UDC: 341.4

M. Y. Yatsyshyn (Department of International Law, ERIIR NAU, Ukraine)

Modern approaches to cybercrime classification in International Law

The article substantiates the need for a uniform concept of cybercrime. The author compared and analyzed basic modern approaches to cybercrime classification used in existing international instruments to refer high-tech crime. The conclusions suggest a generalized concept for the classification of cybercrime.

The emergence of the latest information technologies, as well as the global spread of them, has led to profound changes in all spheres of human activity. Together with the creation of new opportunities for the development of society, previously unknown threats of a worldwide scale have emerged, among which, first, it is necessary to determine cybercrime.

The number of cyber-attacks around the world is increasing every day. At the same time, their nature is constantly complicated. Thus, according to data released by the Prosecutor General's Office of Ukraine, over 3,000 offenses in the use of electronic computers, systems and computer networks of telecommunication were registered on the territory of Ukraine in 2017 (in accordance with Articles 361-363 of the Criminal Code of Ukraine). For comparison, in 2015, this figure was - 778 violations.

As a result, cybercrime leads to significant losses that amount to billions of dollars annually throughout the world. According to Microsoft, direct losses of all companies in the world in this area amounted $ 400 billion each year, and by 2020, the world economy will lose more than $ 3 trillion. According to various estimates, the profit from cybercrime can be comparable with profits from the trafficking of drugs and weapons. However, cybercrime threatens not only material losses. The means and technological processes controlled with the help of computer and network technologies affect not only material values but also the life and health of the population, security, integrity and order of the states.

Since the number and cybercrime effects are constantly increasing, we have to argue, that international legal cooperation in the area of countering and preventing high-tech crime is not sufficiently effective. One of the reasons for the non-compliance of international rule making with contemporary challenges is the lack of a unified cybercrime concept that would contain the basic terms and classification of unlawful acts subject to criminalization. In the absence of universal international legal standards, the national criminal laws of the states establish responsibility for various unlawful acts using information and communication technologies. Consequently, offenders may use such gaps to facilitate their illegal activities, on the one hand, and to mitigate or even avoid criminal responsibility, on the other.

The problem of cybercrime was repeatedly defined as a subject of scientific research, in spite of its relevance. Among the foreign and domestic scientists, certain problems were investigated by: Brenner M., Goodman S., Williams F., Denning D., Ziber U., Lewis D., Kabee M., Colin B., Shelley L., Shinder D. , Pazyuk A., Korynevich A., Golubev V., Zabara I., Baler A., Bachilo I., Baturin Y., Voloveds

A., Kruty A., Novikov A., Talimonchik V., Fedorova A. and others. Despite the high level of scientific interest in issues related to the fight against cybercrime, insufficient attention is paid to the analysis of international legal cooperation of states in a certain area, although its relevance is constantly increasing.

Special teams of experts from Interpol and the UN developed first classifications of cybercrime. The Classifier, generated by the Interpol Working Group in 1991, contains the main 6 types of cybercrime, including: unauthorized access and interception (QA); replacement of computer data (QD); computer fraud (QF); unauthorized copying (QR); computer sabotage (QS) and other computer crimes (QZ). In contrast, a group of UN experts conducted a study on the states legislation and identified a list of criminal offenses referred to cybercrime: computer crimes related to the use of personal data, computer crimes related to copyrights and trademarks, computer crimes related to personal injury, computer crimes related to racism and xenophobia, using a computer for luring and grooming children and computer crimes related to spam.

The current stage of development of an international cybercrime counteraction manifested as regionalization and intensification of national legislation unification. The current regional agreements regulating the cooperation of states in the fight against cybercrime are:

1) Council of Europe Convention on Cybercrime dated 21.11.2001;
2) Arab Convention on Combating Information Technology Offences dated 21.12.2010;
3) Agreement on cooperation between the member states of the Commonwealth of Independent States in combating computer-related crime dated 01.06.2001;
4) Agreement on cooperation in the field of providing international information security of the Shanghai Cooperation Organization dated 16.07.2009;
5) Convention on Cybersecurity and Protection of Personal Data of the African Union dated 27.06.2014.

The most significant impact on the international legal cooperation of States in the fight against cybercrime was the adoption in Budapest on November 23, 2003 of the Convention on Cybercrime. The mentioned convention came into force in 61 states, 18 of which are not members of the Council of Europe and are located in other regions.

In fact, in the texts of all the aforementioned treaties there is a list of certain types of acts subject to criminalization. After analyzing these provisions, we conclude, that different legislation criminalize various acts as cybercrime. Moreover, significant crimes in the cyberspace remain beyond the criminal responsibility. For example, there is no prohibition on cyberwar in existing international treaties. It is not only individuals, groups or organizations (including terrorists), who are active in cyberspace, but also states or coalitions of states. Particularly beneficial "borders erosion" between war and peace. In fact, "cyberattacks" can be carried out separately or in combination with other attacks and threaten the sovereignty and security of the state.

In addition to the above classifications of cybercrime in the scientific literature, we find another approach, according to which distinguish:

a) Aggressive cybercrimes - cyberterrorism, the threat of physical punishment (for example, transmitted via e-mail), cyber-stalking (illegal sexual harassment and persecution of another person over the Internet), child pornography (creation of pornographic materials made with children, distribution of these materials, obtaining access to them);

b) Non-aggressive cybercrimes - cyber-bullying, cyber vandalism, cyber-scam, cyber-espionage, spam and viral programs.

We consider the principle distribution of cybercrime into two large groups: crimes against computer networks, systems and technologies, and crimes committed with their use. Fraud involving electronic devices or terminal hacking, for example, remains fraudulent and does not acquire at any rate signs of cybercrime. Therefore, in our opinion, it is justified to distinguish classical crimes committed with the help of cybernetic technologies from the scope of cybercrime. It seems like a logical struggle with them by allocating an aggravating circumstance in the syllables of the corresponding crimes.

Conclusions

Modern international legal counteraction to cybercrime characterized as the lack of uniformity. National systems criminalize various types of offensive acts, using concepts and terms that are different. We consider it necessary to form a united unified concept of cybercrime in international law. Within this framework, it is necessary to unify and systematize the classification of criminal acts subject to criminalization both at the international and national levels.

As a result of the study, we propose the following generalized classification of cybercrime, based on the principles of international public and international criminal law (The basis of our classification is the system of criminal acts, proposed by Blischenko I. and Fesenko I.):

1. Cybercrime under international law (cyberwarfare);
2. International cybercrime:

   2.1. Crimes against computers, systems and networks (illegal access, unauthorized interception, data interference, device abuse, content crime ets.)

   2.2. Crimes committed using computers, systems and networks (cyberterrorism, threat of physical punishment, cyber-stalking, child pornography, cyber-scam etc.).

References

1. Всесторонее исследование проблемы киберпреступности и ответных мер со стороны государств-членов, международного сообщества и частного сектора 23-28.02.2013 г. [Электронный ресурс] – Режим доступа: https://www.unodc.org/documents/organized-crime/UNODC_CCPCJ_EG.4_2013/UNODC_CCPCJ_EG4_2013_2_R.pdf

2. Конвенція Ради Європи про кіберзлочинність від 21.11.2001 р. [Електронний ресурс] – Режим доступу : http://zakon4.rada.gov.ua/laws/ show/994_575.
3. Arab Convention on Combating Information Technology Offences 21.12.2010 [Електронний ресурс] – Режим доступа : http://cms.unov.org/DocumentRepositoryIndexer/GetDocInOriginalFormat.drsx?DocID=3dbe778b-7b3a-4af0-95cea8bbd1ecd6dd.
4. Соглашение о сотрудничестве государств-участников Содружества Независимых Государств в борьбе с преступлениями в сфере компьютерной информации от 01.06.2001 г. [Електронний ресурс] – Режим доступа : http://zakon4.rada.gov.ua/laws/show/997_353.
5. Соглашение между правительствами государств – членов Шанхайской организации сотрудничества О сотрудничестве в области обеспечения международной информационной безопасности от 16.06.2009 г. [Електронний ресурс] Режим доступу : http://base.spinform.ru/show_ doc.fwx?rgn=28340
6. Convention on Cybersecurity and Protection of Personal Data of the African Union 27.06.2014. [Електронний ресурс] – Режим доступу : https://www.au.int/web/sites/default/files/treaties/29560-treaty-0048_-_african_union_convention_on_cyber_security_and_personal_data_protection_e.pdf
7. Протидія кіберзлочинності в Україні : правові та організаційні засади : навч. посіб. / О. Є. Користін, В. М. Бутузов, В. В. Василевич та ін. – К. : Видавничий дім «Скіф», 2012. – 728 с.