Mechanism of legal regulation of fight against cybercrime in Ukraine

I.R. Serkevych, Lviv State University of Internal Affairs

I.M. Yevkhutych, Lviv State University of Internal Affairs

Iryna Hazdayka-Vasylyshuyn, Lviv State University of Internal Affairs

Taras Sozanskiy, Lviv State University of Internal Affairs

Oleksiy Pasyeka, Lviv State University of Internal Affairs

Abstract

The article provides a theoretical generalization and a new solution to the scientific problem, which consists in determining the theoretical and legal foundations of the legal regulation of the fight against cybercrime. Cybercrime is the most dangerous cyberoffences, the commission of which at various stages is directly related to the use of computer technology through computer systems, or to computer systems, and for which the current legislation provides for criminal liability. The system of features of the fight against cybercrime is defined as two-level. The general ones, that is, characteristic of the phenomenon of the fight against crime as a whole, include the following: (1) activity; (2) determination; (3) collection; complexity. In the process of analyzing the legal doctrine, the following are distinguished as special ones, namely characteristic exclusively of the fight against cybercrime: (1) a sign of the possibility of a counter attack from the side of cybercriminals; (2) a sign of commitment by exclusively competent entities possessing the specialized knowledge and necessary resources; (3) a sign of inter-statehood; 4) a sign of unity of states. Three main tendencies in the development of legal regulation of the fight against cybercrime in Ukraine are identified: (1) the tendency of development of the legal framework and terminology in the fight against cybercrime in Ukraine; (2) the tendency of intensifying international cooperation in the fight against cybercrime in Ukraine; (3) the tendency of increasing the level of control over Internet users.

Keywords

Legal Regulation, Cybercrime, Fight Against Cybercrime, Legal Mechanism, Cyberspace Crimes.

Introduction

Cybercrime is not a traditional crime, but a relatively young phenomenon that is associated with the emergence and spread of the global network Internet. Since its inception, this type of crime has proven to be convenient for attackers. The special nature of the World Wide Web has ensured globality and anonymity to its users, which undoubtedly has become a prerequisite for the emergence of this type of crime.

Countering any negative impact requires the formation of an understanding of the essence of the problem and knowledge of its genesis. As the pace of development of society is inextricably linked with the achievements of scientific and technological progress and criminal manifestations, it is also important to address the issue of the historical development of introducing legal mechanisms to combat cybercrime in the world.

That is why the relevance of the study of the concept, essence, and features of the fight against cybercrime is due to the fact that the development of information technology leads to the appearance of this destructive phenomenon, establishes progressive trends in the development of the criminal

world and the emergence of new forms and types of criminal attacks. Accordingly, a proper analysis, determination of basic concepts and identification of features of the fight against cybercrime will allow formulating the theoretical foundations of this institution, which will increase the efficiency of the search for tools to combat the phenomenon under study.

Review of Previous Studies

Criminals actively use the latest advances in information technology in their criminal activities, which is evidence that research of issues concerning the fight against cybercrime should be of an ongoing nature. An analysis of the scientific development of the concept, essence, and features of the fight against cybercrime has shown that at the present stage this issue is little studied (Drobyazko et al., 2019).

Thus, researchers mainly turned to the consideration of certain aspects of this institution, primarily related to the activities of competent law enforcement agencies and international cooperation in this field (Hilorme et al., 2019) Under such conditions, the degree of scientific development of the conceptual apparatus for fight against cybercrime is at a fairly low level (Maher, 2017).

The global computer network Internet has brought together billions of people around the world and has provided unique opportunities for communication, dissemination and receipt of information, and support for business relations, etc. (Boes & Leukfeldt, 2017).

At the same time, the network is a safe haven for a large number of criminals who, due to their anonymity and the limitlessness of the Internet, use it to carry out illegal activities (Dupont, 2017).

Given the rapid globalization of cybercrime, it is obvious that humanity needs an immediate fight against this phenomenon (E-Silva, 2017). In this regard, the creation of legal and scientific mechanisms to counter computer crimes (Jhaveri et al., 2017) arises as an urgent problem.

It is worth noting that almost the majority of scientists to one degree or another investigated the problems of legal regulation of the fight against cybercrime in various aspects, but they did not comprehensively study the retrospective analysis of this legal phenomenon, development trends, and the mechanism of legal regulation of the fight against cybercrime. In today's reality, this area of science of the theory and history of state and law is becoming particularly relevant.

Methodology

The provisions, conclusions, and recommendations contained in the paper are sufficiently reasoned, scientifically substantiated and reliable. The scientific research is based on the application of the general system-structural method, the main elements of which provided a high effect of constructing models for solving the tasks. The system of methodology for scientific analysis of genesis and development tendencies and the mechanism of legal regulation of the fight against cybercrime is based on the following methods: dialectical method allows investigating the inner essence of things in the course of their development, as well as internal and external contradictions, in particular, the genesis of legal regulation of the fight against cybercrime has been analyzed using this method; historical method helps to understand the genesis of legal regulation of the fight against cybercrime; systemic method made it possible to carry out a full and objective study of the relevant specific subject, in particular, to study the structure of the mechanism of legal regulation of the fight against cybercrime, as well as to find out the specifics of international legal regulation of the fight against cybercrime.

Results and Discussion

Each person is endowed with the right to own, use, and dispose of its property, the results of intellectual and creative activity. In turn, the duty of the state is to ensure their protection and implementation, since one of the functions of the state is to protect the interests of citizens from external and internal threats. Recently, the dependence of mankind on new technologies has been growing at an incredible rate. However, this progressive trend, unfortunately, has negative consequences.

The rapid introduction of new technologies in the fields of electronics, communication and digital technologies at the end of the 20th and beginning of the 21st centuries led to the emergence of new social relations and related problems related to the desire of mankind to develop, facilitate work, and improve living conditions. Most important in this process is the technology of the Internet, which provided virtually unlimited opportunities in the transmission, distribution, and receipt of information, communication, and the performance of a number of actions, regardless of the time and place of stay of the person. At the same time, the opening of new horizons for the world community is inextricably linked with the emergence of new forms of criminal activity and other manifestations of unfair use of the achievements of scientific and technological progress.

The need to improve the fundamentals of the legal regulation of the fight against cybercrime is one of the priorities. Therefore, the relevant legal standards must meet the requirements of time and modern conditions. Accordingly, each stage of the establishment of this institute in the world has had a significant impact on the legal regulation of Internet activity and protection of citizens' interests against cyber threats.

The latest phase of cybercrime is now underway-the stage of the emergence of new forms of cybercrime. Among them, the following should be noted:

1. Internet War: For the first time, groups of computer activists, condemning Yugoslavia and NATO military action, hacked government computers and spread anti-war Internet propaganda;

2. Internet Strike: This is a group activity, which leads to an overload of the Internet site and the impossibility of visiting it by other users and the like.

Obviously, such a list of new forms is far from inexhaustible, but its main purpose is to demonstrate that the issue of legal regulation of the fight against cybercrime in the world needs constant evolution and improvement, because computer criminals are constantly changing directions and methods of their activity. Therefore, the main features of the current stage are:

1. The evolution of cybercrime, the emergence of its new forms;

2. Attempts by legislators to adequately respond to these changes.

However, the most important sources according to the selected criterion have been objectively identified. Highlighting their features, it should be noted that today the regulation of issues related to regulating the fight against cybercrime is not carried out by them in full. Features of national legal acts that regulate the fight against cybercrime include:

Systematicity

Systematicity is a currently created extensive system of laws, by-laws and regulations that, in unity, ensure the cybersecurity of Ukraine at this stage. The system operates as follows: in accordance with the Constitution of Ukraine, the assurance of the cybersecurity of Ukraine is defined as one of the most important functions of the state. The Criminal Code of Ukraine defines the negative acts associated with this phenomenon, for which criminal liability and sanctions for offenders are established. Numerous Laws of Ukraine regulate public relations in this area. By-laws and regulations

establish mechanisms for regulating this type of relations and vectors for the further development of the entire sphere. That is, the legal regulation of the fight against cybercrime is possible only under the condition of systematic implementation of the requirements of the analyzed legislative acts;

All-Inclusiveness

Laws and regulations adopted in this area cover the regulation of issues of state cybersecurity, cyberspace, protection of the rights and interests of citizens, countering computer crime and computer terrorism, and the like. That is, the fight against cybercrime is a process that provides for the integrated application of measures, and legal regulation ensures the reinforcement of relevant mechanisms;

Prospects

Some by-laws and regulations have been adopted with the aim of establishing vectors for the further evolution of this sphere. Therefore, the current state of the national legal regulation of the fight against cybercrime indicates that this institution is still at the initial stages of its development;

Detailing

The fight against cybercrime is simultaneously considered in several aspects: as an unlawful act provided for by the norms of the Criminal Code of Ukraine, which caused damage to citizens of Ukraine; as a direction of public policy; as a threat to national security; as one of the ways to consolidate citizens, etc.

Considering that at present the only understanding of what constitutes cybercrime is still unformed, it should be noted that the regulation of this institute is still implemented at a high level. However, an urgent problem is the lack of harmonization between regulations and the lack of a single conceptual apparatus, which should be eliminated in the coming years.

The next subcategory of regulatory acts includes those that regulate the activities of anti-cybercrime agencies. These should include the Security Service of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, the National Bank of Ukraine, and other bodies involved in this issue. However, in the first place, a specially created law enforcement agency, which performs specific functions in this field, should be highlighted.

The following analyzed regulatory acts are by-laws and concern the formation of the Department of Cyber Police and certain aspects of the regulation of the activities of the National Police as a whole. First of all, the legislation related to the activities of this law enforcement body should be singled out, since it is the Department of Cyber Police that directly deals with the fight against cybercrime. As for other organs, their role is episodic and concerns only certain elements of this struggle. Therefore, by-laws and regulations regarding the Department of Cyber Police are crucial for the mechanism of ensuring national legal regulation of the fight against cybercrime.

Therefore, on the basis of the conducted analysis, one can distinguish the following features of laws and regulations that regulate the activities of bodies fighting against cybercrime:

1. Focus on regulating the activities of the Cyber Police Department of the National Police of Ukraine, the Security Service of Ukraine, the State Service for Special Communications and Information Protection of Ukraine, the National Bank of Ukraine, etc.

2. The importance of the role of by-laws regulations.

3. Complex combination of vectors of prevention and counteraction to cybercrime.

Summarizing this group of sources of national legal regulation of the fight against cybercrime, it is advisable to note its general imperfection and inconsistency. The main problem is that the legal acts as instruments of legal regulation have not formed a single system. The main laws and by-laws and regulations were adopted at different stages of the genesis of the Institute for the Fight against Cybercrime in Ukraine and subsequently did not adapt to these changes within the understanding of this phenomenon that occurred during its development. Therefore, the same phenomena may have different names or broad and narrow understanding at the same time.

Recommendations

The conducted doctrinal study gives grounds to argue that to create the conditions for a proper and effective activity to counter cybercrime, there are not enough resources of one law enforcement or law enforcement of a certain state. This kind of activity should be complex in nature and involve the participation of many countries, which requires the necessary regulatory framework at the international level. Today, actions are underway to set the foundations for international cooperation in the fight against cybercrime within the framework of both universal and regional agreements. In addition to that, these measures are not sufficient for full-fledged activities, which require a revitalization of activity by each subject of the international community in order to create an effective mechanism for the international legal regulation of the fight against cybercrime.

Conclusions

The mechanism of legal regulation of the fight against cybercrime is a well-defined and organized system of legal tools that provides legal influence through the application of normative prescriptions on public relations that arise, change, and terminate in the sphere of counteraction to committing information crimes, which allows influencing the desired behavior of such participants, with a view of achieving a proper and effective fight against cybercrime.

The features of the legal framework of the Ukrainian legal regulation of the fight against cybercrime are the following:

1. Existence of the system of national legal regulation of the fight against cybercrime, but the insufficient level of unity of its elements, which consists in differences in terminology, differences in formulations, gaps, and other problems;

2. Combination in the legal system of norms of legislation and international legal acts ratified by the state;

3. Existence of international agreements on bilateral cooperation in the field of legal regulation of combating cybercrime.

4. Existence of the Cybersecurity Strategy of Ukraine, which determines the further development of the national legal regulation of the fight against cybercrime.

References

Boes, S., & Leukfeldt, E.R. (2017). Fighting cybercrime: A joint effort. In *Cyber-Physical Security* (pp. 185-203). Springer, Cham.

Drobyazko, S., Hryhoruk, I., Pavlova, H., Volchanska, L., & Sergiychuk, S. (2019). Entrepreneurship innovation model for telecommunications enterprises. *Journal of Entrepreneurship Education* ,22(2), 1-6.

Drobyazko, S., Makedon, V., Zhuravlov, D., Buglak, Y., & Stetsenko, V. (2019). Ethical, technological and patent aspects of technology blockchain distribution. *Journal of Legal, Ethical and Regulatory Issues, 22*(2S), 1-6.

Dupont, B. (2017). Bots, cops, and corporations: On the limits of enforcement and the promise of polycentric regulation as a way to control large-scale cybercrime. *Crime, Law and Social Change, 67*(1), 97-116.

E-Silva, K.K. (2017). How industry can help us fight against botnets: Notes on regulating private-sector intervention. *International Review of Law, Computers & Technology, 31*(1), 105-130.

Hilorme, T., Perevozova, I., Shpak, L., Mokhnenko, A., & Korovchuk, Y. (2019). Human capital cost accounting in the company management system. *Academy of Accounting and Financial Studies Journal,* 23(2S), 1-6.

Hilorme, T., Shurpenkova, R., Kundrya-Vysotska, O., Sarakhman, O., & Lyzunova, O. (2019). Model of energy saving forecasting in entrepreneurship. *Journal of Entrepreneurship Education, 22*(1S), 1-6.

Jhaveri, M.H., Cetin, O., Gañán, C., Moore, T., & Eeten, M.V. (2017). Abuse reporting and the fight against cybercrime. *ACM Computing Surveys,* 49(4), 1-27.

Maher, D. (2017). Can artificial intelligence help in the war on cybercrime? *Computer Fraud & Security, 2017*(8), 7-9.