FIGHTING AGAINST CYBERCRIME: PROBLEMS AND PROSPECTS IN UKRAINE AND THE WORLD

Andrii Borko, Admiral Makarov National University of Shipbuilding
Vadym Nehodchenko, Dnipro Humanitarian University
Olena Volobuieva, Donetsk Law Institute MIA of Ukraine
Ivan Kharaberiush, Mariupol State University
Yevheniia Lohvynenko, Kharkiv National University of Internal Affairs

ABSTRACT

The article deals with the features of fighting against cybercrime through the creation of appropriate cyber units in Ukraine and in the world. Official data on losses incurred annually by the state as a result of committing cybercrime are presented. Attention is drawn to the fact that by 2021 the losses from cybercrime in the world will reach 6 trillion dollars. It is revealed that the main international act for European states in the field of fighting against cybercrime is the Council of Europe cybercrime convention, according to which cyber units were created in Ukraine and in a number of European Union member states. The peculiarities of counteraction and struggle of cybercrime in Ukraine, Finland, Estonia, France, the USA are considered. The conclusion is made on the importance of harmonization of legislation in the area of fighting against cybercrime, as well as the establishment of cross-border cooperation in this area and cooperation with private actors, in particular those providing Internet services.

Keywords: Cybercrime, Cyberpolice, Fighting Against Cybercrime.

INTRODUCTION

The development of information and computer technology in recent years is accompanied by a number of threats that encroach on virtually all spheres of public life. One of such threats is the use of computer technologies for committing socially dangerous acts that is cybercrime. Thus, according to official data for 2017, in the United States, 59% of Americans identified the possibility of stealing their money or personal data, while 49% were cyberattacks (Global Cybersecurity Index, 2017). According to the data of the General Prosecutor's Office of Ukraine, in 2017 year, 3178 cybercrime were registered, and 1076 proceedings for such offenses were sent to the court. According to the experts of Kaspersky Lab, the absolute leader in the number of internal and external cyber threats in Europe is Ukraine itself. At the same time, according to preliminary data, the losses from cybercrime around the world in 2021 reached 6 trillion dollars (Steve, 2017).

Formulation of the Problem

The growing number of cybercrimes, as well as the damage inflicted to the interests of society and the state, makes the states of the world focus not only on a theoretical study of the essence and characteristics of cybercrime compared to other types of crimes, but also practically implement the mechanisms of counteraction and fighting against cybercrime.

LITERATURE REVIEW

We consider it expedient to start a review of recent scientific studies from the position of Drew, J.M. and Farrell, L., who point out that the emergence of new methods of cybercrime committing indicates the ineffectiveness of traditional methods of police reaction to such crimes, as well as the prevention of such crimes (Drew & Farrell, 2018). Sharma et al. emphasize that in the 21st century cybercrime is often committed in cooperation, which makes cybercrime a serious problem for the whole world. Cybercrime generally covers several types of crime: financial crime, cyber-pornography, gambling on the Internet, cyber-slander, viruses, and email and used data forgery. Accordingly, in the world there are several organizations that constantly work to prevent cybercrime, for example, government agencies, police departments, bureau of cybercrime, etc. (Sharma et al., 2017). While Tsakalidis et al. emphasize that cybercrime is often interchanged with other technology-related offenses, such as cyberwarfare, cyberterrorism, which leads to wrong interpretation of the first (Tsakalidis et al., 2019).

In the opinion of Boes & Leukfeldt, it is the law-enforcement bodies that play an important role in fighting against cybercrime. But one of the strategies to fight against this kind of crime is the formation of partnerships with private institutions formalized cooperation between public authorities and stakeholders (Boes & Leukfeldt, 2017). Whereas, Donalds & Osei-Bryson, argue that for such cooperation it is necessary to develop a general understanding of cybercrime and the classification of offenses covered by this notion (Donalds & Osei-Bryson, 2019).

At the same time, not only the issue of general understanding of cybercrime remains relevant, in particular, it concerns the problem of determining the metrics that are suitable for the assessment by the competent authorities of the threat and harm from cybercrime, as well as its impact on national and human security (Levi, 2017).

METHODOLOGY

The basis of the study of the issue of cybercrime in Ukraine and the world were general scientific and special methods of scientific knowledge. But the method of critical analysis was central, which allowed not only to analyze the results of recent scientific research on the mentioned topics, to generalize the experience of Ukraine and foreign states in the field of activity of cyber-units, but also to highlight the existing problem issues of the effective functioning of such bodies.

FINDINGS AND DISCUSSIONS

The spread of cybercrime has caused the use of measures by states and regional organizations to counteract and fight against the manifestations of this negative phenomenon. One of the regional initiatives to improve cooperation in the field of countering and fighting against cybercrime, of which Ukraine is also a member, is the Convention on Cybercrime adopted by the Council of Europe on November 23, 2001, which provided for the creation by the parties that joined the specified international act at the national level of the body for contacts 24 hours a day in order to provide immediate assistance for investigation or prosecution of criminal offenses related to computer systems and data and for the purpose of gathering evidence in electronic form relating to a criminal offense.

In Ukraine, in pursuance of the above-mentioned provisions of the international act, a Department of Cyberpolicies of the National Police of Ukraine was created. According to the information on the official website of the mentioned body, its tasks include: (1) implementation of the state policy in the field of cybercrime counteraction; (2) timely informing the public of the emergence of new cybercriminals; (3) implementation of software tools for the systematization of cyber incidents; (4) responding to requests from foreign partners. At the same time, the Law of Ukraine "*On National Police of Ukraine*" itself does not contain norms defining the powers of the employees of the Department of Cyberpolicy, given the specifics of their activities. Therefore, it is necessary to agree with the scientists, in particular, Solntseva who consider it appropriate to supplement the Law of Ukraine "*On National Police of Ukraine*" with a separate section on "*Provision of cybersecurity*", which will include the principles of the process and determine the powers of cyberpolice officers.

In the United States and the European Union, similar bodies also exist-in particular, the cyber unit of the Federal Bureau of Investigation of the United States, which provides assistance to other FBI units in the investigation of crimes committed with the help of computer and telecommunication technology. The structure of the FBI cyber unit includes departments to counteract illegal interference in the work of computer networks, fraud, intellectual property infringement, child pornography. In this case, the feature of cybercrime counteracting in the United States is the functioning along with the cyberspace of the FBI of the United States Round-the-clock command centre of cybersecurity.

As for the states of the European Union, the analogue of cyberpolice in Ukraine is the Service of counteraction to abuses in the sphere of information technologies of France. At the same time, there are countries where there are no separate police units that oppose cyberpolicy, but there are reaction groups capable of quickly processing a significant amount of computer information and thus counteracting cybercrime. An example of such a state is Estonia. Leppänen & Kankaanranta in their investigation of cybercrime in Finland, draw attention to the fact that the Finnish police structure also has a special unit, and key players in the investigation of cybercrime cases are computer criminologists who carry out pre-trial examination and investigators who carry out a tactical investigation. At the same time, finding out the specifics of the models by the computer criminologists and investigators of their tasks helps to establish educational qualification requirements for those applying for such positions and accordingly develop an educational program for the training of such specialists (Leppänen & Kankaanranta, 2017).

As Pereira, points out, the application of the principle of territoriality to cybercrime, due to its cross-border nature, is not appropriate in the face of particular difficulties in understanding such types of offenses that strongly affect the economic sector, as well as its revelation, termination and investigation, it is international cooperation that is an effective means of counteracting them (Pereira, 2016). In addition, as noted by Olga et al. the lack of established cooperation between law enforcement agencies is one of the shortcomings of its activities (Olga et al., 2018). Accordingly, in January 2013, the European Centre for Fighting against Cybercrime was opened in Europol, which became the main focal point for the European Union member states in the field of fighting against cybercrime.

In addition to cross-border cooperation of relevant cyber units in different countries, their cooperation with other actors is important. It is necessary to agree with Velasco, who justifies the role of Internet service providers in co-operation with cyber units in detecting, terminating and investigating cybercrime (Velasco, 2015).

Another area in the fight against cybercrime is the harmonization of the regulatory framework for law enforcement in all Member States of the European Union, especially in cases of cross-border cooperation in this area (Kavallieros et al., 2018). According to Harkin et al. equally important are the issues: (1) increasing of workload due to the increase in the level of cybercrime as a modern social problem; (2) the discrepancy between the resources of cyber units and demand; (3) insufficient level of skills and training of employees of cyberpolice units to solve emerging issues in cybercrime (Harkin et al., 2018).

RECCOMENDATIONS

The public danger of cybercrime causes particular attention to the issue of countering and fighting against such types of crimes. Taking into account the international experience of Ukraine, it is advisable to pay attention to the staffing of the Cyberpolicy Department of the National Police of Ukraine. Here is an example of the experience of Finland itself. In turn, Ukraine and other states, in order to effectively counteract and fight against cybercrime, need to establish cross-border cooperation, as well as co-operation with private actors providing Internet services.

CONCLUSIONS

The rapid increase in the level of cybercrime in Ukraine and in the world increases the role of law enforcement agencies in protecting society and the state from such threats and forming in its structure specialized units responsible for countering and fighting against cybercrime. However, the effectiveness of its activities in this area depends on staffing of such units, as well as the establishment of cross-border cooperation and cooperation with private actors within the state.

REFERENCES

Boes, S., & Leukfeldt, E.R. (2017). Fighting cybercrime: A joint effort. *Cyber-Physical Security: Protecting Critical Infrastructure at the State and Local Level*, *3*(1), 185-203.

Donalds, C., & Osei-Bryson, K.M. (2019). Toward a cybercrime classification ontology: A knowledge-based approach. *Computers in Human Behavior*, *92*(1), 403-418.

Drew, J.M., & Farrell, L. (2018). Online victimization risk and self-protective strategies: Developing police-led cyber fraud prevention programs. *Police Practice and Research, 19*(6), 537-549.

Global Cybersecurity Index. (2017). Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/d-str-gci. 01-2017-pdf-e.pdf

Harkin, D., Whelan, C., & Chang, L. (2018). The challenges facing specialist police cyber-crime units: An empirical analysis. *Police Practice and Research, 19*(6), 519-536.

Kavallieros, D., Chalanouli, C., Kokkinis, G., Panathanasiou, A., Lissaris, E., Leventakis, G., Giataganas, G., & Germanos, G. (2018). Searching for crime on the web: Legal and ethical perspectives. *International Conference on Cyber Security and Protection of Digital Services, Cyber Security.*

Leppänen, A., & Kankaanranta, T. (2017). Cybercrime investigation in Finland. *Journal of Scandinavian Studies in Criminology and Crime Prevention*, *18*(1), 1-19.

Levi, M. (2017). Assessing the trends, scale and nature of economic cybercrimes: Overview and issues. *Crime, Law and Social Change, 67*(1), 3-20.

Olga O.V., Nadiia, S.A., Oleg, M.R., Vyacheslav, V.V., & Kateryna, D.Y. (2018). International aspect of a legal regulation in the field of financial crime counteraction by the example of special services of Ukraine and the CIS Countries. *Journal of Legal, Ethical and Regulatory Issues, 22*(1), 1-8.

Pereira, B. (2016). The fight against cybercrime: From the abundance of the standard has its perfectibility. *Revue Internationale de Droit Economique, 30*(3), 387-409.

Sharma, P., Doshi, D., & Prajapati, M.M. (2017). Cybercrime: Internal security threat. *Proceedings of 2016 International Conference on ICT in Business, Industry, and Government*.

Steve, M. (2017). *2017 Cybercrime report.* Rtetrieved from https://cybersecurityventures.com/2015 -wp/wp-content/uploads/2017/10/2017-Cybercrime-Report.pdf

Tsakalidis, G., Vergidis, K., Petridou, S., & Vlachopoulou, M. (2019). A cybercrime incident architecture with adaptive response policy. *Computers and Security, 29*(1), 45-72.

Velasco, C. (2015). Cybercrime jurisdiction: Past, present and future. *ERA Forum*, *16*(3), 331-347.

This article was originally published in a Special Issue 2, entitled: **"Business Laws and Legal Rights: Research and Practice",** Edited by **Dr. Svetlana Drobyazko**