REVISTA RELAÇÕES INTERNACIONAIS DO MUNDO ATUAL

unicuritiba

Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

FACTORS OF CYBERCRIME IN UKRAINE

BOHDAN HOLOVKIN
Yaroslav Mudryi National Law University, Criminalistics Department
61024, 77 Pushkinska street, Kharkiv, Ukraine
https://orcid.org/0000-0002-0333-9806

SERHII CHERNIAVSKYI
National Academy of Internal Affairs
03035, 1 Solomjanska Square, Kyiv, Ukraine
https://orcid.org/0000-0002-2711-3828

OLEKSII TAVOLZHANSKYI
Yaroslav Mudryi National Law University
61024, 77 Pushkinska street, Kharkiv, Ukraine
https://orcid.org/0000-0001-8798-4820

ABSTRACT

The relevance of the research topic is determined by the need to form a holistic scientific approach to explaining the factors of cybercrime in the context of the global COVID-19 pandemic, the armed aggression of the Russian Federation against Ukraine, the accelerated digital transformation of the economy and society, the intensification of hybrid cyber threats, and the existence of a general upward trend in cybercrime. The purpose of the article is to identify, analyse and classify the factors of cybercrime, and to assess their impact on the level of cyberattacks and cybercrime. To achieve this goal, the author uses general scientific methods of cognition (system analysis, classification, synthesis, comparison) and special methods of criminological research (document study, factor analysis, statistical methods, expert opinions). It is found that the most significant impact on the growth of cybercrime is exerted by political (geopolitical and military-political), economic, socio-cultural, socio-psychological, technological factors, which are expressed in the escalation of geopolitical struggle, Russia's use of cyber means to gain an information advantage in the war against Ukraine, and functioning in the dark web of the criminal market of goods and services, insufficient social control over the digital environment, increased connectivity, ease of cyberattacks, low income, social exclusion, informal norms and values, opportunistic attitudes, criminogenic stereotypes of thinking and behaviour in cyberspace during electronic communications and online business. It is stated that favourable conditions for committing cybercrime are the depletion of resources and overload of cybersecurity entities of Ukraine due to the protracted war, vulnerabilities in computer and mobile device software, shortcomings in the cyber security system of public and private information resources, critical infrastructure facilities, and users' non-compliance with the rules of safe behaviour.

Keywords: factors of cybercrime, Russian cyber aggression, criminal market, hacker groups, cyber vulnerabilities, electronic communications.

Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

1 INTRODUCTION

The United Nations and the Council of Europe have identified cybercrime as a key threat to the rule of law, global, regional and national security and sustainable development. Doha Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels,and Public Participation, adopted by the resolution of the 13th United Nations Congress on Crime Prevention and Criminal Justice (Doha, Qatar, 12-19 April, 2015) (Thirteenth United Nations Congress on Crime Prevention and Criminal Justice, 2015), as well as the Kyoto Declaration on Advancing Crime Prevention, Criminal Justice, and the Rule of Law: Towards the Achievement of the 2030 Agenda for Sustainable Development, adopted by the resolution of the 14th United Nations Congress on Crime Prevention and Criminal Justice (Kyoto, Japan, 12-12 December 2021) , Member States are encouraged to develop and improve comprehensive crime prevention policies and national strategies to prevent the most dangerous forms and manifestations of crime by identifying and addressing the factors (root causes) of crime (Fourteenth United Nations Congress on Crime Prevention and Criminal Justice, 2021).

The problem of determining cybercrime is mainly paid attention to in foreign criminology. The essence of the problem is to explain the nature of the factors of cybercrime, to determine the set of factors related to cybercrime, and to assess the weight of their impact on the level of cybercrime. It is believed that the factors of cybercrime are multiple, interrelated, and require interdisciplinary research. The understanding of the nature of cybercrime factors largely depends on the resolution of the scientific dilemma of what are the root causes of cybercrime: Is it the "human factor" or the possibility of dual use of digital technologies and the anonymity of communications in cyberspace? Scholars have developed at least three methodological approaches to solving this problem: technological, classical criminological and pluralistic. Representatives of computer science and information security experts consider the causes of cyberattacks and cybercrime to be the vulnerabilities of hardware and software, developed digital infrastructure, and information and communication technologies used for criminal purposes (Burdin et al., 2018). However, the vast majority of criminologists see the root causes of cybercrime as the "human factor". This refers to the phenomena and processes associated with globalisation and the digital transformation of the economy and society, which negatively affect the thinking and behaviour of Internet users and lead to cybercrime activity (Gazizova, 2020). The criminological approach involves explaining the determinants of cybercrime from the standpoint of anomie theory, routine activity theory, social learning theory, self-control theory, criminal opportunity theory, general deformation theory, differential relationship theory, and victimological theories. The pluralistic approach is based on the convergence of technological determinants and factors related to the peculiarities of human behaviour in society and cyberspace. A special place in explaining the causes of cybercrime is occupied by individual private criminological theories, such as the theory of space (spatial) transition, the actor-network theory (hybrid cyberdeviance and cybervictimization), and others.

The study of the determinants of cybercrime is of great scientific importance for the modernization of the general theory of crime determination, the further development of cybercriminology as a private criminological theory, and a branch of knowledge about cybercrime, cybercrime behaviour, and cybervictimization. The practical significance of the study of this problem is to update the policy of combating cybercrime and identify effective strategies to counteract all its forms and manifestations, forecast trends in the spread of cybercrime, manage risks in the field of global, regional and national security, develop medium-term programmes and plans of preventive measures aimed at eliminating or minimising the impact of cybercrime factors.

A recent thematic publication investigated the relationship between unemployment and GDP per capita growth and the number of cyberattacks in eight countries (UAE, USA, Spain, Italy, Japan, the Netherlands, China, Belgium, India and Canada) during 2000-2017. The results of the study showed that the number of cybercrimes in the United States, the UAE, Belgium, China, and Italy does not depend on the level of unemployment (statistically insignificant correlation values of p = 0.836, 0.141, 0.353, 0.323, and 0.892, respectively). However, in the Netherlands, India and Spain, a more significant correlation between these indicators was found (p = 0.002, 0 and 0, respectively). It is concluded that there are many more factors influencing the growth of cybercrime.

The author suggests that the causes of cybercrime are formed under the criminogenic influence of globalisation, and such causes are divided into immediate and remote ones. The proximate causes of cybercrime are personal and situational factors that directly affect individual behaviour. The remote causes are deeper, covering cultural, socio-psychological, economic and political-institutional factors that form and strengthen motivation and create opportunities for committing cybercrime (Gazizova, 2020).

No studies of the determinants of cybercrime have been conducted in Ukraine. Most publications in this area are devoted to the development of cybersecurity policy, the study of current and projected cyber threats to national security, the causes of their emergence in the context of globalisation, the global COVID-19 pandemic, hybrid warfare, and corruption as a threat to cybersecurity (Sinha et al., 2015; Holovkin et al., 2021).

The purpose of this study is to identify, analyse and classify the factors of cybercrime and assess their impact on the level of malicious activity in cyberspace and the volume of cybercrime in general, as well as in the context of Russia's war against Ukraine, in particular.

2 Materials and Methods

The study is based on the analysis of the norms and provisions of international agreements, acts of national legislation, policy documents, reports, reviews and statistics, namely: The Convention on Cybercrime (ETS No. 185) of 23 November 2001 (The Convention on Cybercrime, 2001), the European Union Cybersecurity Strategy for the Digital Decade of 16 December 2020 (The European Commission and the High Representative of the Union for Foreign Affairs and Security Policy, 2020), the Europol analytical report "Internet Organised Crime Threat Assessment (IOCTA) 2021" (Europol, 2021), the report of the Joint Research Centre of the European Commission (JRC) "Cybersecurity, our digital anchor, a European perspective 2020" (European Commission, 2020), the Interpol Global Survey "Cybercrime: COVID-19 Impact 2020" (Interpol, 2020),

Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

analytical review of the International Institute for Strategic Studies "Russia's War in Ukraine: Examining the Success of Ukrainian Cyber Defences" (Black, 2023), "Cybersecurity Strategy of Ukraine. Secure cyberspace is the key to the country's successful development" (Decree of the President of Ukraine, 2021a), Information security strategy (Decree of the President of Ukraine, 2021b), as well as the results of international research and rating assessments.

The research methodology involves the use of the dialectical method of cognition as well as general scientific methods (system analysis, synthesis, classification, comparison) and special methods of criminological research (document study, factor analysis, statistical methods).

The dialectical method of scientific cognition is used to identify and study the totality of criminogenic phenomena of public life and global cyberspace related to cybercrime, to understand their essence, form and manifestations, to study the unity and contradictions of physical and virtual space, to reveal the content and structure of the determinants of cybercrime in connection with other phenomena and processes of objective reality.

The method of systematic analysis was used to study various sources of information on the subject of research and to create a general idea of the system of determinants of cybercrime. To this purpose, the author analysed the constituent elements of the Convention on Cybercrime and the European Union's Cybersecurity Strategy for the Digital Decade to identify the signs and types of cybercrime, as well as the complex problems that generate cybercrime and affect its volume. In addition, the constituent elements of each cybercrime factor were analysed in detail. As a result of the systemic analysis, the initial provisions, concepts and categories used in this study were formed.

The synthesis method is used to combine information on cybercrime and related phenomena into a single system of knowledge about the factors of cybercrime.

The classification method is used to distribute, organise and group the array of information on the factors of cybercrime according to certain criteria (sources, content, time period, areas of research, research scope, territorial principle). The factors of cybercrime are classified by content and scope into political, economic, socio-cultural, technological, information and psychological, regulatory, organisational and administrative, victimogenic, and factors related to ineffective law enforcement.

The comparison method ensured the comparison of data from official statistical information with the results of empirical studies, indicators of rating assessments, and reports of non-governmental organisations, in order to check the information for objectivity, completeness and reliability. Different factors of cybercrime at global, regional and national scales were also compared.

Using the documentary research method, the materials and digital indicators of the European Union's Cybersecurity Strategy for the Digital Decade, the Europol analytical report "Internet Organised Crime Threat Assessment (IOCTA) 2021", the JRC report "Cybersecurity - Our Digital Anchor, a European perspective 2020", the Interpol Global Survey "Cybercrime: COVID-19 Impact 2020", analytical review of the International Institute for Strategic Studies (IISS) "Russia's War in Ukraine: Examining the Success of Ukrainian Cyber Defences" and other studies. The study of these documents provided an idea of the cyber threat landscape, general trends in cybercrime, and allowed us to identify an approximate list of factors related to cybercrime (Vakulyk et al., 2020).

Factor analysis is used to find and classify factors that affect the level of cybercrime, to establish causal and other deterministic links between cybercrime and the phenomena that generate and determine it. Statistical methods were used to collect, process, analyse and interpret statistical data on the number of cybercrimes registered in Ukraine in 2014-2022, the number of Internet users, indicators of the vulnerability of countries to cyberattacks, total revenues from cybercrime on a global scale, calculations of economic development indicators, and living standards.

3 RESULTS AND DISCUSSIONS

According to experts, in 2020 the losses of the global economy from cybercrime will amount to 5.5 trillion euros, which is twice as much as in 2015 (2.7 trillion euros). According to Europol's classification, typical forms of cybercrime are high-tech crimes, abuse of the dark web, data theft, Internet fraud, sexual exploitation of children, counterfeiting of money and means of payment, crimes against intellectual property. According to the analytical report "Internet Organized Crime Threat Assessment (IOCTA) 2021", cybercrime is evolving and turning into an organied criminal business. Forums and markets for criminal goods and services operate on the dark web; new technologies and schemes of cyberattacks are created; cryptocurrencies are used for calculations, concealment and legalization of criminal income; and measures are taken to increase the operational security of criminals.

The cybercrime world has its own infrastructure, a system of communication between criminals, and platforms for training newcomers and professionalising experienced hackers. Cybercrime penetrates the public and private sectors, targeting the supply chains of large international companies and government agencies to compromise them. In addition, international hacker groups, in cooperation with governments and intelligence services of authoritarian states, including the Russian Federation, conduct targeted cyberattacks on military, energy and logistics facilities, information and communication systems of the public and private sectors, and critical information infrastructure, as well as engage in industrial espionage, steal confidential information, and participate in cyber sabotage.

In other words, modern cybercrime is multidisciplinary. It functions as an organised criminal business, as a planned activity of Russian information operations forces, or as the criminal activity of individuals. Cybercrime is a tool of geopolitical struggle, a means of cyber aggression, and a key threat to global and regional security. In addition to illicit enrichment, cybercrime is aimed at undermining international security, economic stability, defence capability, social cohesion and trust in cyberspace.

The war in Ukraine has demonstrated that Russia is using cybercrime to support military operations for a full-scale invasion of the territory of a sovereign state. The results of the Global Cybercrime Survey during the COVID-19 pandemic (2020) conducted by Interpol revealed the rapid spread of cybercrime in the world, as well as the change in the focus of cybercrime attacks from individuals and small businesses to large corporations, governments and critical infrastructure (Interpol, 2020).

In terms of structure, cybercrime consists of Internet fraud and phishing related to the COVID-19 pandemic (59%), the use of malware and ransomware, including for illegal data collection (36%), the use of malicious domains (22%), and the spread of disinformation (14%) (Interpol, 2020). Recently, transnational cybergroups have been actively engaged in cryptojacking, fraudulent acquisition of charitable donations for Ukrainians. Organised cybercrime activities are carried out by Russian information operations troops, which include cyber sabotage, cyber espionage, and cyber terrorism against Ukraine.

According to the statistical report of the State Service of Special Communications and Information Protection of Ukraine "On the work of the system of detecting vulnerabilities and responding to cyber incidents and cyber attacks", in 2022, the total number of cyber incidents in Ukraine increased by 2.8 times compared to 2021. In the structure of cyber incidents, the largest increase in cyber attacks using malicious software code (18.3 times) as well as the gathering of confidential information (credentials, etc. - 2.2 times) is recorded. In general, Russia's cyber aggression against Ukraine is aimed at damaging defence capabilities, disabling information and communication systems, committing illegal actions with confidential information processed in them, destabilising the situation inside the country and compromising Ukraine in the international arena (State Centre of Cyber Defence, 2022; Black, 2023).

The exponential growth of data, intensive development of digital infrastructure, an increase in the number of users, the number of connections and the time spent in cyberspace in the conditions of imperfect cybersecurity significantly complicate the criminal situation with the spread of cybercrime in the world and in Ukraine. The Microsoft Digital Defense Report - 2021 shows that in July 2020 - June 2021 Ukraine was the second largest country (19%) among the countries targeted by hacker attacks, behind only the United States (46%) (Microsoft Digital Defense Report, 2021). It is also noteworthy that from 2014 to 2017, the level of cybercrime in Ukraine increased almost sixfold (443 cybercrimes against 2573), after which there was a slight decrease in the number of recorded cybercrimes (2018 - 2301, 2019 - 2204, 2020 - 2498, October 2021 - 2790). However, in the first year of Russia's war against Ukraine, there was a sharp increase in cybercrime (2022 - 3415) (On registered criminal offences and the results of their pre-trial investigation for the period 2014-2022, n.d.). In the context of the war, cybercrime in Ukraine has both a general criminal orientation and serves as a tool to

Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

support the conduct of hostilities by the aggressor state. It is a means of encroachment on the independence and state sovereignty of Ukraine in the information space, and it is also a way of committing war crimes (The international tribunal should consider Russia's cyberattacks on Ukraine as a war crime, 2023). According to a study by the American corporation McAfee "The Hidden Costs of Cybercrime 2020", since 2018, the total losses from cybercrime have amounted to 1% of global GDP, or $1 trillion. At the same time, the cost of cybercrime for the global economy increased by 50% in 2018-2020 (The Center for Strategic and International Studies & the American corporation McAfee, 2020).

The level, structure and dynamics of cybercrime are significantly influenced by various phenomena and processes with which it is interconnected and interdependent. According to the content and scope, the determinants of cybercrime can be classified into political, economic, socio-cultural, technological, psycho-informational, regulatory, organisational, managerial, victimological, and factors related to ineffective law enforcement activities (Chyzhmar et al., 2020).

The political determinants of cybercrime can be divided into foreign policy determinants, consisting of geopolitical and military-political determinants, and domestic political determinants.

Foreign policy (geopolitical and military-political) determinants include:

– turning cyberspace into an environment of geopolitical competition for technological dominance in the digital world, monopolising the market of intellectual property and knowledge-intensive products, exercising covert influence on political and social processes, interfering in the foreign policy of sovereign states;

– militarization of cyberspace, its use for intelligence, terrorism, sabotage and other subversive activities aimed at weakening the defence capabilities of sovereign states, blocking, disabling communications and automated control systems for the latest types of weapons and troops, reducing the organisational and technical capabilities of the forces and means of the security and defence sector of potential adversaries;

– planning of military conflicts and armed aggression against sovereign states, creation of professionally trained cyber forces of the Russian army and use of an extensive network of pro-Russian hacker organisations for military, political and terrorist purposes;

– the desire of the aggressor state to gain a decisive advantage in the information space, both in the temporarily occupied territories of Ukraine and in the government-controlled territories, as well as to establish psychological and informational control over the consciousness and behaviour of users of the national segment of the Internet;

– strengthening the effectiveness of the full-scale invasion of the Russian army on the territory of Ukraine by massive network attacks on information infrastructure objects;

– escalation of confrontation in cyberspace by the Russian forces of information operations against the cyber forces of the armies of NATO member states, as well as allies of Ukraine in the Russian-Ukrainian war;

– insufficient level of cyber resilience of networks, information systems and critical infrastructure objects of EU member states against cyber threats and cyber crimes;

– non-compliance by public and private sector organisations of various countries with international cyber security norms and standards;

– declarative policy and insufficient coordination of preventive measures of the EU and NATO member states to deter and effectively counter the Russian Federation's use of hybrid warfare technologies in cyberspace against Ukraine and other sovereign states, combining military and non-military cyber means of destabilizing the socio-political situation, creating a state of uncertainty, and provoking international conflicts and complications in relations with key foreign partners;

– deployment of malware in cyberspace and large-scale operations to steal restricted information for political, economic or military purposes, as well as confidential cooperation of customers of criminal services with hacker groups and developers, and operators of malicious software;

– wide opportunities for conducting global disinformation campaigns in cyberspace that threaten world order, democratic development and international stability by promoting right-wing radical ideology, supporting the policies of authoritarian governments, polarising the community of users of the Global Network on the basis of linguistic, religious, ethnic, ideological and other contradictions, and fuelling protest moods;

– financing and use for geopolitical interests by special services and intelligence agencies of states claiming dominance in cyberspace, illegal services of international

Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

hacker organisations, transnational criminal groups, organised groups of cybercriminals and professional hackers;

– the instability of cyberspace, the constant increase in the number and changing nature of global challenges and threats to the sustainable functioning of the national information infrastructure, the emergence of new vulnerabilities in networks, information and telecommunication systems and critical infrastructure facilities.

Domestic political determinants of the spread of cybercrime include:

– shortcomings of the concept of state policy in the field of ensuring cyber security and countering cybercrime, which are caused by such:

a) dominance of state-centred ideology in the relations between the state, private sector and citizens in the field of cybersecurity, focus of the authorities on the implementation of power and control functions and state coercion, instead of creating conditions for the safe satisfaction of users' needs and interests, and providing services to strengthen cyber defence of objects vulnerable to cybercrime;

b) declarative nature of the principle of ensuring protection of the rights of users in the information and telecommunications system and consumers of information electronic services, primarily the human right to privacy, prohibition of disclosure of personal data, as well as lack of real mechanisms for protecting corporate information with limited access, rights and legitimate interests of business entities;

c) preservation of a reactive approach in the activities of cyber security entities, aimed at deterring malicious actions in cyberspace and ensuring the information stability of protection objects, instead of a comprehensive implementation of a proactive approach based on the identification, assessment and management of existing and potential cyber risks, including criminal ones;

– failure to strengthen the political will of the top leadership of the state regarding the sustainable development of the information society and the creation of a safe communication environment by providing sufficient financial, material, technical and other resources for the technological modernization of the information infrastructure and the reliable functioning of the mechanism for minimizing cyber threats and combating cybercrime;

– insufficient level of harmonization of international cyber security standards with the legislation of Ukraine, improper unification of approaches, methods and means of ensuring cyber security with established practices of the EU and NATO member states;

– incomplete reform of the system of protection of information with limited access;

– shortcomings in the organisation and implementation of educational work among the population on issues of safe behaviour in cyberspace and reporting cybercrimes to the competent authorities;

– underdeveloped mechanism of communication in the field of cybersecurity and combating cybercrime aimed at spreading correct information about the latest trends in cybercrime, the state of cybersecurity in the public and private sectors; improving trust in authorised entities and forming an unacceptable attitude of users towards any manifestations of malicious actions in cyberspace and criminal offences;

– an ineffective system of training qualified cyber security specialists, as well as a lack of training programs for specialists in the detection, investigation, termination and prevention of cybercrimes;

– underdeveloped international cooperation with key foreign partners in the field of ensuring cyber security and combating cybercrime.

The economic determinants of cybercrime are as follows:

– low-cost, low-risk and high-profitability of cybercriminal activity (according to the report of the cyber security company "Bromium", as well as according to the research of the company "Atlas VPN", the annual income from cybercrime is $1.5 trillion per year (Anton, 2020), while the total volume of the cyber security market in 2019 is estimated at only $136 billion (Revenue from cybercrime is eleven times greater than security costs, 2019));

– functioning of the outsourcing model of organised criminal business in cyberspace (Crime-as-a-Service), provision of paid services to users for organising customised DDos attacks, selling or renting malware codes, etc.;

– high commercial demand among users for malicious software, criminal services of operators of such products and hackers whose criminal activity is aimed at maximising

Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Review*e-
ISSN: **2316-2880**

the income of users and customers, minimising their expenses, discrediting and eliminating competitors in the digital market;

– a large offer on the dark web, closed groups of malware, other illegal products and criminal services for their use for illegal purposes;

– illicit trafficking in digital technologies, products and services developed in the dark web of cyberspace, used by both novice and professional hackers for illegal purposes;

– innovation backwardness of the economy and its low competitiveness, export orientation of information and communication technologies;

– the intensive pace of digitalisation of the financial sector and the transition to electronic payment systems, the development of e-commerce during the global COVID-19 pandemic, as well as e-services and the related concentration of the lion's share of cash resources in these areas, which contributes to the spread of online theft and cyber fraud;

– wide opportunities for making confidential payments, concealing funds and legalising the proceeds of cybercrime through the misuse of cryptocurrencies (bitcoin, Monero) converted through exchange services and other means (Europol, 2021);

– insufficient amount of state funding of the digital sector, including cyber security measures (less than half a percent of GDP);

– saving costs by public and private entities for the purchase and operation of computer hardware and equipment of outdated versions; the use of unlicensed software that does not meet modern cybersecurity requirements and has a low level of cyber protection;

– an increase in employment in the IT sector, an increase in the number of programmers and other specialists in this area who can use their professional skills and competences for criminal purposes;

– functioning of the illegal circulation of counterfeit software and unlicensed antivirus products in the national segment of the Internet of Ukraine;

– absence of a competitive market for telecommunications services; wide opportunities for abuse of monopoly position by telecommunications operators and providers by setting inflated prices for telecommunications services, non-compliance with the procedure for routing traffic on telecommunications networks, failure to protect telecommunications networks, telecommunications facilities, and restricted information;

– low domestic demand for high-tech software products, technical solutions and breakthrough technologies in the telecommunications market due to their high cost.

The social determinants of cybercrime include the following:

– changes in social behaviour caused by the digitalization of the state and society, which are expressed in the transition to a virtual model of communication instead of physical interaction;

– blurring the boundaries between real and virtual life, which creates the illusion of security;

– abuse of digital rights and freedoms in cyberspace by users for illegal purposes;

– use of social engineering technologies to change the way of thinking and behaviour of people and their associations in cyberspace;

– the functioning in cyberspace of a large number of closed social groups with a criminal orientation that use technical means of secret communication and teach methods of committing cybercrime;

– deformation of the moral and legal consciousness of users under targeted psycho-informational destructive influence and as a result of consumption of illegal content;

– psychological dependence of a significant part of society on the use of mobile devices, applications, social networks and other means of electronic communications;

– growth in the audience of users and increased time spent in cyberspace (in 2021, the number of global smartphone users was 5.22 billion; the number of Internet users was 4.66 billion; the number of social media users was 4.2 billion (Stanislavsky, 2021). In 2021, there were 26 million Internet users in Ukraine, with 60% of the population using social media (Kondratenko, 2021);

– low level of digital literacy among users of the Internet, E-services, information resources; lack of formation of digital skills and digital competences and a culture of safe behaviour in cyberspace.

Normative and legal determinants of cybercrime include:

– lack of a comprehensive regulatory framework for cybersecurity and combating cybercrime, ambiguity of terminology, inconsistency of legal provisions in laws and regulations, low level of harmonisation of national legislation with EU legislation and NATO standards in this area;

– legal uncertainty of the procedure for the circulation of cryptocurrencies, regulatory unresolved issues related to electronic communications, the use of artificial intelligence, the Internet, things and other information and communication technologies, as well as outdated legislation in the field of information protection;

– incomplete implementation of the Convention on Cybercrime in the Criminal Code of Ukraine, in terms of establishing a complete list of cybercrimes and strengthening sanctions for their commission, as well as failure to enshrine in the Criminal Procedure Code of Ukraine the powers, measures and procedures for collecting evidence in electronic form (digital evidence), in particular, for urgent preservation and partial disclosure of data on the movement of information (Article 17); collection of data on the movement of information in real time (Article 20); interception of data on the content of information (Article 21); provision of information about users by service providers to the competent authorities (Article 18), which significantly complicates the investigation and proof in this category of criminal proceedings (The Convention on Cybercrime, 2001);

– the Law of Ukraine "On Telecommunications" does not regulate the procedure for interaction between cybersecurity entities and telecommunications operators and providers; in particular, on the identification of end users of telecommunications services and provision of information about them; storage of information (about the user of services, about the movement of information); access to it (including in electronic format); the term of storage and the procedure for destruction of information, as well as procedures for temporarily restricting subscribers' access to identified information*;*

– slow pace of approximation of national legislation in the field of personal data protection to EU legislation, in particular, Directive (EU) 2016/680 on the protection of individuals with regard to the processing of personal data by the competent authorities for the purposes of the prevention, investigation, detection or prosecution of criminal offences or the enforcement of criminal penalties and on the free movement of such data and repealing Council Framework Decision 2008/977/EC, as well as the provisions of

Regulation (GDPR) 2016/679 on the protection of individuals with regard to the processing of personal data and on the free movement of such data (General Data Protection Regulation, 2016);

– insufficient level of harmonization of national legislation on critical infrastructure and its protection with the norms of Directive (EU) 2016/1148 on measures for a high common level of security of network and information systems in the territory of the European Union, as well as Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and assessment of the need to improve their protection (Directive (EU) 2016/1148, 2016; Council Directive 2008/114/EC, 2008);

– *low efficiency of protection of the rights of citizens and business entities in cyberspace due to incomplete implementation of Directive 2002/58/*EU *on the processing of personal data and the protection of privacy in the electronic communications sector in national legislation (*Directive on privacy and electronic communications, 2002*)*;

– imperfection of the regulatory framework in the field of electronic trust services due to incomplete implementation of Regulation (EU) 910/214 on electronic identification and trust services for electronic transactions in the internal market, which introduces cross-border electronic identification and authentication for the purpose of secure and uninterrupted interaction between public authorities, businesses and citizens (Regulation (EU) 910/214, 2014);

– unresolved issue of introducing a risk-based approach and a mechanism for its implementation in the system of cybersecurity, prevention and counteraction to cybercrime at the legislative level;

– imperfect organisational and legal mechanisms of public-private cooperation in the field of cybersecurity and combating cybercrime, insufficient synergy of efforts of the state, private sector and citizens;

– unclear legal regulation of the forms and mechanisms of participation of operators, telecommunication service providers and other private sector entities, as well as civil society in the implementation of the strategy and measures to prevent and combat cybercrime.

Organisational and managerial factors of cybercrime are as follows:

– organisational incompleteness of the architecture of the national cybersecurity system; lack of formation of such components as the national critical infrastructure protection system, the organisational and technical model of cybersecurity of this system, the national mechanism for combating cybercrime and preventing cybercrime, the cyber risk management system in the areas of electronic communications, information security and cyber defence; the national cloud platform of cybersecurity services, etc.;

– insufficient institutional capacity of the actors countering cybercrime; limited staffing, technological, technical, operational and personnel potential; unsatisfactory information and analytical support for law enforcement and preventive activities; ineffective management; insufficient interagency cooperation and coordination in this area;

– lack of cybersecurity units and relevant cybersecurity specialists in a significant number of government agencies, local governments, and business entities classified as critical infrastructure facilities;

– failure to audit the state of cybersecurity at various levels in the public and private sectors;

– insufficient state funding for the development of the national cyber defence system and countering cyber threats;

– low level of training and professional development of information and cyber security specialists, lagging behind the system of educational services in meeting the needs of the labour market;

– insufficient level of technical security of state information resources and critical information infrastructure facilities;

– insufficiently developed international cooperation on cybersecurity with the European Union, NATO member states, intergovernmental and non-governmental organisations and key foreign partners, as well as poor integration of the national cybersecurity system into the European cybersecurity space;

– failure to develop a mechanism of public control over the legality and effectiveness of cybersecurity and cybercrime entities;

– lack of a national programme for digital literacy of the population.

The technological determinants of cybercrime include:

– technological and technical backwardness of the digital infrastructure of Ukraine; moral obsolescence of computer equipment, databases and telecommunication networks, means of communication and technical protection; critically low level of use of the latest information and communication technologies, equipment, IT services, hardware and software of the latest generation by the public and private sectors;

– Ukraine's high technological dependence on foreign manufacturers of information and communication technology products; the absence of a system for assessing the compliance of such products with security requirements, which increases the degree of vulnerability of the information infrastructure from undeclared functions and narrows the capabilities of countering cyber threats (Decree of the President of Ukraine, 2021a);

– bureaucratization of the procedure for certification and examination of the Integrated Information Protection System and the high cost of its implementation, which leads to the failure of telecommunications service providers to fulfil their statutory obligations to protect state information resources or restricted information;

– high vulnerability of software and hardware for cryptographic and technical protection of restricted information due to technological obsolescence;

– the use of unlicensed and uncertified software, tools and information processing systems in the public and private sectors;

– many owners and users of state information resources do not have information protection services and system administrators that are responsible for ensuring information protection and control;

– the ability to penetrate the local networks of enterprises, organisations, and institutions by connecting via the Remote Desktop Protocol (RDP) and gain unauthorised access to servers and databases through vulnerabilities in VPN services;

– violation of general requirements for cyber security of critical infrastructure facilities by owners or managers of enterprises, institutions, organisations related to such facilities;

– an unreliable system of cyber protection of information with limited access to legal entities of state and private ownership (violation by administrators and users of the order of access, handling and established regulations for the collection, processing, storage, distribution or transmission of information, lack of means of identification and authentication of users and administrators, failure to use the encryption method information, failure to monitor traffic for the presence of malicious code, malware viruses, etc.);

– lack of protection of communication channels, e-mail, telecommunication networks, servers and databases, individual access points to the information and telecommunications systems of state bodies, legal entities of state and private ownership from unauthorised access by third parties and targeted attacks on the entire network infrastructure;

– use of outdated antivirus software, unreliable passwords, failure to implement innovative Endpoint Detection & Response (EDR) technological solutions that allow detecting malicious activity at endpoints and preventing illegal encroachment;

– non-compliance by business entities operating in the EU market with the requirements of the General Data Protection Regulation (GDPR);

– lack of a Unified Register of Risk and Threat Assessment at various levels and objects of cyber defence;

– absence of a secure DNS server (Domain Name System) containing a distributed hierarchical database of domain names of servers (hosts) and allowing to determine the IP address of a computer, service or information resource connected to the Internet by name;

– lack of secure exchange of identification data of individuals and legal entities processed in the information systems of state bodies and the private sector; inconsistency in the choice of identifiers; lack of confirmation of identification data (Order of the Cabinet of Ministers of Ukraine, 2018);

– use of technologically incompatible mechanisms, algorithms and protocols of electronic identification and recognition in registration and access control systems to information systems (Order of the Cabinet of Ministers of Ukraine, 2018).

The victimological determinants of cybercrime are as follows:

– intensive development of electronic services due to the transition to remote operation during the global COVID-19 pandemic, in particular internet banking, online auctions, cashless payment methods, online platforms for e-commerce, electronic document management, electronic public services and the associated massive use of mobile applications by individuals and legal entities, which significantly expands the range of risks and threats and increases the vulnerability of cyber defence objects to cybercrime;

– the increase in the number of devices connected to the global Internet and other local networks, which expands the opportunities for cybercrime;

– professional victimisation of certain categories of users who provide services and conduct business in cyberspace (telecommunication service providers/operators, administration and staff of financial institutions, business entities engaged in electronic commerce);

– high risks of victimisation for civil servants who do not adhere to the basics of cyber hygiene when working with public and restricted information;

– cost savings on software and technical information protection systems (use of old versions of browsers, lack of anti-virus software, firewalls, ignoring updates of security software, etc.);

– creation and self-distribution by minors of compromising materials of an intimate nature and personal data in cyberspace;

– indiscriminate dating on the Internet, joining various groups, open communication, sending photos and video files to unfamiliar users;

– visiting little-known websites and web pages of online stores, clicking on pop-up advertising tabs, consuming dubious content on the labour market, and making subscriptions for undelivered goods or services not provided;

– excessive gullibility when using Internet banking services, SMS banking and communicating with persons posing as payment system operators;

– engaging in illegal e-commerce, as well as providing illegal paid services to users of the Internet or other global data networks.

Factors related to the ineffective activities of law enforcement agencies:

– uncertainty of the state policy on combating cybercrime; lack of a concept of preventing and combating cybercrime; lack of national and regional programmes for countering cybercrime; lack of strategic priorities and a corresponding set of measures to prevent the most common types of cybercrime;

– focus of cybercrime counteraction actors during the armed aggression on the implementation of priority tasks for Ukraine's cyber defence; lack of forces and means to counter cybercrime activities;

– absence of a central body responsible for combating cybercrime in Ukraine, which would coordinate the activities of all actors at the national level, ensure interagency interaction and international cooperation;

– lack of cyber experts, operatives, investigators and prosecutors specialising in the prevention, detection, investigation, and suppression of cybercrime;

– insufficient provision of law enforcement agencies with special technical means of detecting and responding to cyberattacks containing signs of cybercrime.

4 CONCLUSION

Thus, based on our research, we can confidently say that cybercrime is a direct and significant threat to the rule of law, national security and law enforcement. The threats to information security faced by the international community during the pandemic and the development of digital technologies, and subsequently the Russian-Ukrainian war, have all confirmed the fact that cybercrime is only gaining momentum and is already actively flourishing in various countries. Every year, more and more new cybercrimes are recorded, while the authorised bodies do not have enough time and resources to respond to them in a timely manner and track down the perpetrators.

During the Russian invasion, we have all witnessed not only massive rocket attacks and active hostilities, but also a significant number of cyberattacks by the Russian Federation. These cyberattacks were aimed at undermining internal peace and order, spreading panic, and, accordingly, stealing data that constitutes state, commercial, and banking secrets. It has once again confirmed the fact that cybercrime is a tool of geopolitical struggle, a means of cyber aggression, and a key threat to global and regional security. In addition to illicit enrichment, cybercrime is aimed at undermining international security, economic stability, defence capabilities, social cohesion and trust in cyberspace.

Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

We have conducted a study of the determinants of cybercrime, which is of great scientific importance for the modernization of the general theory of crime determination, the further development of cybercriminology, the field of knowledge about cybercrime, cybercrime behaviour, and cybervictimization. Our in-depth analysis of the determinants of cybercrime can serve as a basis for updating the policy of combating cybercrime and identifying effective strategies to counteract all its forms and manifestations. In addition, the characteristic components of the determinants of cybercrime will help in forecasting trends in the spread of cybercrime, managing risks in the field of global, regional and national security, and developing medium-term programmes and plans for preventive measures aimed at eliminating or minimising the impact of cybercrime factors.

It is important to summarise in our study that the level, structure and dynamics of cybercrime are significantly influenced by various phenomena and processes with which it is interconnected and interdependent. According to their content and scope, the determinants of cybercrime are classified into political, economic, socio-cultural, technological, psycho-informational, regulatory, organisational and managerial, victimological, as well as factors related to the ineffective operation of law enforcement agencies.

REFERENCES

Anton, P. (2020). Cybercrime annual revenue is 3 times bigger than Walmart’s. Retrieved from https://atlasvpn.com/blog/cybercrime-annual-revenue-is-3-times-bigger-than-walmarts

Black, D. (2023). Russia's War in Ukraine: Examining the Success of Ukrainian Cyber Defences. Retrieved from https://www.iiss.org/research-paper//2023/03/russias-war-in-ukraine-examining-the-success-of-ukrainian-cyber-defences

Burdin, M., Gnusov, Yu., & Kalyakin, S. (2018). Certain aspects of combating new generation cyber attacks. *Actual issues of combating cybercrime and human trafficking: Proceedings of the All-Ukrainian scientific and practical conference* (pp. 23-26). Kharkiv: Kharkiv National University of Internal Affairs.

Chyzhmar, K., Dniprov, O., Korotiuk, O., Shapoval, R., & Sydorenko, O. (2020). State information security as a challenge of information and computer technology development. *Journal of Security and Sustainability Issues, 9*(3), 819–828

Council Directive 2008/114/EC on the identification and designation of European critical infrastructures and the assessment of the need to improve their protection. (2008). Retrieved from https://eur-lex.europa.eu/legal-content/en/ALL/?uri=CELEX:32008L0114

Decree of the President of Ukraine "On the Decision of the National Security and Defence Council of Ukraine of 14 May 2021 'On the Cybersecurity Strategy of Ukraine'". (2021a). Cybersecurity Strategy of Ukraine. Secure cyberspace is the key to the country's successful development. Retrieved from https://zakon.rada.gov.ua/laws/show/447/2021#Text

Decree of the President of Ukraine "On the Decision of the National Security and Defence Council of Ukraine of 15 October 2021 "On the Information Security Strategy". (2021b). Strategy of Information Security. Retrieved from https://zakon.rada.gov.ua/laws/show/n0080525-21#Text

Directive 2016/1148 concerning measures for a high common level of security of network and information systems across the Union. (2016). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/?uri=celex:32016L1148

Directive on privacy and electronic communications. (2002*)*. Retrieved from https://eur-lex.europa.eu/legal-content/EN/ALL/?uri=CELEX%3A32002L0058

European Commission, Joint Research Centre, Baldini, G., Barrero, J., Draper, G., et al. (2020). Cybersecurity, our digital anchor: a European perspective. Retrieved from https://data.europa.eu/doi/10.2760/352218

Europol. (2021). Internet Organised Crime Threat Assessment (IOCTA). Retrieved from https://www.europol.europa.eu/publications-events/main-reports/iocta-report

Fourteenth United Nations Congress on Crime Prevention and Criminal Justice. (2021). Kyoto Declaration on Advancing Crime Prevention, Criminal Justice, and the Rule of Law: Towards the Achievement of the 2030 Agenda for Sustainable Development. Retrieved from https://www.unodc.org/documents/commissions/Congress/21-02815_Kyoto_Declaration_ebook_rev_cover.pdf

Gazizova, Yu. (2020). Cybercrime in Ukraine. The era of digital technologies is the era of new crimes. *Lawyer And Law, 12*. Retrieved from https://uz.ligazakon.ua/ua/magazine_article/%20EA013606

General Data Protection Regulation. (2016). Retrieved from https://gdpr-info.eu

Submetido em: 03/06/23
Aprovado em: 02/07/2023
Avaliação: *Double Blind Reviewe*-
ISSN: **2316-2880**

Holovkin, B. M., Tavolzhanskyi O. V., & Lysodyed O. V. (2021). Corruption as a Cybersecurity Threat in the New World Order. *Connections: The Quarterly Journal, 20*(2), 75-87.

Interpol. (2020). Cybercrime: COVID-19 Impact. Retrieved from https://content.next.westlaw.com/practical-law/document/I19be3764d6f111eabea4f0dc9fb69570/COVID-19-Interpol-report-on-cybercrime-analysis?viewType=FullText&transitionType=Default&contextData=(sc.Default)&firstPage=true

Kondratenko, M. (2021). During the year, the number of Ukrainians on social networks increased by seven million. Retrieved from https://www.dw.com/uk/za-rik-karantynu-kilkist-ukraintsiv-u-sotsmerezhakh-zrosla-na-sim-milioniv/a-56899697

Microsoft Digital Defense Report. (2021). Retrieved from https://query.prod.cms.rt.microsoft.com/cms/api/am/binary/RWMFIi

On registered criminal offences and the results of their pre-trial investigation for the period 2014-2022. (n.d.). Retrieved from https://gp.gov.ua/ua/posts/pro-zareyestrovani-kriminalni-pravoporushennya-ta-rezultati-yih-dosudovogo-rozsliduvannya-2

Order of the Cabinet of Ministers of Ukraine "On Approval of the Concept of Development of the Digital Economy and Society of Ukraine for 2018-2020 and Approval of the Action Plan for its Implementation". (2018). Concept of development of the digital economy and society of Ukraine for 2018-2020. Retrieved from https://zakon.rada.gov.ua/laws/show/67-2018-p#Text

Regulation (EU) 910/214 on electronic identification and trust services for electronic transactions in the internal market. (2014). Retrieved from https://eur-lex.europa.eu/legal-content/EN/TXT/PDF/?uri=CELEX:32014R0910

Revenue from cybercrime is eleven times greater than security costs. (2019). Retrieved from https://cybercalm.org/novyny/dohid-vid-kiberzlochyniv-v-odynadtsyat-raziv-perevyshhuye-vytraty-na-bezpeku/

Sinha, A., Nguyen, T. H., Kar, D., Brown, M., Tambe, M., & Jiang, A.X. (2015). From Physical Security to Cybersecurity. *Journal of Cybersecurity 1*(1), 19-35. https://doi.org/10.1093/cybsec/tyv007

Stanislavsky, Yu. (2021). The number of Internet users in the world reached 4.66 billion. Retrieved from https://root-nation.com/ua/news-ua/it-news-ua/ua-new-internet-records/#lwptoc

State Centre of Cyber Defence. (2022). Statistical report on the results of the System for Detecting Vulnerabilities and Responding to Cyber Incidents and Cyber Attacks in 2022. Retrieved from https://scpc.gov.ua/article/233

The Center for Strategic and International Studies, & the American corporation McAfee. (2020). The Hidden Costs of Cybercrime. Retrieved from https://www.mcafee.com/enterprise/en-us/assets/reports/rp-hidden-costs-of-cybercrime.pdf.

The Convention on Cybercrime. (2001). Retrieved from https://zakon.rada.gov.ua/laws/show/994_575#Text

The European Commission and the High Representative of the Union for Foreign Affairs and Security Policy. (2020). The EU’s Cybersecurity Strategy for the Digital Decade. Retrieved from https://digital-strategy.ec.europa.eu/en/library/eus-cybersecurity-strategy-digital-decade-0

The international tribunal should consider Russia's cyberattacks on Ukraine as a war crime. (2023). Retrieved from https://ssu.gov.ua/novyny/mizhnarodnyi-trybunal-maie-rozghliadaty-kiberataky-rf-na-ukrainu-yak-voiennyi-zlochyn-illia-vitiuk

Thirteenth United Nations Congress on Crime Prevention and Criminal Justice. (2015). Doha Declaration on Integrating Crime Prevention and Criminal Justice into the Wider United Nations Agenda to Address Social and Economic Challenges and to Promote the Rule of Law at the National and International Levels, and Public Participation. Retrieved from https://www.unodc.org/documents/congress/Declaration/V1504151_English.pdf

Vakulyk, O., Petrenko, P., Kuzmenko, I., Pochtovyi, M., & Orlovskyi, R. (2020). Cybersecurity As A Component Of The National Security Of The State. *Journal of Security & Sustainability Issues 9* (3), 775-784