Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies, 17*(2), 220-239. doi:10.14254/2071-8330.2024/17-2/12

Journal of International Studies

Centre of Sociological Research

Scientific Papers

Cybersecurity and cybercrime: Current trends and threats

Aleksandra Kuzior
Faculty of Organization and Management,
Silesian University of Technology, Poland
aleksandra.kuzior@polsl.pl
ORCID 0000-0001-9764-5320

Inna Tiutiunyk
Department of Financial Technologies and Entrepreneurship,
Sumy State University, Ukraine
i.tiutiunyk@biem.sumdu.edu.ua
ORCID 0000-0001-5883-2940

Anetta Zielińska
Wroclaw University of Economics and Business,
Wrocław, Poland
anetta.zielinska@ue.wroc.pl
ORCID 0000-0001-8592-3530

Roland Kelemen
Széchenyi István University,
Faculty of Law and Political Sciences,
Gyor, Hungary
kelemen.roland@ga.sze.hu
ORCID 0000-0002-5419-8425

Abstract. The rapid development of digital technologies and their active implementation in all spheres of the economy, on the one hand, contribute to increased control over the activities of economic entities, and on the other hand, create new challenges associated with the dynamic development of cybercrime. The purpose of the article is to analyze the global trends in cybercrime in 2016-2023 (by calculating national levels of cybercrime) and to model the mechanisms of combating it in order to form a global, open and safe cyberspace, protect the population from cyber threats and cyber fraud, increase the effectiveness of financial monitoring procedures and control over transactions in cyberspace. The article presents the dominant directions, evolutionary, temporal and spatial patterns of the development of crime in cyberspace, clustering of the countries,

Received:
May, 2023
1st Revision:
March, 2024
Accepted:
June, 2024

DOI:
10.14254/2071-8330.2024/17-2/12

and identification of leaders and outsiders in the field of cybercrime (through visualization density maps based on the construction of self-organized Kohonen maps). The results of the calculations confirm a significant increase in the level of cybercrime in the world since 2016 (in particular, due to the COVID-19 pandemic and active digital transformation). A comparative analysis of the indicator across countries made it possible to distinguish those with the highest rates of cybercrime (Slovenia, Iceland, Moldova, Georgia) and those with a significantly higher level of cyber security (Greece, Belgium, France, Germany).

Keywords: cybercrime, cybersecurity, digital transformation, cyberspace, cyber fraud.

JEL Classification: C38, F52, O17

1. INTRODUCTION

Statistics and reports provide compelling evidence of the world becoming increasingly digital, with more transactions and activities taking place online. The growth in e-commerce, digital payments, digital transformation initiatives, internet and mobile usage, and cloud computing adoption all underscore this trend.

In 2023, global retail e-commerce sales were estimated at 5.8 trillion U.S. dollars (Statista, n.d.; Mouna & Yassine, 2024). In the current year, they are projected to surpass 6.3 trillion U.S. dollars (van Gelder, 2024), with expectations for continued growth in the years ahead to surpass eight trillion dollars by 2027. United Nations Conference on Trade and Development reported that e-commerce's share of global retail sales increased from 16% in 2019 to 19% in 2021, indicating a shift towards online shopping. World Payments Report 2023 (Capgemini Research Institute, 2023) revealed that non-cash transactions have remained robust as consumers and businesses, both small and large, embraced digital payment methods. The report indicated that non-cash transaction volumes were expected to accelerate with a compound annual growth rate of 15% from 2022 to 2027. This growth is driven by improving macroeconomic conditions, the expansion of digital payment infrastructure, and the proliferation of new payment instruments. Digital (non-cash) payment transactions are forecasted to reach 1.3 trillion by 2023, i.e., 16.6% year-over-year growth rate. Mobile payments, contactless cards, and digital wallets are driving this growth, reflecting an increasing preference for online transactions.

Gartner reports that 91% of organizations are engaged in some form of digital initiative, with 87% of senior business leaders considering digitalization a company priority. The digital transformation market is expected to grow from $469.8 billion in 2020 to $1,009.8 billion by 2025. IDC (IDC, n.d.) predicts that global spending on digital transformation will reach $3.9 trillion in 2027 with a five-year compound annual growth rate of 16.1%.

Increase in Internet and Mobile Device Usage is also a stable modern trend. ITU (ITU, n.d.) reports that by the end of 2023, 67% of the global population was using the Internet, up from 51% in 2019. The number of mobile phone users reached 78 percent of the global population aged 10 and over in 2023. Next digitalisation trend is cloud computing adoption, for instance, according to Flexera 2023 State of the Cloud Report (Flexera, 2024) 89% of enterprises have a multi-cloud strategy, and 73% have a hybrid cloud strategy, indicating widespread adoption of cloud technologies. The shift to cloud computing supports the increasing digitalization of business operations and online activities. Gartner (Gartner, 2023) forecasts that global public cloud spending will grow on 20.4% to total $678.8 billion in 2024 up from $563.6 billion in 2023.

Cloud infrastructure and services are critical enablers of digital transactions and activities (Lozano-Almansa et al., 2023).

As the world becomes increasingly digital, with more transactions and activities taking place online, the risk and impact of cybercrime grow. Various reports, statistics, and expert analyses demonstrate cybercrime's increasing frequency and sophistication, including hacking, phishing, ransomware, and other malicious activities. These problems concern developed countries. For example, The FBI's Internet Crime Complaint Center reported that cybercrime resulted in $10.3 billion in losses in 2022, up from $6.9 billion in 2021. The IC3 received 800,944 complaints in 2022, indicating a steady increase in the number of incidents reported year over year.

The Verizon Business published 2024 Data Breach Investigations Report (Verizon Business, 2024), which highlights an increase during 2023 in ransomware attacks, accounting for 23% of all breaches analysed and, 20% of users reported phishing in simulation exercises, and 11% of those who clicked the email also reported it.

Sophos State of Ransomware 2024 (Sophos Whitepaper, 2024) reports in 2023, 59% of organizations were targeted by ransomware, showing a slight yet welcome decrease from the 66% reported in each of the previous two years. Despite this reduction, with over half of organizations still facing attacks, it remains crucial to stay vigilant. As result all revenue segments saw a reduction in ransomware attack rates last year, although the decrease for the $500M-$1B segment was less than one percentage point. However, even the smallest organizations, those with less than $10M in revenue, remain frequent targets, with just under half (47%) experiencing ransomware attacks last year. Many attacks are carried out by sophisticated, well-funded groups, there is a rising trend of lower-skilled threat actors using crude, inexpensive ransomware. The average ransom demands differ significantly by industry, for instance, the IT, technology, and telecom sectors reported the lowest median ransom payment at $300,000, followed by distribution and transport at $440,000. On the higher end of the spectrum, both lower education and central/federal government sectors paid median ransoms of $6.6 million.

Cybercrime leads to significant financial losses. Businesses suffer from operational disruptions, reputational damage, and direct financial theft. Worldwide according to (IBM, 2024), in 2023 the average cost of a data breach increased to USD 4.45 million, up by USD 100,000 from 2022. This marks a 2.3% rise from the 2022 average cost of USD 4.35 million. Since 2020, when the average total cost was USD 3.86 million, the overall average cost has risen by 15.3%.

As mentioned in a recent Interpol report (Interpol, 2024), crime convergence often occurs around financial fraud, with cybercrimes-as-a-service and money-laundering-as-a-service playing crucial roles in enabling both individual fraudsters and criminal groups.

With more personal information stored online, protecting this data from breaches is crucial for maintaining privacy and trust. For instance, the report 2023 Data Breach Investigations Report (Verizon Business, 2023) found that 83% of data breaches involved sensitive personal information, highlighting the critical need for robust data protection measures to safeguard privacy and maintain trust among users and customers. The proliferation of IoT devices introduces new vulnerabilities, as many of these devices have weak security protocols, as an example can be mentioned Mirai Botnet incident in 2016 (CISA, 2016). The Mirai malware exploited weak security protocols in IoT devices, such as default usernames and passwords, to create a massive botnet. This botnet was then used to launch a series of powerful Distributed Denial of Service attacks, including one that significantly disrupted major websites and online services like Twitter, Netflix, and Reddit. The Mirai botnet highlighted the security risks associated with poorly secured IoT devices and demonstrated how they could be leveraged to cause widespread disruption.

Cyber-attacks on critical infrastructure (e.g. power grids, healthcare systems) can have devastating consequences for national security. For instance, evidence supporting this statement is the 2021 Colonial

Pipeline ransomware attack, information was published in many media. This attack caused a major disruption in the fuel supply across the eastern United States, leading to widespread panic buying, fuel shortages, and significant economic impacts. The incident highlighted the vulnerability of critical infrastructure to cyber-attacks and underscored the severe national security risks posed by such disruptions.

Both cybercriminals and cybersecurity professionals have adopted AI and ML. Cybercriminals have increasingly adopted AI to create sophisticated malware that can evade traditional security measures. An example is malware that uses machine learning to modify its behaviour based on the environment it infects. A notable case is the use of AI to develop polymorphic malware, which changes its code to avoid detection. This has been reported in various instances where malware adapts its behaviour to avoid signature-based detection systems and employs AI to identify vulnerabilities in targeted systems. On the defensive side, cybersecurity professionals employ AI and ML to enhance threat detection and response capabilities. Machine learning algorithms analyse vast amounts of data to identify patterns and anomalies that could indicate cyber threats. For example, the use of AI in Security Information and Event Management systems helps in real-time analysis of security alerts generated by applications and network hardware. These systems leverage machine learning to detect unusual patterns that might signify an ongoing attack, allowing for quicker and more accurate responses (Sowmya & Mary Anita, 2023).

Consequently, governments are enacting stricter regulations to protect data, necessitating robust cybersecurity measures, for instance, the General Data Protection Regulation (Directive 95/46/EC, GDPR) was implemented in the European Union. Since its implementation in 2018, GDPR has imposed stringent requirements on data protection and privacy, leading to significant fines for non-compliance. For example, in 2021, Amazon was fined a record €746 million ($888 million) for GDPR violations (Bodoni, 2021). This enforcement highlights the increasing regulatory pressure on organizations to adopt robust cybersecurity measures to protect data and comply with strict privacy laws.

Cybersecurity and cybercrime are crucial topics to investigate due to the widespread and evolving nature of cyber threats, the growing dependency on digital systems, and the significant impacts on economic, personal, and national security. Addressing these challenges requires ongoing investment, education, and collaboration across all sectors of society.

2. LITERATURE REVIEW

Cybercrime poses multifaceted challenges to individuals, organizations, and societies, necessitating concerted efforts in research, policy, and technology to mitigate risks and enhance cybersecurity resilience. Scientific literature underscored the importance of continuous vigilance, collaboration, and innovation in addressing evolving cyber threats and safeguarding digital ecosystems.

Much research (Yamin & Murwaningsari, 2023; Ponomarenko et al., 2024; Wang et al., 2024; Ivashchenko & Polischuk, 2018; Chytilová et al., 2024; Anton, 2024; Pereira & Shafique, 2024; Musyaffi, 2024; Kliestik et al., 2023; Aliane et al., 2023; Krajčík et al., 2023; Chang & Ku, 2023; Červinka, 2023; Agboola et al., 2023; Odei Addo & Keelson, 2023; Lytvyn et al., 2024) was provided on the level of enterprises and organisations. For example, the article (Yarovenko et al., 2021) aims to develop a rapid methodology for assessing the risk of information and knowledge loss management. It outlines an eight-step implementation process, utilizing a modified risk mapping method based on risk factors and incidents, incorporating elements from set theory, and formalizing with binary estimates. The methodology considers five major events caused by company staff, technical problems, software issues, cybercriminals, and viral attacks, as well as 66 factors influencing company incidents. Consequently, a risk map comprising 9 groups was created for a Ukrainian enterprise. The study (Kuzior et al., 2023) aims to develop a composite indicator of company cybersecurity to assess development needs using constructing a superposition matrix based on

the growth rates of cyber threats and risks and calculating their quantitative characteristics along with a composite indicator. The computations use data from 2016-2022, which include indicators of cybersecurity vulnerabilities and the impacts of cyber threats. These indicators encompass the share of companies experiencing one or six or more successful cyberattacks, the likelihood of successful attacks in the next 12 months, security threat and concern indices, the proportion of companies with increasing security budgets affected by ransomware, the shortage of skilled IT security personnel, and the cost of stolen or compromised credentials.

The research question of cybercrime and cybersecurity appears (Zámek & Zakharkina, 2024; Farkačová et al., 2023; Aden Dirir et al., 2023; Melnyk et al., 2022) on a macro-level detection that involving cybercrime rates and different indexes of cyber security and cyber resilience at the national level. There are some existing research that examined cybercrime at the national level, but mostly in terms of inference, rather than clustering. For instance, the article (Kuzior et al., 2022b) provides evidence for the existence of convergence processes in the realm of countries' digitization. It considers various factors such as the number of Internet users, individuals with advanced skills, and indicators related to infrastructure (e.g., network coverage, population covered by 3G and 4G mobile networks), access (e.g., access to ICT at home, active mobile broadband subscriptions, fixed broadband subscriptions), enablers (e.g., fixed broadband exceeding 10 Mbps, mobile data and voice services, high consumption), and barriers (e.g., enhanced broadband access from 256 kbps to 2 Mbps, from 2 Mbps to 10 Mbps mobile data and voice services, low consumption) of digital development. Other authors such as A. Kigerl (2016), Bilan et al. (2023b) have published articles dedicated to analysis of interdependences of internet connectivity of citizenships of different countries and their technological development. As results in investigation (Kigerl, 2016) performing a K-means clustering analysis on a sample of 190 countries, considering seven dimensions of cybercrime, including malware, fraud, spam, and digital piracy, along with measures of GDP and internet usage. The analysis revealed that countries could be categorized into four distinct groups based on their cybercrime activity: low cybercrime countries, non-serious cybercrime countries, advanced fee fraud countries, and phishing scam countries. The article (Yarovenko et al., 2023b) analyses the socio-economic profiles of countries that fall victim to cybercrimes resulting from malicious programs, viruses spread through email applications, and vulnerabilities in information systems and computer networks. Cluster analysis confirms that leading countries, such as the USA, China, Germany, and France, are both targets and initiators of cyberattacks. The analysis of country clusters based on associative rules strongly supports the notion that a country's level of socio-economic development can indirectly motivate cybercriminals to carry out mass cyberattacks. The study (Yarovenko, 2020) aims to evaluate the threat level to countries' information security using a comprehensive index. It suggests employing five indicators that characterize specific aspects of information security, along with 37 indicators of global development selected from the World Bank database. The outcome is illustrated on a map displaying countries categorized by their information security threat index, thus creating five distinct groups. In developing nations, where addressing information threats significantly impacts the economy, the information security level is deemed "acceptable." Countries with lower levels of development and information security are classified labelled as "poor" and "very poor," indicating a heightened threat level to their information security. The chapter of the book (Mokhtar & Rohaizat, 2024) aims to provide an overview of cybercrime and trends in combating it, the changes due to increasing internet and computer connectivity, the rapid rise in internet user penetration during the COVID-19 pandemic, and Cyber Governance in both the ASEAN and EU regions.

Separate vector of research (Benghebrid & Sahnouni, 2023; Oe & Yamaoka, 2023; Konczos Szombathelyi et al., 2023; Streimikiene et al., 2023; Fülöp et al., 2023; Androniceanu & Georgescu, 2023; Benchea & Ilie, 2023; Kupenko et al., 2023) analyses the personal characteristics of cybersecurity. In the article (Dunn Cavelty et al., 2023, Porkodi et al., 2023), the authors argue that cybersecurity exhibits a social

dimension characterized by two fundamental elements: vulnerability and uncertainty and propose viewing cybersecurity as a combination of a technical problem and human's issue or a social problem merged with technology challenge. The challenges linked with digital skills are considered by Bilan et al. (2023a), Jurek et al. (2021), Straková et al. (2022). Similarly, the study (Nifakos et al., 2021) asserts that, alongside cyberattacks targeting vulnerabilities in information technology infrastructures, a novel form of cyberattack has emerged: social engineering attacks, which seek to exploit human weaknesses. The study (Yarovenko et al., 2023a) aims to analyse IT users' behaviour regarding their personal protection against potential cybercrimes. The research is based on survey data collected by the European Commission in 2020-2021 from 35 European countries. Canonical analysis revealed that 66.67% of cybercrime cases (such as phishing, pharming, and online identity theft) influence individuals' choices of personal protection methods (such as using a security token, social media logins, and electronic identification). Kohonen's self-organizing maps were used to create 9 clusters of countries based on IT users' attitudes toward personal cybersecurity.

Many studies (Benachour & Tarhlissia, 2024; Hrytsenko et al., 2024; Holtfort & Horsch, 2024; Shafranova et al., 2024; Niftiyev& Kheyirkhabarli, 2024; Filatova et al., 2023; Polishchuk, 2023; Shakatreh et al., 2023; Waliszewski et al., 2024; Piotrowski & Orzeszko, 2023; Hrytsenko et al., 2023; Alhanatleh et al., 2024; Vitvitskiy et al., 2021; Dewi et al., 2023; Minh Sang, 2024) are devoted to implementing digital technologies in financial institutions and the risks associated with these processes. The article (Kuzior et al., 2022a) aims to forecast information trends related to the most prevalent cyberattacks, which are seen as consequences of cybercrimes reflected on the Internet. The authors developed additive and multiplicative cyclical and trend-cyclical models with an exponential trend for predicting cyberattacks on computer systems and cloud infrastructure. They also created a trend-cyclic additive model with a damped tendency for predicting cyberattacks on network infrastructure. The findings suggest that the U.S. can expect cybercrimes targeting its financial system in the short and medium term, enabling the development of appropriate countermeasures for financial institutions to mitigate potential financial losses. The study (Yarovenko et al., 2023c) aims to formulate a scientific and methodological approach for modelling the potential behaviour of insider cyber fraudsters within banks. This approach involves a sophisticated combination of principal component analysis, k-means clustering, and associative analysis. The research reveals that the primary interests of potential insider cybercriminals in banks include obtaining personal financial information of clients, accessing client profiles in online banking systems, and gaining entry to their phone data.

Other group of articles (Ninassi & Burrell, 2023; Pakhnenko & Pudło, 2023; Szigeti & Jozsa, 2023; Orlandić et al., 2024; Lăzăroiu et al., 2024; Suhanyi et al., 2024; Seniutis et al., 2024; Ejdys et al., 2024) dedicated to analysis of public areas, e. i. healthcare digitalisation and their hazards. For instance, the article (Graf & Burrell, 2024) delves into the intricate terrain of shareholder resistance encountered during software implementation projects. It investigates the roots of this issue, its various forms, as well as its pros, cons, and repercussions. Additionally, the article scrutinizes this challenge through the lenses of Lewin's Change Model and the Transtheoretical Model of Change, illustrating it with examples from Information Technology Company and Microsoft. Strategic recommendations are provided for healthcare organizations to adeptly navigate and alleviate these hurdles, thereby enabling a smooth transition to the healthcare technology landscape. The study (Wright, 2023) examines how healthcare organizations collectively evaluate, handle, and alleviate cyber threats and vulnerabilities within their supply chains to safeguard patient well-being, secure data, and fortify organizational resilience. It also delves into the specific alterations that can be suggested, implemented, and assessed to bolster cybersecurity within these supply chains. Mačiulytė-Šniukienė, 2023 examines the convergence of transport and ICT infrastructure in EU member states and NUTS 2 regions across different time periods.

Some research investigates the issues of ethics of data losses and their security in different areas. For instance, the study by (Pakhnenko & Kuan, 2023) employs bibliometric, comparative, and statistical analysis

methods. It identifies three ethical issues: 1) privacy, security, and data protection; 2) transparency and accountability; and 3) inclusion, accessibility, and non-discrimination. The third category is highlighted as particularly pertinent presently. Given the widening digital gap globally, there is a pressing need to explore effective strategies to enhance digital inclusion and guarantee equitable e-government access for all stakeholders. Other research (Asare & Samusevych, 2023) also provided comprehensive bibliometric analysis of research on financial fraud, tax tools, and economic security. Some research (Venkateswaran ey al., 2024; Shaleh et al., 2024) investigate possibility and risks of digitalization in agriculture.

While existing literature often focuses on the technical aspects of cyber threats and the responses of developed nations or large corporations, there is limited research on how cybercrime affects vulnerable populations and less economically developed countries. Research could investigate how cyber threats exacerbate existing inequalities and vulnerabilities, such as financial insecurity, lack of access to digital resources, and limited cybersecurity awareness. Additionally, studies could explore the specific challenges faced by marginalized communities in responding to and recovering from cyberattacks, including financial losses, identity theft, and disruptions to essential services. Furthermore, there is a need to examine the effectiveness of current cybersecurity strategies and policies in addressing the needs of vulnerable populations and developing regions. This could involve evaluating the accessibility and affordability of cybersecurity tools and resources, as well as identifying gaps in support and assistance for affected communities.

The current study aims to fill this void by conducting a cluster analysis of 33 countries globally. Through this analysis, each country will be assigned to a distinct typological category, differentiated from nations of other types. This classification will be based on five cybercrime measures. Prior research has established these variables to have a significant correlation with cybercrime. Thus, the purpose of this study is to investigate the trends of changes in the level of crime in the digital space of the countries of the world by means of their typology (clustering) depending on the values of the comprehensive indicator of the level of cybercrime.

3. METHODOLOGY

The main hypothesis of this study was that the rapid development and active introduction of digital technologies into all spheres of life in society negatively affect the level of crime in cyberspace and lead to the constant expansion of criminal activity schemes in digital space. At the first stage, an assessment of the level of cybercrime of the country will be carried out. This indicator can be considered as an indicator that characterizes the degree of protection of the country against cyberattacks on computer systems and networks, cybercrime, unauthorized access to databases (the level of its cyber security). And therefore, its calculation allows us to assess the effectiveness of the state policy of ensuring cyber security. Countries with a high level of cybersecurity tend to be significantly less likely to be subject to or initiate unauthorized attacks.

The calculation of the complex indicator is based on taking into account 5 indices characterizing the level of cybercrime in the country: 1) The National Cyber Security Index (NCSI) is a global index that determines the efforts of countries in the direction of solving cyber threats and managing cyber incidents (E-Governance Academy, 2024), the main of which are Denial of e-services – services are not accessible, Data integrity breach – unauthorized modification, Data confidentiality breach – secrecy is exposed. In general, this index contains 49 indicators, within 3 categories and 12 capacities. 2) ICT Development Index (ICTDI)– a composite indicator characterizing the level of development of the information and communication technologies sector (ITUCOUNCIL Geneva, 2024); The use of this index allows us to take into account not only crime indicators directly, but also the degree of development and security of digital

infrastructure, effective interaction of their components (information and telecommunication technologies, human capital, favorable business climate; effective management) from the point of view of preventing cyber attacks. In addition, the calculation of this index is based on taking into account the level of digital literacy of the population. When calculating, the values of this index will be taken into account as disincentives (from the point of view of the development of cybercrime). 3) Global Cybersecurity Index (GCI) – an index, the use of which is aimed at increasing awareness of cyber security in various industries and sectors of the economy and measuring the commitment of countries to cyber security(European Commission, 2024); 4) Global Terrorism Index (GTI) allows to assess the global trends of terrorism and takes into account a number of indicators of the development of terrorism in the country: the number of incidences, fatalities, injuries and hostages (Institute for Economics and Peace, 2024). Given that cybercrime includes a number of types of illegal activities and given the lack of a single internationally accepted definition of terrorism, taking into account the values of this index will allow us to approach this issue more comprehensively. Thus, the developers of the Global Terrorism Index define terrorism as the threatened or actual use of illegal force to attain a political, economic, religious, or social goal. These criteria for classifying a crime can also be applied to certain types of crimes in cyberspace. Thus, taking this index into account when calculating a comprehensive indicator of cybercrime will allow us to take into account certain types of terrorist activity carried out in cyberspace. 5) The Global Organized Crime Index (CI) an indicator that determines the level of life safety in certain countries of the world (Numbeo Doo, 2024). This indicator is based on taking into account three components: the scope and impact of criminal markets, influence of criminal actors and capacity of resilience measures against organized crime. In block 2 "Criminal markets" one of the components is cyber-dependent crimes, which will form the basis of our calculations.

The data of the World Bank, the E-Governance Academy, the ITU Council Geneva, the Institute for Economics and Peace, the European Commission and the Organization for Economic Cooperation and Development are the information base of the research. The object of the study is data from 33 countries, the study period is 2016-2023. The use of this number of countries allows to investigate cybercrime trends for countries with both high and low levels of digital development and the development of illegal activities and to determine their interdependencies.

At the first stage, based on a linear mathematical model, a complex indicator characterizing the level of cybercrime in the country is calculated:

$$\boldsymbol{CCSI} = \sum_{i=1}^{n} \boldsymbol{w_i} \times \boldsymbol{CCSI_{i_t}} \quad (1)$$

where CCSI is a comprehensive indicator of the level of cybercrime, w_i is a weighting coefficient of i-indicator of a complex indicator characterizing the level of cybercrime in the country. It is determined using the Fishburn formula:

$$w_i = (2 \cdot (\mathrm{n} - \mathrm{i} + 1))/(\mathrm{n} \times (\mathrm{n} + 1)) \quad (2)$$

where n – the total number of indicators; i – the rank of an indicator, which is defined based on the cluster analysis.

At the next stage, countries are clustered depending on the values of cybercrime indicators in the country. The number of clusters is determined using the "Single Linkage" technique.

This method is based on cluster grouping, at each step, and consists in combining two clusters containing the closest pair of elements:

$$D(X,Y) = min_{x \in X. y \in Y} d(x,y) \quad (3)$$

where X and Y are any two sets of elements considered as clusters, d(x,y) is the distance between the two elements x and y.

At the third stage, self-organizing Kohonen maps will be constructed using algorithms of artificial neural networks. This allows you to present data in the form of maps with preservation of the data structure, in which neurons are located on a two-dimensional grid.

The essence of the algorithm is that the vectors x of the input layer are compared with the vectors w to find the nearest neuron according to the formula, which is the square of the Euclidean distance between the vector of bank indicators and the vector of weights of neuron j:

$$d(x_i, w_j) = (x_i - w_j)'(x_i - w_j),$$

where x = {xi: i = 1, … , n} is the n-dimensional set of bank variable vectors in the input layer; w = {wj: j = 1, … , k} is a set of dimension k of vectors of weight coefficients of neurons in the output layer.

Then the input vectors begin to be introduced into the model iteratively. After the input data is fed to the model, the weights of the output layer are adjusted so that the weights of the best matching unit are closest to the input vector, while the neighboring neurons are adjusted slightly less depending on their distances to the best matching unit. The further the neuron is from the best matching unit, the smaller its adjustment. Thus, after many iterations, our original two-dimensional map acquires a topological structure. With the help of a heuristic algorithm of mapping a multidimensional array onto a two-dimensional Kohonen map, we get a result where homogeneous groups (clusters) are colored in the appropriate colors. The closer the position of the points on the map, the closer the value of the indicators, but taking into account all these values at the same time. The position of the object on the map depends on the value of all indicators, on its location in n-dimensional space.

4. EMPIRICAL RESULTS AND DISCUSSION

The results of calculating the level of cybercrime for 33 countries in 2016-2023 (table 1) indicate a gradual increase in the level of crime in cyberspace in the world. This is connected both with the increase in the level of general crime in the world, and with the active development of digital technologies and their introduction into all spheres of society. Among the analyzed countries, Slovenia (0.56), Iceland (0.55), Moldova (0.55), Georgia (0.53) had the lowest level of cybercrime in 2023, while Greece, Belgium, France, Germany had the highest values of this complex indicator (more than 0.7). Analysis of the dynamics of changes in the level of cybercrime shows that Malta (71% compared to 2016), Slovenia (62%), Iceland (60%), Moldova (57%), Slovakia (56%) have the highest rate of its growth. While Estonia and France have the lowest growth rate of this indicator (9%).

Table 1

The level of cybercrime in the countries of the world

Country	2016	2017	2018	2019	2020	2021	2022	2023
AUT	0.45	0.48	0.55	0.57	0.58	0.66	0.65	0.62
BEL	0.57	0.65	0.68	0.70	0.72	0.75	0.72	0.74
BGR	0.49	0.49	0.52	0.54	0.51	0.53	0.61	0.62
HRV	0.47	0.47	0.56	0.57	0.60	0.61	0.63	0.64
CYP	0.41	0.41	0.46	0.45	0.52	0.53	0.57	0.57
CZE	0.54	0.54	0.53	0.53	0.57	0.59	0.66	0.66
DNK	0.54	0.55	0.61	0.62	0.65	0.65	0.66	0.65
EST	0.61	0.62	0.63	0.64	0.66	0.66	0.66	0.67
FIN	0.58	0.60	0.64	0.64	0.66	0.68	0.67	0.65
FRA	0.68	0.70	0.72	0.73	0.71	0.76	0.76	0.73
GEO	0.47	0.50	0.50	0.51	0.48	0.49	0.52	0.53
DEU	0.60	0.63	0.68	0.69	0.72	0.76	0.76	0.73
GRC	0.56	0.57	0.60	0.61	0.74	0.77	0.80	0.76
HUN	0.44	0.46	0.54	0.55	0.58	0.58	0.60	0.60
ISL	0.35	0.35	0.37	0.38	0.49	0.50	0.55	0.55
IRL	0.59	0.60	0.63	0.63	0.65	0.62	0.67	0.65
ITA	0.56	0.58	0.65	0.67	0.70	0.72	0.72	0.68
LVA	0.50	0.52	0.55	0.56	0.62	0.62	0.63	0.63
LTU	0.50	0.50	0.62	0.65	0.66	0.67	0.68	0.68
LUX	0.45	0.44	0.54	0.55	0.58	0.58	0.59	0.60
MLT	0.36	0.38	0.41	0.42	0.53	0.55	0.60	0.61
MDA	0.35	0.37	0.44	0.45	0.48	0.49	0.55	0.55
NLD	0.55	0.59	0.63	0.65	0.68	0.66	0.68	0.65
POL	0.49	0.51	0.59	0.59	0.63	0.63	0.66	0.66
PRT	0.50	0.51	0.59	0.59	0.65	0.65	0.66	0.66
ROU	0.52	0.52	0.52	0.53	0.58	0.63	0.67	0.66
SVK	0.43	0.44	0.55	0.56	0.61	0.63	0.64	0.67
SVN	0.34	0.34	0.45	0.47	0.47	0.49	0.55	0.56
ESP	0.54	0.57	0.70	0.69	0.69	0.72	0.71	0.70
SWE	0.61	0.63	0.62	0.67	0.69	0.70	0.66	0.69
CHE	0.47	0.45	0.51	0.49	0.54	0.60	0.70	0.63
UKR	0.54	0.55	0.58	0.59	0.59	0.57	0.68	0.67
GBR	0.58	0.59	0.60	0.67	0.71	0.71	0.68	0.70

Source: own calculation

Clustering of countries is an important stage in the study of trends in the level of cybercrime in the world. This will make it possible to identify and systematize the most characteristic features of the policy of ensuring cyber security in the world. The prerequisite of these processes is the determination of the number of clusters into which the analyzed countries should be divided. For this purpose, a clustering tree diagram was constructed using the single linkage method. The results presented in Figure 1 indicate the expediency of selecting three clusters of countries

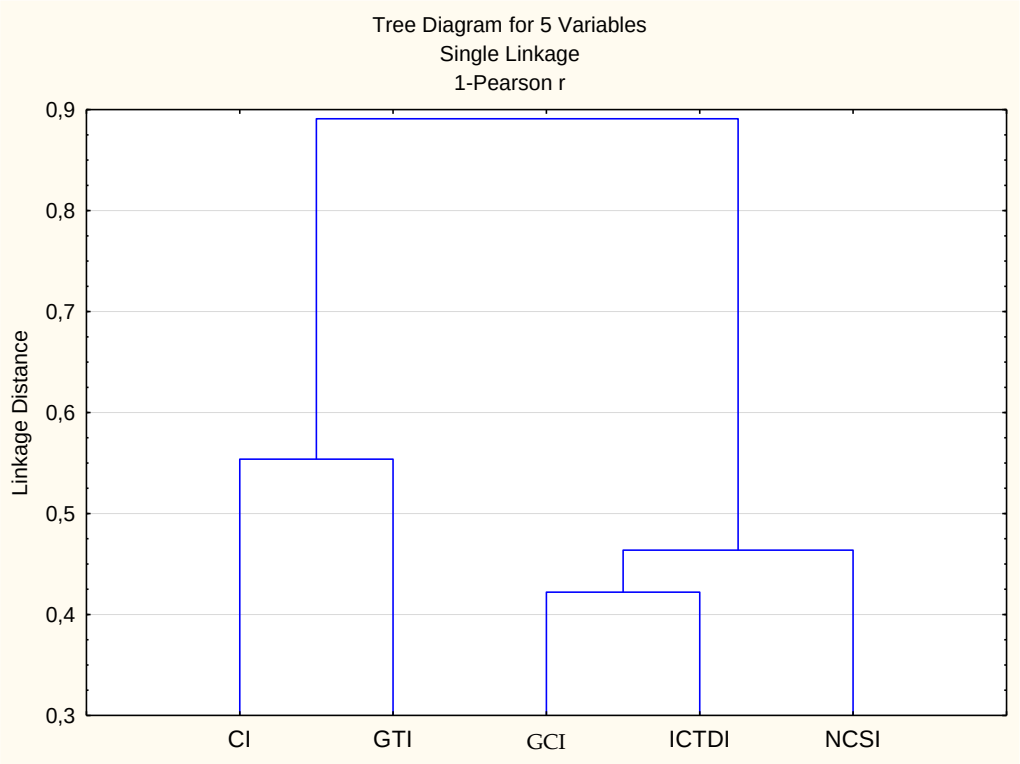

Figure 1. Clustering tree diagram by single linkage method

Source: Authors' results

The values of indices characterizing the level of cybercrime in the world shown in Table 2 indicate that the second cluster should include countries with the lowest values of The National Cyber Security Index, ICT Development Index and Global Cybersecurity Index and the highest values of the Global Terrorism Index and Crime Index. The third cluster is characterized by the highest values of The National Cyber Security Index, ICT Development Index and Global Cybersecurity Index and average values of the Global Terrorism Index and Crime Index.

Table 2

Cluster means

Variable	Cluster Means (Spreadsheet2)		
	Cluster No. 1	**Cluster No. 2**	**Cluster No. 3**
NCSI	59.92184	55.21518	81.23785
ICTDI	81.66589	68.55742	85.04462
GCI	0.76080	0.70390	0.85284
GTI	0.43688	2.63282	1.64814
CI	28.99825	45.14630	34.53951

Source: Authors' results

The results of the calculations of descriptive statistics indicators (table 3) allow us to conclude that within each of the selected clusters the National Cyber Security Index, ICT Development Index and Crime Index are characterized by a significant range of values, while the Global Cybersecurity Index has the least variability.

Table 3

Descriptive statistics for clusters

Variable	Descriptive Statistics for Clusters (Spreadsheet2) Cluster contains 162 cases		
	Mean	**Standard Deviation**	**Variance**
Cluster 1			
NCSI	59.92184	6.214067	38.61462
ICTDI	81.66589	6.375060	40.64138
GCI	0.76080	0.208602	0.04351
GTI	0.43688	0.937802	0.87947
CI	28.99825	6.436461	41.42803
Cluster 2			
NCSI	55.21518	8.086134	65.38557
ICTDI	68.55742	7.319060	53.56865
GCI	0.70390	0.169554	0.02875
GTI	2.63282	2.567930	6.59427
CI	45.14630	3.294369	10.85287
Cluster 3			
NCSI	81.23785	5.973136	35.67835
ICTDI	85.04462	5.971387	35.65746
GCI	0.85284	0.161859	0.02620
GTI	1.64814	1.689659	2.85495
CI	34.53951	8.367360	70.01272

Source: Authors' results

A comparison of the average values of the indicators within each cluster (Figure 2) confirms the previous conclusions. The average values of the Global Cybersecurity Index and the Global Terrorism Index for all three clusters are almost the same, while the values of the remaining indicators of the level of cybercrime in the country differ significantly among themselves.

To carry out a dynamic analysis of the change in the level of cybercrime in the country, the grouping of countries and the comparison of the trends of the transition of countries from one cluster to another were carried out using Kohonen's self-organizing maps (Figures 3, 4).

The analysis of the countries in the section of the National Cyber Security Index shows that the lowest values of this indicator are those at the bottom of the figure (Moldova, Iceland, the Czech Republic), and the highest are the countries of the first cluster (top of the figure). The largest in size is the first cluster, which includes countries with an above-average value of the National Cyber Security Index (Estonia, Sweden, Poland, Greece, Romania, etc.), the smallest is the third cluster, which includes only 2 countries (Bulgaria and Ukraine. Data countries have one of the lowest values of the analyzed indicator.

Analysis of Kohonen's constructed maps for other indicators confirms the same size and characteristics of selected clusters (number and names of countries). At the same time, in terms of the Global Terrorism Index, the third cluster includes countries with the highest Global Terrorism Index values, while the first and second clusters include countries with low values of this indicator.

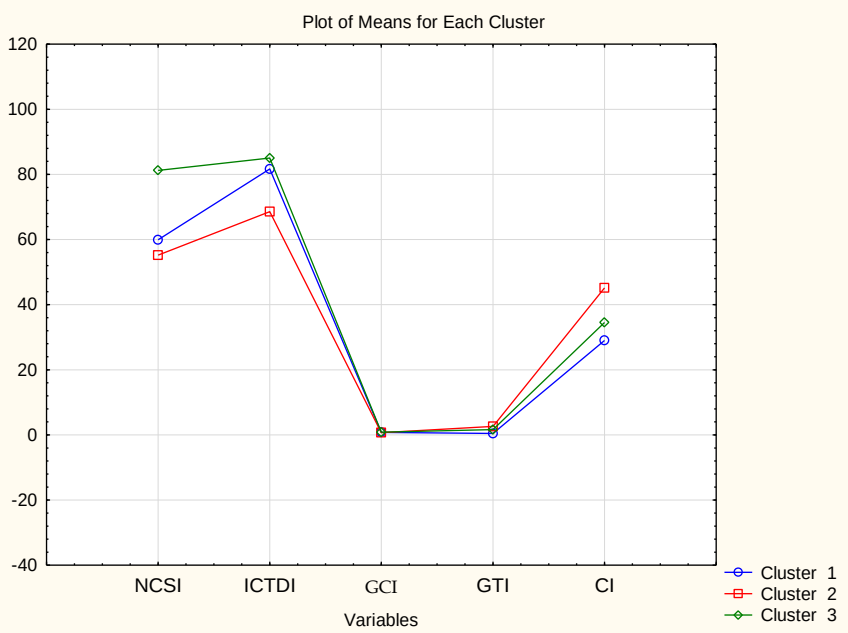

Figure 2. Plot of means for each cluster

Source: Authors' results

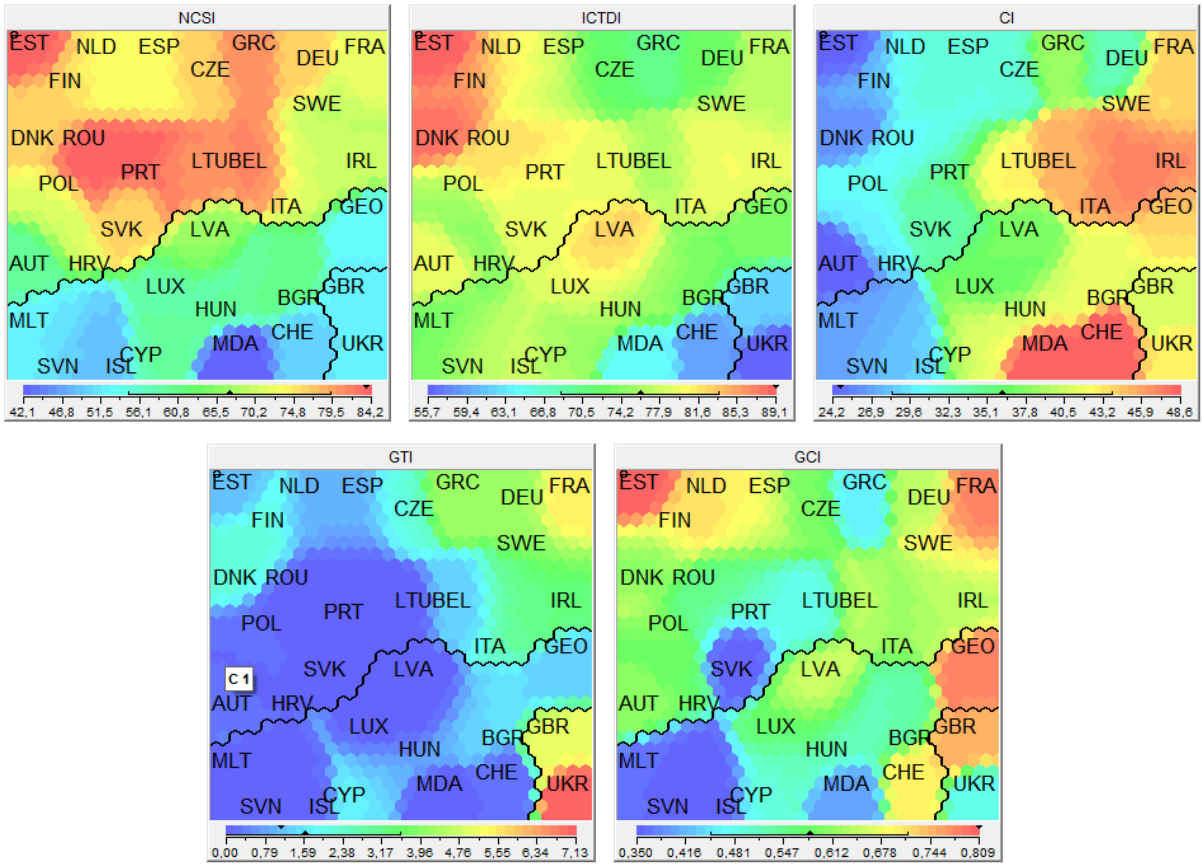

Figure 3. Kohonen maps for indicators characterizing the level of cybercrime in the countries in 2016

Source: Authors' results

The comparative analysis of clusters for the values of indicators in 2023 shows significant changes in the structure and size of the formed clusters. Thus, there was an expansion of the third cluster (6 countries instead of 2), which indicates negative trends in the development of cybercriminal activity. In addition, within each of the five indicators of the development of cybercriminal activity, there is a deterioration in the values of the indicators. A comparison of Kohonen maps for Crime Index in 2016 and 2023 shows that in 2023 most countries have low values of this indicator (blue circles), while in 2016 orange and yellow colors prevailed (typical for index values of 0.4 and above).

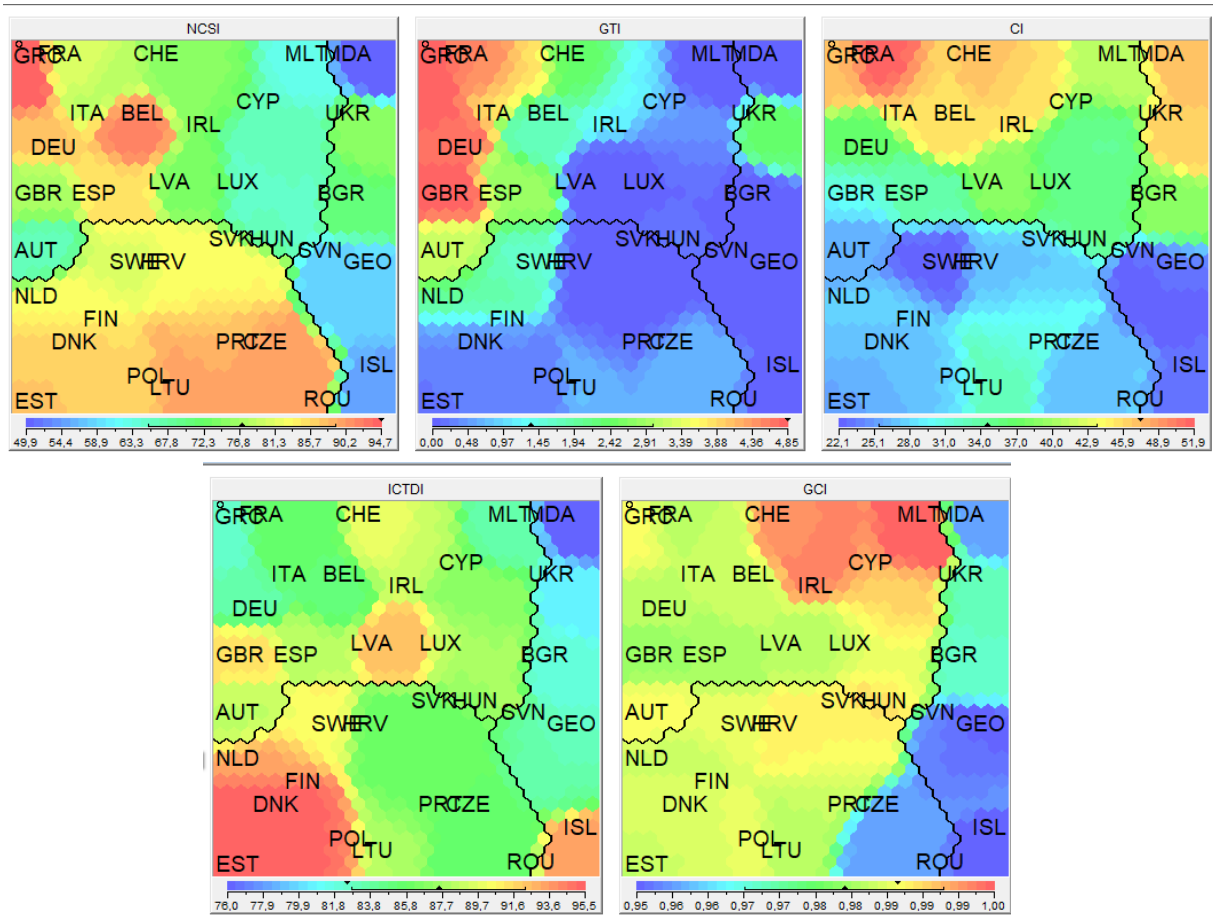

Figure 4. Kohonen maps for indicators characterizing the level of cybercrime in the countries in 2023

Source: Authors' results

5. CONCLUSION

The article analyzes the trends of changes in the level of cybercrime in the countries of the world. The study is devoted to testing the hypothesis about the negative impact of the rapid development of digital technologies on the level of crime in cyberspace and the promotion of the expansion of criminal activity schemes in digital space. The verification of this hypothesis was carried out using data from 33 countries of the world for the period 2016-2023.

The results of calculating the level of cybercrime in 2016-2023 proved its gradual growth in the world. Thus, the rate of growth of the level of cybercrime in individual countries of the world during the analyzed period exceeds 50% (Malta, Slovenia, Iceland, Moldova, Slovakia). In 2023, Slovenia (0.56), Iceland (0.55),

Moldova (0.55), Georgia (0.53) had the lowest level of cybercrime among the analyzed countries, while Greece, Belgium, France, Germany had the highest. Using the single linkage method and Kohonen's self-organizing maps, three clusters of countries were identified depending on the values of the indicators characterizing the level of cybercrime in the country: the National Cyber Security Index, ICT Development Index, Global Cybersecurity Index, Global Terrorism Index, Crime Index. In addition, the comparative analysis of the clusters for the values of the indicators in 2023 and 2016 showed significant changes in their structure and size. Thus, the expansion of the third cluster indicates negative trends in the development of cybercriminal activity.

Thus, the established dependencies confirm the conclusions of previous studies about a significant increase in the level of cybercriminal activity and the low efficiency of the existing mechanisms for improving cyber security in most countries of the world (Aliane et al, 2023; Kliestik et al, 2023; Kuzior et al, 2022b). The obtained results serve as the basis for revising the existing toolkit for fighting crime in cyberspace and using best practices (according to the results of clustering of countries) in combating crime in the conditions of rapid development of digital technologies.

ACKNOWLEDGEMENT

This research was funded by the projects "Modeling the mechanisms of combating organized and transnational cybercrime in war and post-war periods" (0124U000550), funding – Ministry of Education and Science of Ukraine.

REFERENCES

Aden Dirir, S. (2023). The potential of macroeconomic factors in shaping the landscape of technological development: a testimonial from upper-middle-income countries. *Business, Management and Economics Engineering*, *21*(1), 84–105. https://doi.org/10.3846/bmee.2023.18360

Agboola, O., Adelugba, I. A., & Eze, B. U. (2023). Effect of financial technology on the survival of micro-enterprises. *International Journal of Entrepreneurial Knowledge*, *11*(1), 1–13. https://doi.org/10.37335/ijek.v11i1.188

Alhanatleh, H., Khaddam, A., Abudabaseh, F., Alghizzawi, M., & Alzghoul, A. (2024). Enhancing the public value of mobile fintech services through cybersecurity awareness antecedents: A novel framework in Jordan. *Investment Management and Financial Innovations*, *21*(1), 417–430. https://doi.org/10.21511/imfi.21(1).2024.32

Aliane N., Gharbi H., Semlali Y. (2023) The role of artificial intelligence, digital capabilities and digital awareness on supply chain management: moderating role of organizational readiness and digital organizational culture. *Transformations in Business and Economics*, 22(3), 832 – 852. Retrieved from http://www.transformations.knf.vu.lt/60a/article/ther

Androniceanu, A. (2024). Artificial intelligence in administration and public management. *Administratie si Management Public*, 42, 99-114. https://doi.org/10.24818/amp/2024.42-06

Androniceanu, A., & Georgescu, I. (2023). Digital competences and human development: a canonical correlation analysis in Romania. *Polish Journal of Management Studies,* 28(1), 43-61. https://doi.org/10.17512/pjms.2023.28.1.03

Anton, S. G. (2024). The impact of digital transformation on entrepreneurial activity. Empirical evidence from the European Union. *Journal of Business Economics and Management*, 25(2), 297–314. https://doi.org/10.3846/jbem.2024.21113

Asare, K., Samusevych, Y. (2023). Exploring Financial Fraud, Tax Tools, and Economic Security Research: Comprehensive Bibliometric Analysis. *Financial Markets, Institutions and Risks*, 7(3), 136-146. https://doi.org/10.61093/fmir.7(3).136-146.2023

Benachour, A. & Tarhlissia, L. (2024). The evolution and development of electronic payment in a bank. Case study: CPA-Bank. *Financial Markets, Institutions and Risks*, 8(1), 1-15. https://doi.org/10.61093/fmir.8(1).1-15.2024

Benchea, L., & Ilie, A. G. (2023). Preparing for a new world of work: Leadership styles reconfigured in the Digital age. *European Journal of Interdisciplinary Studies*, *15*(1), 135–143. https://doi.org/10.24818/ejis.2023.10

Benghebrid, R., Sahnouni, M. (2023). Telework: What is impact on the Algerian employee?. SocioEconomic Challenges, 7**(**3), 55-62. https://doi.org/10.61093/sec.7(3).55-62.202

Bilan, Y., Mishchuk, H., & Samoliuk, N. (2023a). Digital Skills of Civil Servants: Assessing Readiness for Successful Interaction in e-society. *Acta Polytechnica Hungarica, 20*(3), 155-174. *DOI: 10.12700/APH.20.3.2023.3.10*

Bilan, Y., Oliinyk, O., Mishchuk, H., & Skare, M. (2023b). Impact of information and communications technology on the development and use of knowledge. *Technological Forecasting and Social Change*, *191*, 122519. DOI: 10.1016/j.techfore.2023.122519

Bionducci, L., Botta, A., Bruno, P., Denecker, O., Gathinji, C., Jain, R., Nadeau, M.-C., & Sattanathan, B. (2023, September 18). On the cusp of the next payments era: Future opportunities for Banks. McKinsey & Company. Retrieved from https://www.mckinsey.com/industries/financial-services/our-insights/the-2023-mckinsey-global-payments-report

Bodoni, S. (2021, July 30). Amazon Gets Record $888 Million EU Fine Over Data Violations. Bloomberg. https://www.bloomberg.com/news/articles/2021-07-30/amazon-given-record-888-million-eu-fine-for-data-privacy-breach FBI's Internet Crime Complaint Center (2022). 2022 internet crime report. Retrieved from https://www.ic3.gov/Media/PDF/AnnualReport/2022_IC3Report.pdf

Capgemini Research Institute (2023). Capgemini Research Institute 's World Payments Report 2023. Where is the cash? Accelerate corporate cash management transformation to build value. Retrieved from https://go.capgeminigroup.com/l/95412/2023-09-12/7tbpd6/95412/1694547172idbuBtLE/WPR_2023_web.pdf

Červinka, T. (2023). Digital Transformation of strategic management of SMES in the Czech Republic. *European Journal of Interdisciplinary Studies*, *15*(1), 144–155. https://doi.org/10.24818/ejis.2023.11

Chang, K.-Y., & Ku, E. C. S. (2023). Discount or Prestige: E-reputation, Compatibility, and Continued Mobile Apps Usage Intention of Low-Cost Carriers. *Journal of Tourism and Services*, *14*(26), 73–91. https://doi.org/10.29036/jots.v14i26.463

Chytilová, E., Talíř, M., Straková, J., & Dobrovič, J. (2024). Impact of digital procurement on economic resilience of enterprises during COVID-19. *Journal of International Studies*, 17(1), 188-204. doi:10.14254/2071-8330.2024/17-1/11

Cybersecurity and Infrastructure Security Agency (CISA). (2016). Simda botnet. Retrieved from https://www.cisa.gov/news-events/alerts/2015/04/15/simda-botnet

Dewi, Y., Suharman, H., Sofia Koeswayo, P., & Dewi Tanzil, N. (2023). Factors influencing the effectiveness of credit card fraud prevention in Indonesian issuing banks. *Banks and Bank Systems*, *18*(4), 44–60. https://doi.org/10.21511/bbs.18(4).2023.05

E-Governance Academy (2024). National Cyber Security Index. Retrieved from https://ncsi.ega.ee/ncsi-index/ (26.05.2024).

Ejdys, J., Czerwińska, M., & Ginevičius , R. (2024). Social acceptance of artificial intelligence (AI) application for improving medical service diagnostics. *Human Technology*, *20*(1), 155–177. https://doi.org/10.14254/1795-6889.2024.20-1.8

European Commission (2024). Global Cybersecurity Index. Retrieved from https://composite-indicators.jrc.ec.europa.eu/explorer/explorer/indices/GCI/global-cyber-security-index (26.05.2024).

Farkačová, L., Zadražilová, I., Tomášková A., et al. (2023). A multi-criteria model approach to extended information literacy as a basis of labour market sustainability in V4 countries. *Polish Journal of Management Studies,* 28(2), 91-107. https://doi.org/10.17512/pjms.2023.28.2.06.

Filatova, H., Tumpach, M., Reshetniak, Y., Lyeonov, S., & Vynnychenko, N. (2023). Public policy and financial regulation in preventing and combating financial fraud: a bibliometric analysis. *Public and Municipal Finance*, *12*(1), 48–61. https://doi.org/10.21511/pmf.12(1).2023.05

Flexera (2024). 2024 state of the Cloud Report. Available at https://info.flexera.com/CM-REPORT-State-of-the-Cloud-2024-Thanks

Fülöp, M. T., Topor, D. I., Ionescu, C. A., Cifuentes-Faura, J. ., & Măgdaş, N. (2023). Ethical concerns associated with artificial intelligence in the accounting profession: a curse or a blessing*?*. *Journal of Business Economics and Management*, 24(2), 387–404. https://doi.org/10.3846/jbem.2023.19251

Gartner. (n.d.). Gartner Forecasts Worldwide Public Cloud End-User Spending to Reach $679 Billion in 2024. Retrieved from https://www.gartner.com/en/newsroom/press-releases/11-13-2023-gartner-forecasts-worldwide-public-cloud-end-user-spending-to-reach-679-billion-in-20240 (27.05.2024).

Graf, D. G., & Burrell, D. N. (2024). Utilising resistance feedback for software implementation in healthcare. *Health Economics and Management Review*, 5(1), 106-116. https://doi.org/10.61093/hem.2024.1-08

Holtfort, T., Horsch, A. (2024). Quantum Economics: A Systematic Literature Review. *SocioEconomic Challenges, 8*(1), 62-77. https://doi.org/10.61093/sec.8(1).62-77.2024

Hrytsenko, L., Pakhnenko, O. Kuzior, A. & Kozhushko, I. (2024). Smart technologies in banking. *Financial Markets, Institutions and Risks*, 8(1), 81-93. https://doi.org/10.61093/fmir.8(1).81-93.2024

Hrytsenko, L., Zakharkina, L., Zakharkin, O., Novikov, V., & Chukhno, R. (2022). The impact of digital transformations on the transparency of financial-economic relations and financial security of Ukraine. *Financial and credit activity problems of theory and practice,* 3(44), 167–175. https://doi.org/10.55643/fcaptp.3.44.2022.3767

IBM (2024) The Cost of a Data Breach Report 2023. Retrieved from https://www.ibm.com/account/reg/signup?formid=urx-52258

IDC. (n.d.). Worldwide Digital Transformation Spending Forecast to continue its double-digit growth trajectory, according to IDC spending guide. Retrieved from https://www.idc.com/getdoc.jsp?containerId=prUS51352323

Institute for Economics and Peace (2024). Global Terrorism Index. Retrieved from https://www.economicsandpeace.org/research/ (26.05.2024).

Interpol (2024) Global Financial Fraud Assessment. Retrieved from https://www.interpol.int/en/content/download/21077/file/24COM005563-01%20-%20CAS_Global%20Financial%20Fraud%20Assessment_Public%20version_2024-03%20v2.pdf

ITU. (n.d.). Statistics. Retrieved from https://www.itu.int/en/ITU-D/Statistics/Pages/stat/default.aspx#gsc.tab=0

ITUCOUNCIL Geneva 2024 (2024). ICT Development Index. Retrieved from https://www.itu.int/en/Pages/default.aspx (26.05.2024).

Ivashchenko A., Polischuk Ye. (2018). Machine learning in estimating of SMEs investment potential in Ukraine. Proceedings of the 14th International Conference on ICT in Education, Research and Industrial Applications. Integration, Harmonization and Knowledge Transfer. Volume I: Main Conference. Kyiv, Ukraine, May 14-17, 77 -93. Retrieved from: http://ceur-ws.org/Vol-2105/

Jurek, P., Korjonen-Kuusipuro, K., & Olech, M. (2021). When technology use causes stress: Challenges for contemporary research. *Human Technology*, *17*(3), 190–196. https://doi.org/10.14254/1795-6889.2021.17-3.1

Kersan-Škabić, I., & Vukašina, M. (2023). Contribution of ESIFs to the digital society development in the EU. *Journal of International Studies*, 16(2), 195-210. doi:10.14254/2071-8330.2023/16-2/13

Kigerl, A. (2016). Cyber crime nation typologies: K-means clustering of countries based on cyber crime rates. *International Journal of Cyber Criminology*, 10(2), 147–169. https://doi.org/ 10.5281/zenodo.163399

Kliestik, T., Nica, E., Durana, P., & Popescu, G. H. (2023). Artificial intelligence-based predictive maintenance, time-sensitive networking, and big data-driven algorithmic decision-making in the economics of Industrial Internet of Things. *Oeconomia Copernicana*, *14*(4), 1097–1138. https://doi.org/10.24136/oc.2023.033

Konczos Szombathelyi, M., Borgulya, Á., & Balogh, G. (2023). Home-based telework: aspects of communication. Evidence from Hungary. *Economics and Sociology*, 16(3), 178-197. https://doi.org/10.14254/2071-789X.2023/16-3/10

Krajčík, V., Novotný, O., Civelek, M., & Semrádová Zvolánková, S. (2023). Digital Literacy and Digital Transformation Activities of Service and Manufacturing SMEs. *Journal of Tourism and Services*, *14*(26), 242–262. https://doi.org/10.29036/jots.v14i26.551

Kupenko, O., Kostenko, A., Kalchenko, L., Pehota, O., & Kubatko, O. (2023). Resilience and vulnerability of a person in a community in the context of military events. *Problems and Perspectives in Management*, *21*(1), 154–168. https://doi.org/10.21511/ppm.21(1).2023.14

Kuzior, A., Brożek, P., Kuzmenko, O., Yarovenko, H., & Vasilyeva, T. (2022a). Countering Cybercrime Risks in Financial Institutions: Forecasting Information Trends. *Journal of Risk and Financial Management*, 15(12), 613. https://doi.org/10.3390/jrfm15120613

Kuzior, A., Vasylieva, T., Kuzmenko, O., Koibichuk, V., & Brożek, P. (2022b). Global Digital Convergence: Impact of Cybersecurity, Business Transparency, Economic Transformation, and AML Efficiency. *Journal of Open Innovation: Technology, Market, and Complexity*, 8(4), 195. https://doi.org/10.3390/joitmc8040195

Kuzior, A., Yarovenko, H., Brożek, P., Sidelnyk, N., Boyko, A., & Vasilyeva, T. (2023). Company Cybersecurity System: Assessment, Risks and Expectations. *Production Engineering Archives*, 29(4), 379–392. https://doi.org/10.30657/pea.2023.29.43

Lăzăroiu, G., Gedeon, T., Rogalska, E., Andronie, M., Frajtova Michalikova, K., Musova, Z., … Geamănu, M. (2024). The economics of deep and machine learning-based algorithms for COVID-19 prediction, detection, and diagnosis shaping the organizational management of hospitals. *Oeconomia Copernicana*, *15*(1), 27–58. https://doi.org/10.24136/oc.2984

Lozano-Almansa, J. M., Tarifa Fernández, J., & Sánchez-Pérez, A. M. (2023). Digital Transformation and Real Options: Evaluating the Investment in Cloud ERP. *Engineering Economics*, *34*(4), 397–411. https://doi.org/10.5755/j01.ee.34.4.30678

Lytvyn, O., Kudin, V., Onyshchenko , A., Nikolaiev , M., & Chaplynska , N. (2024). Integration of digital means in the financial sphere: the potential of cloud computing, blockchain, big data and AI. *Financial and Credit Activity Problems of Theory and Practice*, *1*(54), 127–145. https://doi.org/10.55643/fcaptp.1.54.2024.4257

Mačiulytė-Šniukienė, A., Dargenytė-Kacilevičienė, L., & Matuzevičiūtė, K. (2023). Convergence in transport and ICT infrastructure: Evidence of EU member states. *Journal of International Studies*, 16(4), 77-96. doi:10.14254/2071-8330.2023/16-4/6

Melnyk, L., Kubatko, O., Piven, V., Klymenko, K., & Rybina, L. (2022). Digital and economic transformations for sustainable development promotion: A case of OECD countries. *Environmental Economics*, *12*(1), 140–148. https://doi.org/10.21511/ee.12(1).2021.12

Minh Sang, N. (2024). Evolution and future directions of Banking Risk Management Research: A Bibliometric analysis. *Banks and Bank Systems*, *19*(2), 1–14. https://doi.org/10.21511/bbs.19(2).2024.01

Mokhtar, R., Rohaizat, A. (2024). Cybercrimes and Cyber Security Trends in the New Normal. In: Kamaruddin, N., Idris, A., Fernandez, K. (eds) The New Normal and Its Impact on Society. Palgrave Macmillan, Singapore. https://doi.org/10.1007/978-981-97-0527-6_4

Mouna, B., & Yassine, M. (2024). Business Leadership in E-Commerce in the USA: The Impact of Blockchain Technology. *Business Ethics and Leadership*, 8(1), 116-128. https://doi.org/10.61093/bel.8(1).116-128.2024

Musyaffi, A.M., Baxtishodovich, B.S. Johari, R.J., Wolor, C.W., Afriadi, B., Muna, A. (2024). Can Financial Advantages and Digital Payments Adoption Provide Effective Solutions to Improve SMEs' Performance?. *Montenegrin Journal of Economics*, Vol. 20, No. 2, pp. 75-89. https://doi.org/10.14254/1800-5845/2024.20-2.7

Niftiyev, I., Kheyirkhabarli, M. (2024). The Impact of Covid-19 Pandemic on Cryptocurrency Adoption in Investments: a Bibliometric Study. *SocioEconomic Challenges*, 8(1), 154-169. https://doi.org/10.61093/sec.8(1).154-169.2024

Ninassi, C.J., & Burrell, D.N. (2023). Teaching business leadership skills to professionals in healthcare cybersecurity, biodefense and biotechnology through experiential learning methods. *Health Economics and Management Review, 4*(3), 82-94. https://doi.org/10.61093/hem.2023.3-07

Numbeo Doo (2024) Crime Index. Retrieved from https://www.numbeo.com/crime/rankings.jsp (26.05.2024).

Odei Addo, J., & Keelson, S. A. . (2023). Moderating role of the media in celebrity endorsement and product adoption. *International Journal of Entrepreneurial Knowledge*, *11*(2), 109–126. https://doi.org/10.37335/ijek.v11i2.206

Oe, H., Yamaoka, Y. (2023). The impact of the digital environment on eco-friendly behavioural change towards nature: Exploring the concept of forest bathing without forest. *SocioEconomic Challenges, 7*(3), 76-93. https://doi.org/10.61093/sec.7(3).76-93.2023

Orlandić, M., Đukić, T., and Mladenović, M. (2024). Upcoming digital transformation and artificial intelligence trends in the public sector. *Administratie si Management Public*, 42, 45-59. https://doi.org/10.24818/amp/2024.42-03

Pakhnenko, O., & Kuan, Z. (2023). Ethics of Digital Innovation in Public Administration. *Business Ethics and Leadership*, 7(1), 113-121. https://doi.org/10.21272/bel.7(1).113-121.2023

Pakhnenko, O., & Pudło, T. (2023). HealthTech in ensuring the resilience of communities in the post-pandemic period. *Health Economics and Management Review, 4*(2), 31-39. https://doi.org/10.21272/hem.2023.2-03

Pereira, E. T., & Shafique, M. N. (2024). The Role of Artificial Intelligence in Supply Chain Agility: A Perspective of Humanitarian Supply Chain. *Engineering Economics*, *35*(1), 77–89. https://doi.org/10.5755/j01.ee.35.1.32928

Piotrowski, D., & Orzeszko, W. (2023). Artificial intelligence and customers' intention to use robo-advisory in banking services. *Equilibrium. Quarterly Journal of Economics and Economic Policy*, *18*(4), 967–1007. https://doi.org/10.24136/eq.2023.031

Polishchuk, Y. (2023). Fintech future trends. *The European Digital Economy*, 204–220. https://doi.org/10.4324/9781003450160-15

Ponomarenko, I., Kovalov, B. L., Melnyk, M. (2024). Business Innovations and Digital Transformation: Trend, Comparative and Bibliometric Analysis. *Business Ethics and Leadership, 8*(1), 74-92. https://doi.org/10.61093/bel.8(1).74-92.2024

Porkodi, S., Al Balushi, S. S., Al Balushi, M. K., Al Hadi, K. O., & Al Balushi, Z. I. (2023). Digital employee experience and organizational performance: A study of the telecommunications sector in Oman. *Business, Management and Economics Engineering*, *21*(02), 248–268. https://doi.org/10.3846/bmee.2023.19498

Seniutis, M., Gružauskas, V., Lileikiene, A., & Navickas, V. (2024). Conceptual framework for ethical artificial intelligence development in social services sector. *Human Technology*, *20*(1), 6–24. https://doi.org/10.14254/1795-6889.2024.20-1.1

Shafranova, K., Navolska, N., Koldovskyi, A. (2024). Navigating the digital frontier: a comparative examination of Central Bank Digital Currency (CBDC) and the Quantum Financial System (QFS). *SocioEconomic Challenges, 8*(1), 90-111. https://doi.org/10.61093/sec.8(1).90-111.2024

Shakatreh, M., Abu Orabi, M.M., Al Abbadi, A.F.A. (2023). Impact of Cloud Computing on Quality of Financial Reports With Jordanian Commercial Banks. *Montenegrin Journal of Economics*, 19(2), 167-178. https://doi.org/10.14254/1800-5845/2023.19-2.14

Shaleh, M. I., Toiba, H., Muhaimin, A. W., Faizal, F. and Rahman, M. S. (2024). The Impact of Information and Communication Technology (ICT) on Pesticides Use of Potato Farmers in Indonesia. *AGRIS on-line Papers in Economics and Informatics*, 16(1), 83-90. https://doi.org/10.7160/aol.2024.160107

Sowmya, T., & Mary Anita, E. A. (2023). A comprehensive review of AI based Intrusion Detection System. *Measurement: Sensors*, 28, 100827. https://doi.org/10.1016/j.measen.2023.100827

Statista (n.d.) Retrieved from https://www.statista.com

Straková, J., Talíř, M., & Váchal, J. (2022). Opportunities and threats of digital transformation of business models in SMEs. *Economics and Sociology, 15*(3), 159171. doi:10.14254/2071-789X.2022/15-3/9

Streimikiene D., Mikalauskiene A., & Macijauskaite – Daunaraviciene, U. (2023). The role of information in shaping sustainable human behaviour. *Economics and Sociology*, 16(3), 198-226. https://doi.org/10.14254/2071-789X.2023/16-3/11

Suhanyi L., Gavura S., Suhanyiova A. (2024). E-government and the sustainable public administration: digital interaction with public authorities in the regions of the EU. *Transformations in Business and Economics,* 23(1(61), 106 – 126. Retrieved from http://www.transformations.knf.vu.lt/61/article/egov

Szigeti, S., & Jozsa, L. (2023). Obtaining Consumer Information for the Purchase of Over-The-Counter Medicines and Food Supplements from Hungarian-Speaking Adult Consumers in Slovakia. *Health Economics and Management Review, 4*(1), 60-70. https://doi.org/10.21272/hem.2023.1-06

Venkateswaran, N., Kiran Kumar, K., Maheswari, K., Vijaya Kumar Reddy, R. and Boopathi, S. (2024) Optimizing IoT Data Aggregation: Hybrid Firefly-Artificial Bee Colony Algorithm for Enhanced Efficiency in Agriculture. *AGRIS on-line Papers in Economics and Informatics*, 16(1), 117-130. https://doi.org/10.7160/aol.2024.160110.

Verizon Business (2024) 2024 Data Breach Investigations Report. Retrieved from https://www.verizon.com/business/resources/T549/reports/2024-dbir-data-breach-investigations-report.pdf

Vitvitskiy, S., Kurakin, N., Pokataev, S., Skriabin, M., & Sanakoiev, B. (2021). Peculiarities of cybercrime investigation in the banking sector of Ukraine: review and analysis. *Banks and Bank Systems*, *16*(1), 69–80. https://doi.org/10.21511/bbs.16(1).2021.07

Waliszewski, K., Cichowicz , E., Gębski , Łukasz, Kliber, F., Kubiczek, J., Niedziółka , P., … Warchlewska , A. (2024). Digital loans and buy now pay later from LendTech versus bank loans in the era of 'black swans': Complementarity in the area of consumer financing . *Equilibrium. Quarterly Journal of Economics and Economic Policy*, *19*(1), 241–278. https://doi.org/10.24136/eq.2982

Wang, F., Jia, Y., Li, G., Monica, L., & Liu, Y. (2024). An Empirical Study of the Relationship Between Digital Transformation, Corporate Social Responsibility and Financial Performance. *Business Ethics and Leadership, 8*(1), 57-73. https://doi.org/10.61093/bel.8(1).57-73.2024

Whitepaper S. (2024) The State of Ransomware 2024. Retrieved from https://assets.sophos.com/X24WTUEQ/at/9brgj5n44hqvgsp5f5bqcps/sophos-state-of-ransomware-2024-wp.pdf

Wright, J. (2023). Healthcare cybersecurity and cybercrime supply chain risk management. *Health Economics and Management Review*, 4(4), 17-27. https://doi.org/10.61093/hem.2023.4-02

Yamin, T., & Murwaningsari, E. (2023). Exploring the Interplay Between Digital Technology, Transformational Leadership and Agility for Enhancing Organisational Performance. *Business Ethics and Leadership*, 7(4), 73-88. https://doi.org/10.61093/bel.7(4).73-88.2023

Yarovenko, H., Bilan, Y., Lyeonov, S., & Mentel, G. (2021). Methodology for assessing the risk associated with information and knowledge loss management. *Journal of Business Economics and Management*, 22(2), 369–387. https://doi.org/10.3846/jbem.2021.13925

Yarovenko, H., Kuzior, A. & Raputa, A. (2023c). The Modeling of the Probable Behaviour of Insider Cyber Fraudsters in Banks. *Financial Markets, Institutions and Risks*, 7(4), 155-167. https://doi.org/10.61093/fmir.7(4).155-167.2023

Yarovenko, H. (2020). Evaluating the threat to national information security. *Problems and Perspectives in Management*, 18(3), 195–210. https://doi.org/10.21511/ppm.18(3).2020.17

Yarovenko, H., Lopatka, A., Vasilyeva, T., & Vida, I. (2023a). Socio-economic profiles of countries - cybercrime victims. *Economics & Sociology*, 16(2), 167–194. https://doi.org/10.14254/2071-789x.2023/16-2/11

Yarovenko, H., Lyeonov, S., Wojcieszek, K. A., & Szira, Z. (2023b). Do IT users behave responsibly in terms of cybercrime protection? *Human Technology*, 19(2), 178–206. https://doi.org/10.14254/1795-6889.2023.19-2.3

Zámek, D., Zakharkina, Z. (2024). Research Trends in the Impact of Digitization and Transparency on National Security: Bibliometric Analysis. *Financial Markets, Institutions and Risks*, 8(1), 173-188. https://doi.org/10.61093/fmir.8(1).173-188.2024