

Combating cybercrime: economic and legal aspects

OLENA V. SVIATUN¹, OLGA V. GONCHARUK², CHERNYSH ROMAN³, OLENA
KUZMENKO⁴, IHOR V. KOZYCH⁵

^{1,2}Department of Comparative and European Law, Taras Shevchenko National University of Kyiv,
UKRAINE

³Department of Science of Law, Polissia National University, Zhytomyr, UKRAINE

⁴Department of Criminal Procedure and Forensic Science, University of the State Fiscal Service of
Ukraine, Irpin, UKRAINE

⁵Department of Criminal Law, Vasyl Stefanyk Precarpathian National University, Ivano-Frankivsk,
UKRAINE

Abstract: - Cybercrime threatens the national security of different countries around the world. The growth of cyberattacks destabilizes the international order and disrupts the normal functioning of international relations. The purpose of the academic paper is to analyze the causes and economic consequences of the level of cybercrime in the world and to identify modern legal arrangements to combat cybercrime. In order to achieve the purpose outlined, the following methods have been used, namely: the method of comparison, analysis, element-theoretical method, method of generalization and analogy. It has been established that the level of cybercrime in the world and the economic consequences of its impact tend to increase. It is estimated that in 2020 the total cost of cybercrime and cybersecurity will exceed one trillion US dollars, which is more than 1% of world gross domestic product. The reasons have been determined why the number of cybercrimes are increasing (electronization and computerization of most industries, public sector; low level of operational cooperation; inconsistency of legal policy with the realities of cybercrime; development of cyber-attack mechanism; modernization of cybercrime; obstacles to international cooperation and so forth). The cause and effect interrelationship between the level of cybercrime, cybersecurity and legal methods of counteraction in different countries of the world has been proven. Three interrelated ways of the legal mechanism of counteraction to cybercrime have been offered, namely: the general, organizational and preventive ones. The expediency of international cooperation in the development of global strategies and other measures to combat cybercrime has been emphasized.

Key-Words: - Cybercrime, Cybersecurity, Cyber Attack, cybercrime legislation, Cost of Cybercrime, Economic Consequences.

Received: October 28, 2020. Revised: April 2, 2021. Accepted: April 12, 2021. Published: April 21, 2021.

1 Introduction

Advanced countries and developing countries are pursuing the electronization of the economy, digitalization of most private and public spheres of life. At the same time, this direction of modernization of various types of economic activities and public spheres attracts cybercriminals.

Cybercrime is one of the biggest threats to the world economy, the national interests of individual states and business. For companies, the costs and losses connected with cybercrime are huge. They combine data corruption and destruction, theft of funds, intellectual property, personal and financial data, disruption of business after a cyberattack, damage to business reputation, loss of productivity,

etc. The rapid growth of cybercrime necessitates the development of effective mechanisms in order to prevent such crimes; however, the detection and prosecution of cybercriminals is quite rare compared to the number of such offenses. The development of strategies for state mechanisms towards modernizing information systems should be aimed at reducing the scale of cybercrime and creating the basic principles of national and international policy in order to combat cybercrime at the international level. Unfortunately, the number of crimes and economic losses from cyberattacks is projected to increase, forasmuch as offenders are usually one step ahead of preventive measures. In addition, the complex nature of cybercrime, which consists in the

territorial scale of the crime, makes it difficult to identify and detect such crimes.

The purpose of the academic paper is to analyze the causes and economic consequences of the level of cybercrime in the world and to identify modern legal arrangements to combat cybercrime.

2 Literature Review

Cybercrime is a developed form of transnational crime. The complex nature of cybercrime is its involvement in organized crime groups. Along with this, criminals and victims are located in different regions, and their effects can spread to societies around the world, necessitating an urgent, dynamic and integrated response. Maillart [1] and Brenner [2] emphasize that there is no crime scene in cyberspace in its traditional sense, where one can find physical evidence, fingerprints, and witnesses. According to the viewpoint of Renu & Pawan, the possibilities of computer technologies and the proliferation of cheap, powerful, user-friendly computers have a positive impact on the economy; however, businesses, enterprises and government agencies may cease to function because of cybercrime [3]. The society has not only significantly increased the use of devices and technologies; however, data assets have also raised that create threats and opportunities for abuse and enhance the potential of criminal activity using digital information generated for malicious purposes [4].

Cybercrime is divided into two separate categories: cybercrime of the first type, which is mostly technological and cybercrime of the second type, which has a more visible human element [5]. A similar approach is used by analytical companies that study cybercrime and the economic losses and costs connected with it [6].

Crimes in the field of the Internet include: the development and spread of computer viruses, bank accounts thefts, fraud using plastic payment cards, theft of information and data contained in the computer, violation of the rules of operation of automated computer systems and others. The features of these crimes are as follows: the difficulty of their detection, the complexity of the investigation, high latency, large amounts of damage, difficulty of proving such cases in court. The classification of cybercrime includes two types: traditional crimes committed in the sphere of computer technology and the Internet and new crimes - with the application of the computer technology [7].

In a globalized economy, the risk of cybercrime attacks is extremely high, while Antonescua & Birău suggest that cybercrime has different financial and non-financial consequences in the countries around the world [8]. As a result, governments of different countries develop adequate legal and economic policies, as well as regulate the costs of cybercrime, forasmuch as the funds spent on preventing, detecting and handling security incidents should be balanced with reducing losses from such offenses. Herewith, practical steps in the field of cybersecurity reveal different perceptions of policies concerning cyberspace protection, forasmuch as it is difficult to clearly assess the economic efficiency of such actions [9].

Examining the costs and losses of cybercrime, analysts at Costs of Cyber Crime Working Group emphasize the complexity of their measurement and further use in international regulation [10]. The costs are proposed to be divided into three categories, namely: the cost of cybercrime anticipation; costs as a consequence of cybercrime; costs in response to cybercrime.

As long as companies continue to believe that their protection against cyberattacks is sufficient and effective, cybercriminals continue to deplete the global economy, causing significant damage to it [11]. The cost of global cybercrime has reached more than 1 trillion USD since 2018, and experts estimate that it will increase by more than 50% over the next two years [12]. As it has been noted by Wicki-Birchler, if cybercrime were compared to a country, it would be the 13th largest economy in the world in terms of gross domestic product, just ahead of Australia and Spain [13]. Consequently, regardless of the level of protection, most likely, cybercriminals will always try to carry out their illegal activities, look for the weakest links in security measures and take advantage of human errors in working with computers.

The Convention on Cybercrime establishes cooperation between states and private companies in order to combat cybercrime and protect legitimate interests in the field of information technology [14]. The Convention determines that an effective fight against cybercrime requires larger, faster and more efficient international cooperation in criminal matters. The Convention identifies the following types of cybercrime: illegal access; illegal interception; data interference; intervention in the system; device misuse; computer-related counterfeiting; computer fraud; offenses related to child pornography; offenses related to copyright and related rights infringement.

The global community that is working on countering cybercrime has created agencies for this purpose, namely: the Federal Bureau of Investigation, the National Cyber Investigative Task Force, the National Security Agency in the USA, the Cyberspace Administration in China, and the European Cybercrime Center in the EU to detect, investigate and prevent cybercrime [15]. Some relevant studies can be found in [16] and [17].

According to the viewpoint of Onwujekwe et al., there is no doubt that cybercrime is growing faster than cybersecurity combating measures. Consequently, businesses and government agencies are more prone to cyberattacks than ever before [18]. In this context, combating crime centers around general organization, which means a set of managerial, organizational, preventive, control and other mutually beneficial actions of various bodies and institutions. Law enforcement activities consist of measures, which are aimed to implement law enforcement and / or law enforcement functions. Crime prevention is an action regulated by law that means preventing the development of criminal intent in the early stages of the crime. Forms of crime prevention, depending on the hierarchy of causes and conditions of crime are as follows: general social, special criminological and individual crime prevention [19].

The mechanism of combating crime is characterized by the complexity of interdependent functions of law enforcement activities, the essence of which centers around certain ways and methods of influencing crime. Such a mechanism includes: a cycle of law enforcement functions provided by law; a number of law enforcement activities aimed at controlling and supervising the organization and implementation of preventive activities at all stages of criminal proceedings; a set of preventive measures. The considered mechanism is formed and functions by means of organizational and legal measures. Along with this, it is modernized in the presence of certain conditions [20].

The effectiveness of the fight against cybercrime depends on the organizational structure. It involves the correctness of the established system of relevant bodies, eliminating duplication and distributing powers. Cybercrime is a global phenomenon. In order to effectively investigate cybercrime, it is necessary to harmonize legislation and develop specific mechanisms for international cooperation [21].

Cybersecurity is a widely used term, the definition of which is often subjective and sometimes uninformative. Too broad interpretation of the term “cybersecurity” hinders technological

and scientific progress, reinforcing a predominantly technical view of cybersecurity, while separating disciplines that should act in concert to address complex cybersecurity issues. “Cybersecurity is the organization and collection of resources, processes and structures used to protect cyberspace and cyberspace-supported systems from events that are de jure incorrectly equated with actual property rights”. The formation of a concise, comprehensive, meaningful definition will strengthen and enrich attention on the interdisciplinary dialectic of cybersecurity, which will solve a number of cybersecurity matters [22].

Thus, the issue of cybercrime is widely reflected in scientific publications in the form of theoretical studies and practical investigations. However, the issue of economic and legal aspects of combating cybercrime remains relevant, open for further research, taking into account current threats to cybersecurity at the level of the world economy, individual states, business and private interests.

3 Materials and methods

A comparative analysis of statistical data has been conducted in the research that characterizes the level of cybercrime in the world and individual countries, as well as indicators of cybersecurity, in particular:

- Cyberthreat Defense Report – Percentage compromised by at least one successful attack; Percentage compromised by at least one successful attack by country; Percentage compromised by at least one successful attack by industry;
- Center for Strategic and International Studies (CSIS) & McAfee Incorporated global report (2013; 2014; 2018; 2020);
- International Telecommunication Union – Cybercrime legislation globally and per region; Global Cybersecurity Index (GCI) most committed countries globally in 2018.

Linear Trend model has been used to forecast the development of the Average Cost of Cybercrime in the world. The selection of the trend function is carried out by the method of least squares. In order to determine the accuracy of the model, a coefficient of determination has been used, which is based on estimates of the variance of empirical data and values of the trend model.

Cluster analysis has been used to classify countries according to the Global Cybersecurity Index. The calculations were performed on the basis of the STATISTICA statistical analysis package. The Americas region, which unites 24 countries with different levels of development and different commitment of countries to cybersecurity, was chosen for the calculation. To unite countries into

clusters, the “nearest neighbor” algorithm was used, the usual Euclidean number was taken as the distance between the objects and the following formula was used:

$$p(x_i x_j) = \sum_{i,j}^{1,2,..,k} |x_i^{1,2,..,k} - x_j^{1,2,..,k}|$$

where: k - number of signs.

Some relevant studies can be found in [23] where Clustering of Countries was used for analyzing Cyber Crime Nation Typologies.

Cybercrime is currently trending upwards, and high-end cybercriminals are as technological as modern information technology companies. They have quickly moved on to the introduction of cloud technology, artificial intelligence, encryption and monetization of stolen funds. The Center for Strategic and International Studies (CSIS), in collaboration with antivirus software developer McAfee Incorporated, has been analyzing the economic losses from cybercrime and the cost of cybersecurity since 2013.

4 Results

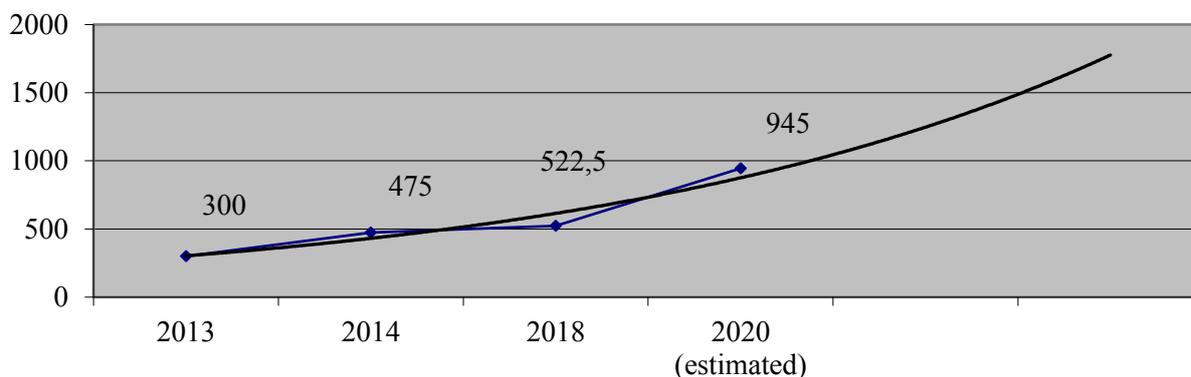


Fig.1. The Average Cost of Cybercrime in the world (billion, USD)

Thus, the cost of global cybercrime is constantly rising, while analysts’ forecasts suggest an increase in both the losses of the world economy from such crimes and the cost of preventing and eliminating their consequences. Consequently, in 2020, the cost of cybercrime will be about 945 billion USD, global spending on cybersecurity - 145 billion USD. Thus, the total cost of the world economy will exceed 1 trillion USD, or slightly more than 1% of world gross domestic product (GDP).

The trend model describing the insurance premiums forecast has been chosen depending on the coefficient of determination. The closer R^2 is to 1, the more accurately the model describes economic processes. According to the results of statistical analysis, the most accurate forecast of the Average Cost of Cybercrime in the world reflects the exponential approximation – a line that confirms that the value of the studied indicator tends to increase, and its value becomes bigger at a higher rate.

The cost of cybercrime varies significantly in different reports, reflecting the lack of uniform

international approaches to determining costs and losses and the availability of different methodologies that are offered by analytical companies. It should be noted that while estimating losses and costs due to cybercrime in the global economy, the following costs are taken into account: costs of anticipating cybercrime; costs as a consequence of cybercrime; costs in response to cybercrime. The hidden costs that companies and governments may not be aware of immediately after the crime, such as lost opportunities, deteriorating business reputation, brand, image, and moral damage, are practically not taken into account. Most of these costs have no direct value, but have long-term economic implications.

Costs and losses from cybercrime in the regions of the world differ territorially (see Table 1). Therefore, it is important to establish the interrelationship between the level of income in the country and the negative economic impact of cybercrime, as well as to determine the effective security measures in individual countries.

Table 1. Regional Distribution of Cybercrime

Region (World Bank)	Region GDP (USD, trillions)	Cybercrime Cost (USD, billions)	Cybercrime Loss (% GDP)
---------------------	-----------------------------	---------------------------------	-------------------------

North America	20.2	140 to 175	0.69 to 0.87%
Europe and Central Asia	20.3	160 to 180	0.79 to 0.89%
East Asia & the Pacific	22.5	120 to 200	0.53 to 0.89%
South Asia	2.9	7 to 15	0.24 to 0.52%
Latin America and the Caribbean	5.3	15 to 30	0.28 to 0.57%
Sub-Saharan Africa	1.5	1 to 3	0.07 to 0.20%
Middle East and North Africa	3.1	2 to 5	0.06 to 0.16%
World	\$75.8	\$445 to \$608	0.59 to 0.80%

The highest rate of loss as a percentage of GDP is observed in Europe and Central Asia, North America and East Asia & the Pacific. Most of the countries in these regions are advanced countries with high incomes. Precisely, in these countries, the Cyber Risk Index is much higher due to the more advanced technological infrastructure compared to other countries, high urbanization and digitalization of both business and government [24]. The head offices of the world's largest multinational corporations are also located in these groups of countries. Iceland, Sweden, the United Arab Emirates, Norway, the United States, and the United

Kingdom are among the countries with the highest risk of cybercrime for the country's economy, government and business. These countries are characterized by high density of public Wi-Fi, extremely widespread Internet and social networks; the most modern technologies are applied there; widespread e-commerce, electronic control and smartphones are used. According to the territoriality of the Cyber Risk Index [25], the most dangerous regions for cybercrime are Northern Europe and North America. India, Nigeria, Iraq, Indonesia and South Africa are the safest among the low-risk countries (see Figure 2).

Countries with the highest cyber risk

No	Country	CRI
1	 Iceland	0.839
2	 Sweden	0.809
3	 United Arab Emirates	0.774
4	 Norway	0.729
5	 United States	0.713
6	 Singapore	0.670
7	 Ireland	0.664
8	 New Zealand	0.660
9	 Denmark	0.657
10	 United Kingdom	0.647

Countries with the lowest cyber risk

No	Country	CRI
41	 Ukraine	0.361
42	 Iran	0.349
43	 Philippines	0.337
44	 Thailand	0.334
45	 China	0.326
46	 South Africa	0.300
47	 Indonesia	0.291
48	 Iraq	0.290
49	 Nigeria	0.239
50	 India	0.186

Fig. 2. Cyber Risk Index

Every year cybercrime is becoming an increasing threat to the global economy and the economies of individual countries. 144,91 million new forms of malicious software (AV-Test) appeared in 2019, and in April 2020, 38,48 million new samples were detected. In 2018, according to the Webroot Threat Report [26], 93,6% of detected malware were of polymorphic nature. This means that they have the ability to constantly change their code in order to avoid detection. About 50% of business computers and 53% of consumer computers hit by a

cyberattack at one time were re-infected during the same year.

Eurojust and Europol's European Cybercrime Center [27] through operational and practical experience, joint discussions and judgement-based contribution have identified problems that threaten the economy of the country, business, individuals, namely: data loss; loss of data location; problems related to national legal frameworks; obstacles to international cooperation; problems of public-private partnership.

Regarding threats to individual companies and businesses, in 2018, 77,2% of surveyed companies were victims of cybercriminals, and in 2020 the amount of such companies was 80,7% [28] (see Fig. 3). Such statistics suggest that existing mechanisms

for combating cybercrime are insufficiently effective or outdated forasmuch as these crimes are being modernized faster than the mechanisms for combating them.

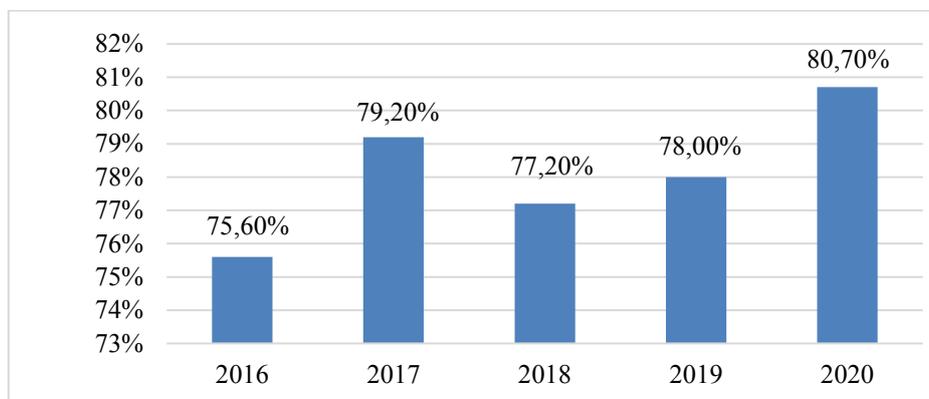


Fig. 3. Percentage compromised by at least one successful attack, by year

According to PricewaterhouseCoopers [29], the vast majority of cyberattacks on individual companies and businesses occur through phishing scam letters by means of well-designed social engineering scenarios. Every third employee opens malicious attachments or links after receiving a phishing scam letter. One in eight employees sends cybercriminals the information they require, demonstrating how low cybersecurity awareness is in most companies. Even considering the number of cyber incidents, small businesses are less protected than large ones, forasmuch as up to 67% of

companies with fewer than 1000 employees are exposed to cyberattacks; most of these companies run the risk of not coming through the harm caused by cyberattacks.

The financial sector is the most vulnerable to cybercrime; it has subjected to cyber attacks in 87,6% of cases, retail trade – 82,7%, communication and technology – 81,9% (see Fig. 4). This situation is such due to electronization and computerization of these spheres, as well as high financial turnover, which is attractive to fraudsters.

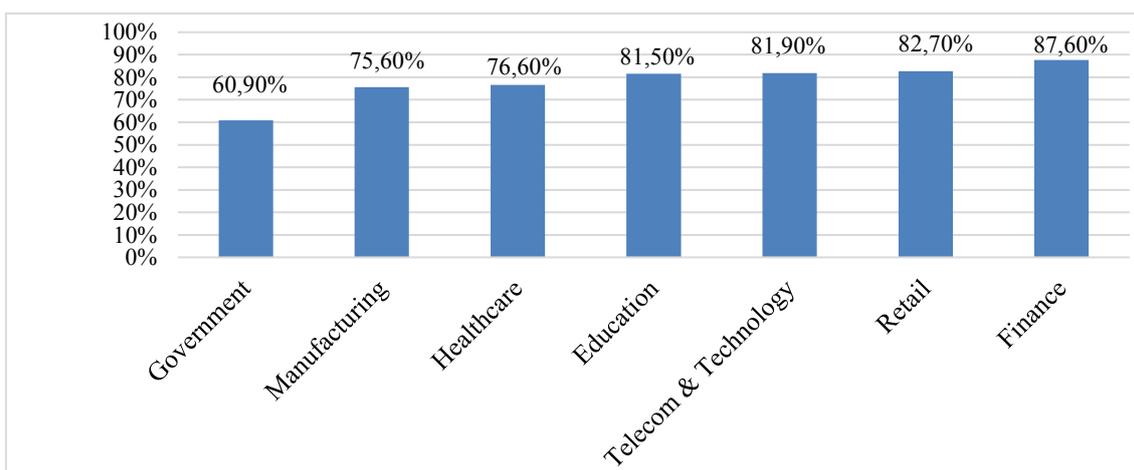


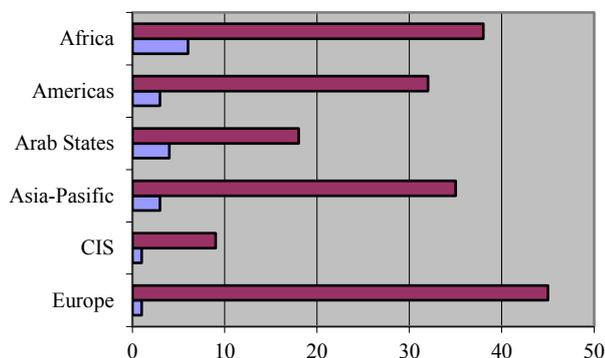
Fig. 4. Percentage compromised by at least one successful attack in 2019, by industry

Cybercriminals attack computer networks and systems of people, businesses, and even global organizations at a time when cybersecurity may be reduced by shifting attention to the particular crisis. At the same time, 42% of companies, businesses of which have been affected by cybercrime, say they

are in better shape after committing a crime against them, and some companies even report revenue growth as a direct result of management decisions to address the consequences of the crisis.

Legal regulation is the main component of combating cybercrime at the state level. Therefore,

the countries of the world establish their own legal mechanisms for combating and countering cybercrime, as well as methods for restoring violated rights as a result of the commission of



	Europe	CIS	Asia-Pacific	Arab States	Americas	Africa
■ Yes	45	9	35	18	32	38
■ No	1	1	3	4	3	6

cybercrimes. Cybercrime legislation has been developed in most countries (91% of 177 countries), with only 9% of countries not enacting legislation [30] (see Fig. 5).

Fig. 5. Cybercrime legislation globally and per region in 2018.

However, in Africa, only 38 of the 44 countries apply cybercrime legislation, in South America 32 out of 35, in the Arab States 18 out of 22, and in the Asia-Pacific region 35 countries out of 38. In the CIS and European countries, the absence of legislation on cybercrime has been recorded only in Belarus. These figures correlate with information provided by UNCTAD [31]: Europe has the highest level of cybercrime legislation, while Asia and the Pacific have the lowest. Along with this, the UN recognizes that cybercrime is a threat to cross-border cooperation and international trade.

In order to create conditions for protection against cybercrime, countries around the world are developing a system of measures, which are grouped into five categories and assessed using the Global Cybersecurity Index (GCI), namely: legal measures, technical measures, organizational measures, capacity building, and cooperation (see Table 2).

Table 2 depicts the countries with the highest level of the Global Cybersecurity Index.

Table 2. Global Cybersecurity Index (GCI) most committed countries globally in 2018 (normalized score)

Rank	Member States	GCI Score	Legal	Technical	Organizational	Capacity building	Cooperation
1	The United Kingdom	0,931	0,200	0,191	0,200	0,189	0,151
2	The United States of America	0,926	0,200	0,184	0,200	0,191	0,151
3	France	0,918	0,200	0,193	0,200	0,186	0,139
4	Lithuania	0,908	0,200	0,168	0,200	0,185	0,155
5	Estonia	0,905	0,200	0,195	0,186	0,170	0,153
6	Singapore	0,898	0,200	0,186	0,192	0,195	0,125
7	Spain	0,896	0,200	0,180	0,200	0,168	0,148
8	Malaysia	0,893	0,179	0,196	0,200	0,198	0,120
9	Norway	0,892	0,191	0,196	0,177	0,185	0,143
10	Canada	0,892	0,195	0,189	0,200	0,172	0,137
11	Australia	0,890	0,200	0,174	0,200	0,176	0,139

The cluster analysis has been used for classifying 24 countries according to the Global Cybersecurity Index. As a result of calculations 4 clusters are

received: Cluster1_(1,2), Cluster2_(3,4,5,6,7), Cluster3_(8,9,10,11,12,13,14,15,16), Cluster4_(17,18,19,20,21,22,23,24). The results of grouping are shown in the table

Table 3. Clusters of the Americas region countries according to the Global Cybersecurity Index

Clusters	Cluster 1	Cluster 2	Cluster 3	Cluster 4
Cluster 1 The United States of America ₁ , Canada ₂	0	0.211	0.411	0.641
Cluster 2 Uruguay ₃ , Mexico ₄ , Paraguay ₅ , Brazil ₆ , Colombia ₇	0.211	0	0.084	0.314

Cluster 3 Cuba ₈ , Chile ₉ , Dominican Republic ₁₀ , Jamaica ₁₁ , Argentina ₁₂ , Peru ₁₃ , Panama ₁₄ , Ecuador ₁₅ , Venezuela ₁₆	0.411	0.084	0	0.103
Cluster 4 Guatemala ₁₇ , Antigua and Barbuda ₁₈ , Costa Rica ₁₉ , Trinidad and Tobago ₂₀ , Barbados ₂₁ , Saint Vincent and the Grenadines ₂₂ , Bahamas ₂₃ , Grenada ₂₄	0.641	0.314	0.103	0

The results of the hierarchical classification of the countries outlined are shown in Fig. 6.

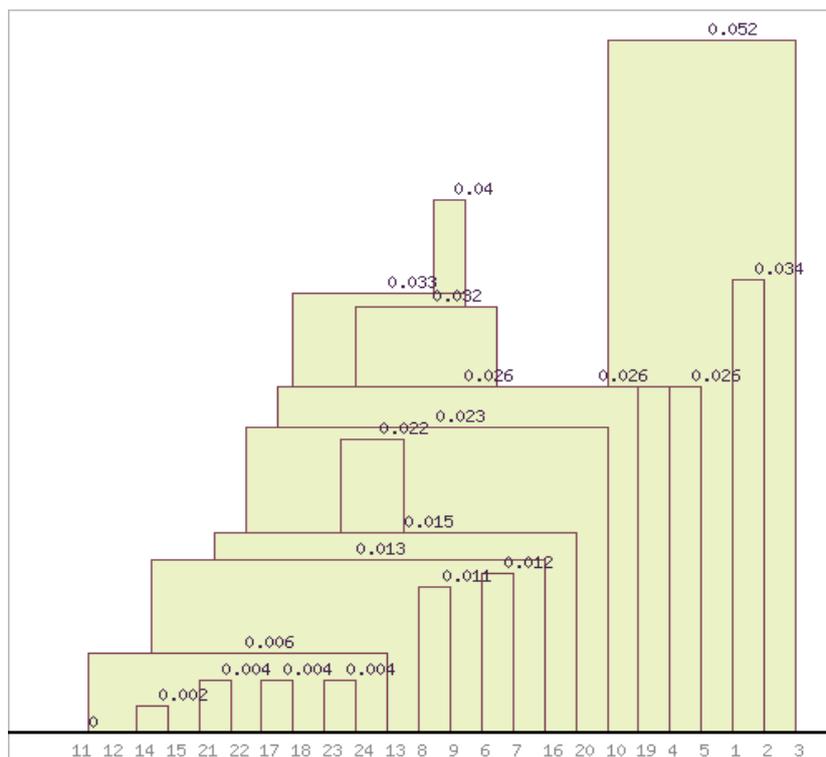


Fig. 6. Dendrogram of clusters of countries according to the Global Cybersecurity Index in 2018

Legal mechanisms enable these states to develop and implement modern ways of responding to cybercrime by investigating and prosecuting criminals, as well as imposing sanctions for non-compliance or violation of the law. The legal framework establishes a minimum ground, based on which companies, government agencies, and individuals can develop further cybersecurity methods. As a matter of fact, the legal framework presupposes the existence of sufficient legislation in order to harmonize practices at the regional / international level and for the international fight against cybercrime. The legal context is assessed on the basis of the number of legal institutions and restrictions related to cybersecurity and cybercrime. The high rate of application of legal methods of protection and the low rate of cooperation is observed in almost all countries, which negatively affects the cyber defense of both individual states

and the world economy as a whole. Operational cooperation to prosecute cybercrime is also rare, and gaps in national and international law faced by key participants in these investigations are not always clear to the legislator. Combating cybercrime also includes prevention; it centers on preventive way to ensure cybersecurity, which, unfortunately, is not used by all countries and companies.

Cyberattacks are sensitive to global crises, and there is a spread of cybercriminals in social engineering after natural disasters, terrorist attacks, mass crimes and pandemics.

The last crisis, observed in 2020, has been caused by the coronavirus. Interpol estimates that cybercriminals are attacking computer networks and systems of global organizations, government agencies, businesses, and people, forasmuch as cybersecurity may be reduced by shifting the focus to the health crisis. Cybercriminals use coronavirus

reports to disguise their activities. Malicious, spyware, and Trojans have been found on interactive coronavirus maps and websites. Spam emails are also used as a means of attracting the attention of users who click on links that download malicious software to their computers or mobile devices.

5 Discussion

Cybercrime is the greatest threat to every company in the world and one of the greatest challenges humanities will face over the next two decades [32; 33]. The growing dependence of the world economy on modern technologies is exacerbated by their increased productivity, efficiency and availability, the desire to digitalize data that require protection of information from unauthorized access [4].

Onwujekwe et al., note that the number of investigations to address the issue of combating cybercrime is insufficient [18]; however, there are more and more hypotheses and assumptions about reliable measures to prevent it. New technologies, developments in the world economy combined with a change in the direction of cyber threats create new challenges to combat complex “actors” who are well motivated, qualified and adapted. In particular, the financial sector is the most vulnerable to economic losses from cybercrime, which was subjected to cyberattacks in 87,6% of cases, as well as retail sector – 82,7%, communications and technology sphere – 81,9%. In addition, cyberattacks are intensifying during global crises, and the spread of cybercrime following natural disasters, terrorist attacks, mass crimes and pandemics is increasing.

Cybercrime negatively affects the country's economy and reputation. Srivastava et al. have grouped the frequency of cybercrime originating in a country into three categories, namely: economic capital, technological capital and cybersecurity [34]. According to their research, economic and technological capitals are the main factors influencing the frequency of cybercrime in the country. It should be noted that there are different approaches to estimating losses and costs due to cybercrime in the global economy. The following costs are taken into account: costs of cybercrime expectations; costs as a consequence of cybercrime; costs in response to cybercrime [10]. However, hidden costs that do not have a direct value expression are not taken into account. Along with this, the real losses from cybercrime are much higher than they are estimated, forasmuch as they have a long-term negative impact on the company's

activities and on the macroeconomic indicators of individual countries.

The cost of cybercrime is unevenly distributed among all countries of the world. According to the data of the Center for Strategic and International Studies, there is a difference by region, income level and level of cybersecurity [12].

The research proves that there is a relationship between a country's income level and the negative economic impact of cybercrime, forasmuch as the economically richer a country is the greater its costs and losses from cybercrime are. Depending on the impact of cybercrime, countries develop adequate legislation and modern legal means of counteraction, which include a general assessment of cybersecurity, legal security, organization, technical support, capacity building, and cooperation. At the same time, low rates of cooperation have a negative impact on cyber defense of both individual countries and the world economy as a whole. However, the relationship between the levels of development of countries with cybercrime is complex, which is also confirmed in the study of Zaharia [35].

6 Conclusion

Based on the research conducted, it has been established that the number of cyberattacks in the world is growing every year. The most vulnerable areas are those that use electronic computing and the Internet in their work as well as have a large financial turnover: financial, retail, communication and technology.

The difficulty in effectively combating cybercrime is its large territory, which makes it difficult to prevent and detect it. It has been proven that countries with a high level of economic development most suffer losses due to cybercrime and at the same time are characterized by an adequate level of cybersecurity, which provides for the use of modern legal methods of countering cybercrime. However, operational cooperation, which is an important way to combat cybercrime, remains low in the countries studied.

The reasons for the growth of cybercrime in the world have been identified, namely: the involvement of computer technology and the Internet in the work of various areas of legal relations; low level of operational cooperation; inconsistency of legal policy with the realities of cybercrime; development of the mechanism of cyberattacks, which makes it difficult to prevent and detect them; modernization of methods of committing cybercrimes, which precedes the

methods of detection and investigation of such crimes by bodies and institutions of counteraction to cybercrime; obstacles to international cooperation and others. One of the main causes of cybercrime is the crisis in the society, which is more vulnerable during this period.

The legal mechanism for combating cybercrime should include three interrelated ways: general, organizational and preventive. The general mechanism provides for the study of the dynamics of cybercrime, the fixation and study of cybercrime (development of key statistical indicators), the study of practice, and the study of cybercrime trends. Organizational mechanism includes the activities of bodies and institutions aimed at preventing, finding, detecting, investigating cybercrimes and restoring violated rights as a result of such a crime; forecasting, coordination, planning. Strategy and tactics development are important in combating cybercrime. Preventive ways to combat cybercrime are the implementation of programs and plans, information policy aimed at informing people who may be potential victims of cyberattacks.

Despite the fact that most countries around the world are developing both their own ways and mechanisms and joint with other countries towards combating cybercrime, the problem of cybersecurity for national economies and the international economy as a whole remains open. Further investigations may focus on the international experience of assessing the hidden losses and costs connected with cybercrime and developing preventive legal and economic mechanisms to combat cybercrime.

References:

- [1] Maillart, J.B. The limits of subjective territorial jurisdiction in the context of cybercrime. *ERA Forum*, 19, 2019, pp. 375–390. <https://doi.org/10.1007/s12027-018-0527-2>
- [2] Brenner, S.W. Toward a criminal law for cyberspace: distributed security. *Journal of Technology Law and Policy*, Vol.V (1). 2004.
- [3] Renu & Pawan. Impact of Cyber Crime: Issues and Challenges. *International Journal of Trend in Scientific Research and Development*, Vol. 3, Issue 3, 2019, pp.1569-1572, <https://www.ijtsrd.com/papers/ijtsrd23456.pdf>.
- [4] Iqbal F., Debbabi M., Fung B.C.M. Cybersecurity And Cybercrime Investigation. In: Machine Learning for Authorship Attribution and Cyber Forensics. *International Series on Computer Entertainment and Media Technology*. Springer, Cham, 2020, https://doi.org/10.1007/978-3-030-61675-5_1
- [5] Gordon, S., Ford, R. On the definition and classification of cybercrime. *Journal in Computer Virology*, 2, 2006, pp. 13–20, <https://doi.org/10.1007/s11416-006-0015-z>.
- [6] Statista. Cyber Crime & Security. Statistics and Market Data on Cyber Crime & Security, 2020, <https://www.statista.com/markets/424/topic/1065/cyber-crime-security/>
- [7] Zavoruyev R., Reznichenko V. Protydiya kiberzlochynnosti v Ukrayini [Countering cybercrime in Ukraine]. Materialy Vseukrayins'koyi naukovo-praktychnoyi konferentsiyi 23-25 lystopada 2016 roku, m. Kropivnyts'kyy. Aktual'ni zavdannya ta dosyahnennya v haluzi kiberbezpeky, 2016, http://dspace.kntu.kr.ua/jspui/bitstream/123456789/5113/1/AUConferenceCyberSecurity_November2016_p49.pdf (in Ukrainian).
- [8] Antonescu M. Birăub R. Financial and Non-financial Implications of Cybercrimes in Emerging Countries, *Procedia Economics and Finance*. Vol. 32, 2015, pp. 618-621, [https://doi.org/10.1016/S2212-5671\(15\)01440-9](https://doi.org/10.1016/S2212-5671(15)01440-9)
- [9] Mulligan, D., Levi, M. Prevalence of Cyber Crime and its Effect on Economy, *Idosr Journal of Arts and Management*, 5(1), 2020, pp. 64-69.
- [10] Understanding the costs of cyber crime. A report of key findings from the Costs of Cyber Crime Working Group, 2018, <https://www.gov.uk/government/publications/understanding-the-costs-of-cyber-crime>
- [11] Wertheim S. Tips for Fighting Off Cybercrime in 2020. *The CPA Journal*, Vol. 90(3), 2020, pp. 64-66.
- [12] Malekos Z.S., Lostri E., Lewis A.J. The Hidden Costs of Cybercrime. Center for Strategic and International Studies (CSIS), McAfee, 2020, <https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf>
- [13] Wicki-Birchler, D. The Budapest Convention and the General Data Protection Regulation: acting in concert to curb cybercrime? *Int. Cybersecur. Law Rev.* 1, 2020, pp. 63–72, <https://doi.org/10.1365/s43439-020-00012-5>
- [14] Convention on Cybercrime. Budapest, ETS No.185. 2001, <https://www.coe.int/en/web/conventions/full-list/-/conventions/treaty/185>.
- [15] Luhanovskaya E. Protyvodeystvye kyberprestupnosti: pravyla korporatyvnoy zashchyty [Countering cybercrime: rules of

- corporate protection]. URL: <https://www.epravda.com.ua/rus/columns/2019/05/15/647756/> (in Ukrainian).
- [16]Galinec D., Luic L., Design of Conceptual Model for Raising Awareness of Digital Threats, *WSEAS Transactions on Environment and Development*, Volume 16, 2020, pp. 493-504.
<https://doi.org/10.37394/232015.2020.16.50>
- [17]Börösök J., Schwarz M., Hafiz M. Ikram, Abdelawwad M., Alsuleiman A., Safe Position Detection Based on Safety System-on-Chip (SSoC) for Wireless IoT Application, *International Journal of Circuits, Systems and Signal Processing*, Vol. 14, 2020, pp. 1040-1046, <https://doi.org/10.46300/9106.2020.14.132>
- [18]Onwujekwe G., Thomas M.A., Osei-Bryson K.M. (2019) Using Robust Data Governance to Mitigate the Impact of Cybercrime. Proceedings of the 2019 3rd International Conference on Information System and Data Mining, April 2019 Pages 70–79. <https://doi.org/10.1145/3325917.3325923>
- [19]Hladkova Y.E. (2018) Protydiya zlochynnosti [Countering crime]. URL: <https://visnikkau.webnode.com.ua/news/protydiya-zlochynnosti/> (in Ukrainian).
- [20]Lytvynov O. (2018) Mekhanizm protydyi zlochynnosti [The mechanism of combating crime]. URL: <https://visnikkau.webnode.com.ua/news/mekhanizm-protidiji-zlochynnosti/> (in Ukrainian).
- [21]Shvets' D. (2017) Derzhavni mekhanizmy borot'by z kiberzlochynnyu [State mechanisms to combat cybercrime]. Aktual'ni pytannya protydyi kiberzlochynnosti ta torhivli lyud'my. Kharkiv, 2017. URL: file:///C:/Users/comp/Desktop/KmOixYXfgKGkCo_xYW-6ykD56dEesLfv.pdf (in Ukrainian).
- [22]Craig D., Diakun-Thibault N., Purse R. (2014) Defining Cybersecurity. *Technology Innovation Management Review*. URL: <https://timreview.ca/article/835>.
- [23]Kigerl A. Cyber Crime Nation Typologies: K-Means Clustering of Countries Based on Cyber Crime Rates. *International Journal of Cyber Criminology*. 2016. Vol. 10 (2): 147–169. DOI: 10.5281/zenodo.163399/ IJ
- [24]Lewis J. (2018) Economic Impact of Cybercrime – No Slowing Down. Center for Strategic and International Studies (CSIS), McAfee. 2019, <https://cdw-prod.adobe.com/content/dam/cdw/on-domain-cdw/brands/mcafee/economic-impact-of-cybercrime-not-slowing-down.pdf>
- [25]Cyber Risk Index. NordVPN. 2020, <https://nordvpn.com/ru/cri/>
- [26]Webroot Threat Report. Phishing Attempts Grew by 640% Last Year. 2020, <https://community.webroot.com/news-announcements-3/2020-webroot-threat-report-phishing-attempts-grew-by-640-last-year-342560>.
- [27]Common challenges in combating cybercrime. Europol and Eurojust, 2019, <https://www.europol.europa.eu/publications-documents/common-challenges-in-combating-cybercrime>.
- [28]Cyberthreat Defense Report, CyberEdge Group, 2020, <https://cyber-edge.com/wp-content/uploads/2020/03/CyberEdge-2020-CDR-Report-v1.0.pdf>.
- [29]PricewaterhouseCoopers. Fighting fraud: A never-ending battle. *PwC's Global Economic Crime and Fraud Survey*, 2020, <https://www.pwc.com/fraudsurvey>.
- [30]International Telecommunication Union. Global Cybersecurity Index 2018, https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf.
- [31]Cybercrime Legislation Worldwide. United Nations, UNCTAD. <https://unctad.org/page/cybercrime-legislation-worldwide>
- [32]Lewis J. The Economic Impact Of Cybercrime And Cyber Espionage. Center for Strategic and International Studies (CSIS), McAfee. http://csis-website-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/60396rpt_cybercrime-cost_0713_ph4_0.pdf
- [33]The 2020 Official Annual Cybercrime Report. Cybersecurity Ventures, <https://www.herjavecgroup.com/the-2019-official-annual-cybercrime-report/>
- [34]Srivastava S.K., Das S., Udo G.J., Bagchi K. Determinants of Cybercrime Originating within a Nation: A Cross-country Study *Journal of Global Information Technology Management*, 2020, <https://doi.org/10.1080/1097198X.2020.1752084>
- [35]Zaharia A. 300+ Terrifying Cybercrime and Cybersecurity Statistics & Trends, <https://www.comparitech.com/vpn/cybersecurity-cyber-crime-statistics-facts-trends/>.

**Creative Commons Attribution
License 4.0 (Attribution 4.0
International , CC BY 4.0)**

This article is published under the terms of the
Creative Commons Attribution License 4.0
[https://creativecommons.org/licenses/by/4.0/deed.en
_US](https://creativecommons.org/licenses/by/4.0/deed.en_US)