CYBERCRIME AS A THREAT TO UKRAINE'S NATIONAL SECURITY

Nataliia Varenia [1], Ihor Avdoshyn[2], Lilia Strelbytska[3], Mykola Strelbytskyy[4], Maksym Palchyk[5],

[1,2,3,4,5] National Academy of Security Service of Ukraine, Kyiv, Ukraine

Summary.

The information space, the main components of which are information resources, means of information interaction, and information infrastructure, is a sphere of modern social life in which information communications play a leading role.

The objective process is the gradual but stable entry of the national information space into the European and world information sphere, in the context of which there is a legitimate question of its protection as one of the components of the national security of Ukraine. However, the implementation of this issue in practice immediately faces the need to respect the rights and fundamental freedoms guaranteed by international regulations and the Constitution of Ukraine, especially in the field of cybersecurity.

The peculiarity of the modern economy is related to its informational nature, which affects the sharp increase in cyber incidents in the field of information security, which is widespread and threatening and affects a wide range of private, corporate, and public interests. The problem of forming an effective information security system is exacerbated by the spread of cybercrime as a leading threat to information security both in Ukraine and around the world.

The purpose of this study is to analyze the state of cybersecurity and on this basis to identify new areas of the fight against cybercrime in Ukraine.

Methods: the study is based on an extensive regulatory framework, which primarily consists of regulatory acts of Ukraine. The main methods were inductions and deductions, generalizations, statistical, comparative, and system-structural analysis, grouping, descriptive statistics, interstate comparisons, and graphical methods.

Results. It is noted that a very important component of Ukraine's national security is the concept of "information terrorism", which includes cyberterrorism and media terrorism that will require its introduction into the law. An assessment of the state of cybersecurity in Ukraine is given. Based on the trend analysis, further growth of cybercrimes was predicted, and ABC analysis showed the existence of problems in the field of security of payment systems. Insufficient accounting of cybercrime and the absence in the current legislation of all relevant components of cybersecurity does not allow the definition of a holistic system of counteraction. Therefore, the proposed new legal norms in the field of information security take into account modern research in the field of promising areas of information technology development and the latest algorithms for creating media content.

Keywords: *cybercrime, cybersecurity, offenses, prevention, Ukraine*.

1. Introduction

Modern conditions for the development of the information economy have formed cyberspace, which involves more and more legal entities, and individuals, which is reoriented by many entities, including for public administration, public and commercial services. Therefore, cyberspace needs an appropriate mechanism of development, which provides for its functioning and appropriate protection. The mismatch between the level of protection of national and interstate cyberspace can lead to paralysis of entire states, regions, etc. (Buddko, 2015).

The peculiarity of the modern economy is related to its informational nature, which affects the sharp increase in cyber incidents in the field of information security, which is widespread and threatening and affects a wide range of private, corporate, and public interests. The problem of forming an effective information security system is exacerbated by the spread of cybercrime as a leading threat to information security in Ukraine and around the world. A significant impact on cyberspace was recorded in 2017 when hackers massively attacked large institutions and organizations around the world 2017 (Irwin, 2018). All this raises the issue of studying and overcoming the manifestations of cybercrime. At present, no country can function without the foundations of the digital economy, but this also causes new risks and threats (Irwin, 2018).

The study aims to form an effective system of measures to combat and combat cybercrime in Ukraine.

To achieve this goal, it is proposed to consider the following research objectives:

- to investigate cybersecurity in Ukraine;
- to analyze the state of cybercrime in Ukraine;

Manuscript received May 5, 2021
Manuscript revised May 20, 2021
https://doi.org/10.22937/IJCSNS.2021.21.5.13

- identify the need to improve the fight against cybercrime in Ukraine.

2. Literature Review

The world community has entered a digital age where technology is constantly evolving and pervasive. The development of technological innovations facilitates our daily lives. However, they also contribute to crime. Cybercrime has become a serious problem around the world. Therefore, research is relevant to correspond to reality, not to lag behind the current state of affairs. There is a great need for more scientists to be involved in cybercrime prevention and cybersecurity research. It is also particularly important to consider this topic at an interdisciplinary level. The work requires not only a criminological lens but also many objectives: economic, financial, legal, sociological, and political, to be able to comprehensively understand the impact of cybercrime around the world and within countries. As half of all Internet users are in Asia, there is a growing need to encourage researchers to research cybersecurity and cybercrime in the Asia-Pacific region (Broadhurst & Chang, 2013).

COVID-19 induced changes in daily life are contributing to a wider transformation in cybercrime. Society is likely to experience an increase in the number of victims of cybercrime and offenders entering its land borders, so the role of the police needs to change. The cybercrime literature has consistently highlighted this role, which has become unquestionable orthodoxy. The capacity of the police to combat cybercrime is limited by its global nature, the geographical boundaries of police jurisdictions, the complexity and cost of transnational investigations, the limited resources and values inherent in "policing culture" for "genuine policing" (Yar and Steinmetz, 2019; Boes and Leukfeldt; 2016; Yar, 2013).

Cherep, Saenko (2021) defining information security (IS) as a component of national security (NS), note that it is necessary to use a full range of monitoring and forecasting mechanisms and has its specifics. In particular, it is noted that IS is one of the new technology sectors of security and is based on the use of modern information technologies (IT). Besides, IS is considered in two aspects: technical (cybersecurity and cyber warfare, others) and ideological (propaganda and information wars, etc.).

Dovgan` and Tkachuk (2018) research is devoted to providing IS of the person, society, the state. It notes that IS is a sub-branch of information law due to a separate subject of legal regulation, a separate legal regime and is characterized by the systematic application of industry-specific methods of legal regulation, significant integration, and specialization of legal institutions that make it up (regulate specific social relations arising from protection information with limited access, licensing of information protection activities, as well as rules governing liability for offenses in the information sphere).

The publication Varen`ya ta Avramenko (2020) is devoted to this area of the NS, in particular in terms of information terrorism and its components - cyberterrorism and media terrorism, as well as forecasting vectors of terrorist threats in the media space.

Therefore, the monitoring data, conclusions, and reconstructions provided by the IS are the basis for forecasting in the entire NS sector.

Chandraa, Snoweb (2020) formed a theoretical taxonomy of cybercrime. The need to systematize cybercrime stems from the lack of definitions and standards for measuring and managing cybercrime. They point to cybercrime as an act in which computer technology is used to commit a crime. The four components of the taxonomy include mutual exclusivity, structure, completeness, and clearly defined categories that provide a theoretical basis.

The findings of domestic researchers of the law indicate a similar relationship. Foros and Kondrasheva (2016) state that "cybersecurity is the security of information and infrastructure in the digital environment" and "information security allows to achieve such goals as information confidentiality; integrity of information and related processes; availability of information; monitoring of all such processes". First, there are similarities between the definition of IS and the corresponding category of crimes of the Council of Europe Convention on Cybercrime. However, without even emphasizing the similarities, the definitions of IS and cybersecurity certainly indicate that the two concepts are intertwined.

The same conclusion was reached by Kosarevs`ka and Novy`cz`ky`j (2016), who talk about the threats of IS, which are manifested through the negative information impact on the conscience and behavior of citizens, as well as through the impact on information resources and information infrastructure. They continue such statements as "guaranteeing effective counteraction to cybercrime can be achieved only through the application of integrated approaches to information security" and "counteraction to cybercrime should be an element of state information security policy".

However, other researchers note that there is no understanding of cybercrime. They are referred sometimes to as "electronic crime", "computer crime", "high-tech crime", "technological crime", "electronic crime", or "cybercrime" (Chang, 2012).

The PwC World Economic Crime Survey used the following definition of cybercrime: "Cybercrime (or "computer crime") is an economic crime committed using computers and the Internet."

The increased risk of cybercrime was explained by media coverage of cyberattacks; ambiguous definition of cybercrime; increased attention from regulators and the use of the latest technologies that "facilitate" the commission of cybercrime.

Thus, Kravczova (2018), specifying the definition for Ukrainian realities, proposes to determine the criminal scope of the concept of "cybercrime" crimes under Articles 361, 361-1, 361-2, 362, 363, 363-1 of the Criminal Code of Ukraine, which contain in Chapter XVI "Crimes in the use of electronic computers (computers), systems and computer networks and telecommunications networks." Moreover, cybercrime means a socio-legal phenomenon that manifests itself in the prohibited by law on criminal liability substantive activity (criminal activity) of the population using computers (telecoms), telecommunications systems, computer networks, and telecommunications networks.

Yelyevceva (2020) researched the legal issues of application and separation of legal regimes for the cybersecurity of Ukraine and proposed directions for developing a system of legal regimes for cybersecurity.

Yacenko, Ismajlov (2016) rightly note that the investigation of crimes in information networks requires rapid analysis and preservation of computer data, which are very vulnerable and can be destroyed quickly. Therefore, the speed of decision-making and action is crucial, but problematic, especially in cases of investigation of transnational cybercrimes. Thus, cybercrime requires more comprehensive, intensive, and systematic international cooperation than existing measures to combat any other form of transnational crime.

International cooperation in the fight against cybercrime is carried out to: personalize the identity of the offender, determine the jurisdiction and choose the most adequate legal influence on the offender to bring him to justice for committing such a crime (Skuly`sh, 2014).

Dubovy` (2018) has comprehensively studied the international experience of public-private partnerships in the field of cybersecurity, which, based on a study of cybersecurity practices in the US, EU, Germany, UK, and Poland, proposes building trust between the public and private sectors on cybersecurity.

Streltsov (2017) notes several key features of the Ukrainian state's approach to cybersecurity. Among them: a clear understanding of the importance of protecting interests related to cyberspace, among other things, also identifying cybersecurity as one of the key areas of national security; understanding cybersecurity as a function of threat-based risk management and adopting a systematic approach to cybersecurity. Thus, he emphasizes that the creation of an effective cybersecurity system is possible through the coordination of various sectoral policies and the use of opportunities of different actors, both public and private.

At the same time, cybersecurity should not be equated with combating cybercrime and criminal law or law enforcement agencies should be given more obligations than they can fulfill, further accusing them of inefficiency, incompetence, or corruption.

Shvedova (2019) points out the corruption risks that pose the most serious threat to the stable and secure operation of many critical infrastructure facilities.

In the field of cybersecurity in many post-Soviet countries, including Ukraine, Marutian (2017) considers it appropriate to note such problem areas as:
lack of CERT coordination centers;
low level of standardization for organizations;
safety of children in cyberspace;
lack of incentive mechanism for the industry;
interdepartmental cooperation.

Syomych, Markina, Diachkov (2018) add to this list:
lack of unification of the categorical apparatus in the legislation of the country in the field of cybercrime;
lack of relevant specialists in the field of cybersecurity;
lack of cybersecurity standards in organizations and professional standards in this area;
lack of sectoral cybersecurity centers;
lack of generally accepted national benchmarking and references for measuring cybersecurity;
the difficulty of identifying, investigating, and disclosing information about cybercrime.

Thus, cybercrime is a current problem that encourages research, as there is a significant threat that can come from any country in the world and go beyond a specific jurisdiction, unlike many other traditional types of economic crime. However, in recent years, insufficient attention has been paid to assessing the state of cybercrime, ensuring cybersecurity, and finding a way to overcome it.

3. Methods

The study is based on an extensive regulatory framework, which primarily consists of regulatory acts of Ukraine. The main methods were induction and deduction, generalization, statistical, comparative, and system-structural analysis, grouping, descriptive statistics and interstate comparisons, graphical method. Given the dynamics of cybercrime in Ukraine was used to predict the polynomial trend line in Excel. This is because this curve is characterized by variables of increase and decrease. For polynomials (polynomials) the number of maximum and minimum values) determines the degree. For example, one extremum (minimum and maximum) is the second degree, two extremums are the third degree, and three are the fourth. The polynomial trend in Excel is used because the crime rate is unstable.

Also, to identify priorities in crimes committed in Ukraine, the ABC analysis, which was conducted in 2019, was used. Note that such an analysis would be appropriate for the cyber police to use regularly to ensure that any trends in crime can be identified and responded to promptly. It should also be supplemented by other methods of analysis, as it takes into account previous rather than current statistics, and requires improvement of the quality and completeness of recorded information on cybercrime and its updating and maintenance in a register of various entities monitoring the study area.

4. Results

To get a clearer view of the object of analysis, it is first necessary to find out what the Ukrainian state provides cybersecurity in legal and organizational perspectives and what its condition is. Unfortunately, this is a difficult task, partly due to the uncertainty in the established relationship between IS and cybersecurity in Ukraine. We consider the latter as part of the first, which, in turn, is an element of the NS.

The analysis of the current legislation allowed forming the subjective composition of cybersecurity:

national level: State Service for Special Communications and Information Protection of Ukraine (Governmental CERT-UA); Security Service of Ukraine; Ministry of Internal Affairs of Ukraine (National Police); Ministry of Defense of Ukraine (General Staff of the Armed Forces of Ukraine), intelligence agencies of Ukraine; The National Bank of Ukraine and other entities specified by current legislation;

international level: Organization of economic cooperation and development; Interpol; Group Eight (G8), Council of Europe, UN, etc.

The study of the legal framework for cybersecurity in Ukraine demonstrates the multilevel and diversified regulation, in particular: supranational regulation through international acts (UN General Assembly Resolution /2 71/28 of 05.12.2016; Council of Europe Convention on Cybercrime (hereinafter - the Convention), Association Agreement between Ukraine and the European Union, Cybercrime@EaP project within the Eastern Partnership), and national regulation (Constitution of Ukraine; Criminal Code of Ukraine, Laws of Ukraine "On Basic Principles of Cyber Security of Ukraine", "On Information Protection in Information and Telecommunication Systems", "On Basic Principles of Domestic and Foreign Policy" and " On National Security of Ukraine ", decrees of the President of Ukraine" On the National Security Strategy of Ukraine "," Cyber Security Strategy of Ukraine ", " Doctrine of Information Security of Ukraine "," On the Concept of Combating Terrorism in Ukraine", resolutions of the Cabinet of Ministers of Ukraine; cybersecurity).

Concerning the object structure of cybersecurity, the Convention defines the following offenses against the confidentiality, integrity, and availability of computer data and systems:

crimes in the field of illegal access to information: illegal interception (Article 3), interference with data (Article 4), interference with the system (Article 5), abuse of devices (Article 6);

crimes related to the illegal use of computers: counterfeiting related to computers (Article 7), fraud related to computers (Article 8);

crimes related to the content, which include the creation, distribution, and storage of child pornography (Article 9);

crimes related to the infringement of copyright and related rights (Article 10).

The closest definition in Ukrainian legislation is cyberterrorism - terrorist activity carried out in cyberspace or with its use (Law of Ukraine "On Basic Principles of Cyber Security of Ukraine", 2017). Nevertheless, it does not cover the required range. Thus, the current activities of terrorist organizations can use as media influence:

- terrorist acts or artificial leaks of information about alleged preparation for such acts;
- criminal offenses not related to terrorist acts;
- man-made accidents and catastrophes that occurred without the intervention of terrorists;
- events modeled and visualized through artificial intelligence using virtual and/or augmented reality (deepfakes);
- any combination of all of the above.

Besides, it is necessary to single out the general direction of building a counter-terrorist narrative, which will not be to artificially create a "script" or "version" but to determine the direction of information intervention, search for groups loyal to the vector we need, which would create high-quality products and their management.

Therefore, it is necessary to rethink the existing definitions of defining the phenomenon of terrorism in the context of expanding the concept of cyber-terrorism/cybercrime to a more general term: information terrorism, which will include a technical and media component - cyber and media terrorism.

Given the above, we propose to amend the Law of Ukraine "On Basic Principles of Cyber Security of Ukraine", namely to introduce the definition of information terrorism as a general term that would include two areas:

1) cyberterrorism (as one aimed at destroying or damaging computer networks, unauthorized interference in their work, destruction or distortion of information in databases, etc.);
2) media terrorism (which uses the information space to artificially change the level of social tension and exert psychological pressure through the dissemination of knowingly unreliable or artificially modeled information in cyberspace).

Therefore, it is expedient to introduce the definition of information (or media) intervention - artificial information influence through the means of disseminating information to exert very psychological pressure, destabilize society, and influence its background emotional state and mentality. In 2020, the Ministry of Justice developed a draft Action Plan between Ukraine and the EU in the field of justice and home affairs: a practical result by 2025, but the issue of IS, information intervention is not sufficiently presented in the document. It is also advisable to single out and detail this area in the new Cyber Security Strategy for the period up to 2025 and the action plan for its implementation. As part of the implementation of the EU institution building tools Twinning and TAIEX, it is planned to implement projects, including in IS:

to strengthen the capacity of the main actors in the electoral process by organizing exercises on cybersecurity and countering disinformation activities;

on training in the field of information and cybersecurity for state bodies of Ukraine;

on the development of cooperation in the field of research and innovation in the field of cybersecurity.

Let us assess the current state of affairs in Ukraine in the field of cybersecurity. Thus, in the PwC survey "Global Economic Crime and Fraud 2018: Results of Ukraine", cybercrime is one of the main economic crimes, affecting 31% of organizations in Ukraine in 2018.

Various indicators of implemented measures in the field of protection of computer and telecommunication networks from cyber-attacks and creating conditions for the safe operation of cyberspace are evaluated and used to monitor and compare the state of cybersecurity in different countries in annual international rankings, the most authoritative of which is the Global Cybersecurity Index. Global Cybersecurity Index, GCI) and the National Cyber Security Index (NCSI). These cybersecurity indices are a kind of risk indicator for corporate, industrial, and government information infrastructure due to the range of cyber threats.

Table. Ukraine in the cybersecurity rankings

Indicator	2017	2018	2019	2020
Global Cyber security Index	59	54	No data	54
National Cyber Security Index	No data	29	28	25
ICT Development Index	79	No data	No data	79
Networked Readiness Index	No data	No data	67	64

Source: summarized by the author

According to these ratings, Ukraine has slightly improved its position in the country's cybersecurity, but the availability and use of ICT, as well as practical skills in the use of ICT by the population, are insufficient. Among the plans of the Government of Ukraine are approval of procedures for compiling lists of critical infrastructure and critical information infrastructure facilities, as well as for organizing a review of the state of cyber protection of state information resources and critical information infrastructure. However, military cyber operations, incident, and cyber crisis management, protection of electronic services, analysis, and informing the public about cyber threats are not sufficiently addressed in regulations.

Determining the current state of cybercrime in Ukraine, we assess this social phenomenon through criteria that reflect its quantitative and qualitative characteristics, in particular by analyzing the prevalence of cybercrime in Ukraine: its level, structure, and more. Regarding the level of cybercrime and its dynamics, it should be noted that the field of the use of computers, systems, and computer networks, and telecommunications networks in Ukraine was studied according to the Prosecutor General of Ukraine (Unified Report on Criminal Offenses) in Fig.1.

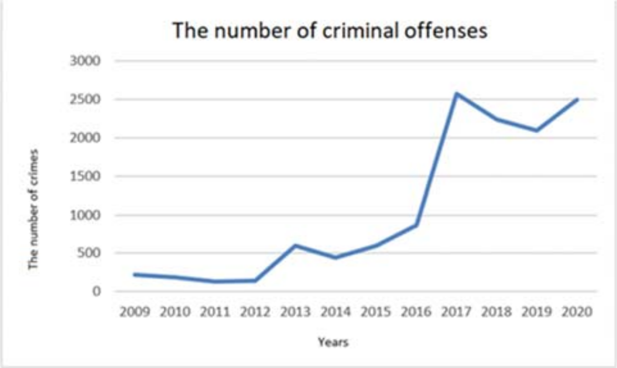

Figure 1. The state of crime in the use of electronic computers, systems, and computer networks and telecommunications networks in Ukraine

Source: data of the Prosecutor General of Ukraine (Unified Report on Criminal Offenses); Kravtsova, M.O. The current state and directions of combating cybercrime in Ukraine/Maryna Kravtsova // Bulletin of the Criminological Association of Ukraine. - 2018. - № 2 (19). - P.155-166.

Such trends have developed under the influence of several factors. Among the main ones are the following: the significant pace of informatization of society; technical backwardness of the law enforcement system and the need to reform it, insufficient funding for cybersecurity measures. The outstripping growth of registered cybercrimes has led to an increase in their share in the total number of crimes in Ukraine, maintaining trends of increase from 0.05% in 2009 to 0.69 in 2020, which is the highest figure since 2009 (Fig. 2).

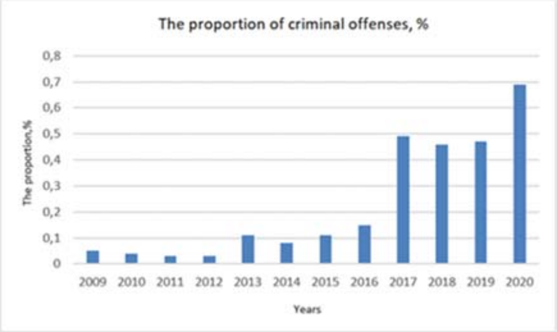

Figure 2. The share of cybercrime in the total number of registered crimes.

Source: data of the Prosecutor General of Ukraine (Unified Report on Criminal Offenses); Kravtsova, M.O. The current state and directions of combating cybercrime in Ukraine/Maryna Kravtsova//Bulletin of the Criminological Association of Ukraine. - 2018. - № 2 (19). - P.155-166

The significant increase in the number of cybercrimes registered in 2017 in Ukraine is the result of mass attacks by hackers around the world. It is expedient to point out the fact that the registration of registered crimes was transferred in the state from the Ministry of Internal Affairs to the General Prosecutor's Office of Ukraine.

As we can see from the obtained crime statistics, cybercrimes have a significant positive increase (Fig. 3).

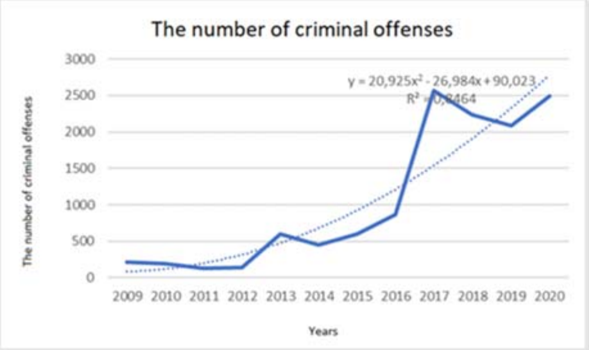

Figure 3. Cybercrime forecasting in Ukraine

Source: data of the Prosecutor General of Ukraine (Unified Report on Criminal Offenses); Kravtsova, M.O. The current state and directions of combating cybercrime in Ukraine/Maryna Kravtsova//Bulletin of the Criminological Association of Ukraine. - 2018. - № 2 (19). - P.155-166

The analysis of the structure of cybercrimes in the dynamics allowed to the state during 2016-2020 the largest share of crimes committed under Article 361 of the Criminal Code of Ukraine:

- unauthorized interference in the work of electronic computers (computers), automated systems, computer networks, or telecommunication networks (from 49 to 57%);
- unauthorized actions with information processing in computers, automated systems, computer networks, or stored on the media of such information, committed by a person who has the right to access it (from 35% to 42%) (Table 1).

Besides, it is due to these crimes that there is an overall increase in the dynamics of cybercrime.

Table 1. Accounted for criminal offenses under Articles Sec. XVI of the Criminal Code of Ukraine (according to the Prosecutor General's Office of Ukraine)

Recorded criminal offenses in the report period	2016	2017	2018	2019	2020
Unauthorized interference in the operation of computers, automated systems, computer networks, or telecommunication networks (Article 361 of the Criminal Code of Ukraine)	494	1795	1007	1137	1146
Creation for use, distribution, or sale of malicious software or hardware, as well as their distribution or sale (Article 361-1 of the Criminal Code of Ukraine)	15	35	134	185	112

Unauthorized sale or dissemination of information with limited access, which is stored in computers, automated systems, computer networks, or on media of such information (Article 361-2 of the Criminal Code of Ukraine)	28	64	38	40	88
Unauthorized actions with information that is processed in computers, automated systems, computer networks or stored on media of such information, committed by a person who has the right to access it (Article 362 of the Criminal Code of Ukraine)	311	670	1042	717	980
Violation of the rules of operation of computers, automated systems, computer networks, or telecommunication networks or the procedure or rules for the protection of information processed in them (Article 363 of the Criminal Code of Ukraine)	15	6	10	5	9
Interference with the work of electronic computers (computers), automated systems, computer networks, or telecommunication networks through the mass distribution of telecommunication messages (Article 363-1 of the Criminal Code of Ukraine)	2	3	10	4	3
Together	865	2573	2241	4107	2338

Source: summarized by the author based on the data of the Prosecutor General of Ukraine (Unified Report on Criminal Offenses)

The next no less important step is to determine the types of cybercrime that will pose the greatest danger, for this, we will use the method of ABC analysis.

To solve this problem, we will conduct an ABC analysis using the "sum" method based on the statistical data of the report of the Head of the National Police in Ukraine for 2019. We summarize the results in Table. 2.

Table 2. ABC analysis of cybercrime

Cybercrime	Number	Part of the factors and the sum of the data factor values, %	The increasing importance PA, %	The increasing value of CHO,%	The sum of CHO and PA,%	Group
in the field of payment systems	1641	38,96936595	38,96936595	25	63,96936595	A
in the field of e-commerce	744	17,66801235	56,63737783	50	106,6373778	B
in the field of cybersecurity	1494	35,47850867	92,1158869	75	167,1158869	B
in the field of illegal content	332	7,884113037	100	100	200	C

Source: *based on data from the Report of the Head of the National Police of Ukraine on the results of the department in 2019*

Summarizing the results obtained, we note that the most vulnerable in Ukraine in 2019 is the field of payment systems. Implementing countermeasures in it can reduce the number of cybercrimes by almost 40% of all possible.

In particular, the NBU intends to set clear requirements for payment market participants regarding information protection and cybersecurity systems and streamlining of actions in the detection of cyber-attacks that reduce the reliability of payment systems. The state regulator intends to introduce a risk-oriented approach to information protection, depending on the number of possible losses; improving the use of information security, access control policy, strengthening IS in the field of money transfer (draft resolution of the Board of the National Bank of Ukraine on approval of the Regulation "On information protection and cybersecurity in payment systems").

The real state of cybercrime is difficult to assess, as there is no legal definition of media terrorism, full generalized statistics are not kept, and only for individual entities and certain periods is incomparable. Also ignored is the fact that cybercrime is characterized by a high level of latency.

A serious problem is the widespread use of artificial intelligence systems - computer systems or programs that mimic one or more aspects of intellectual behavior, which have a higher degree of self-determination (autonomy) and independence from the will of the developer or user compared to other computer systems or programs. Some intelligent systems are capable of learning and self-learning. Already, such systems can be actively used to identify the weaknesses of potential victims of fraud, as well as to simulate human activity. They threaten the entire existing public order, provoking an "information apocalypse" (Stover, 2018), in which the fact becomes indistinguishable from fiction, and people stop trying to understand the difference. This undermines the credibility of any information and can destabilize society.

At the current stage of overcoming cybercrime in Ukraine, taking into account the political situation and threats from Russia, information terrorism, which includes cyberterrorism and media terrorism, as an important component of IS and NS, has become relevant. Insufficient attention to this area forms the foundation for cyber threats, needs to be ensured in the context of anti-terrorist security, in particular regarding information and legal regulation, training of specialists with legal education in combating media terrorism, management of anti-terrorist security in the conditions of development of virtual media.

According to the established hypothesis, it is determined that the effectiveness of the fight against cybercrime in Ukraine primarily depends on the anti-terrorist component, which is not given enough attention. Therefore, a promising area of research is the detailed development of a program of actions necessary for the formation of an additive mechanism for anti-terrorist security and cyber protection of the domestic information space. Thus, the fight against media terrorism is the newest direction of the national system of combating terrorism in the information sphere. Only if the proposed changes are made, the more correct and detailed adjustment of the legal framework in terms of responsibility for the implementation of acts of media terrorism. More importantly, in the field of preventive measures, change the principles of analysis of information space monitoring to identify signs of media space on the media-terrorism, the creation of an appropriate procedure for carrying out operational and investigative actions in this area, etc.

5. Discussion

Further digitalization of the economy is expected to increase cybercrime. This will be a consequence of the fact that legal entities and individuals will fully use electronic services and use the capabilities of information storage (Nikolina, Gulivata, 2020) confirmed this thesis by modeling the introduction of digitalization in the economy. The COVID-19 crisis has led to changes in the interests, needs, and daily lives of the population, and this has opened up new opportunities for cybercriminals trying to adapt and take advantage of the situation, mainly through adaptations related to changing goals and cyberspace. In particular, this is due to the increase in information interactions for remote work, intensification of non-cash payments, and psychological pressure on citizens.

In particular, Dubov (2021) notes that further escalation of panic may be one of the goals of influence operations by other states that may wish to take advantage of the situation. He also proposed a new version of the Cyber Security Strategy of Ukraine, which should be based on the National Security Strategy of Ukraine, which was adopted in 2020, and identified the following 9 blocks of strategic goals:

effective cyber defense;
development of asymmetric deterrence instruments and international cooperation;
reduction of cybercrime capabilities, in particular, the impossibility of using cybercriminals by foreign states to carry out hostile military-political actions and against the security of the state as a whole;
national cyber readiness;
training and professional development;
cyber awareness and cyber hygiene;
formation of a cybersecurity ecosystem;
the service model of state participation in cybersecurity issues;
transparency and accountability.

It is also worth agreeing to his proposal to expand the range of actors providing cybersecurity, including the Ministry of Foreign Affairs of Ukraine, the Ministry of Education and Science of Ukraine, the Ministry of Digital Transformation of Ukraine, sectoral ministries (in terms of defining tasks and policies), National Academy Sciences of Ukraine and other institutions.

6. Conclusions

Summing up, we note that Ukraine has recognized cybercrime as a major threat to national security and stability. However, the processes of globalization in post-industrial society, despite certain centrifugal tendencies, continue to accelerate, due in part to the increasing informatization of human civilization. This also applies to extremist and terrorist crimes, which are becoming increasingly transnational.

The risk of intimidation of public authorities, local governments, or international organizations related to intimidation and/or violence through the misuse of information and telecommunications technologies, i.e. cyberterrorism. Thus, social networks, messengers, video hosting services, video broadcasts, and other resources provide unprecedented opportunities for organizing mass riots.

The ability to use various Internet resources to conduct special information operations, from news agencies and public opinion leaders to the use of completely artificial, fake accounts, now allows Russia to relatively, constantly, and cheaply create constant information pressure on Ukraine, so cyberspace is recognized as a new space for military action.

References

[1] Badyuk, M.O., Fopoc, G.B. (2016). Deyaki acpekty` shhodo ppoblem zapobigannya ta ppoty`diyi kibepzlochy`nnocti [Some aspects of the problems of prevention and counteraction of cybercrime] Kibepbezpeka v Ukpayini: ppavovi ta opganizaczijni py`tannya: matepialy` vceykp. nayk.-ppakt. konf., m. Odeca [Cybersecurity in Ukraine: legal and organizational issues: materials all. nayk.-ppakt. konf., m. Odeca] 233[in Ukrainian]

[2] Boes, S. and Leukfeldt, E. (2016). Fighting cybercrime: A joint effort, Clarke, R. and Hakim, S. (Eds) Cyber-Physical Security, Springer, London, 185-203.

[3] Broadhurst, R., & Chang, L. Y. C. (2013). Cybercrime in Asia: Trends and Challenges. In J. Liu, B. Hebenton, & S.Jou (Eds.), Handbook of Asian Criminology (49–63). New York: Springer

[4] Buddko, M. V. (2015). Cybercrime as a threat to the world economy generated by informatization. Economy and society, 2-1(15), 776-779. (In Russian)

[5] Chandraa, A., Snoweb, M. J.A(2020). Taxonomy of cybercrime: Theory and design International Journal of Accounting Information Systems. 38, 100467 https://doi.org/10.1016/j.accinf.2020.100467

[6] Chang, L. Y. C. (2012). Cybercrime in the Greater China Region: Regulatory responses and crime prevention across the Taiwan Strait. Cheltenham: Edward Elgar Publishing.). 272

[7] Cherep, O. H., Saenko, M. V. (2021). Problematic issues of cybersecurity and ways of overcoming cybercrime in Ukraine. Bulletin of Zaporizhzhia National University. Economic sciences. 1 (49) DOI https://doi.org/10.26661/2414-0287-2021-1-49-25

[8] Constitution of Ukraine (1996) https://zakon.rada.gov.ua/laws/show/254%D0%BA/96-%D0%B2%D1%80#Text[in Ukrainian]

[9] Convention on Cybercrime (2005) https://zakon.rada.gov.ua/laws/show/994_575#Text [in Ukrainian]

[10] Criminal codex of Ukraine (2001) https://zakon.rada.gov.ua/laws/show/2341-14#Text[in Ukrainian]

[11] Decree of the President of Ukraine (2016) About the CyberSecurity Strategy of Ukraine https://zakon.rada.gov.ua/laws/show/96/2016#Text [in Ukrainian]

[12] Decree of the President of Ukraine (2017) Doctrine of information security of Ukraine http://www.president.gov.ua/documents/472017-21374 [in Ukrainian]

[13] Decree of the President of Ukraine (2019) About the Concept of Counter-Terrorism in Ukraine https://zakon.rada.gov.ua/laws/show/53/2019#Text [in Ukrainian]

[14] Decree of the President of Ukraine (2020) On the National Security Strategy of Ukraine https://www.president.gov.ua/documents/3922020-35037 [in Ukrainian]

[15] Department of Justice (2020). Proyekt Planu dij mizh Ukrayinoyu ta YeS u sferi yusty`ciyi ta vnutrishnix sprav: prakty`chny`j rezul`tat do 2025 roku [Draft Action Plan between Ukraine and the EU in the field of Justice and Home Affairs: practical outcome by 2025] https://minjust.gov.ua/m/proekt-planu-diy-mij-ukrainoyu-ta-es-u-sferi-yustitsii-ta-vnutrishnih-sprav-praktichniy-rezultat-do-2025-roku [in Ukrainian]

[16] Dovgan,` O.D., Tkachuk T.Yu. (2018). Pravove zabezpechennya informacijnoyi bezpeky` derzhavy` yak pidgaluz` informacijnogo prava: teorety`chny`j dy`skurs [Legal provision of information security of the state as a branch of information law: theoretical discourse] Information and law 2(25). 73-85 [in Ukrainian]

[17] Dubov, D. (Ed.) (2018). Derzhavno-pry`vatne partnerstvo u sferi kiberbezpeky`: ta mozhly`vosti dlya krayiny`[Public-private partnership in the field of cybersecurity: and opportunities for the country] : analit. dop. K.: NISD. 84 [in Ukrainian]

[18] Dubov, D.V. (2020). FORMUYuChY` NOVU STRATEGIYu KIBERBEZPEKY` UKRAYiNY`: ChY` MOZhEMO UNY`KNUTY` POMY`LOK PERShOYi SPROBY` STRATEGUVANNYa?`[FORMING A NEW CYBER SECURITY STRATEGY IN UKRAINE: CAN

WE AVOID THE ERRORS OF THE FIRST ATTEMPT TO STRATEGY?] https://niss.gov.ua/sites/default/files/2021-01/tezy-dubov-2.pdf [in Ukrainian]

[19] Dybov, D. B. (2014). Kibepppoctip yak novy`j vy`mip geopolity`chnogo cypepny`cztva Cyberprocity as a new dimension of geopolitical society]: monogpafiya K .: HICD, 328[in Ukrainian]

[20] Fopoc G.B. Kondpasheva K.C. Infopmaczijne cycpil`ctvo ta kibepbezpeka [Information cycling and cybersecurity] .//Kibepbezpeka v Ukpayini: ppavovi ta opganizaczijni py`tannya: matepialy` vceykp. nayk.-ppakt. konf., m. Odeca, 21 zhovtnya 2016 p. Odeca [Cybersecurity in Ukraine: legal and organizational issues: materials in all. nayk.-ppakt. conf., Odessa, October 21, 2016 p]. Odessa: ODUBC. 233 [in Ukrainian]

[21] Horgan, S., Collier, B., Jones, R. & Shepherd, L. (2020) 'Re-territorialising the policing of cybercrime in the post COVID-19 era: towards a new vision of local democratic cyber policing', Journal of Criminal Psychology. DOI: https://doi.org/10.1108/JCP-08-2020-003

[22] Irwin, A.S .M. (2018). Double-Edged Sword: Dual-Purpose Cyber Security Methods. Cyber Weaponry. Springer, Cham, 101-102

[23] Ismajlov, K.Yu., Yacenko, Ya.S. (2016). Deyaki suchasni tendenciyi kiberzlochy`nnosti [Some modern trends in cybercrime] Aktual`ni zadachi ta dosyagnennya u galuzi kiberbezpeky`: materialy` Vseukrayins`koyi naukovo-prakty`chnoyi konferenciyi (m. Kropy`vny`cz`ky`j, 23-25 ly`stopada 2016 r.) [Current challenges and achievements in the field of cybersecurity: materials of the All-Ukrainian scientific-practical conference (Kropyvnytskyi, November 23-25)] 54-55. http://dspace.oduvs.edu.ua/handle/123456789/177?locale =uk[in Ukrainian]

[24] Kocapevc`ka, O.B., Hovicz`ky`j, O.I. (2016). Ppoty`Diya kibepzlochy`nnocti yak ckladova infopmaczijnoyi bezpeky` depzhavy`[ Prevention of cybercrime as a component of information security of the state] Kibepbezpeka v Ukpayini: ppavovi ta opganizaczijni py`tannya: matepialy` vceykp. nayk.-ppakt. konf [Cybersecurity in Ukraine: legal and organizational issues: materials in materials. nayk.-ppakt. conf] [in Ukrainian] Odeca: ODUBC. 233

[25] Kravczova, M. O. (2018). Suchasny`j stan i napryamy` proty`diyi kiberzlochy`nnosti v Ukrayini [The current state and directions of combating cybercrime in Ukraine] Bulletin of the Criminological Association of Ukraine 2 (19). 155-166. [in Ukrainian]

[26] Kravczova, M. O., Ly`tvy`nov, O. M. (2016) Zapobigannya kiberzlochy`nnosti v Ukrayini [Prevention of cybercrime in Ukraine] : monografiya. Xarkiv : Panov [in Ukrainian]

[27] Law of Ukraine (1994) On protection of information in information and telecommunication systems https://zakon.rada.gov.ua/laws/show/80/94-%D0%B2%D1%80#Text[in Ukrainian]

[28] Law of Ukraine (2010) On Basic Principles of Domestic and Foreign Policy https://zakon.rada.gov.ua/laws/show/2411-17#Text [in Ukrainian]

[29] Law of Ukraine (2018) On National Security of Ukraine https://zakon.rada.gov.ua/laws/show/2469-19#Text [in Ukrainian]

[30] Law of Ukraine Convention on Cybercrime (2006) On Ratification of the Convention on Cybercrime http://zakon2.rada.gov.ua/laws/show/2824-15 [in Ukrainian]

[31] Law of Ukraine On Basic Principles of CyberSecurity Protection of Ukraine (2017) http://zakon5.rada.gov.ua/laws/show/216319 [in Ukrainian]

[32] Marutian, R. (2017) Ukraine took 56th place in the global index of cyber security. MATRIX. http://matrixinfo.com/2017/06/28/ukrayina-posila-56-mistse-u-globalnomu-index-kiberb ezpeky/ Accessed 20 Jul 2018

[33] Mykoida P.B., Shelexov, A.O. (2016). Zakonodavctvo Ukpayiny` y cfepi bopot`by` z kibepzlochy`nnictyu [Legislation of Ukraine in the field of combating cybercrime] Kibepbezpeka v Ukpani: ppavovi ta opganizaczijni py`tannya: matepialy` vceykp. nayk.-ppakt. konf., m. Odeca, 21 zhovtnya 2016 p [.// Cybersecurity in Ukraine: legal and organizational issues: materials in general. nayk.-ppakt. conf., Odessa, October 21, 2016 p.] Odessa: ODUBC. 233 [in Ukrainian]

[34] NBU. (2020). Proyekt postanovy` Pravlinnya Nacional`nogo banku Ukrayiny` pro zatverdzhennya Polozhennya «Pro zaxy`st informaciyi ta kiberzaxy`st v platizhny`x sy`stemax» [raft resolution of the Board of the National Bank of Ukraine on approval of the Regulation “On information protection and cyber protection in payment systems”] https://bank.gov.ua/admin_uploads/article/Project_of_resolution_11082020.pdf?v=4 [in Ukrainian]

[35] Nikolina, I.I., Gulivata, I.O. (2020.) MODELYuVANNYa KIBERZLOChY`NNOSTI YaK ZAGROZY` CY`FROVIZACIYi EKONOMIKY [SIMULATION OF CYBER CRIME AS A THREAT TO DIGITALIZATION OF THE ECONOMY] Computer-integrated technologies: education, science, production 39 DOI: 10.36910/6775-2524-0560-2020-39-31 [in Ukrainian]

[36] Ofis General`nogo prokurora (2009-2020) [Office of the Attorney General] Yedy`ny`j zvit pro kry`minal`ni pravoporushennya [Single report on criminal offenses] https://www.gp.gov.ua/ua/stat_n_st?dir_id=113897&libid=100820&c=edit&_c=fo [in Ukrainian]

[37] Peter G.. Prokuratura ta pravooxoronni organy` Ukrayiny` v period zlochy`nnogo rezhy`mu Yanukovy`cha i yiyi peretvorennya s`ogodni [The Prosecutor's Office and law enforcement agencies of Ukraine during the criminal regime of Yanukovych and its transformation today]. URL: http://www.3republic.org.ua/ua/ideas/13397[in Ukrainian]

[38] PwC (2011). Ukraine World Review of Economic Crimes Cybercrime is in the spotlight https://www.pwc.com/ua/uk/press-room/assets/gecs_ukraine_ua.pdf [in Ukrainian]

[39] PwC (2016) Review of global economic crime in 2016. https://www.pwc.by/en/publications/otherпублікації /

опитування про економічну злочинність-2016 [in Ukrainian]

[40] PwC. (2018) Vsesvitnye doslidzhennya ekonomichny`x zlochy`niv ta shaxrajstva 2018 roku: rezul`taty` opy`tuvannya ukrayins`ky`x organizacijVy`vedennya shaxrajstva z tini [World Economic Crimes and Fraud Survey Results of a Survey of Ukrainian OrganizationsRemoving Fraud from the Shadows] https://www.pwc.com/ua/uk/survey/2018/pwc-gecs-2018-ukr.pdf [in Ukrainian]

[41] Shvedova, G. (2019). KORUPCIYa YaK ZAGROZA KIBERBEZPECI OB'YeKTIV KRY`TY`ChNOYi INFRASTRUKTURY`[CORRUPTION AS A THREAT TO CYBER SECURITY OF CRITICAL INFRASTRUCTURE OBJECTS] . Bezpeka social`no-ekonomichny`x procesiv v kiberprostori : materialy` Vseukr. nauk.-prakt. konf. (Ky`yiv, 27 berez. 2019 r.). [Security of socio-economic processes in cyberspace: materials All-Ukrainian. scientific-practical conf. (Kyiv, March 27, 2019).] – Ky`yiv : Ky`yiv. nacz. torg.-ekon. un-t 244. 43-44 [in Ukrainian]

[42] Skuly`sh, Ye.D. (2014). MIZhNARODNO-PRAVOVE SPIVROBITNY`CzTVO U SFERI PODOLANNYa KIBERZLOChY`NNOSTI [INTERNATIONAL LEGAL COOPERATION IN THE FIELD OF OVERCOMING CYBER CRIME] Information and Law 1(10). 93-100 http://www.ippi.org.ua/skulish-%D1%94d-mizhnarodno-pravove-spivrobitnitstvo-u-sferi-podolannya-kiberzlochinnosti[in Ukrainian]

[43] Stover, D. (2018). Garlin Gilchrist: Fighting fake news and the information apocalypse. Bulletin of the Atomic Scientists, 74(4), 283-288

[44] Streltsov, L. (2017). The System of Cybersecurity in Ukraine: Principles, Actors, Challenges, Accomplishments European Journal for Security Research. 2, 147–184 https://link.springer.com/article/10.1007/s41125-017-0020-x

[45] Syomych, M., Markina, I., Diachkov, D. (2018). Cybercrime as a leading threat to information security in the countries with transitional economy https://doi.org/10.2991/icseal-18.2018.49

[46] Varenia, N., Avramenko, S. (2020). Virtual`na real`nist` yak novy`j svitovy`j chy`nny`k dlya analizu rivnya terory`sty`chnoyi zagrozy [Virtual reality as a new world factor for the analysis of the level of terrorist threat] Ukrainian Journal of International Law. 2. 46-60 [in Ukrainian]

[47] Yar, M., & Steinmetz, K. F. (2019). Cybercrime and society. SAGE Publications Limited.

[48] Yelyevceva, D.O. (2020). PY`TANNYa ZASTOSUVANNYa PRAVOVY`X REZhY`MIV ZABEZPEChENNYa KIBERBEZPEKY` V UKRAYiNI [ON THE APPLICATION OF LEGAL REGIMES FOR CYBER SECURITY IN UKRAINE] INFORMATION AND LAW. 4(35). 106-112 http://il.ippi.org.ua/article/view/221235 [in Ukrainian]

[49] Zvit Golovy` Nacional`noyi policiyi Ukrayiny` pro rezul`taty` roboty` vidomstva u 2019 roci [Report of the Head of the National Police of Ukraine on the results of the department's work in 2019] https://www.kmu.gov.ua/storage/app/sites/1/17-civik-2018/zvit_2019/zvit-npu-2019.pdf [in Ukrainian]