Tiutiunyk, Inna; Pozovna, Iryna; Zaskorski, Wojciech

Article

Innovative approaches to ensuring cybersecurity and public safety : the socio-economic dimension

Marketing i menedžment innovacij

Marketing and Management of Innovations, ***15(4)***, *2024*

Innovative Approaches to Ensuring Cybersecurity and Public Safety: The Socio-Economic Dimension

Inna Tiutiunyk [1*], Iryna Pozovna [2], Wojciech Zaskorski [3],

[1] Department of Financial Technologies and Entrepreneurship, Sumy State University, Ukraine
[2] Economic Cybernetics Department, Faculty, Sumy State University, Ukraine
[3] Department of Management, Faculty of Applied Sciences, WSB University, Poland
[*] Corresponding author: Inna Tiutiunyk, i.tiutiunyk@biem.sumdu.edu.ua

Type of manuscript: research paper

Cite as: Tiutiunyk, I., Pozovna, I., & Zaskorski, W. (2024). Innovative Approaches to Ensuring Cybersecurity and Public Safety: The Socio-Economic Dimension. *Marketing and Management of Innovations*, *15*(4), 127–140. https://doi.org/10.21272/mmi.2024.4-10

Received: 10 May 2024
Revised: 15 October 2024
Accepted: 26 November 2024

Publisher & Founder: Sumy State University

Abstract: This study is devoted to the analysis of socio-economic aspects of the development of cybercrime and the involvement of society, both as victims and direct initiators, in this activity. The paper examines the impact of socio-economic development indicators, in particular gross national income, spending and remittances, literacy and unemployment, on the dynamics of cybercrime worldwide, and analyses trends in public awareness and involvement in criminal activity in the digital space. The methodological tools of the study are the methods of correlation and canonical analysis, implemented in the Statistica 12 software. The analysis of the relationship between the socio-economic conditions of society and cybercrime-related behaviour established a dual impact of these factors on vulnerability to cybercrime and participation in criminal activity as a way of income generation. On the one hand, socio-economic disparities, in particular income inequality and unemployment, contribute to the increasing vulnerability of society to cybercrime. On the other hand, a high level of poverty among the population motivates a certain part of it to participate in cybercriminal activities. The results of the study indicate that socio-economic inequality and unemployment play a critical role in managing cybercrime risks. A higher level of economic development and social security is accompanied by greater resilience to cyberthreats, while a high level of unemployment and significant economic inequality increase the vulnerability of society to such risks. The findings also revealed that the socio-economic development of the country largely depends on the level of its cybercrime. This highlights the need to integrate cybersecurity measures into national economic development strategies. The practical significance of the obtained results lies in the application of a comprehensive approach to understanding cybercrime, which considers both victimization and active participation of society in this activity. This study can serve as a basis for the development of targeted measures to prevent cybercrime and increase the resilience of society to cyberthreats. The findings highlight the importance of integrating economic and social components in the development of effective cybersecurity strategies, which will contribute to minimizing the risks associated with the use of digital space and strengthening the socio-economic stability of the country.

Keywords: cybercrime; data manipulation; economic development; fraud; information accessibility; population income; social inequality.

Funding: This research was funded by Ministry of Education and Science of Ukraine, grant number 0124U000550.

1. Introduction. One of the features of modern society is the rapid penetration of digital technologies into all aspects of life - from economic activity to personal communication. Along with numerous advantages, such as increased speed and efficiency of operations, greater accessibility of information, the digital era is accompanied by new challenges for state institutions, business entities and individuals, regarding the growth of cybercrime.

In conditions of low digital literacy and insufficient readiness to use digital technologies and artificial intelligence, society is increasingly becoming a target of cybercrime: misappropriation of their funds by disabling equipment, stealing or destroying information, work disruption through the spread of viruses, violating data privacy, etc (Isaia et al., 2024; Rey-Ares et al., 2024). Under these conditions, cybercrime becomes a key threat not only to individuals and organizations, but also to the state. Its consequences are manifested in the form of significant economic losses, loss of personal data, decreased trust in digital platforms, etc. The COVID-19 pandemic has exacerbated the problem of cybercrime due to the increased dependence of society on digital technologies (Chen et al., 2024; John, 2024). Isolation, restrictions on physical contact, and increased online activity have created a favourable environment for attackers. This has become a threat not only to cyber victims, but also to the entire global community, which is faced with new forms of pressure and manipulation of society (Monteith et al., 2021). In 2023, Ukraine alone recorded 2,365 cyberattacks affecting over 343 million people, with financial losses exceeding UAH 1 billion, which is 96% more than in 2021 (John, 2024).

On the other hand, high levels of socio-economic and digital inequality contribute significantly to the proliferation of cybercrime. (Khan et al., 2023). Societies facing financial instability, lack of stable employment, and limited development opportunities often perceive cybercrime as an alternative means of income generation. Furthermore, socio-economic and digital disparities hinder the development and use of digital technologies in various areas, negatively affect the level of knowledge and skills of society in terms of implementing cybersecurity measures (Dodel & Mesch, 2018).

Thus, modern cybercrime can be considered as a result of the manifestation of global socio-economic imbalances. Its prevention requires transformative changes in the mechanisms of combating cyber threats, information protection and ensuring digital security. The global nature of these problems requires a comprehensive approach that combines technological solutions, efforts to combat inequality and social exclusion, and improvements in the regulatory framework of public policy. The aim of the paper is to investigate the role of socio-economic factors in both increasing a society's vulnerability to cybercrime and motivating its individual groups to engage in cybercriminal activity as a means of generating income.

The paper is structured as follows: Section 2 presents a literature review on the socio-economic aspects of cybercrime, examining economic losses, psychological consequences, and the impact of income, employment and educational levels on cybercrime; Section 3 provides the research methodology and methods, describes the dataset used in the study, and formulates the research hypothesis; Section 4 discusses the empirical results, trends in queries reflecting the vulnerability of society to cyberthreats, the relationship between socio-economic indicators, such as GNI per capita, unemployment and population expenditure, and the dynamics of cybercrime; Section 5 discusses the impact of socio-economic factors on cybercrime: both contributing to the vulnerability of society and motivating a part of the population to participate in cybercrime, analysing the results in the context of previous studies; Section 6 concludes the paper and offers recommendations for integrating cybersecurity measures into national economic development strategies, considering both societal vulnerability to cyberthreats and the drivers of cybercriminal activity.

2. Literature Review. The socio-economic aspects of cybercrime development attract the attention of scientists and practitioners worldwide (Shettar et al., 2024; Phillips et al., 2022; Leukfeldt & Yar, 2016; Boppre et al., 2018; Martineau et al., 2023) The multifaceted nature of this activity, coupled with significant economic losses, its psychological and social consequences, highlights the importance of identifying the drivers of the development of criminal activity and the population's sensitivity to them.

One of the key areas of research focuses on the economic losses caused by the rapid growth of criminal activity in cyberspace. Anderson et al. (2019), analysed the dynamics of changes in the scale of losses, particularly economic, caused by cybercrime, demonstrating that approximately half of all property crimes, both in terms of volume and cost, occur online. The authors divide all costs from cybercrime into three groups: direct costs (such as financial losses), indirect costs (including reduced trust in online transactions), and protection costs (expenses for data protection programs). Moreover, a current trend is the increasing prevalence of cybercrime on social networks, which poses new risks to both users and companies (Alharbi et al., 2024; Rao et al., 2021).

Research into the social, economic, political, and technological drivers of cybercrime has been conducted by a significant group of scholars (Chen et al., 2023; Achim et al., 2021; Dodel & Gustavo, 2019). Most researchers argue that the highest levels of cybercrime are observed in countries with high incomes and developed technological infrastructure (North America, Europe, East Asia), whereas low-income countries have significantly lower levels of cybercrime due to limited access to technology. Among the social factors, the most impactful are the level of population density, education, and income (Yigzaw et al., 2023). At the same time, in middle- and high-income countries, income inequality has a statistically significant impact on cybercrime prevalence (Chen et al., 2023). Achim et al. (2021) and Sulich et al. (2021) emphasize that economic and sustainable development lead to the emergence of various types of economic and financial crimes. Corruption, the shadow economy and cybercrime are most prevalent in countries with low levels of financial satisfaction among the population and may gradually decrease as financial well-being improves. Such crimes are mostly characteristic of low-income countries.

The organizational aspects of cybercrime and the mechanisms of functioning of criminal groups have been examined in the works of a significant group of scientists (Ngo & Paternoster, 2011; Nguyen & Luong, 2021; Odinot et al., 2017). Luo (2024) considers cybercrime as a holistic industry, focusing on its structural organization, financial flows and internal hierarchy. Lusthaus et al. (2024) investigate transnational cybercrime, focusing on models of cooperation between criminals. Kwon et al. (2024) analyze the patterns of criminal activity and the effectiveness of response measures through the analysis of appeals to law enforcement agencies.

Researchers pay special attention to social risks and the features of virtual interaction (Wissink et al., 2023; Lusthaus, 2012; AlDairi & Tawalbeh, 2017). Moubarak & Afthanorhan (2024) examine how the digital environment affects the dynamics of family relationships in Saudi Arabia, highlighting the transformative nature of virtual communications and their impact on social structure. Meanwhile, Zhou et al. (2024) examine the phenomenon of metacrime, exploring its relationship with traditional cybercrime. They analyze new forms of digital threats that go beyond classic cybercrimes and the mechanisms of their evolution in the modern information space.

At the same time, crimes such as money laundering require a high level of education and knowledge (Lee & Chua, 2024; De Kimpe et al., 2022). These types of crimes are more characteristic of countries with high levels of economic development, whose population has a sufficient level of competence and resources to carry out complex fraud schemes, often at the international level. In general, scientists generally include GDP per capita, unemployment rate and education as the most influential socio-economic factors closely related to the prevalence of cybercrime in various countries (Ilievski & Bernik, 2016). Knowledge and awareness in the field of cyber security have a positive effect on society's willingness to use electronic banking (Afzal et al., 2024), contribute to the minimization of cyber risks both among young people (Ahmead et al., 2024) and elderly people (Havers et al., 2024)

One of the important aspects of studying the consequences of cybercrime is the socio-psychological dimension of its impact. Analysing and addressing this dimension enables researchers to understand how society reacts to threats, identify psychological risks faced by cybervictims, and develop effective mechanisms for their support. A separate group of scholars focuses on the socio-economic aspects of cybercrime examining its influence on social integration and the psychological health of the population. Research highlights critical issues such as the socio-psychological consequences of cyberattacks, gender inequality in the context of cyberviolence, the impact of the COVID-19 pandemic on cybercrime, public awareness of cyberthreats and the social consequences of cybercrimes (Brewer et al., 2018; Donner et al., 2014; Martineau et al., 2024).

Studies confirm that cybercrimes significantly affect the psychological well-being of both victims and society (financial costs, psychological consequences and social polarization). The authors argue that beyond economic losses, cybercrime leads to emotional trauma, such as stress, fear, and loss of trust (Wright & Kumar, 2023; Bada & Nurse, 2019). Moreover, cognitive vulnerabilities of victims are one of the key factors that cybercriminals use to manipulate society. Therefore, the development and implementation of tools to combat cybercrime should consider two groups of factors: those that can be measured (operational) and factors that are difficult to quantify (conceptual). Martineau et al. (2023) reviewed the cyberbehavioral analytics literature, analyzing how users' psychological characteristics influence their vulnerability to cybercrime. Brewer et al. (2018) examined the relationship between Internet use and criminal behavior among youth, identifying early risk factors for cybercrime.

An equally important area of research is the gender dimension of cybercrime. Scientists argue that women are more vulnerable to cybercrime, which has long-term negative effects on their psychological health,

including depression and anxiety (Pandian & Maraimalai, 2024; Wright & Wachs, 2020; Forssell, 2020; Hoy & Milne, 2010; El Asam & Katz, 2018). Women who have become victims of cyberbullying are more likely to focus on negative emotions through "anger rumination", which intensifies the impact of their experience (Zsila, 2019).

These findings emphasize the need to consider gender aspects in the implementation of cybercrime prevention measures and support systems for victims. This is relevant in the context of minimizing long-term psychological consequences, such as depression and anxiety, which are frequently experienced by victims of cybercrime.

The constant growth in the scale and consequences of cybercrime leads to increased attention of scientists to the issues of improving tools for combating it (Cotrina et al., 2024; Steinmetz et al., 2024; Choi et al., 2024).

Blockchain and digital forensics play a key role in preventing cybercrime. Ratul et al. (2024) proposes the use of blockchain to enhance the reliability of digital evidence in criminal investigations, while Rich & Aiken (2024) integrate forensic cyberpsychology and digital forensics to improve cyber threat prediction.

Boussi et al. (2024) propose the use of machine learning to predict phishing attacks. The developed model allows analysing the behavioural characteristics of websites and automatically identifying potentially malicious resources. In turn, Patil et al. (2024) propose a comprehensive forensic approach to cyber defence, which includes multi-level analysis of digital evidence, methods for attribution of cybercrimes, and improving mechanisms for identifying criminals in the digital environment.

One of the important factors in the formation of digital security is the increase in the level of public awareness of cyber threats and ways to counter them. Low awareness of cybercrime increases vulnerability to attacks and strengthens public distrust of technology (Lee & Lim, 2019). Enhancing cybersecurity potential in low-income countries requires consideration of social and cultural aspects of the country's development. Efforts to improve public awareness and shape social and cultural attitudes (values, perceptions, and behaviours related to online security among individuals, businesses, industries, and government) can be particularly effective in low-income countries, especially among the population that has no prior experience using the Internet (Creese et al., 2021). Analysis of the main cyber threats in various sectors of the economy, including energy, transport, water supply, and healthcare, has demonstrated that artificial intelligence serves as an effective tool for monitoring device operations and enforcing security standards (Dawson et al., 2021). A key strategy for enhancing the effectiveness of measures to combat cybercrime is the integration of the social factor. This approach allows for assessing how society reacts to cyber threats or, conversely, how it may foster interest in certain types of illegal online activities. It is essential to consider societal tolerance for illicit online behaviour, public attitudes toward online security, and perceptions of cybercriminals.

3. Methodology and research methods. It explores both the willingness to participate in criminal activities within cyberspace and the degree of individual vulnerability to cybercrime. The main hypothesis of the study is that a country's level of economic and social development determines the nature and intensity of cybercrime.

The study utilizes an array of input data to determine the impact of economic and social indicators on two aspects: the willingness to participate in cyberfraudulent activities and vulnerability to cybercrime. The indicators were categorized into components relevant to each aspect (Tables 1-3). The period of study was 2014-2024, the object of analysis is global data. The list of economic and social indicators is presented in Table 1.

Table 1. Economic and social indicators of the country's development.

№	Indicator symbol	Indicator	Units of measurement
1	Soc_econ1	GNI per capita	US$
2	Soc_econ2	Expense	% of GDP
3	Soc_econ3	Literacy rate, youth total	% of people ages 15-24
4	Soc_econ4	Unemployment, total	% of total labour force
5	Soc_econ5	Personal remittances	US$

Sources: systematized by the authors based on World Bank data (2024).

Given the nature of potential fraudulent actions of cybercriminals, an input array of variables for assessing the consequences of vulnerability to these threats includes the following combinations of search queries obtained from the Google search engine in English on a global scale (Table 2). Data for these search queries were collected monthly throughout the study period. A total of ten search queries were formulated.

Table 2. An input data set comprising a list of search queries designed to assess the impact of vulnerability to cyber threats.

Symbol	Search query	Symbol	Search query
cyb_w1	Cyber police number	cyb_w6	Phone scam
cyb_w2	Phishing is	cyb_w7	Hacked social media
cyb_w3	Theft of personal data	cyb_w8	Scam links
cyb_w4	Card fraud	cyb_w9	Dangerous online shopping
cyb_w5	Tech support scam is	cyb_w10	Set up two-factor authentication

Sources: systematized by the authors based on Google Trends.

A third dataset was generated based on search queries reflecting individuals' willingness to participate in cyber-fraud activities. The proposed dataset includes combinations of search queries obtained globally in English from the Google search engine (Table 3). The collection of results for these search queries was carried out similarly to the second dataset (based on monthly data during the study period).

Table 3. Dataset characterizing individuals' willingness to engage in cyberfraud activities.

Symbol	Search query	Symbol	Search query
cyb_h1	Customer contact database	cyb_h6	Psychological pressure
cyb_h2	How to find out the password	cyb_h7	Your guaranteed win
cyb_h3	How to fake a password	cyb_h8	Ddos attack algorithm
cyb_h4	How to clone a website	cyb_h9	Creating of reviews
cyb_h5	How to fake an account	cyb_h10	How to bypass antivirus

Sources: systematized by the authors based on Google Trends.

Based on correlation analysis and the construction of a correlation matrix of type (1), independent indicators will be selected from each input dataset. The correlation coefficient between these indicators will not exceed the absolute value of 0.7. This approach enables the identification of the functional impact of economic and social indicators on two aspects: the willingness to participate in cyberfraudulent activities and vulnerability to cybercrime.

$$\begin{pmatrix} 1 & r_{12} & r_{13} & \dots & r_{1n} \\ r_{21} & 1 & r_{23} & \dots & r_{2n} \\ r_{31} & r_{32} & 1 & \dots & r_{3n} \\ \dots & \dots & \dots & 1 & \dots \\ r_{n1} & r_{n2} & r_{n2} & r_{nm} & 1 \end{pmatrix} \quad (1)$$

where r_{nm} is the pairwise correlation coefficient between n and m indicators.

Canonical analysis will be used as a method for determining these functional dependencies. This statistical technique enables the analysis of relationship between two sets of multidimensional variables, represented as linear combinations of variables. In canonical analysis, these sets of variables are referred to as canonical variables and are denoted as U and V, defined by the following equations (2,3):

$$U = a_1x_1 + a_2x_2 + \cdots + a_ix_i \quad (2)$$

$$V = b_1y_1 + b_2y_2 + \cdots + b_iy_i \quad (3)$$

where a_i, b_i are canonical weights; x_i, y_i are input indicators.

The closer the correlation between the canonical variables (weighted sums), the better the model explains the relationship. Canonical variables are used to determine canonical roots, which represent a set of "hidden" variables underlying the phenomenon under study. The number of possible canonical roots is equal to the number of variables in the smaller set of indicators. Each subsequent pair of canonical roots accounts for a progressively smaller proportion of the extracted variance. All calculations were performed using STATISTICA 12 software.

4. Results. A graphical representation of the frequency of results obtained for the generated search queries, which enables the assessment of vulnerability to cyber threats, is presented in Figure 1.

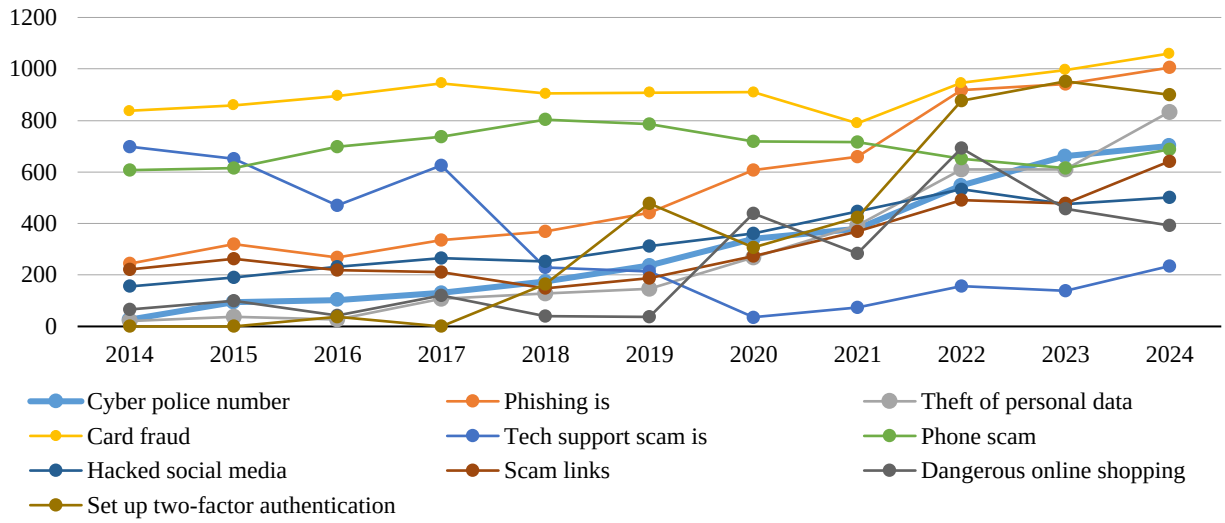

Figure 1. Frequency of search queries used to assess the consequences of vulnerability to cyber threats (2014-2024).
Sources: compiled by the authors.

Considering the presented graph (Fig. 1), the following trends were obtained:

– starting from 2019, the number of Google search queries analysed began to increase significantly.

during the studied period, the most frequent search queries were "Card fraud", "Phone scam", and "Phishing is" (on average 914, 694 and 555 queries, respectively);

– the query with the lowest frequency during the studied period was "Tech support scam is", with an average of 321 queries.

Figure 2 presents a graph of the frequency of search queries characterizing people's willingness to participate in cyber-fraud activities during 2014-2024.

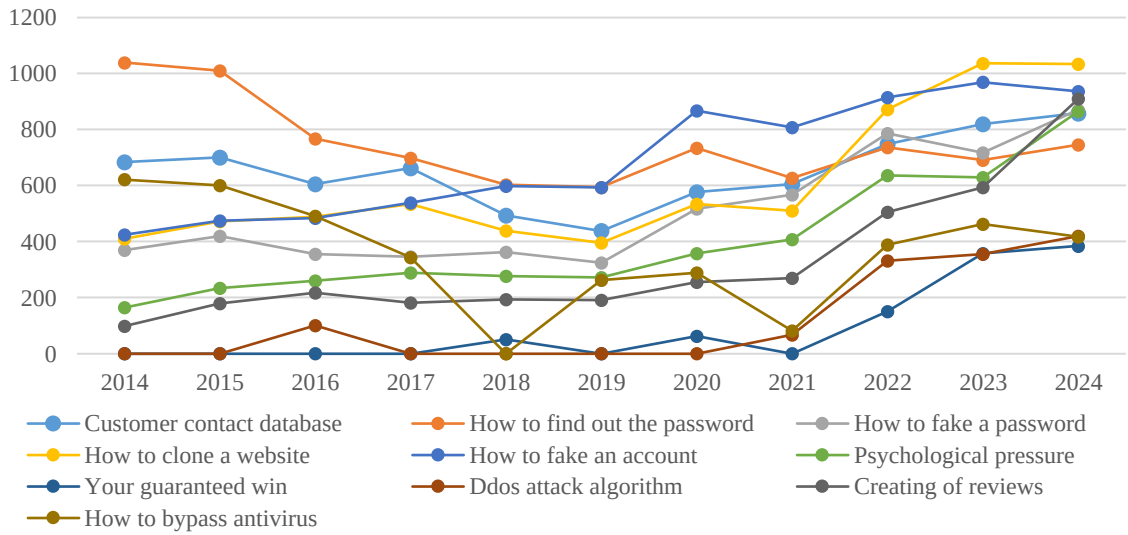

Figure 2. Frequency of search queries characterizing people's willingness to participate in cyberfraud activities (2014-2024).
Sources: compiled by the authors.

Considering the presented graph (Fig. 2), the following trends were observed:

– for this group of queries, the tendency for their frequency to increase after 2019 is also evident;

– the most frequent search queries during the studied period were: "How to fake an account", "How to find out the password", and "Customer contact database", (on average 692, 750 and 654 queries, respectively);

– the query with the lowest frequency during the studied period was "Your guaranteed win", with an average of 92 queries.

The results of the correlation analysis for economic and social indicators are summarized in Table 4.

Table 4. Correlation matrix for economic and social indicators.

	Soc_econ1	**Soc_econ2**	**Soc_econ3**	**Soc_econ4**	**Soc_econ5**
Soc_econ1	1.00	0.49	0.68	-0.56	0.55
Soc_econ2	0.49	1.00	0.60	0.42	0.61
Soc_econ3	0.68	0.60	1.00	-0.22	0.90
Soc_econ4	-0.56	0.42	-0.22	1.00	-0.43
Soc_econ5	0.55	0.61	0.90	-0.43	1.00

Sources: compiled by the authors.

Since the studied economic and social indicators are combined into one group, the correlations between them should be insignificant (less than 0.7 in absolute value). This condition is satisfied by the values in the correlation matrix (Table 4) of three of the five indicators: Soc_econ1, Soc_econ2 and Soc_econ4. Accordingly, these three indicators will be used in the canonical analysis.

The correlation matrix of search queries for assessing the consequences of vulnerability to cyber threats is presented in Table 5.

Table 5. Correlation matrix of search queries for assessing the consequences of vulnerability to cyber threats

	cyb_w1	**cyb_w2**	**cyb_w3**	**cyb_w4**	**cyb_w5**	**cyb_w6**	**cyb_w7**	**cyb_w8**	**cyb_w9**	**cyb_w10**
cyb_w1	1.00	0.99	0.98	0.67	-0.60	-0.17	0.95	0.91	0.82	0.96
cyb_w2	0.99	1.00	0.98	0.63	-0.69	-0.21	0.96	0.92	0.87	0.96
cyb_w3	0.98	0.98	1.00	0.67	-0.62	-0.20	0.94	0.95	0.81	0.94
cyb_w4	0.67	0.63	0.67	1.00	-0.22	-0.02	0.52	0.61	0.44	0.64
cyb_w5	-0.60	-0.69	-0.62	-0.22	1.00	-0.34	-0.67	-0.41	-0.61	-0.69
cyb_w6	-0.17	-0.21	-0.20	-0.02	-0.34	1.00	-0.06	-0.43	-0.34	-0.16
cyb_w7	0.95	0.96	0.94	0.52	-0.67	-0.06	1.00	0.85	0.86	0.93
cyb_w8	0.91	0.92	0.95	0.61	-0.41	-0.43	0.85	1.00	0.78	0.85
cyb_w9	0.82	0.87	0.81	0.44	-0.61	-0.34	0.86	0.78	1.00	0.79
cyb_w10	0.96	0.96	0.94	0.64	-0.69	-0.16	0.93	0.85	0.79	1.00

Sources: compiled by the authors.

The correlation matrix of search queries reflecting people's willingness to participate in cyberfraud activities is presented in Table 6.

Table 6. Correlation matrix of search queries reflecting people's willingness to participate in cyberfraud activities

	cyb_h1	**cyb_h2**	**cyb_h3**	**cyb_h4**	**cyb_h5**	**cyb_h6**	**cyb_h7**	**cyb_h8**	**cyb_h9**	**cyb_h10**
cyb_h1	1.00	0.38	0.66	0.62	0.46	0.60	0.64	0.68	0.63	0.57
cyb_h2	0.38	1.00	-0.11	-0.14	-0.45	-0.28	-0.15	-0.14	-0.20	0.62
cyb_h3	0.66	-0.11	1.00	0.92	0.88	0.96	0.85	0.92	0.92	0.07
cyb_h4	0.62	-0.14	0.92	1.00	0.81	0.94	0.95	0.97	0.94	0.19
cyb_h5	0.46	-0.45	0.88	0.81	1.00	0.87	0.77	0.75	0.79	-0.25
cyb_h6	0.60	-0.28	0.96	0.94	0.87	1.00	0.91	0.94	0.98	-0.01
cyb_h7	0.64	-0.15	0.85	0.95	0.77	0.91	1.00	0.91	0.94	0.14
cyb_h8	0.68	-0.14	0.92	0.97	0.75	0.94	0.91	1.00	0.94	0.20
cyb_h9	0.63	-0.20	0.92	0.94	0.79	0.98	0.94	0.94	1.00	0.09
cyb_h10	0.57	0.62	0.07	0.19	-0.25	-0.01	0.14	0.20	0.09	1.00

Sources: compiled by the authors.

Given the results of the correlation matrices (Table 5 and 6) three indicators from the group of Google search queries assessing the consequences of vulnerability to cyberthreats (cyb_w4, cyb_w5, cyb_w6) will be included in the canonical analysis. Similarly, from the group of Google search queries characterizing people's willingness to participate in cyberfraudulent activities, the selected indicators are cyb_h1, cyb_h2, and cyb_h10.

Thus, two canonical models will be constructed in this study:

– the first canonical model, where the canonical variables will consist of economic and social indicators (*V*) and Google search queries assessing vulnerability to cyberthreats (*U1*);

– the second canonical model, where the canonical variables will consist of economic and social indicators (*V*) and Google search queries reflecting people's willingness to participate in cyberfraudulent activities (*U2*).

The results of the canonical analysis for the first canonical model are presented in Table 7.

Table 7. Canonical analysis for the first canonical model.

	Left Set	Right Set
No. of variables	3	3
Variance extracted	100.000%	100.000%
Total redundancy	41.6680%	49.6063%
Variables: 1	cyb_w4	soc_econ1
2	cyb_w5	soc_econ2
3	cyb_w6	soc_econ4

Note: Canonical R - 0.95481; Chi²(9) - 14.527 p - 0.10482

Sources: compiled by the authors.

Based on the presented results (Table 7), the obtained canonical correlation value R = 0.95 confirms the presence of a strong correlation between the studied groups of indicators. The value of the Total Redundancy indicator also provides important insights. On one hand, 41.7% of the changes in the dynamics of Google search queries, which assess the consequences of vulnerability to cyber threats, are attributable to changes in the studied economic and social indicators. On the other hand, 49.6% of the changes in the studied economic and social indicators are explained by changes in Google search queries assessing the consequences of vulnerability to cyber threats. These findings demonstrate that a country's economic and social situation is directly influenced by the population's vulnerability to cyber threats.

In the next step of the canonical analysis, it is necessary to identify statistically significant canonical roots. The obtained canonical roots and their statistical significance criteria are presented in Table 8.

Table 8. Results of canonical roots and their statistical significance for the first canonical model.

Root removed	Canonical R	Canonical R^2	Chi-sqr.	df	p	Lambda
0	0.95	0.91	24.53	9.00	0.00	0.04
1	0.74	0.55	23.61	4.00	0.04	0.45
2	0.01	0.00	0.00	1.00	0.99	1.00

Sources: compiled by the authors.

The statistical significance of the Chi- square criterion for the zero and first values of the canonical roots ($p<0.05$) indicates that only the first canonical root should be used for further analysis. The factor structure of the selected canonical roots for both groups of indicators is presented in (Table 9).

Table 9. Factor structure of canonical roots for both groups of indicators of the first canonical model.

Indicator	Root1	Root2	Root3
cyb_w4	-0.29	-0.95	0.06
cyb_w5	-0.81	0.27	-0.53
cyb_w6	-0.08	-0.24	0.97
Soc_econ1	0.79	-0.26	0.56
Soc_econ2	0.91	0.00	-0.41
Soc_econ4	0.07	0.47	-0.88

Sources: compiled by the authors.

Considering the obtained factor loadings, not all indicators demonstrate the highest correlation coefficients with the first canonical root. Only cyb_w5, Soc_econ1 and Soc_econ2 demonstrate significant values. The canonical weights of the indicators for the first canonical model are presented in Table 10.

Table 10. Canonical weights of indicators of the first canonical model.

Indicator	Root1	Root2	Root3
cyb_w4	-0.17	-1.01	-0.26
cyb_w5	-1.12	0.34	-0.01
cyb_w6	-0.60	0.24	1.04
Soc_econ1	1.01	4.08	2.24
Soc_econ2	0.18	-3.86	-2.03
Soc_econ4	0.55	4.37	1.23

Sources: compiled by the authors.

The regression equations for the first canonical model are as follows (Equations 4 and 5):

$$U1 = -0{,}17cyb_{w4} - 1{,}12cyb_{w5} - 0{,}6cyb_{w6} \quad (4)$$

$$V = 1{,}01Soc\_econ1 + 0{,}18Soc\_econ2 + 0{,}55Soc\_econ4 \quad (5)$$

Thus, among the indicators identifying the population's vulnerability to cyber fraud, the most influential is cyb_w5 ("Tech support scam is"). Regarding economic and social indicators, the greatest influence is exerted by the Soc_econ1 (GNI per capita) and Soc_econ4 (Unemployment) indicators. Therefore, according to the results of the first canonical model, it can be concluded that the vulnerability of the population to the consequences of cyber fraud has a significant impact on the economic and social situation of the country. At the same time, the inverse relationship is weaker.

The final results of the canonical analysis for the second canonical model are presented in Table 11.

Based on the presented results (Table 11), the obtained canonical correlation value R = 0.97, confirming the presence of a strong correlation between the studied groups of indicators, as observed in the previous canonical model. Regarding the results of Total redundancy, 14.9% of the change in the dynamics of Google search queries characterizing people's willingness to participate in cyberfraudulent activities, is due to a change in the studied economic and social indicators. Conversely, 25.5% of the change in the studied economic and social indicators is explained by a change in the corresponding search queries. These findings indicate that the economic and social situation of the country is largely determined by cyberfraudulent actions.

Table 11. Canonical analysis for the second canonical model.

		Left Set	Right Set
No. of variables		3	3
Variance extracted		100.000%	100.000%
Total redundancy		14.9309%	25.4527%
Variables:	1	cyb_h1	soc_econ1
	2	cyb_h2	soc_econ2
	3	cyb_h10	soc_econ4

Note: Canonical R - 0.96958; Chi²(9) - 14.193 p - 0.01568

Sources: compiled by the authors.

In the next step of the canonical analysis, it is necessary to select statistically significant canonical roots. The obtained canonical roots and the criteria for their statistical significance for the second canonical model are presented in Table 12.

Table 12. Results of canonical roots and their statistical significance for the second canonical model.

Root removed	Canonical R	Canonical R^2	Chi-sqr.	df	p	Lambda
0	0.97	0.94	114.19	9.00	0.02	0.04
1	0.53	0.29	111.53	4.00	0.02	0.71
2	0.06	0.00	0.01	1.00	0.91	1.00

Sources: compiled by the authors.

The statistical significance of the Chi- square criterion for the zero and first values of the canonical roots ($p<0.05$) indicates that for further analysis it is sufficient to use only the first canonical root. The factor structure of the selected canonical roots for both groups of indicators is presented in Table 13.

Table 13. Factor structure of canonical roots for both groups of indicators in the second canonical model.

Indicator	Root1	Root2	Root3
cyb_h1	-0.23	-0.10	-0.97
cyb_h2	0.49	0.30	-0.82
cyb_h10	0.14	0.65	-0.75
Soc_econ1	-0.41	-0.81	0.41
Soc_econ2	-0.16	-0.81	-0.56
Soc_econ4	0.47	0.00	-0.89

Sources: compiled by the authors.

Considering the obtained factor loadings, the indicators with the highest correlation coefficients with the first canonical root are cyb_h2, Soc_econ1 and Soc_econ4. The canonical weights of the indicators for the second canonical model are presented in Table 14.

Table 14. Canonical weights of indicators in the second canonical model.

Indicator	Root1	Root2	Root3
cyb_h1	-0.85	-0.69	-0.76
cyb_h2	1.95	-0.86	-0.38
cyb_h10	-1.04	1.83	0.06
Soc_econ1	3.78	-2.11	1.98
Soc_econ2	-3.79	0.88	-1.99
Soc_econ4	4.17	-1.55	1.06

Sources: compiled by the authors.

The regression equations for the first canonical model are as follows (Equations 6 and 7):

$$U2 = -0{,}85cyb_{h1} + 1{,}95cyb_{h2} - 1{,}04cyb_{h10} \quad (6)$$

$$V = 3{,}78Soc\_econ1 - 3{,}79Soc\_econ2 + 4{,}14Soc\_econ4 \quad (7)$$

Thus, among the search queries characterizing people's willingness to participate in cyberfraud activities, the most influential indicator is cyb_h2 ("How to find out the password"). As for economic and social indicators, all three studied indicators demonstrate significant impact. Therefore, based on the results of the second canonical model, it can be concluded that, similar to the results of the first canonical model, the potential activity of cyberfraudsters has a greater influence on the economic and social situation of the country than vice versa.

5. Discussion. This study found that socio-economic factors significantly influence both the vulnerability of the population to cybercrime and the willingness of society to engage in such activities. The results of correlation and canonical analyses showed that economic indicators such as GNI per capita, unemployment rate, and spending as a percentage of GDP are strong determinants of both individual and collective cybercrime-related behaviour. Furthermore, the findings confirm that the vulnerability of the population to cyberfraud has a far greater impact on the socio-economic situation of the country than the reverse. The results confirm the findings of previous studies that highlight the roles of income inequality and unemployment in fostering cybercrime (Ilievski & Bernik, 2016; Achim et al., 2021). These findings are consistent with Dodel & Gustavo (2018), who highlighted the critical role of digital inequality in determining safe online behaviour. However, the peculiarity of this study is that it takes into account the relationship between social vulnerability of society and the socio-economic environment of the country, demonstrating how economic downturns and social inequality can increase vulnerability to cyberthreats.

A significant contribution of this study is the analysis of the interaction of society with cybercrime - from both the victim and the perpetrator's perspective. The analysis identifies societal tolerance for certain cyber activities and limited public awareness of cybersecurity as key drivers of these issues. These results can be taken into account when formulating recommendations for countries with different levels of economic development.

The key contribution of this study is to identify two crucial aspects: the significant influence of population vulnerability to cyber threats on socio-economic processes and the confirmation of individual search queries as indicators of societal readiness for cyber fraud. These findings highlight the need to increase digital literacy, reduce unemployment, and take into account economic and social factors into cybersecurity strategies. The

results obtained confirm the need to apply a multifaceted innovative approach to combating cybercrime, combining technological advances, digital literacy, material well-being, and social security of society. The practical significance of the findings lies in their potential to inform the development of targeted measures to prevent cybercrime and increase the resilience of society to cyber threats.

6. Conclusions. This study is devoted to the analysis of socio-economic factors influencing the development of cybercrime and the involvement of society in this activity, both as victims and potential criminals. It highlights the impact of socio-economic indicators, such as GNI per capita, unemployment rate and spending as a percentage of GDP, on the dynamics of cybercrime. Additionally, the study examines trends in public awareness and engagement with cyberthreats.

The analysis explores the links between socio-economic conditions and behaviours related to cybercrime. It demonstrates the significant role of socio-economic inequality and unemployment in managing cybercrime risks and emphasizes the dual nature of the relationship between socio-economic development and cybercrime. On one hand, these indicators determine society's vulnerability to cybercrime; on the other hand, they encourage certain segments of the population to engage in criminal schemes as a means of generating income.

The analysis showed that economic conditions, such as high unemployment and low digital literacy, correlate with increased vulnerability to cyberthreats, confirming the findings of Dodel & Gustavo (2018). The results also highlighted the significant role of public awareness, as countries with high literacy levels demonstrate greater resilience to cybercrime.

Unlike previous studies, this research reveals a much greater impact of cybercrime on the indicators of socio-economic development than vice versa. This indicates that a country’s socio-economic development largely depends on the level of its cybersecurity, and cybercrime is not only a consequence of socio-economic inequality, but also a factor that worsens these conditions. These findings highlight the need to improve existing mechanisms for combating cybercrime and integrating these measures into national economic development strategies.

Despite the practical contribution of this study to the development of mechanisms for combating cybercrime, it has several limitations that can be considered in further research. Thus, previous studies (Padyab et al., 2024; Chen et al., 2023) emphasize the value of cross-regional analyses to uncover the specific relationships between indicators and enable comparisons across countries or regions. At the same time, the data obtained from search queries do not fully reflect the complexity of the dynamics of cybercrime.

In addition, for further research, it is important to consider a larger number of factors influencing the development of cybercrime and to assess the long-term and short-term relationships between these indicators.

The findings of this study may be useful to policymakers in forming strategies to combat cybercrime. They confirm the necessity of adopting an integrated approach to cyber risk management that incorporates both economic and social dimensions.

Author Contributions: conceptualization, I. T., W. Z., and I. P.; methodology, I. T., W. Z., and I. P.; software, I. P.; validation, I. T., W. Z., and I. P.; formal analysis, I. T., W. Z., and I. P.; investigation, I. T., W. Z., and I. P.; resources, I. T., W. Z., and I. P.; data curation, I. T., W. Z., and I. P.; writing-original draft preparation, I. T., W. Z., and I. P.; writing-review and editing, I. T., W. Z., and I. P.; visualization, I. T., W. Z., and I. P.; supervision, I. T., W. Z., and I. P.; project administration, I. T., W. Z., and I. P.; funding acquisition, I. T., W. Z., and I. P.

Conflicts of Interest: Authors declare no conflict of interest.

Data Availability Statement: Data on economic and social development indicators were obtained from open sources of the World Bank (World Bank data, 2024). The dataset for assessing the vulnerability of the population to cyber threats was obtained from the Google search engine based on the analysis of monthly search queries (Google Trends, 2024).

Informed Consent Statement: Not applicable.

References

1. Achim, M. V., Văidean, V. L., Borlea, S. N., & Florescu, D. R. (2021). The Impact of the Development of Society on Economic and Financial Crime. Case Study for European Union Member States. *Risks*, *9*(5), 97. [Google Scholar] [CrossRef]

2. Afzal, M., Ansari, M. S., Ahmad, N., Shahid, M., & Shoed, M. (2024). Cyberfraud, usage intention, and cybersecurity awareness among e-banking users in India: an integrated model approach. *Journal of Financial Services Marketing, 29*, 1503–1523. [Google Scholar] [CrossRef]

3. Ahmead, M., El Sharif, N., & Abuiram, I. (2024). Risky online behaviors and cybercrime awareness among undergraduate students at Al Quds University: a cross sectional study. *Crime Science*, *13*, 29. [Google Scholar] [CrossRef]
4. AlDairi, A., & Tawalbeh, L. (2017). Cyber Security Attacks on Smart Cities and Associated Mobile Technologies. *Procedia Computer Science*, 109, 1086–1091. [Google Scholar] [CrossRef]
5. Alharbi, N., Alkalifah, B., Alqarawi, G., & Rassam, M. A. (2024). Countering Social Media Cybercrime Using Deep Learning: Instagram Fake Accounts Detection. *Future Internet*, *16*(10), 367. [Google Scholar] [CrossRef]
6. Anderson, R., Barton, C., Böhme, R., Clayton, R., Van Eeten, M., Levi, M., Moore, T., & Savage, S. (2019). Measuring the changing cost of cybercrime. *Journal of Cybersecurity*, *5*(1), 1–12. [Google Scholar]
7. Bada, M., & Nurse, J. (2019). The Social and Psychological Impact of Cyber-Attacks. Emerging Cyber Threats and Cognitive Vulnerabilities, 73-92. [Google Scholar] [CrossRef]
8. Boppre, B., Salisbury, E.J., Parker, J. (2018). Pathways to Crime. In *Oxford Research Encyclopedia of Criminology and Criminal Justice*. Oxford University Press: Oxford, UK. [Google Scholar] [CrossRef]
9. Boussi, O., Gupta, H., & Hossain, S. (2024). A machine learning model for predicting phishing websites. *International Journal of Electrical and Computer Engineering (IJECE)*, *14*, 4228. [Google Scholar] [CrossRef]
10. Brewer, R., Cale, J., Goldsmith, A., & Holt, T. (2018). Young People, the Internet, and Emerging Pathways into Criminality: A Study of Australian Adolescents. *International Journal of Cyber Criminology*, *12*, 115–132. [Google Scholar] [CrossRef]
11. Chen, S., Ding, F., Buil-Gil, D., Hao, M., Maystadt, J. F., Fu, J., ... & Jiang, D. (2024). The impact of COVID-19 lockdown on fraud in the UK. *Humanities and Social Sciences Communications*, *11*(1), 1-11. [Google Scholar] [CrossRef]
12. Chen, S., Hao, M., Ding, F., Jiang, D., Dong, J., Zhang, S., Guo, Q., & Gao, C. (2023). Exploring the global geography of cybercrime and its driving forces. *Humanities and Social Sciences Communications*, *10*(71). [Google Scholar] [CrossRef]
13. Choi, K.S., Chawki, M., & Basu, S. (2024). Digital shadows: analyzing factors influencing sentencing in child sexual abuse material (CSAM) cases. *Journal of Aggression, Conflict and Peace Research*, *16*(4), 363-381. [Google Scholar] [CrossRef]
14. Cotrina, L., León, P., Reyes, C., Arbulú Ballesteros, M., Guzmán, M., Castillo, J., Acosta, R., & Morales, A. (2024). Cyber Crimes: A Systematic Review of Evolution, Trends, and Research Approaches. *Journal of Educational and Social Research*, *14*(5), 96. [CrossRef]
15. Creese, S., Dutton, W. H. & Esteve-González, P. (2021). The social and cultural shaping of cybersecurity capacity building: a comparative study of nations and regions. *Personal and Ubiquitous Computing, 25*, 941–955. [Google Scholar] [CrossRef]
16. Dawson, M., Bacius, R., Gouveia, L. B., & Vassilakos, A. (2021). Understanding the challenge of cybersecurity in critical infrastructure sectors. *Land Forces Academy Review*, *26*(1), 69–75. [Google Scholar] [CrossRef]
17. De Kimpe, L., Walrave, M., Verdegm, P., & Ponnet, K. (2022). What we think we know about cybersecurity: An investigation of the relationship between perceived knowledge, internet trust, and protection motivation in a cybercrime context. *Behaviour & Information Technology*, 41(8), 1796–1808. [Google Scholar] [CrossRef]
18. Dodel, M., & Gustavo M. (2019). An integrated model for assessing cyber-safety behaviors: how cognitive, socioeconomic and digital determinants affect diverse safety practices. *Computers & Security*, *86*, 75–91. [Google Scholar] [CrossRef]
19. Dodel, M., & Gustavo, M. (2018). Inequality in Digital Skills and the Adoption of Online Safety Behaviors. *Information, Communication & Society*, *21*(5), 712–728. [Google Scholar] [CrossRef]
20. Dodel, M., & Mesch, G. (2018). Inequality in digital skills and the adoption of online safety behaviors. *Information, Communication & Society*, *21*(5), 712–728. [Google Scholar] [CrossRef]
21. Donner, C.M., Marcum, C.D., Jennings, W.G., Higgins, G.E., Banfield, J. (2014). Low self-control and cybercrime: Exploring the utility of the general theory of crime beyond digital piracy. *Computers in Human Behavior*, *34*, 165–172. [Google Scholar] [CrossRef]
22. El Asam, A., & Katz, A. (2018). Vulnerable young people and their experience of online risks. *Human–Computer Interaction*, *33*, 281–304. [Google Scholar] [CrossRef]
23. Forssell, R. C. (2020) Gender and organisational position: predicting victimisation of cyberbullying behaviour in working life. *The International Journal of Human Resource Managemente*, *31*, 2045–2064. [Google Scholar] [CrossRef]
24. Google Trends (2024). [Link]
25. Havers, B., Tripathi, K., Burton, A., McManus, S., & Cooper, C. (2024). Cybercrime victimisation among older adults: A probability sample survey in England and Wales. *PLoS ONE*, *19*(12), e0314380. [Google Scholar] [CrossRef]
26. Hoy, M. G., & Milne, G. (2010). Gender differences in privacy-related measures for young adult Facebook users. *Journal of Interactive Advertising*, 10(2), 28–45. [Google Scholar] [CrossRef]
27. Hytönen, E., Trent, A., & Ruoslahti, H. (2022). Societal Impacts of Cyber Security in Academic Literature – Systematic Literature Review. *Proceedings of the 21st European Conference on Cyber Warfare and Security*, 21(1), 86-93. [Google Scholar] [CrossRef]

28. Ilievski, A., & Bernik, I. (2016). Social-economic aspects of cybercrime. *Innovative Issues and Approaches in Social Sciences*, 9(3), 8-22. [Google Scholar] [CrossRef]
29. Isaia, E., Oggero, N., & Sandretto, D. (2024). Is financial literacy a protection tool from online fraud in the digital era? *Journal of Behavioral and Experimental Finance*, *44*, 100977. [Google Scholar] [CrossRef]
30. John, M. S. (2024). *Cybersecurity Stats: Facts And Figures You Should Know*. Forbes. [Link]
31. Khan, N. F., Ikram, N., & Saleem, S. (2023). Effects of socioeconomic and digital inequalities on cybersecurity in a developing country. *Security Journal*, *37*, 214–244. [Google Scholar] [CrossRef]
32. Kwon, D., Borrion, H., Wortley, R. (2024). Measuring Cybercrime in Calls for Police Service. *Asian Journal of Criminology*, 19, 329–351. [Google Scholar] [CrossRef]
33. Lee, C. S., & Chua, Y. T. (2024). The Role of Cybersecurity Knowledge and Awareness in Cybersecurity Intention and Behavior in the United States. *Crime & Delinquency*, *70*(9), 2250-2277. [Google Scholar] [CrossRef]
34. Lee, H., & Lim, H. (2019) Awareness and Perception of Cybercrimes and Cybercriminals. *International Journal of Cybersecurity Intelligence & Cybercrime*, 2(1), 1-3. [Google Scholar] [CrossRef]
35. Leukfeldt, E.R., & Yar, M. (2016). Applying Routine Activity Theory to Cybercrime: A Theoretical and Empirical Analysis. *Deviant Behavior*, *37*, 263–280. [Google Scholar] [CrossRef]
36. Luo, Q. (2024). Cybercrime as an industry: examining the organisational structure of Chinese cybercrime. *Humanities and Social Sciences Communications*, *11*, 1554. [Google Scholar] [CrossRef]
37. Lusthaus, J. (2012). Trust in the world of cybercrime. *Global Crime*, 13(2), 71–94. [Google Scholar] [CrossRef]
38. Lusthaus, J., Kleemans, E., Leukfeldt, R., & Holt, T. (2024). Cybercriminal networks in the UK and Beyond: Network structure, criminal cooperation and external interactions. *Trends in Organized Crime*, 27, 364–387. [Google Scholar] [CrossRef]
39. Martineau, M., Spiridon, E., & Aiken, M. (2024). Pathways to Criminal Hacking: Connecting Lived Experiences with Theoretical Explanations. *Forensic Sciences*, *4*(4), 647-668. [Google Scholar] [CrossRef]
40. Martineau, M., Spiridon, E., Aiken, M. A (2023). Comprehensive Framework for Cyber Behavioral Analysis Based on a Systematic Review of Cyber Profiling Literature. *Forensic Sciences*, *3*, 452–477. [Google Scholar] [CrossRef]
41. Monteith, S., Bauer, M., Alda, M., Geddes, J., Whybrow, P. C., Glenn T. (2021). Increasing Cybercrime Since the Pandemic: Concerns for Psychiatry. *Current Psychiatry Reports*, *23*(18). [Google Scholar] [CrossRef]
42. Moubarak, H. F. A., & Afthanorhan, A. (2024). Risk assessments of virtual interactions on Saudi families. *Humanities and Social Sciences Communications*, *11*, 281. [Google Scholar] [CrossRef]
43. Ngo, F.T., & Paternoster, R. (2011). Cybercrime victimization: An examination of individual and situational level factors. *International Journal of Cyber Criminology*, *5*, 773. [Google Scholar]
44. Nguyen, T., & Luong, H. T. (2021). The structure of cybercrime networks: transnational computer fraud in Vietnam. *Journal of Crime and Justice*, 44(4), 419–440. [Google Scholar] [CrossRef]
45. Odinot, G., Verhoeven, M. A., Pool, R. L. D., & De Poot, C. J. (2017). Organised cyber-crime in the Netherlands: empirical findings and implications for law enforcement. WODC, Den Haag. Cahier 2017-1. [Google Scholar]
46. Padyab, M., Padyab, A., Rostami, A., & Ghazinour, M. (2024). Cybercrime in Nordic countries: a scoping review on demographic, socioeconomic, and technological determinants. *SN Social Sciences*, *4*, 205. [Google Scholar] [CrossRef]
47. Pandian, T., & Maraimalai, N. (2024). Understanding cybercrime's impact on women's physical and psychological well-being. *African Journal of Reproductive Health / La Revue Africaine de La Santé Reproductive*, *28*(5), 103–112. [Google Scholar] [CrossRef]
48. Patil, R.Y., Patil, Y.H., Despande, H., & Bannore, A. (2024). Proactive cyber defense through a comprehensive forensic layer for cybercrime attribution. *International Journal of Information Technology*, *16*, 3555–3572. [Google Scholar] [CrossRef]
49. Phillips, K., Davidson, J. C., Farr, R. R., Burkhardt, C., Caneppele, S., & Aiken, M. P. (2022). Conceptualizing Cybercrime: Definitions, Typologies and Taxonomies. *Forensic Sciences*, *2*, 379–398. [Google Scholar] [CrossRef]
50. Rao, S., Verma, A. K., & Bhatia, T. (2021). A review on social spam detection: Challenges, open issues, and future directions. *Expert Systems with Applications*, *186*, 115742. [Google Scholar] [CrossRef]
51. Ratul, M. H. A., Mollajafari, S., & Wynn, M. (2024). Managing Digital Evidence in Cybercrime: Efforts Towards a Sustainable Blockchain-Based Solution. *Sustainability*, *16*(24), 10885. [Google Scholar] [CrossRef]
52. Rey-Ares, L., Fernández-López, S., & Álvarez-Espiño, M. (2024). The role of financial literacy in consumer financial fraud exposure (via email) and victimisation: evidence from Spain. *International Journal of Bank Marketing*, 42(6), 1388-1413. [Google Scholar] [CrossRef]
53. Rich, M. S., & Aiken, M.P. (2024). An Interdisciplinary Approach to Enhancing Cyber Threat Prediction Utilizing Forensic Cyberpsychology and Digital Forensics. *Forensic Sciences*, *4*, 110–151. [Google Scholar] [CrossRef]
54. Shettar, I., Hadagali, G.S., Kaddipujar, M., Bulla, S.D., Agadi, K., Ganjihal, G.A., Hiremath, R., Dundannanavar, A., & Babu, B.R. (2024). Scientometric analysis of global cyber security research output based on Web of Science. *Iberoamerican Journal of Science Measurement and Communication*, *4*(2), 1-15. [Google Scholar] [CrossRef]

55. Steinmetz, K. F., Schaefer, B. P., McCarthy, A. L., Brewer, C. G., & Kurtz, D. L. (2024). Exploring Cybercrime Capabilities: Variations Among Cybercrime Investigative Units. *Criminal Justice Policy Review*, *35*(4), 194-215. [Google Scholar] [CrossRef]
56. Sulich, A., Rutkowska, M., Krawczyk-Jezierska, A., Jezierski, J., & Zema, T. (2021). Cybersecurity and sustainable development. *Procedia Computer Science, 192*, 20–28. [Google Scholar] [CrossRef]
57. Wissink, I. B., Standaert, J.C.A., Stams, G.J.J.M., Asscher, J.J., Assink, M. (2023). Risk factors for juvenile cybercrime: A meta-analytic review. *Aggression and Violent Behavior, 70*, 101836. [Google Scholar] [CrossRef]
58. World Bank (2024). *World Bank Open Data* [Link]
59. Wright, D., & Kumar, R. (2023). Assessing the socio-economic impacts of cybercrime. *Societal Impacts, 1*(100013). [Google Scholar] [CrossRef]
60. Wright, M. F., & Wachs, S. (2020). Adolescents' Cyber Victimization: The Influence of Technologies, Gender, and Gender Stereotype Traits. *International Journal of Environmental Research and Public Health*, *17*(4), 1293. [Google Scholar] [CrossRef]
61. Yigzaw, Y., Mekuriaw, A., & Amsalu, T. (2023). Analyzing physical and socio-economic factors for property crime incident in Addis Ababa, Ethiopia. *Heliyon, 9*(2), e13282. [Google Scholar] [CrossRef]
62. Zhou, Y., Tiwari, M., Bernot, A., & Lin, K. (2024). Metacrime and Cybercrime: Exploring the Convergence and Divergence in Digital Criminality. *Asian Journal of Criminology*, *19*, 419–439. [Google Scholar] [CrossRef]
63. Zsila, Á., Urbán, R., Griffiths, M. D., & Gemetrovics, Z. (2019). Gender Differences in the Association Between Cyberbullying Victimization and Perpetration: The Role of Anger Rumination and Traditional Bullying Experiences. *International Journal of Mental Health and Addiction*, *17*, 1252–1267. [Google Scholar] [CrossRef]

Інноваційні підходи до забезпечення кібербезпеки та громадської безпеки: соціально-економічний вимір

Інна Тютюник, Сумський державний університет, Україна
Ірина Позовна, Сумський державний університет, Україна
Войцех Заскорський, Університет WSB, Польща

Це дослідження присвячене аналізу соціально-економічних аспектів розвитку кіберзлочинності та залученості суспільства, як у ролі жертв, так і безпосередніх ініціаторів до цієї діяльності. У роботі розглянуто вплив індикаторів соціально-економічного розвитку, зокрема валового національного доходу, обсягу витрат та грошових переказів, рівня грамотності та безробіття, на динаміку кіберзлочинності в світі, проведено аналіз тенденцій поінформованості громадськості та їх залучення до злочинної діяльності у цифровому просторі. Методичним інструментарієм дослідження є методи кореляційного та канонічного аналізу, реалізовані за допомогою програмного забезпечення Statistica 12. За результатами аналізу взаємозв'язку між індикаторами соціально-економічного розвитку суспільства та поведінкою, пов'язаною з кіберзлочинністю, встановлено дуальний вплив цих факторів на вразливість до кіберзлочинів та участь у злочинній діяльності як способі отримання доходу. З одного боку, соціально-економічні диспропорції, зокрема нерівність доходів і безробіття, сприяють зростанню вразливості суспільства до кіберзлочинів. З іншого боку, високий рівень бідності населення стимулює певну його частину до участі у кіберзлочинній діяльності. Результати дослідження свідчать про те, що соціально-економічна нерівність і безробіття відіграють ключову роль в управлінні ризиками кіберзлочинності. Вищий рівень економічного розвитку та соціальної захищеності суспільства супроводжується більшою стійкістю до кіберзагроз, тоді як високий рівень безробіття та значна економічна нерівність збільшують вразливість суспільства до даних ризиків. Дослідження засвідчило, що соціально-економічний стан країни значною мірою залежить від рівня кіберзлочинності, що підкреслює необхідність інтеграції заходів з кібербезпеки в національні стратегії економічного розвитку. Практична значущість отриманих результатів полягає в застосуванні комплексного підходу до розуміння кіберзлочинності, який враховує як віктимізацію, так і активну участь суспільства у даній діяльності. Результати дослідження можуть стати основою для розробки цільових заходів з профілактики кіберзлочинності та підвищення стійкості суспільства до кіберзагроз. Отримані результати підкреслюють важливість врахування економічної і соціальної складових у процесі розробки ефективних стратегій забезпечення кібербезпеки, які сприятимуть мінімізації ризиків використання цифрового простору і посиленню соціально-економічної стабільності країни.

Ключові слова: кіберзлочинність; маніпулювання даними; економічний розвиток; шахрайство; інформаційна доступність; доходи населення; соціальна нерівність.