describe in a representative form the dynamics of the spread of criminal threats in cyberspace, and also a method of continuous analysis, the use of which allowed to conduct an overview comparison of theoretical positions regarding the concept of "cybercrime".

6. Findings

A comparative legal analysis of the above regional conventions allows us to come to the conclusion about different approaches to the legal regulation of liability for acts committed through the use of information and communication technologies. On the one hand, there are general aspects of the political and legal definition of acts as computer crimes, which include: 1) acts against confidentiality, integrity and availability of computer data and systems; 2) actions performed through the use of computers to extract personal or financial benefits, as well as causing harm; 3) acts related to computer content.

On the other hand, there are different approaches to the definition of crimes related to computer content (affiliated with other crimes). For instance, in art. 3 of the African Union Convention, incitement to hatred through the use of computer technology and the production, distribution or possession of child pornography are related to these types of crimes. The League of Arab States Convention on Cybercrimes related to computer content includes the distribution of pornographic or offensive materials, as well as information related to gambling, sexual exploitation, the spread of ideas of terrorism or incitement to ethnic or religious hatred.

On the opposite, the Council of Europe Convention refers to crimes related to computer content offenses only related to child pornography (Art. 9), and the CIS Agreement does not categorize such acts at all as computer crimes at all.

Regional experience in countering computer crimes related to terrorist activities worthy to note. So, Art. 15 of the Arab League Convention discloses the legal content of terrorism-related crimes connected with terrorism committed through information technology. Such crimes include: dissemination and propaganda of ideas and principles of terrorist groups; financing and preparation of terrorist operations, as well as providing communication between terrorist organizations; the proliferation of methods of making explosives for use in terrorist operations; spreading ideas of religious enmity. A mandatory contextual feature is the condition for the commission of these acts, which is expressed in the use of information technologies.

The African Union Convention there is special rule regulating the adaptive connection of computer crimes and certain terrorist crimes. An illustrative example in this regard is the rule of clause "b" of Part 1 of Art. 30 of this document, where it is determined that the participating States must take the necessary regulatory and legal measures that enshrine as an aggravating circumstance the use of information and

https://doi.org/10.15405/epsbs.2021.06.03.77
Corresponding Author: Dmitriy V. Lobach
Selection and peer-review under responsibility of the Organizing Committee of the conference
eISSN: 2357-1330

communication technologies to commit theft, fraud, concealment of stolen property, breach of trust, extortion, money laundering and terrorism.

A fundamentally different approach to the criminalization of socially dangerous acts that are committed through the use of information and communication technologies (cybercrimes) is presented in the SCO Agreement, 2009. In this document there is a delineates information crime from other threats to information security (information war; information terrorism; use of the dominant position in the information space, etc.). There is a notable skilful delimitation of information crime from information terrorism, which de-facto correlate with each other as a general (generic) and private (specific) concept. Within the meaning of clause 3 of Appendix 2 to this document, information criminality is defined as the use of information resources and (or) the impact on them in the information space for illegal purposes. From the standpoint of actus reus, such acts can be represented by penetration into information systems to violate the integrity, availability and confidentiality of information; deliberate production and distribution of computer viruses and other malicious programs; implementation of the DOS attacks (denial of service) and other negative impacts; causing damage to information resources; violation of the legal rights and freedoms of citizens in the information area, including intellectual property rights and privacy; using information resources and methods to commit fraud, theft, extortion, smuggling, illegal drug trade, distribution of child pornography. In contrast to the regional conventions discussed above, the 2009 SCO Agreement leaves open the list of criminal acts constituting information crime. At the same time, the document provides a legal definition of information terrorism, which should be understood as the use of information resources and (or) the impact on them in the information space for terrorist purposes. It seems that from the standpoint of a systemic interpretation and the general trend of combating crime in the practice of international relations, information terrorism cannot be considered without regard to the broader concept of information crime.

In turn, the theory of the criminological cycle also lacks a common understanding of cybercrime. Analysis of various theoretical approaches to understanding this phenomenon (Agapov, 2014; Furnell et al., 2015; McQuade, 2006; Nomokonov & Tropina, 2012; Wall, 2007) allows to reveal only general contours that are expressed in the functional connection of the act and informational communication technologies. In this aspect, cybercrime covers not only computer crimes (illegal access to computer information, creation and distribution of malware, etc.), but also other acts committed through the use of hardware, networks and communication services. Meanwhile, there is the absence of a clear, unambiguous list of acts covered by the general concept of "cybercrime" creates place for wide discretion and generates a natural uncertainty in the likely identification of an act as a cybercrime. Indeed, the definition of cybercrime across the entire spectrum of criminal acts in the field of information technology does not stand up to criticism, since almost every criminal offense committed through the use of a computer can be extrapolated to the level of cybercrime (for example, forging a document through the use of special programs installed on a personal computer, or driving to suicide in information and telecommunication networks).

In the context of various definitions of the phenomenon under consideration and taking into account the provisions of the above conventions, cybercrime can be defined as a historically changeable social and criminal law negative phenomenon, representing the entire set of crimes in the field of information and

communication technologies that branches on the security of information systems and threaten confidentiality, integrity and the availability of computer data and systems, public health and public morality, and also to the public relations arising in connection with the exercise of the powers of the owner and in the implementation of copyright and related rights committed in the information and communication space in a certain period of time.

7. Conclusion

Concluding the analysis of regional documents that regulate the criminalization of socially dangerous acts committed through information and communication technologies, as well as individual theoretical approaches to the phenomenon of cybercrime, the following conclusions can be drawn.

Firstly, the presence of regional documents regulating relations in the field of information security through the criminalization of relevant acts demonstrates the tendency of interstate cooperation in the direction of countering criminal cyber threats. The development of a regional conventional mechanism for countering these threats shows the political and legal recognition of cybercrime as a destructive phenomenon of social reality, which is a natural consequence of the digital transformation of social relations.

Secondly, the generalization of theoretical positions regarding the conceptual certainty of the phenomenon under consideration also indicates that there is still no common understanding of cybercrime in criminological science. At the same time, it should be recognized that both in legal science and in the regulatory sphere, general contours of this phenomenon have already been developed, and are expressed in the functional connection of the act with information and communication technologies.

Thirdly, despite the development of a regional convention mechanism for countering cyber threats, however, in modern conditions there is still no universal (unified, generally accepted) system of crimes that infringe on information security. This circumstance predetermines the possibility of developing only a relevant definition of cybercrime.

Acknowledgments

This work was financially supported by the Grant of the President of the Russian Federation No. NSh-2668-2020.6 "National-cultural and digital trends in the socio-economic and political-legal development of the Russian Federation in the XXI century".

References

Agapov, P. V. (2014). Protivodeystviye kiberprestupnosti v aspekte obespecheniya natsional'noy bezopasnosti: monografiya [Countering cybercrime in the aspect of ensuring national security] Academy of General Prosecutor's Office of Russian Federation. [in Russ.].

Furnell, S., Emm, D., & Papadaki, M. (2015). The challenge of measuring cyber-dependent crimes *Computer Fraud & Security, 10*, 5-12.

Internet crime report. (2019). https://pdf.ic3.gov/2019_IC3Report.pdf

Kenney, M. (2015). Cyber-Terrorism in a Post-Stuxnet World. *Orbis,* (59), 111-128.

Lawson, S. (2013). Beyond Cyber-Doom: Assessing the Limits of Hypothetical Scenarios in the Framing of Cyber-Threats. *Journal of Information Technology & Politics, 10*(1), 86-103.

McQuade, S. C. (2006). *In Understanding and managing cybercrime.* Boston: Allyn and Bacon.

Nomokonov, V. A., & Tropina, T. L. (2012). Kiberprestupnost' kak novaya kriminal'naya ugroza [Cybercrime as a new criminal threat.]. *Kriminologiya: vchera, segodnya, zavtra*, *24*, 45-55. [in Russ.]

Okutan, A., & Çebi, Y. A. (2019). Framework for Cyber Crime Investigation *Procedia Computer Science, 158*(25), 287-294.

The Ultimate List Of Cyber Security Statistics For 2019. Looking for the latest cyber security stats and trends? We've got you covered. (2020, September 12). https://purplesec.us/resources/cyber-security-statistics/

Wall, D. S. (2007). *Cybercrimes: The transformation of crime in the information age*. Polity.

Yakoviyk, I. V., Shestopal, S. S., Baranov, P. V., & Blochina, N. A. (2018). State sovereignty and sovereign rights: EU and national sovereignty. *Opción: Revista de Ciencias Humanas y Sociales*, *85*(2), 376-385.