Mathematical Methods for Assessing the Level of Cybersecurity and Digital Development of Countries*

Kseniia Verhal[1,†], Oksana Kushnirenko[2,†], Oleksandr Bykonia[2,†], Nazarii Romanovskyi[3,†] and Ivan Opirskyy[4,*,†]

[1] National University "Yuri Kondratyuk Poltava Polytechnic", 24 Pershotravnevyi ave., 36011 Poltava, Ukraine
[2] State Organization "Institute for Economics and Forecasting, NAS of Ukraine", 26 Panasa Myrnoho str., 01011 Kyiv, Ukraine
[3] Kyiv National Taras Shevchenko University, 4 Akademika Glushkova ave., 03680 Kyiv, Ukraine
[4] Lviv Polytechnic National University, 12 Stepan Bandera str., 79000 Lviv, Ukraine

Abstract

The digital revolution and Industry 4.0 have significantly integrated information technology across economic sectors, driving rapid digitalization and economic transformation. However, this advancement also heightens cybersecurity risks, making national economies more vulnerable to cyber threats. Addressing these risks is essential for maintaining economic stability and safeguarding sensitive information. This study employs cluster analysis to assess cybersecurity and digital development levels at the national level. Using the National Cybersecurity Index (NCSI) and Digital Development Level (DDL) as key indicators, the k-means clustering algorithm was applied to categorize 71 countries into three clusters. The Elbow and Silhouette methods were used to determine the optimal number of clusters. The results identified three clusters with distinct cybersecurity preparedness: (1) high cybersecurity maturity (e.g., Moldova), (2) low cybersecurity preparedness (e.g., Libya), and (3) moderate cybersecurity development (e.g., Saudi Arabia). Countries in the highest cluster exhibit advanced cybersecurity strategies and well-established regulatory frameworks. In contrast, nations in the lower cluster face significant vulnerabilities due to weak regulations and limited cyber defense mechanisms. The findings emphasize the need for continuous cybersecurity enhancements, particularly in digitally emerging economies, to mitigate cyber threats and enhance national security.

Keywords

digital economy, cybersecurity, National Cybersecurity Index, digital development, cluster analysis, k-means, Elbow method, Silhouette method, cyber threats

1. Introduction

1.1. Relevance

The integration of digital knowledge and information technology into all economic sectors is driven by the digital revolution and Industry 4.0 [1, 2].

The incorporation of information technology into various economic sectors is propelled by the advancements of the digital revolution and Industry 4.0. The digital economy stands out as one of the most dynamic, innovative, and influential economic models, playing a crucial role in driving national economic growth [3]. This economy is defined by the exchange of goods and services through digital platforms, following a unique operational structure. Its expansion is closely tied to the development of information and communication technologies, leading to the rapid transformation and integration of related industries [4–6]. However, alongside these advancements, the increasing reliance on digital technologies introduces significant cybersecurity risks. The interconnected nature of digital infrastructures makes national economies more susceptible to cyber threats, including data breaches, financial fraud, and critical system

* DECaT'2025: Digital Economy Concepts and Technologies, April 4, 2025, Kyiv, Ukraine
* Corresponding author.
† These authors contributed equally.
itm.verhal@nupp.edu.ua (K. Verhal); kushnksena@gmail.com (O. Kushnirenko); alexbikonya@ukr.net (O. Bykonia); knuromnazar@gmail.com (N. Romanovskyi); ivan.r.opirskyi@lpnu.ua (I. Opirskyy)
0000-0001-6611-0489 (K. Verhal); 0000-0002-3853-584X (O. Kushnirenko); 0000-0002-5309-7032 (O. Bykonia); 0000-0002-5071-5624 (N. Romanovskyi); 0000-0002-8461-8996 (I. Opirskyy)

disruptions. The complexity of these challenges underscores the need for proactive cybersecurity measures to safeguard economic stability and protect sensitive information.

Addressing cybersecurity threats linked to the use of information and communication technologies is essential for organizations, governmental institutions, and individuals to effectively pursue their developmental objectives. This underlines the necessity of strengthening cybersecurity capabilities. By mitigating the negative consequences associated with digital technology usage, governments can enhance their ability to maintain a robust level of cybersecurity, ensuring a safer and more resilient digital landscape [7].

1.2. Related work

The concept of cluster analysis was initially introduced by R. C. Tryon in 1939. Tryon described cluster analysis as: “A general logical procedure formulated as a procedure by which we group objectively individuals into groups based on their similarities and differences” [8].

Cluster analysis has been effectively utilized to solve data clustering challenges across various fields, including goverment, manufacturing, finance, cyber security, urban development, industry, sales, and marketing [9–11]. Extracting valuable insights from data in these areas is crucial for enhancing services and increasing profitability. The data generated in real-world scenarios are often large, unlabeled, and multi-dimensional, which complicates the clustering process. Determining the number of clusters in such datasets cannot be easily achieved. As a result, identifying the optimal number of clusters in real-world data with high density and dimensionality is a challenging task for traditional clustering methods. This creates a significant hurdle for conventional clustering techniques that require the number of clusters to be pre-specified as an input.

In recent studies, considerable focus has been placed on integrating cybersecurity technologies and machine learning methods for monitoring and predicting IT security threats. In the study [12], the author introduced a robust approach for detecting suspicious domains involved in advanced persistent threat (APT) activities. The research evaluates various clustering algorithms and highlights K-means as the most commonly used method. In the study [13], the author discusses the growing importance of network security in today's digital landscape, particularly focusing on the use of the K-means clustering algorithm in data mining for network security. In the study [14], the author explores the use of cluster analysis for automating the matching of cyber threat intelligence reports in an Internet-of-Vehicles (IoV) environment.

2. Methods

We will perform a clustering analysis of data that describe the levels of cybersecurity and digitalization at the national level. To achieve this, we will analyze the National Cyber Security Index, Digital Development Level.

Data clustering algorithms are typically categorized into two main groups [15]: hierarchical clustering algorithms and partitional clustering algorithms. Hierarchical clustering methods organize data objects into clusters in a hierarchical structure, either through a bottom-up approach (agglomerative method) or a top-down approach (divisive method). In the agglomerative method, individual data points are iteratively merged based on their similarity. The divisive method, on the other hand, starts with the entire dataset as a single cluster and iteratively divides it using data object similarities until each object forms its own cluster, or until a predefined condition is met. The hierarchical clustering algorithm generates a dendrogram, which visually represents the process of merging (agglomerative) or splitting (divisive) data objects, illustrating the hierarchical structure of clusters as the output of the cluster analysis. The dendrogram serves as a visual depiction of the nested groupings of data objects, indicating the level of similarity at which each grouping changes.

K-means is the most popular clustering formulation in which the goal is to maximize the expected similarity between data items and their associated cluster centroids [16].

K-means algorithm with K input parameters, N objects ware distributed into K clusters, that makes a similar high similarity in the one cluster, low similarity between clusters. K-means algorithm process as follows [17].

The K-means clustering algorithm [15] is outlined below and consists of the following steps:

Input:

- K: the number of the clusters.
- D: contain N object in data set.

Output:

- K: clusters collection.

Method:

1. Choose K objects as initial cluster centers; from D.
2. Repeat.
3. Each object is assigned to the most similar clusters based on the mean value of the object in the cluster.
4. Profile of the mean of each cluster, and calculating the mean of each cluster.
5. Until no change.

The division of a set of objects into clusters should generally meet the following two requirements:

Objects within a single cluster should be similar in a certain sense.

Clusters that are similar in a certain sense should be located close to each other.

K-means clustering begins with the selection of k randomly positioned centroids (samples that represent the center of a cluster). Each element is assigned to the nearest centroid. After the assignment is made, the centroid is moved to the point calculated as the average of all the elements assigned to it. Then, the assignment is performed again. This procedure is repeated until the stopping condition is met.

The algorithm works in such a way that it aims to minimize the mean squared deviation at the points of each cluster:

$$V = \sum_{i=1}^{k} \sum_{x_j \in S_i}^{S_k} (x_j - \mu_i)^2, \tag{1}$$

where k is a number of clusters, S_i is a obtained clusters, where $i = 1, 2, \ldots, k$, μ_i are centroids of the vectors, where $x_j \in S_i$.

During the algorithm's operation, at each iteration, the centroid of each cluster obtained in the previous step is recalculated. Then, the vectors are reassigned to clusters based on which of the new centroids is closest to the vector according to the chosen metric. The algorithm terminates when, at any iteration, no change in the clusters occurs.

For this research, two methods will be employed to determine the optimal number of clusters: the Elbow method [18] and the Silhouette method.

The Elbow method [18] is one of the earliest techniques for identifying the potentially optimal number of clusters in a given dataset. Its fundamental concept involves initializing K = 2 and incrementally increasing K by one until reaching a predefined maximum. The optimal number of clusters, K, is then determined at the plateau point. This optimal K value is characterized by a sharp decrease in the indicator value before reaching K, followed by minimal change beyond this point, forming a distinct "elbow" shape. One of the limitations of the Elbow method is that when the plotted curve is relatively smooth.

The Silhouette method [19–21] has been discussed in sources where it is described as a technique for estimating the potentially optimal number of clusters. This method evaluates clustering quality by considering the average distance between a data point and others within the same cluster, as well as comparing it to the average distance between different clusters. The effectiveness of clustering is measured using the silhouette coefficient (S), which is calculated as

$$S = \frac{(b - a)}{\max(a, b)}, \quad (2)$$

where a is the mean intra-cluster distance, b is a mean distance to the nearest neighboring cluster.

Based on the obtained Silhouette Score values, a conclusion is made about the optimal number of clusters for further clustering $s(i)$:

- Close to 1 means that the point is well placed within its cluster.
- Close to 0 indicates that the point is on the boundary between two clusters.
- Close to −1 suggests that the point was likely assigned to the wrong cluster.

This approach is commonly applied to determine the optimal number of clusters and assess clustering performance in various scenarios.

The quality of k-means clustering is measured through the within-cluster squared error criterion [22].

The k-means algorithm, Elbow method and the Silhouette method was implemented in Python during the analysis of the indicators.

3. Results

According to the e-Governance Academy Foundation [23], the National Cybersecurity Index and Digital Development Level indicators were used for clustering with the k-means method.

The National Cyber Security Index (NCSI) is a global live index, which measures the preparedness of countries to prevent cyber threats and manage cyber incidents. The NCSI is also a database with publicly available evidence materials and a tool for national cyber security capacity building.

The NCSI focuses on measurable aspects of cyber security implemented by the central government:

1. Legislation in force—legal acts, regulations, orders, etc.
2. Established units—existing organisations, departments, etc.
3. Cooperation formats—committees, working groups, etc.
4. Outcomes—policies, exercises, technologies, websites, programmes, etc.

The NCSI Score indicates the percentage that a country has achieved out of the maximum value of the indicators. The maximum NCSI Score is consistently 100 (100%) regardless of any additions or removals of indicators.

$$NCSI = \frac{Country\ Points \times 100}{Maximum\ Points}. \quad (3)$$

The index table also shows the Digital Development Level (DDL). The DDL is calculated according to the E-Government Development Index (EGDI) and Networked Readiness Index (NRI). The DDL is the average percentage the country received from the maximum value of both indexes. The average percentage of the maximum values for EGDI and NRI is displayed in the DDL.

$$DDL = \frac{EGDI(\%) + NRI(\%)}{2}, \quad (4)$$

To create the dataset and perform clustering, a CSV file was generated containing information about the country name, National Cybersecurity Index, and Digital Development Level.

Table 1
Example of a CSV file with data [23]

Country	National Cybersecurity Index	Digital Development Level
Albania	70.83	62.34
Angola	17.50	33.37
Antigua and Barbuda	18.33	30.72
Argentina	58.33	67.36

A total of 71 countries were analyzed, all of which had corresponding values for the National Cybersecurity Index and Digital Development Level indicators.

To determine the optimal number of clusters, the necessary calculations were performed, and a visualization using the Elbow method was created. The graphic was obtained from Sum Square Error (SSE) calculation. The number of the cluster was determined by looking at the point position on the "elbow" arm. [24].

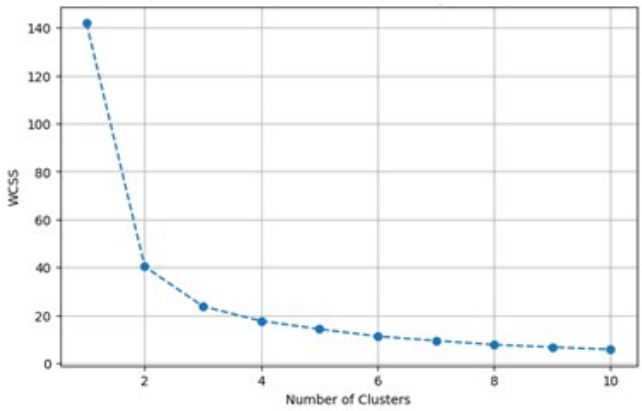

Figure 1: Elbow Method [(calculated based on [23])]

As seen in Fig. 1, according to this method, the optimal number of clusters is 3.

Let's perform a verification using the Silhouette method (Fig. 2 and 3). Based on the Silhouette Score analysis, the most optimal number of clusters is 3. Although the first cluster appears to be larger than the other two according to the visualized silhouette thickness, this clustering configuration remains preferable. The Silhouette Score, which measures how well each data point fits within its assigned cluster relative to other clusters, reaches its highest value for $k = 3$, indicating a well-structured partitioning of the dataset.

From a clustering quality perspective, the silhouette coefficient evaluates both intra-cluster cohesion and inter-cluster separation. The relatively high silhouette score for k = 3 suggests that, on average, countries within the same cluster are more similar, while the separation between clusters remains significant. Although increasing the number of clusters to $k = 4$ or $k = 5$ might lead to finer segmentation, it also results in smaller clusters with decreased cohesion and lower silhouette scores, making the overall structure less distinct.

Additionally, when analyzing the silhouette thickness for different clusters at $k = 3$, it is evident that one of the clusters is more populated compared to the others. However, this does not

necessarily indicate an imbalance in clustering but rather a natural distribution of the data, where one segment may contain countries with similar cybersecurity and digital development characteristics. Furthermore, compared to the models with $k = 4$ or $k = 5$, the three-cluster solution ensures a relatively proportional distribution of countries while avoiding unnecessary fragmentation.

Thus, selecting = 3 is supported both by the quantitative metric (Silhouette Score) and qualitative assessment of cluster interpretability, ensuring a meaningful and practical division of countries based on their National Cybersecurity Index and Digital Development Level.

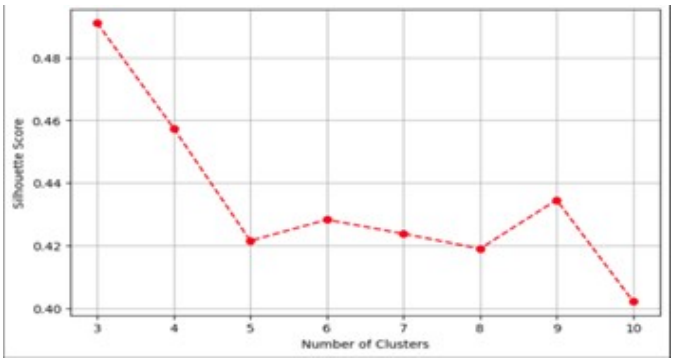

Figure 2: Silhouette method [(calculated based on [23])]

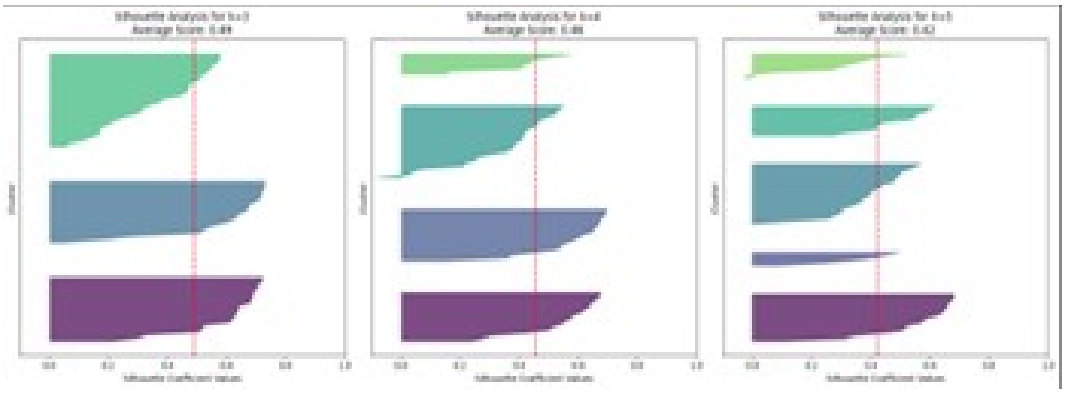

Figure 3: Silhouette method [(calculated based on [23])]

Using the proposed clustering algorithm, the dataset was successfully segmented into three distinct clusters based on the National Cyber Security Index (NCSI) and Digital Development Level (Fig. 4).

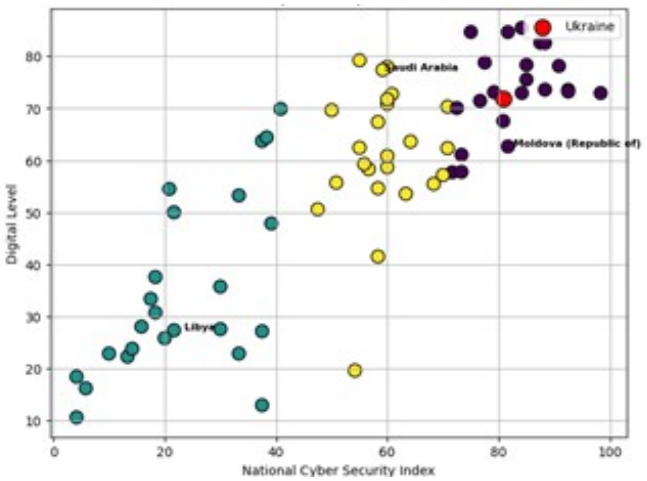

Figure 4: K-means clustering [(calculated based on [19])]

The results of the clustering process are as follows (Table 2):

Table 2
Country clustering results [(calculated based on [23])]

Cluster	Number of Countries	NCSI Range	Representative Country
Cluster 0	18 countries	71.67–98.33	Moldova (Republic of)
Cluster 1	27 countries	4.17–40.83	Libya
Cluster 2	26 countries	47.50–70.83	Saudi Arabia

Conclusions

The results of the cluster analysis conducted to assess the level of national cybersecurity and digital development of countries allow us to examine these indicators in the context of grouping states based on their cybersecurity levels. An important aspect is that countries with high, medium, and low cybersecurity levels demonstrate different approaches to addressing digital resilience, which influences their strategic initiatives and international cooperation in this field. In particular, clustering helps identify patterns and significant differences in approaches to cybersecurity among various countries.

1. Cluster 0 includes 18 countries with a high NCSI range (71.67–98.33). The representative country, Moldova (Republic of), is a fitting example due to its strong cybersecurity framework, legislative advancements, and cybersecurity incident response mechanisms. Moldova has made significant progress in strengthening its national cybersecurity framework, adopting comprehensive policies and establishing key institutions to enhance its cyber resilience. The country's efforts reflect its commitment to protecting critical infrastructure and responding effectively to cyber threats, especially given its strategic geopolitical position between the European Union and Russia. A new national cybersecurity law, which will come into effect on January 1, 2025, marks a major milestone in Moldova's cybersecurity strategy. Developed with support from the EU Cybersecurity Rapid Assistance Project, this legislation establishes clear guidelines for cybersecurity governance. Under the new law, a competent national authority will determine which institutions and service providers must meet specific cybersecurity standards. These essential service providers will be required to report major cyber incidents to the national authority, ensuring greater transparency and responsiveness in cyber threat management. The legal framework is aligned with European best practices, reinforcing Moldova's integration into European cybersecurity structures. Vice Prime Minister Dumitru Alaiba, Minister of Economic Development and Digitalization, emphasized that cybersecurity is a fundamental priority for Moldova due to its vulnerable geopolitical position. The law reflects European standards, ensuring that Moldova adopts advanced cybersecurity measures.

Moldova has received strong international support in developing its cybersecurity capabilities. On January 21, 2021, NATO launched a Cyber Incident Response Center for Moldova's Armed Forces. This initiative, developed in collaboration with the NATO Communications and Information Agency and supported by the NATO Science for Peace and Security (SPS) Programme, aims to minimize threats arising from cyber incidents, ensure rapid and effective recovery in case of cyberattacks, and prevent future cyber threats through advanced cybersecurity mechanisms. In 2024, Moldova established two key institutions dedicated to cybersecurity: the National Cybersecurity Agency, responsible for protecting critical government and public infrastructure from cyberattacks, ensuring high-level security of networks and information systems in both public and private sectors, and the National Institute for Cybersecurity Innovation ("Cybercor"), focused on cyber threat prevention, research, and innovation in digital security. These institutions will play a crucial role in enhancing Moldova's cybersecurity preparedness, resilience, and innovation, ensuring a secure digital ecosystem for both public and private entities. Moldova's

recent cybersecurity advancements demonstrate a proactive and strategic approach to digital security. By adopting a new cybersecurity law, strengthening cooperation with NATO and the EU, and establishing key institutions, Moldova is positioning itself as a leader in cybersecurity among emerging economies. These developments highlight a structured, well-coordinated national effort to combat cyber threats and align Moldova's cybersecurity policies with European and global standards.

Countries in the cluster 0 exhibit well-established cybersecurity strategies, comprehensive infrastructure, and government initiatives focused on digital resilience. Notably, Ukraine is also part of this cluster, signifying its relatively high cybersecurity preparedness.

2. Cluster 1: Low National Cyber Security Index. Cluster 1 consists of 27 countries with an NCSI range of 4.17–40.83, representing nations with relatively low cybersecurity preparedness. Libya is the representative country of this cluster. Libya, as a country experiencing political instability and conflicts, faces numerous challenges in the field of cybersecurity. Libya is one of the most vulnerable countries to significant cybersecurity threats in 2023, ranking 90th globally. This high risk is attributed to insufficient security measures against cybercrimes, making them highly susceptible to attacks. These country has weak or entirely absent legislation against cybersecurity threats, putting sensitive transactions at significant risk [25–28].

The lack of a stable government and centralized control complicates the development and implementation of effective cyber protection strategies, making state and private information systems vulnerable to cyber threats [29]. However, despite these difficulties, Libya demonstrates some potential in cybersecurity development. The presence of an educated youth and a growing interest in information technology create prerequisites for the formation of specialists in this field. Additionally, international organizations and partners provide support to Libya in strengthening its cybersecurity infrastructure, contributing to a gradual improvement of the situation. One of the key regulatory bodies in cybersecurity is NISSA (National Information Security and Safety Authority), which has released the NISSA Policy Guide. However, Libya still lacks a comprehensive cybersecurity strategy, though NISSA has been mandated to develop one in cooperation with the Ministry of Communications and Informatics. Despite the absence of a unified strategy, the country has specialized institutions addressing cybersecurity issues. Notably, under the Ministry of Interior, the "Administration for Combating IT Crimes" is responsible for investigating cybercrimes. Additionally, the national cybersecurity incident response team, Libya-CERT (Libyan Computer Emergency Response Team), operates under NISSA. It was established with the support of the International Telecommunication Union (ITU) and is responsible for preventing, detecting, and mitigating cyber threats at the national level.

However, despite ongoing efforts, certain aspects of its cybersecurity policies may still be developing. Countries in this group likely have fragmented cybersecurity frameworks, limited resources allocated to cyber defense, and emerging regulatory frameworks.

Cluster 2: Moderate National Cyber Security Index. Cluster 2 contains 26 countries with an NCSI range of 47.5–70.83. The representative country, Saudi Arabia, typifies this group as it is in a transitional stage of cybersecurity development.

Saudi Arabia has been actively working to improve its cybersecurity; however, its relatively low cybersecurity index may be attributed to several factors. Firstly, while the country has made significant progress in digitalizing government services, the rapid pace of digital transformation may outstrip the development of corresponding cybersecurity measures. Secondly, as a major oil producer, Saudi Arabia is an attractive target for cyberattacks, necessitating continuous advancements in defensive strategies. Additionally, although the country is implementing digital governance strategies such as "Saudi Vision 2030" to enhance citizens' quality of life, these initiatives may take time to achieve full effectiveness in cybersecurity.

An analysis of Saudi Arabia's cybersecurity framework has highlighted key risks associated with its development model. While assessments based on International Telecommunication Union (ITU) standards have yielded relatively positive results, Saudi Arabia has demonstrated a catch-up approach to cybersecurity development and continues to experience challenges in national cyber

defense. Some of these challenges are global in nature, such as legislative gaps, while others stem from the specifics of the national governance model. The most prominent risks include an imbalance between the civilian and military cybersecurity sectors, regional disparities in cybersecurity readiness, and weak integration of the local hacker community into the national cybersecurity framework [30].

Nations in this cluster have moderate cybersecurity strategies, often influenced by economic, political, and technological challenges that affect their ability to implement robust cybersecurity measures.

According to the results of the cluster analysis, countries with a high level of cybersecurity (Cluster 0) demonstrate well-developed infrastructure, clearly defined national strategies, and effective government policies in the field of digital security. The selection of Moldova as the representative of this cluster highlights the importance of having appropriate legislation, international support, and strategic institutions for creating a stable and resilient cybersecurity ecosystem. In countries of this cluster, a high level of organizational maturity in countering cyber threats is observed, enabling them to effectively respond to incidents and implement innovative technologies to enhance cyber resilience.

On the other hand, countries with a low level of cybersecurity (Cluster 1) face numerous challenges, including political instability, the absence of or weak legislation, and limited resources for developing national cybersecurity strategies. The example of Libya, the representative of this cluster, demonstrates how crucial international assistance is for strengthening cybersecurity infrastructure, as well as creating specialized organizations capable of responding to cyber threats in a timely manner. Considering the limited capacity of such countries to implement effective strategies, further cooperation with international partners is critical to improving their cybersecurity defenses.

Given the identified characteristics, it is recommended that countries with low levels of cybersecurity, such as Libya and others with similar issues, actively seek international support to establish basic cybersecurity standards and create specialized institutions for responding to cyber incidents. An essential step is also strengthening the training and preparation of specialists, which will help reduce the risks of cyber threats in these countries.

Countries with a moderate level of cybersecurity, such as Saudi Arabia, should focus on improving their cybersecurity strategies by enhancing the integration of civilian and military sectors, as well as strengthening cooperation with international partners to achieve sustainable development in digital security.

Declaration on Generative AI

While preparing this work, the authors used the AI programs Grammarly Pro to correct text grammar and Strike Plagiarism to search for possible plagiarism. After using this tool, the authors reviewed and edited the content as needed and took full responsibility for the publication's content.

References

[1] A. Fagarazzi, Impact of Digital Development Level on National Cybersecurity Index, Poslovna izvrsnost, 18(2) (2024) 37–61. doi:10.22598/pi-be/2024.18.2.37

[2] O. Kushnirenko, The Industry of Ukraine Facing the Challenges of Industry 4.0: Evaluation of Limitations and Policy TASKS, Economy of Ukraine, 63 (2020) 53–71. doi:10.15407/economyukr.2020.05.053

[3] L. Guo, The Impact Mechanism of the Digital Economy on China's Total Factor Productivity: An Uplifting Effect or a Restraining Effect?, South China J. Econom. 40 (2021) 9–27.

[4] M. Chyzhevska, et al., Tokenomics and Perspectives of Proof of Stake, in: Digital Economy Concepts and Technologies, vol. 3665, 2024, 61–69.

[5] M. Chyzhevska, et al., Dual Impact of Crypto Industry Technologies on the Energy Poverty, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3421, 2023, 293–299.
[6] M. Chyzhevska, et al., Behavioral Biometry as a Cyber Security Tool, in: Cybersecurity Providing in Information and Telecommunication Systems, vol. 3188, 2021, 88–97.
[7] Z. Homburger, The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace, Global Society 33 (2019) 224–242. doi:10.1080/13600826.2019.1569502
[8] R. C. Tryon, Cluster Analysis: Correlation Profile and Orthometric (Factor) Analysis for the Isolation of Unities in Mind and Personality, Edwards Brothers, Ann Arbor, 1939.
[9] A. M. Ikotun, et al., K-Means Clustering Algorithms: A Comprehensive Review, Variants Analysis, and Advances in the Era of Big Data, Information Sciences, 622 (2023) 178–210. doi:10.1016/j.ins.2022.11.139
[10] A. Belhadi, et al., Space–Time Series Clustering: Algorithms, Taxonomy, and Case Study on Urban Smart Cities, Eng. Appl. Artificial Intell. 95 (2020). doi:10.1016/j.engappai.2020.103857
[11] D. Parnes, A. Gormus, Prescreening Bank Failures with K-Means Clustering: Pros and Cons, Int. Rev. Financial Anal. 93 (2024) 103222. doi:10.1016/j.irfa.2024.103222
[12] G. Yan, et al., AULD: Large Scale Suspicious DNS Activities Detection via Unsupervised Learning in Advanced Persistent Threats, Sensors 19(14) (2019) 3180. doi:10.3390/s19143180.
[13] C. Bu, Network Security Based on K-Means Clustering Algorithm in Data Mining Research, in: Advances in Computer Science Research, vol. 83, 2018, 642–645. doi:10.2991/snce-18.2018.130.
[14] G. Raptis, C. Katsini, C. Alexakos, Towards Automated Matching of Cyber Threat Intelligence Reports based on Cluster Analysis in an Internet-of-Vehicles Environment, in: IEEE International Conference on Cyber Security and Resilience (CSR), 2021, 366–371. doi:10.1109/CSR51186.2021.9527983
[15] A. K. Jain, et al., Data Clustering: A Review, ACM Computing Surveys, 31(3) (1999) 264–323. doi:10.1145/331499.331504
[16] N. Slonim, et al., Hartigan's K-Means Versus Lloyd's K-Means—Is It Time for a Change?, in: Proceedings of the Twenty-Third International Joint Conference on Artificial Intelligence, 2013, 1677–1684.
[17] J. Cui, et al., Research on K-Means Clustering Algorithm and its Implementation, in: Proceedings of ICCSEE, 2013. doi:10.2991/iccsee.2013.452
[18] D. J. Ketchen, C. L. Shook, The Application of Cluster Analysis in Strategic Management Research: an analysis and critique, Strategic Manag. J. 17(6) (1996) 441–458. doi:10.1002/(SICI)1097-0266(199606)17:6<441::AID-SMJ819>3.0.CO;2-G
[19] P. J. Rousseeuw, Silhouettes: A Graphical Aid to the Interpretation and Validation of Cluster Analysis, J. Computat. Appl. Math. 20 (1987) 53–65. doi:10.1016/0377-0427(87)90125-7.
[20] O. Arbelaitz, et al., An Extensive Comparative Study of Cluster Validity Indices, Pattern Recognition, 46(1) (2013) 243–256. doi:10.1016/j.patcog.2012.07.021
[21] R. Tibshirani, et al., Estimating the Number of Clusters in a Data Set via the Gap Statistic, J. Royal Statistical Society: Series B (Statistical Methodology), 63(2) (2001) 411–423. doi:10.1111/1467-9868.00293
[22] C. Yuan, H. Yang, Research on k-Value Selection Method of k-Means Clustering Algorithm, Multidisciplinary Sci. J. 2(2) (2019) 226–235. doi:10.3390/j2020016
[23] E-Governance Academy Foundation. URL: https://ncsi.ega.ee/methodology
[24] H. Hestry, R. Rasyidah, Determining the Appropriate Cluster Number Using Elbow Method for K-Means Algorithm, in: EAI Proceedings, 2020.
[25] Y. Kostiuk, et al., A System for Assessing the Interdependencies of Information System Agents in Information Security Risk Management using Cognitive Maps, in: 3rd Int. Conf. on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN), Kyiv, Ukraine, vol. 3925, 2025, 249–264.

[26] Y. Kostiuk, et al., Models and Algorithms for Analyzing Information Risks during the Security Audit of Personal Data INFORMATION System, in: 3rd Int. Conf. on Cyber Hygiene & Conflict Management in Global Information Networks (CH&CMiGIN), Kyiv, Ukraine, vol. 3925, 2025, 155–171.
[27] S. Shevchenko, et al., Information Security Risk Management using Cognitive Modeling, in: Cybersecurity Providing in Information and Telecommunication Systems II, CPITS-II, vol. 3550 (2023) 297–305.
[28] S. Zybin, et al., Approach of the Attack Analysis to Reduce Omissions in the Risk Management, in: Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 2923 (2021) 318–328.
[29] V. Astapenya, et al., Conflict Model of Radio Engineering Systems under the Threat of Electronic Warfare, in: Cybersecurity Providing in Information and Telecommunication Systems, CPITS, vol. 3654 (2024) 290–300.
[30] L. Cukanov, Saudi Arabia National Cyber Security System: Specificity and Development Risks, in: Bulletin of Kemerovo State University, Series: Political, Sociological and Economic Sciences, 2022, 435–443. doi:10.21603/2500-3372-2021-6-4-435-443