“The impact of national cybersecurity on global competitiveness: A data mining approach”

AUTHORS	Vitaliia Koibichuk David Fulep Oleksandr Kubatko Alina Yefimenko Andrii Skrylnyk Kseniia Mohylna

ARTICLE INFO	Vitaliia Koibichuk, David Fulep, Oleksandr Kubatko, Alina Yefimenko, Andrii Skrylnyk and Kseniia Mohylna (2026). The impact of national cybersecurity on global competitiveness: A data mining approach. *Problems and Perspectives in Management*, *24*(3), 336–356. doi:10.21511/ppm.24(3).2026.22
DOI	http://dx.doi.org/10.21511/ppm.24(3).2026.22
RELEASED ON	Tuesday, 18 August 2026
RECEIVED ON	Thursday, 19 February 2026
ACCEPTED ON	Tuesday, 14 July 2026

JOURNAL	"Problems and Perspectives in Management"
ISSN PRINT	1727-7051
ISSN ONLINE	1810-5467
PUBLISHER	LLC “Consulting Publishing Company “Business Perspectives”
FOUNDER	LLC “Consulting Publishing Company “Business Perspectives”

NUMBER OF REFERENCES	NUMBER OF FIGURES	NUMBER OF TABLES
40	3	7

BUSINESS PERSPECTIVES

LLC "CPC "Business Perspectives"
Hryhorii Skovoroda lane, 10,
Sumy, 40022, Ukraine

www.businessperspectives.org

Vitaliia Koibichuk (Ukraine), **David Fülep** (Hungary), **Oleksandr Kubatko** (Ukraine), **Alina Yefimenko** (Ukraine), **Andrii Skrylnyk** (Ukraine), **Kseniia Mohylna** (Ukraine)

THE IMPACT OF NATIONAL CYBERSECURITY ON GLOBAL COMPETITIVENESS: A DATA MINING APPROACH

Type of the article: Theoretical Article

Received on: 19th of February, 2026
Accepted on: 14th of July, 2026
Published on: 18th of August, 2026

Vitaliia Koibichuk, Ph.D. (Economics), Associate Professor, Department of Economic Cybernetics, Sumy State University, Ukraine.

David Fülep, Ph.D., Associate Professor, Department of International and Applied Economics, Széchenyi István University, Hungary. (Corresponding author)

Oleksandr Kubatko, D.Sc. in Economics, Professor, Department of Economics, Entrepreneurship and Business Administration, Faculty of BIEM, Sumy State University, Ukraine.

Alina Yefimenko, Ph.D. (Economics), Associate Professor, Department of Economic Cybernetics, Sumy State University, Ukraine.

Andrii Skrylnyk, Associate Professor, Department of Economics, Entrepreneurship and Marketing, Doctoral student of the Department of Finance, Banking and Taxation, National University "Yuri Kondratyuk Poltava Polytechnic", Ukraine.

Kseniia Mohylna, Researcher, Department of Economic Cybernetics, Sumy State University, Ukraine.

Abstract

National cybersecurity opens new opportunities for digital transformation and helps counter the growing threat of cyberattacks. The purpose of this study is to develop a methodology and identify the most influential predictors of national cybersecurity in global competitiveness, utilizing the data mining approach. To assess the impact of cybersecurity characteristics, modern machine learning methods were implemented in the Salford Predictive Modeler software environment, including Classification and Regression Trees, Random Forest, Stochastic Gradient Boosting, Multivariate Adaptive Regression Splines, Generalized Path Seeker, and classical regression. Data mining was conducted using the World Competitiveness Ranking (WCR) indicators, constructed by the Institute for Management Development, and the National Cybersecurity Index (NCSI), constructed by the e-Governance Academy, for 64 countries as of 2024. Three groups of countries were identified with different predicted levels of competitiveness, underscoring the importance of balancing the development of both external and internal components of cyber defense. The empirical results demonstrate that countries with strong cybersecurity management capabilities achieve higher competitive positions, even with limited participation in global cyber initiatives. At the same time, active global involvement without sufficient internal readiness does not create sustainable competitive advantages. The regression tree provided a transparent allocation of key subfactors, with global cybersecurity contribution and cybersecurity management playing leading roles. The significance of the study lies in shaping methodology and state policy in cybersecurity, human resource development, regulatory framework enhancement, and digital ecosystem strengthening.

Keywords cybersecurity, global competitiveness, machine learning models, CART algorithm, cybersecurity management, global cybersecurity contribution, e-Governance Academy

JEL Classification F52, C51, O33

INTRODUCTION

Determining the role of cybersecurity in shaping economic security is undoubtedly complex and multifaceted. However, in an era of exponential growth in digital processes and the implementation of innovative systems and approaches that rely on digital data across all areas of state activity, it is undeniable that a country's global competitiveness will directly depend on the state and quality of its cybersecurity. Today, cyber threats can paralyze entire sectors of the economy, inflict billions in losses on businesses, and undermine trust in digital technologies, making cybersecurity an integral component of national strategic planning. Several factors determine the relevance of studying the relationship between cybersecurity and national competitiveness. First, the COVID-19 pandemic accelerated the digital transformation of economies, increasing the volume and complexity of cyber incidents. Second, the recent geopolitical crisis has demonstrated that cyberattacks can be used as an instrument of hybrid warfare to de-

Conflict of interest statement:
Author(s) reported no conflict of interest

http://dx.doi.org/10.21511/ppm.24(3).2026.22

stabilize economies and undermine countries' competitive positions on the international stage. Third, the digital economy is becoming an essential component of national wealth, and a country's ability to ensure a secure digital environment directly affects its attractiveness to investors, innovation potential, and economic security. Considering the growing recognition of cybersecurity as a strategic component of digital transformation and national resilience, the specific relationship between institutional cybersecurity capacities and national competitiveness remains insufficiently operationalized in empirical research. In particular, limited attention has been devoted to identifying which dimensions of national cybersecurity preparedness are most strongly associated with cross-country differences in competitiveness performance. Since the National Cyber Security Index (NCSI) captures institutional, organizational, and operational dimensions of cybersecurity governance, its subfactors provide a relevant analytical framework for examining how cybersecurity capacity may contribute to competitiveness outcomes in the digital economy. Therefore, the methodological problem addressed in this study concerns identifying the most influential cybersecurity management factors affecting national competitiveness using data mining techniques. Despite the growing number of studies on cybersecurity and competitiveness, insufficient attention has been devoted to identifying which dimensions of national cybersecurity capacity are most strongly associated with differences in competitiveness across countries using machine learning methods.

1. THEORETICAL BASIS

The digital transformation of the economy and growing dependence on technology have led to new factors in national competitiveness. Digitalization capabilities are increasingly interpreted as drivers of cyber resilience and sustainable competitiveness because they strengthen organizational adaptability, technological continuity, and innovation capacity within the digital economy (Annarelli & Palombi, 2021). Therefore, research on the relationship between cybersecurity and competitiveness is a relevant direction that has emerged at the intersection of economics, information technology, and management. The contemporary scientific landscape in this area encompasses both theoretical foundations and empirical studies at macro and micro levels, gradually shifting focus from company protection to the strategic significance of state cyber resilience.

From a theoretical perspective, national cybersecurity may be considered a component of institutional and digital resilience that supports sustainable competitiveness within the digital economy. Contemporary approaches to competitiveness increasingly emphasize that competitive advantage is no longer determined solely by traditional economic factors such as labor productivity or industrial capacity, but also by states' ability to ensure secure digital infrastructure, cyber resilience, technological trust, and the continuity of critical digital services (World Economic Forum, 2023; I. Vasiu & L. Vasiu, 2018). Thus, cybersecurity performs both a protective and an enabling institutional function that supports innovation, investment attractiveness, digital governance, and international economic integration. Modern approaches to cyber governance also emphasize that effective cybersecurity strategies increasingly require proactive, resilience-oriented frameworks that combine institutional coordination, adaptive response mechanisms, and strategic cyber capacity development (Safitra et al., 2023). Therefore, the relationship between cybersecurity and competitiveness can be theoretically interpreted through the interaction between digital transformation, institutional capacity, and national resilience.

The growing complexity of the digital economy increases countries' exposure to cyber risks and simultaneously strengthens the importance of institutional cybersecurity capacity for maintaining sustainable competitiveness. These trends directly affect the country's competitiveness, as low and volatile growth rates increase the economy's sensitivity to risks, ranging from macroeconomic to cyber threats. The slowdown in economic activity also limits states' ability to invest in infrastructure modernization, the development of digital solutions, and support for innovative development.

Scientific interest in the relationship between cybersecurity and competitiveness is growing rap-

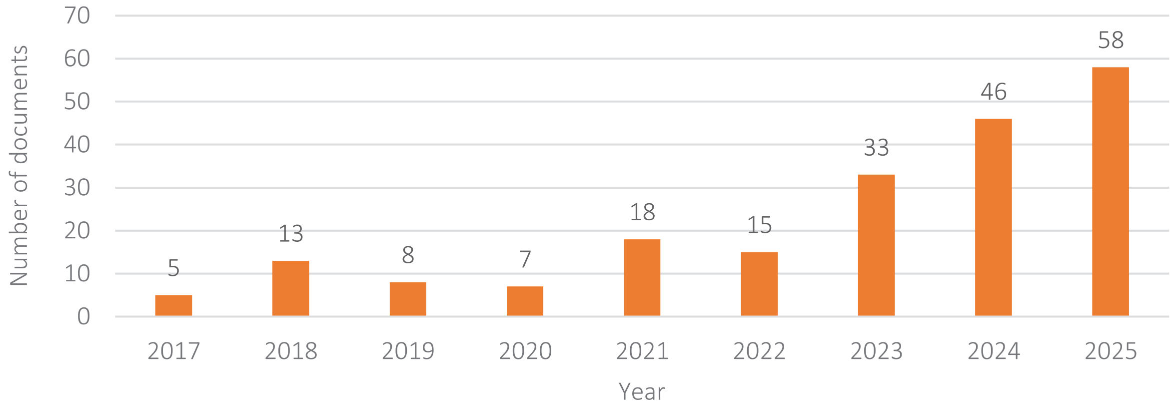

Figure 1. Dynamics of publications related to "competitiveness" and "cybersecurity" in the Scopus database during 2017–2025

idly, as evidenced by positive publication dynamics in the Scopus database: the number of documents containing the keywords "competitiveness" and "cybersecurity" increased from 5 in 2017 to 58 in 2025, with accelerated growth from 2023 onwards. The publication dynamics illustrate growing academic attention to the intersection of cybersecurity and competitiveness; however, the existing literature still lacks a sufficiently integrated theoretical and empirical framework explaining how specific dimensions of national cybersecurity influence competitiveness outcomes (Figure 1).

The selection of NCSI subfactors in this study is theoretically grounded in the multidimensional understanding of national cybersecurity governance. Unlike purely technical cybersecurity indicators, the NCSI framework incorporates institutional, organizational, educational, operational, and international dimensions of cyber resilience. In particular, subfactors such as Cybersecurity Management (CSM), Global Cybersecurity Contribution (GCC), Cyber Incident Response (CIR), Cyber Crisis Response Development (CRD), and Education and Professional Development (EPD) reflect different components of state cyber capacity that may influence countries' competitiveness through institutional stability, digital trust, innovation support, crisis resilience, and international cybersecurity cooperation. Therefore, the NCSI subfactors provide an appropriate analytical basis for examining the relationship between cybersecurity preparedness and competitiveness outcomes.

Mussayeva et al. (2025) focus on the development of the global digital economy using Porter's Five Forces model. They analyze, using SWOT and qualitative comparative analyses of global markets, how digital factors (including cybersecurity) change the competitive environment. By 'global markets,' they mean not just a set of national markets but a single, integrated economic environment that operates at the global level through digital technologies (e-commerce, fintech, IT services). Global markets are closely related to cybersecurity because, first, trust between market participants depends on data protection (Morales-Sáenz et al., 2024); second, cyberattacks disrupt the functioning of international markets; and third, the level of cyber protection affects the investment attractiveness and competitiveness of countries and companies. Their results showed that a high level of cyber risks reduces the competitiveness of digital platforms, and countries and companies with better cybersecurity have more stable competitive positions. Recent empirical studies also demonstrate the growing application of machine learning methods to analyze cybersecurity resilience and its organizational and economic implications in digitally intensive environments. In particular, Fernandez de Arroyabe et al. (2023) emphasize the analytical potential of data-driven approaches for identifying complex relationships between cybersecurity capabilities, resilience factors, and organizational sustainability. These approaches support the relevance of applying machine learning techniques to the analysis of interactions between national cybersecurity and competitiveness.

http://dx.doi.org/10.21511/ppm.24(3).2026.22

Overall, the existing literature demonstrates that cybersecurity increasingly functions as a strategic component of digital competitiveness. However, most existing studies either focus on firm-level digital transformation, analyze cybersecurity from a purely technical perspective, or investigate macroeconomic competitiveness without operationalizing specific dimensions of cybersecurity governance. Consequently, insufficient attention has been devoted to identifying which institutional cybersecurity capacities are most strongly associated with cross-country differences in competitiveness.

Thematically, the scientific output is interdisciplinary, with dominance of works in computer science (24%) and engineering (16%), reflecting the technical nature of cyber threats. However, a significant share falls on business, management and accounting (11%), social sciences (10%), and economics, econometrics and finance (7%), emphasizing the gradual transition of focus from purely technical aspects to the strategic and economic impact of cyber resilience at national and corporate levels. A significant portion of scientific output focuses on the micro level, examining the impact of cybersecurity on companies' competitive advantage. However, these models and conclusions are an important foundation for understanding macro-level processes. At the company level, cybersecurity is viewed as a potential source of competitive advantage. For example, the conceptual model of cybersecurity competitive advantage explains that regulatory compliance provides a basic level of protection, but the development of specific dynamic capabilities in cybersecurity creates sustainable competitive advantage for enterprises (Kosutic & Pigni, 2020; Kosutic, 2021). Additionally, for small and medium-sized enterprises, cybersecurity is considered a "merit good" due to its significant social benefits and gaps in adoption, indicating the presence of market failures (Arroyabe et al., 2024). Wiki communities can reduce cybersecurity risks, since they contain no closed data (Kalinichenko et al., 2024).

At the state level, the information and communication technology sector has become a strategic asset, important not only for the economy but also for national security and defense (Erixon et al., 2024; European Commission, n.d.a, n.d.b). National cybersecurity strategies play a key role in forming a systematic approach to protecting digital space. For example, analysis of G20 countries' strategies revealed common goals, specific priorities, and latent themes reflecting the complexity of multinational cybersecurity dynamics (Çifci & Ergüner, 2025). Currently, the economic digital transformation resembles quasi-viral trends (Melnyk et al., 2025), while the global digital economy exhibits high dynamism, competition, and structural transformations, where digital adoption and search for new technological assets as temporary safe havens during COVID-19 were a usual strategy among investors (Pollák et al., 2026).

Cybersecurity has gradually transformed from a technical problem into a strategic factor of national competitiveness. Information security, innovation development, and governance efficiency have a significant impact on a country's image and global competitiveness (Petroye et al., 2020). Moreover, analysis of over 10,000 disclosed cyber incidents in 190 countries confirmed a statistically significant negative relationship between the frequency of cyber incidents and GDP per capita in developing economies, with particularly noticeable consequences for the public sector, telecommunications, finance, and education (Vergara Cobos et al., 2024). Given this, it is expected that, to strengthen competitive positions, states need investments in the digital industry, increased digital literacy among the population, and improvements to the legal framework for cybersecurity (Miethlich et al., 2020).

However, research on the impact of cybersecurity on national competitiveness is not without challenges; specifically, evidence highlights the importance of transitioning from simplified to dynamic, stochastic, and generalizing models to understand the economic aspects of cybersecurity better (Kianpour et al., 2021). Furthermore, the economic aspects of national cybersecurity strategies remain insufficiently studied due to a lack of data to measure cybersecurity costs and evaluate the economic effectiveness of strategies (Brangetto & Kert-Saint Aubyn, 2015). Another complication in modeling the relationship between competitiveness and cybersecurity is the bidirectional linkage. Research indicates that, beyond the impact of cyber threats on the economy, there is also a reverse influence: economic growth and digital infrastructure development positively correlate with a country's cybersecurity level, as economically successful states can invest more in developing their cyber defense strategies and capabilities (Kolat & Unver, 2025).

Recent literature further confirms that cybersecurity preparedness should be analyzed as a multidimensional socio-economic and institutional phenomenon rather than a purely technical issue. Digitalization creates new opportunities for competitiveness, but it also increases exposure to cybercrime, cyber-fraud, corruption risks and broader feelings of insecurity in the digital age (Dobrovolska & Rozhkova, 2024a; Korjonen-Kuusipuro & Wojciechowski, 2025; Kuzior et al., 2024; Yarovenko et al., 2025b). At the macro level, digital readiness strengthens countries' ability to combat corruption and cyber threats, especially when technological capacity is supported by institutional maturity and governance quality (Yarovenko et al., 2025a). At the sectoral and organizational levels, Industry 4.0 awareness, digital training priorities, and machine learning applications in fraud detection demonstrate that cybersecurity capacity depends on both technological tools and human competences (Morshed & Khrais, 2025; Dobrovolska & Rozhkova, 2024b). Moreover, the use of XGBoost to forecast the impact of illicit practices on conflict-affected economies confirms the growing relevance of advanced data-driven methods for analyzing security-related risks in conditions of instability (Yarovenko et al., 2026). Therefore, these studies strengthen the theoretical justification for examining how specific dimensions of national cybersecurity capacity influence competitiveness outcomes.

The abovementioned papers demonstrate an interdisciplinary approach to researching the relationship between cybersecurity and competitiveness, combining computer science, economic analysis, strategic management, and public policy. Despite the growing number of studies, there remains a need for empirical evidence that quantitatively assesses the impact of specific subfactors of national cybersecurity on countries' global competitiveness using modern data analysis methods.

Therefore, the purpose of this study is to develop a methodology and identify the most influential predictors of national cybersecurity in global competitiveness utilizing the data mining approach.

2. RESULTS

To assess the impact of specific factors of national cybersecurity on global competitiveness, this study applies data mining and machine learning techniques. Using the World Competitiveness Ranking as a proxy for economic security, the data from 64 countries in 2024 were used to identify the key determinants of states' competitive positions in the digital era. The application of various machine learning algorithms – from classification and regression trees (CART) to ensemble methods (Random Forest, Stochastic Gradient Boosting) and multivariate adaptive regression splines (MARS) – enables identification of the most influential cybersecurity factors shaping countries' economic capacity to compete globally.

To forecast the impact of cybersecurity indicators on global competitiveness, it is proposed to use machine learning methods in Salford Predictive Modeler (a software suite for predictive analytics). This software uses machine learning methods such as Classification and Regression Tree (CART), Random Forest (RF), TreeNet (commercial name for the Gradient Boosting Method in Salford Predictive Modeler), Multivariate Adaptive Regression Spline (MARS), Generalized Path Seeker (GPS – generalized path finding method for regularised regressions), and Regression.

The study's methodological framework consisted of five main stages. At the first stage, a comparative dataset was formed based on the IMD World Competitiveness Ranking (WCR) and the subfactors of the National Cyber Security Index (NCSI) for the analyzed countries.

At the second stage, the target variable was defined. Since WCR represents an ordinal ranking variable in which lower values indicate stronger competitiveness positions, the indicator was transformed into an inverse competitiveness score using:

$$WCR^{*} = 68 - WCR, \tag{1}$$

where higher values correspond to stronger competitiveness outcomes.

At the third stage, the NCSI subfactors were selected as explanatory variables representing the

http://dx.doi.org/10.21511/ppm.24(3).2026.22

following dimensions of cybersecurity capacity: cyber governance, crisis management, protection of digital services, cyber incident response, and international cybersecurity cooperation.

At the fourth stage, several data mining algorithms (CART, Random Forest, TreeNet, and MARS) were comparatively tested to identify the model with the highest predictive and interpretative potential.

At the fifth stage, the obtained models were evaluated using comparative forecasting performance indicators, after which the CART model was selected for detailed interpretation due to its interpretability and stable predictive performance.

Popular machine learning tools are extensions of modeling tools. Machine learning algorithms used in classification and regression trees were first proposed by Breiman et al. (1984). Thus, CART is a decision tree algorithm that works by creating a set of "yes" or "no" rules that split the response variable (target variable) into partitions (parts) based on predictor settings. The splitting of predictor parameters is performed sequentially, one predictor at a time, in order of their influence on the target variable. A prediction is created for each partition.

The CART (Classification and Regression Trees) algorithm builds decision trees using a greedy, recursive splitting process that follows four steps:

- Step 1. Splitting Criterion – Mean Squared Error (MSE). At each step, CART selects the feature j and split point that minimizes the total squared error.
- Step 2. Leaf Node Prediction. Once the tree is built, predictions for a new data point X^* are made by assigning it to a leaf node and taking the average of the training values in that region.
- Step 3. Reaching maximum tree depth (stopping criterion). The recursive algorithm stops when one of three criteria is reached.
- Step 4. Pruning (Cost Complexity Pruning, CCP). To prevent overfitting, a pruning technique is applied based on a complexity parameter α, which balances tree size and error.

The original IMD World Competitiveness Ranking 2024 includes 67 countries. However, Hong Kong SAR, the Republic of Korea, and Puerto Rico were excluded from the final sample because corresponding NCSI observations were unavailable for 2024. Consequently, the final analytical dataset consisted of 64 countries represented in both databases. Since the exclusion criterion was based solely on data availability and was not related to the countries' competitiveness positions or cybersecurity performance, the risk of systematic selection bias is considered limited. Moreover, the excluded countries represent only 4.5% of the original population, suggesting that their omission is unlikely to materially affect the predictive relationships identified in the study.

Therefore, to select the best model for forecasting competitiveness levels on the global stage for 64 countries in the study, six machine learning models and a classical regression model were built. The best model is selected based on the smallest MSE value.

To analyze the forecast of countries' global competitiveness under the influence of national cybersecurity indicators, we use these values directly (Appendix A). However, to determine the best model among CART, TreeNet, RF, MARS, GPS, and Regression for further development of the forecast, they were normalized using the modified logarithmic normalization formula (sigmoid normalization):

$$K = \frac{1}{1+e^{-3\frac{x_i - md}{mx - md}}}, \quad (2)$$

where K – normalized value of the input variables, x_i – the input value of the indicator $i = 1, \ldots 64$, md – the median of the input indicator, *and* mx – the maximum value of the input indicator.

The calculation of the theoretical quantiles was carried out using

$$Z_i = NORM.S.INV\left(\frac{Rank_i - 0.5}{N}\right), \quad (3)$$

where Z_i – theoretical quantile, $NORM.S.INV$ – formula in MS Excel

$$\frac{Rank_i - 0.5}{N} = p,$$

probability for each position, N – total number of residues.

Thus, Equation (3) determines the quantile of the standard normal distribution N(0,1). The constructed QQ-plot shows that the residuals of the Tree1 model follow a normal distribution, as the points lie approximately on a straight line.

To normalize the input data, the sigmoid normalization formula was used. Unlike other normalization methods (Z-score, min-max normalization, Feature scaling to a certain interval, Unit vector normalization (normalization by vector length), Robust scaling, based on IQR), it firstly allows smoothing the contrast between the average and extreme points. Secondly, the use of median significant figures takes into account resistance to outliers, and thirdly, it combines the advantages of statistical stability and nonlinear interpretation, which are used by data mining methods.

This study proposes determining the degree of influence of each national cybersecurity subfactor on a country's global competitiveness and developing a machine learning-based forecast.

The IMD World Competitiveness Ranking (World Competitiveness Center, 2024) includes 67 countries (as of 2024). The list of these countries is determined by various factors, including:

1) data availability (the ranking is based on comprehensive economic and business data that must be collected and verified, but not all countries have sufficient, reliable, and comparable data for analysis);

2) business conditions and economic relevance (the ranking focuses on economies that have a significant global or regional impact in terms of competitiveness);

3) methodological limitations (IMD uses precise data – GDP, productivity, infrastructure, and survey data from business executives, but certain countries lack sufficient responses from business leaders to ensure statistically significant results).

Values for the cybersecurity and global competitiveness subfactors were used for 64 countries, which were jointly accounted for by both databases (WCR-Rankings – IMD, NCSI: Ranking).

The dependent variable was based on the IMD World Competitiveness Ranking (WCR), with lower rankings indicating stronger national competitiveness. To ensure a consistent and intuitive interpretation of the machine learning results, the original ranking variable was transformed into an inverse competitiveness score using the transformation (1), where 68 represents the total number of ranking positions plus one in the IMD World Competitiveness Ranking. As a result, higher values of the transformed indicator correspond to higher levels of competitiveness. This transformation preserves the relative ordering of countries. It does not affect the structure of the CART model, variable importance, or terminal node composition, while enabling more interpretable comparison of predicted outcomes across country groups.

To develop a forecast using machine learning methods regarding the impact of cybersecurity level on economic security level, and to determine the role and place of national security indicators in the economic security system, indicators for 2024 are presented in Appendix B.

Based on the values of 12 indicators, the e-Governance Academy determines the country's national cybersecurity index. The e-Governance Academy (eGA) is a non-profit organization in Estonia dedicated to digital governance, cybersecurity, and e-democracy. Founded in 2002, it aims to help governments worldwide implement digital transformation, using Estonia's successful e-government model as a benchmark.

Before constructing machine learning models, a Pearson correlation matrix (Table 1) was generated to examine the relationships between the transformed competitiveness indicator (WCR*) and the NCSI subfactors. Correlation analysis allows identifying the strength and direction of linear associations between cybersecurity di-

http://dx.doi.org/10.21511/ppm.24(3).2026.22

Table 1. Pearson correlation matrix for national cybersecurity indicators and transformed competitiveness level

	WCR*	CP	GCC	EPD	CRD	CCII	CDE	CTAAR	PPD	CIR	CSM	FAC	MCD
WCR*	1.000												
CP	0.097	1.000											
GCC	0.386	0.403	1.000										
EPD	0.228	0.393	0.403	1.000									
CRD	0.286	0.097	0.366	0.201	1.000								
CCII	0.083	0.694	0.220	0.458	0.106	1.000							
CDE	0.179	0.624	0.240	0.544	0.075	0.700	1.000						
CTAAR	0.104	0.408	0.275	0.410	0.181	0.535	0.461	1.000					
PPD	0.332	0.503	0.454	0.220	0.783	0.790	0.478	0.403	1.000				
CIR	0.061	0.718	0.239	0.444	–0.062	0.817	0.695	0.465	0.519	1.000			
CSM	0.321	0.526	0.460	0.372	0.334	0.529	0.459	0.459	0.487	0.435	1.000		
FAC	–0.048	0.686	0.149	0.496	0.152	0.671	0.612	0.524	0.454	0.752	0.443	1.000	
MCD	0.138	0.232	0.353	0.331	0.308	0.186	0.239	0.396	0.390	0.236	0.329	0.312	1.000

Note: WCR* means World Competitiveness Ranking; CP means Cybersecurity policy; GCC means Global cybersecurity contribution; EPD means Education and professional development; CRD means Cybersecurity research and development; CCII means Cybersecurity of critical information infrastructure; CDE means Cybersecurity of digital enablers; CTAAR means Cyber threat analysis and awareness raising; PPD means Protection of personal data; CIR means Cyber incident response; CSM means Cybersecurity management; FAC Fight against cybercrime; MCD Military cyber defense.

mensions and competitiveness outcomes, as well as detecting potential multicollinearity among explanatory variables. The transformation of the original competitiveness ranking into WCR* aligns higher values with stronger competitiveness outcomes, ensuring a more intuitive interpretation of relationships.

The correlation analysis demonstrates that several cybersecurity dimensions are positively associated with transformed competitiveness outcomes, particularly Global Cybersecurity Contribution (GCC), Cybersecurity Management (CSM), Protection of Personal Data (PPD), and Cyber Crisis Response (CRD). Among these indicators, GCC (r = 0.386) and CSM (r = 0.321) demonstrate relatively stronger positive associations with competitiveness performance, supporting the assumption that international cybersecurity engagement and institutional cybersecurity management capacity are important components of digital competitiveness.

At the same time, the absence of extremely high pairwise correlations among most explanatory variables suggests an acceptable level of multicollinearity for subsequent machine learning modeling. Therefore, the correlation matrix was used primarily as an exploratory analytical tool before applying CART, Random Forest, TreeNet, and MARS models.

Six predictive models were developed using the automated modeling procedure implemented in Salford Predictive Modeler. The dataset was randomly partitioned into training and validation subsets, with 80% of observations used for model training and 20% reserved for validation through the option "Fraction of cases selected as random = 20%". Model performance was evaluated using the Mean Squared Error (MSE) criterion. The model with the lowest MSE was considered the most accurate predictive model, while the final model selected for interpretation additionally accounted for transparency and interpretability.

The methods for building models describing the impact of cybersecurity subfactors on a country's competitiveness level, as a determinant of economic security, are presented in Table 2.

Table 2. Automated results (TARGET=WCR*)

Model	Model Complexity, Nodes, Trees, Coeffs	MSE	Method
Tree 1	12	0.06604	CART
TreeNet 1	118	0.06894	TreeNet
RF 1	200	0.06503	RF
MARS 1	2	0.07729	MARS
GPS 1, E=2.0	12	0.06968	GPS
Regress 1	12	0.06749	Regression

The comparative evaluation of machine learning models (Aria et al., 2021; Nosratabadi et al., 2020) demonstrates that the Random Forest algorithm achieved the lowest mean squared error (MSE = 0.06503), indicating the highest predictive accuracy among the tested approaches. However, the difference in prediction error between Random Forest and CART (MSE = 0.06604) is relatively small.

Although Random Forest provides slightly superior predictive performance, the CART model was selected for further analysis and interpretation due to its high transparency and interpretability. Unlike ensemble methods, CART generates explicit decision rules and hierarchical relationships among predictors, allowing the identification of specific cybersecurity factors associated with different competitiveness outcomes. Therefore, the selection of CART was driven not only by predictive performance but also by the objective of obtaining interpretable decision rules suitable for economic and policy analysis.

Consequently, Random Forest may be considered the most accurate predictive model, whereas CART represents the most interpretable model for explaining the relationship between national cybersecurity indicators and competitiveness outcomes. Its implementation was performed using SPM software.

The first stage of CART model development involves V-fold cross-validation. Such validation is necessary to assess the model's predictive performance and prevent overfitting. V represents the number of subsets into which the dataset is divided. In SPM, V-fold cross-validation is often used with values of 5 or 10. These values are recommended by SPM (Classification Modeling, 2019) if the input data sample is small and a reliably trained model is needed. For example, if V = 10 is specified in SPM, the input sample will first be divided into 10 equal parts, and the model will be trained 10 times, with one part reserved for validation. The 10 validation results are then averaged for a reliable assessment. Thus, when V = 10, the model is trained 10 times on 9 subsets, each time using a different subset as the validation set, while the remaining V-1 subsets serve as the training set. Performance metrics (MSE) are averaged across V runs to provide a more reliable assessment of model performance.

The classification and regression tree is built directly, and the best model is selected based on the MSE. The interpretation of the tree structure is presented in Table 3. Root node 1 is the first and most important split; it concerns the global cybersecurity contribution (GCC). The overall average competitiveness indicator, as an economic security factor, is 34.625 units across the 64 countries in the study.

Therefore, terminal node 1 includes 24 countries with indicator values of GCC <= 4.50000 and CSM <= 3.50000. The group of countries (Argentina, Bahrain, Brazil, Bulgaria, Chile, Colombia, France, Ghana, Iceland, Indonesia, Japan, Kuwait, Mexico, Mongolia, Nigeria, Peru, the Philippines, Romania, the Slovak Republic, Slovenia, South Africa, Turkey, the UAE, and Venezuela) demonstrates the lowest predicted competitiveness out-

Table 3. Structure of the optimal regression tree regarding the relationship between cybersecurity subfactors and competitiveness

<table>
<tr><th colspan="2">Branch 1 (Left) GCC ≤ 4.5</th><th>Branch 2 (Right) GCC > 4.5</th></tr>
<tr><td colspan="2">35 countries meet this condition</td><td rowspan="2">29 countries</td></tr>
<tr><td colspan="2">Analysis of node 2</td></tr>
<tr><th>Terminal Node 1 CCM ≤ 3.5</th><th>Terminal Node 2 CCM > 3.5</th><th>Terminal Node 3</th></tr>
<tr><td>24 countries</td><td>11 countries</td><td>Avg = 42.828 – the highest competitiveness outcome.</td></tr>
<tr><td>Avg = 19.625, the lowest competitiveness outcome</td><td>Avg = 38.455 – moderate competitiveness outcome</td><td rowspan="2">These countries demonstrate the highest predicted levels of competitiveness. The results suggest that strong global cybersecurity contributions are associated with more favorable competitive positions within the digital economy framework.</td></tr>
<tr><td>These countries demonstrate the lowest levels of competitiveness. The results suggest that limited global cybersecurity contribution, combined with weaker cybersecurity management capacities, is associated with lower competitiveness performance.</td><td>This group demonstrates moderate competitiveness outcomes, suggesting that stronger cybersecurity management capacities partially compensate for lower levels of global cybersecurity contribution.</td></tr>
</table>

http://dx.doi.org/10.21511/ppm.24(3).2026.22

comes. These countries, characterized by insufficient internal cybersecurity management capacity and limited global cybersecurity engagement, tend to occupy weaker competitive positions in the global economy.

Terminal node 2 (GCC <= 4.50000 and CSM > 3.50000) consists of the following countries: China, Greece, Ireland, Israel, Italy, Kazakhstan, Latvia, Lithuania, the Netherlands, Poland, and Portugal, with low GCC but high CSM. Countries with stronger internal cybersecurity management capabilities demonstrate moderate competitiveness outcomes even under relatively limited participation in international cybersecurity initiatives. This suggests that effective cyber crisis management partially compensates for lower levels of global cybersecurity engagement.

Terminal node 3 is formed by 29 countries with GCC value >4.5. This group of countries (Australia, Austria, Belgium, Botswana, Canada, Croatia, Cyprus, the Czech Republic, Denmark, Estonia, Finland, Germany, Hungary, India, Jordan, the Korea Rep., Luxembourg, Malaysia, New Zealand, Norway, Qatar, Saudi Arabia, Singapore, Spain, Sweden, Switzerland, Thailand, the United Kingdom, and the USA) is characterized by relatively balanced values of GCC and CSM. The highest predicted competitiveness outcomes are characteristic of countries with high levels of global cybersecurity contribution. Active participation in international cybersecurity cooperation, combined with relatively balanced internal cybersecurity capacities, is associated with stronger competitive positions.

The GCC indicator serves as the first splitting criterion at the root node of the regression tree, indicating its systemic role in the model's structure. The importance level of the GCC variable is 85.77% (second place after CSM). At the same time, the analysis of terminal nodes showed that a high level of global activity in cybersecurity, in the absence of a sufficiently developed internal cybersecurity management system, does not yield a high forecast level of competitiveness. Thus, GCC is a significant factor, but its impact is realized only in interaction with internal institutional capabilities.

The CSM indicator received the highest importance level in the model (100%), confirming its key role in determining forecast values. Countries characterized by a CSM value > 3.5 demonstrate moderate predicted competitiveness outcomes (38.455), indicating that strong internal cyber crisis management contributes positively to national competitiveness even under limited international cybersecurity engagement. However, the highest predicted competitiveness values (42.828) are observed among countries with higher levels of global cybersecurity contribution.

After training the CART machine learning model, which proved optimal among other models, forecast values of competitiveness level were developed for the 64 countries in the study as a determinant of economic security using the Score Data procedure in SPM software. The forecast results are displayed in the Response column (Appendix C).

To assess the stability of the regression tree (Appendix D), the Random Seed Stability Check procedure was used, which performs cross-validation across different subsets. The generation of trees with varying subset values (Seed 5, Seed 7, Seed 10, Seed 15, and Seed 20) showed the same splits, which completely coincide with the distribution obtained from the regression tree. Thus, the developed regression model, Tree 1, using the CART method, is stable. To substantiate the statistical significance of Tree 1, we will verify the normality of the model residuals' distribution using a Quantile-Quantile Plot (QQ-Plot, Figure 2).

The X axis displays the theoretical quantiles (expected values that have a normal distribution), and the Y axis displays the empirical quantiles (actual, sorted residuals of the model). The calculated residuals and theoretical quantiles are given in Appendix E.

The results of intelligent data analysis confirm that cybersecurity is an important determinant of countries' global competitiveness, and that competitive stability is built on the harmonization of internal institutional mechanisms and external integration. The analysis showed that the lowest results are characteristic of countries with underdeveloped internal crisis management, regardless of their level of global activity. The highest competitiveness indicators are observed in countries characterized by high levels of global cybersecuri-

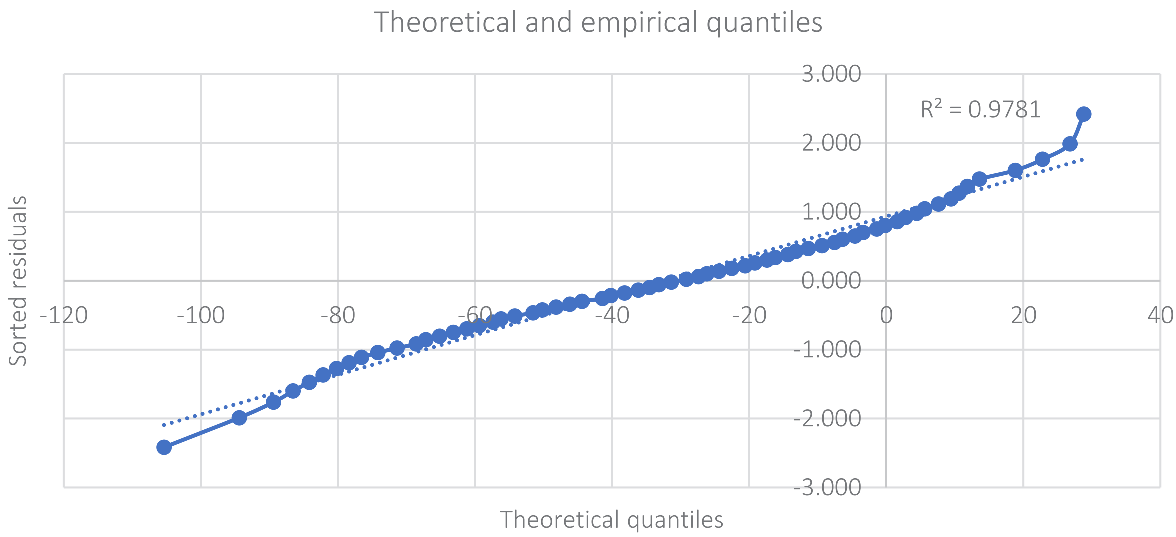

Figure 2. Checking the normality of the distribution of forecast residuals

ty contribution. At the same time, strong internal organizational capacity helps maintain moderate competitiveness even at lower levels of international engagement.

3. DISCUSSION

The results confirm that national cybersecurity management plays a critical role in shaping global competitiveness, particularly amid digital transformation and rising cyber threats. First, the results align with the study on cyber resilience, which demonstrates that institutional capacity and government effectiveness significantly influence national cybersecurity performance, especially during periods of crisis (Shkolnyk et al., 2025). This supports the idea that cybersecurity management should be viewed as an institutional mechanism that directly contributes to national competitiveness. Second, the moderating role of technological infrastructure highlighted in fintech studies confirms that the effectiveness of digital innovations depends on the reliability and security of IT systems (Alzghoul & Al-kasasbeh, 2024). This implies that without effective cyber crisis response mechanisms, the benefits of digitalization for competitiveness may be significantly reduced. Additionally, the variable importance analysis confirmed that other highly influential subfactors include Education and Professional Development in cybersecurity (EPD), Cyber Threat Analysis and Public Awareness Raising (CTAAR), and Cyber Research and Development (CRD). This emphasizes the need for a comprehensive national policy that considers not only technical aspects but also human capital, transparency of information, and innovation.

The findings of Koilo (2024) are consistent with the present study and emphasize the dual role of digitalization: increasing competitiveness while simultaneously increasing the impact of cyber risks. Koilo (2024) examines how digitalization contributes to the formation of sustainable competitive advantages at the company and national levels. She considers digital transformation a key driver of increased efficiency in business processes, optimized resource use, and the creation of new value models. The evidence emphasizes that the introduction of digital technologies enables companies to adapt more quickly to external changes, improve customer interactions, and increase productivity. The relationship between digital innovations, economic efficiency, and the environmental and social components of sustainable development are analyzed. Particular attention is paid to the fact that digitalization not only creates opportunities, but also generates new risks. Among the key results, it is determined that digitalization is a powerful driver of competitiveness, as it enhances business flexibility, innovation, and the quality of management decisions. At the same time, the paper emphasizes that cyber risks and data security threats can significantly limit these benefits. An insufficient level of cybersecurity can offset the positive effects of digital transformation by leading to loss of user trust, financial losses, and reputational damage. The con-

http://dx.doi.org/10.21511/ppm.24(3).2026.22

clusion is that to achieve sustainable development and long-term competitiveness, it is necessary to integrate cybersecurity measures into digital strategies, treating them as an integral element of the digital economy rather than a technical aspect.

The identified relationship between the level of cyber protection, the efficiency of digital infrastructure, and international competitive positions is consistent with previous research, which emphasizes the strategic importance of digital and information security for economic development (Miethlich et al., 2020; Petroye et al., 2020). Although the present model does not separately include variables measuring innovativeness, digital service stability, or economic performance, the identified relationship between cybersecurity capacity and transformed competitiveness outcomes is theoretically consistent with prior research emphasizing the strategic role of cybersecurity in supporting digital innovation, institutional resilience, and economic development. This interpretation also aligns with contemporary views on cybersecurity as a component of national digital power (The International Institute for Strategic Studies, 2023). The results suggest that the impact of cybersecurity on competitiveness manifests through two main pathways. The first is economic, associated with increased trust in digital platforms, reduced cyberattack risk, and greater resilience of economic operations. This effect is supported by World Bank studies showing that countries with stronger cybersecurity commitments exhibit better macroeconomic indicators and more stable sectoral performance (Vergara Cobos et al., 2024). The second pathway is organizational-strategic, linked to the formation of dynamic cyber-defense capabilities that become an essential component of competitive advantage for both the state and businesses. As highlighted by Kosutic and Pigni (2020) and Kosutic (2021), the ability to adapt to cyber threats and integrate technological, managerial, and human factors ensures a long-term advantage that competitors find difficult to replicate.

In the context of economic development, the positive correlation between the level of digital infrastructure and cybersecurity, demonstrated by Kolat and Unver (2025), is consistent with our conclusions concerning the importance of a systemic approach. Thus, countries with growing GDP have greater opportunities to invest in cyber defense, which in turn strengthens their competitiveness. This creates a cyclical effect in which economic growth and cybersecurity mutually reinforce each other.

Despite the significant results, the study has several limitations. The primary limitation lies in the data used. As noted by Brangetto and Kert-Saint Aubyn (2015), the economic aspects of cybersecurity are often difficult to measure due to the lack of precise data on costs and the effectiveness of strategies. The use of index-based indicators (NCSI and WCR) represents a certain simplification of the actual situation. Furthermore, although the CART method is effective for interpreting and visualizing decision rules, it – like most static models – may fail to account for the stochastic nature of cyber threats. Kianpour et al. (2021) rightly stress that modern research should shift from simplified models toward more dynamic and stochastic approaches.

Future research should focus on a deeper examination of the mechanisms by which cybersecurity management (CSM) affects economic development, identifying and analyzing sectoral differences in economic vulnerability, and considering regional and cultural factors in the formulation of protection strategies. Moreover, the dynamic development of technologies, including artificial intelligence, quantum computing, and 5G, requires regular updates of models to ensure adaptive assessment of the impact of emerging cyber threats on global competitiveness.

CONCLUSION

The purpose of this study was to develop a methodology and identify the most influential predictors of national cybersecurity in global competitiveness utilizing the data mining approach.

Machine learning methods were implemented in the Salford Predictive Modeler software environment, including Classification and Regression Trees, Random Forest, Stochastic Gradient Boosting, Multivariate Adaptive Regression Splines, and Generalized Path Seeker. Accordingly, three groups of countries were identified with different predicted levels of competitiveness, underscoring the importance of balancing the development of both external and internal components of cyber defense.

The constructed regression tree showed that two subfactors exert the greatest influence on competitiveness: global contribution to cybersecurity and cybersecurity management. These indicators served as the key criteria for country segmentation in the model, and the CART algorithm determines the predicted competitiveness outcomes for each subgroup based on the mean value of the transformed target variable within the corresponding terminal node.

The CART model classified countries into three main groups, with different average predicted competitiveness values based on the transformed competitiveness indicator WCR⊠=68–WCR, where higher values correspond to stronger competitiveness outcomes.

Lowest forecast group (Avg = 19.625) includes countries characterized by low levels of both global cybersecurity contribution (GCC ≤ 4.5) and cybersecurity management capacity (CSM ≤ 3.5). The results indicate that insufficient institutional preparedness and weak cyber crisis management are associated with lower competitiveness outcomes.

Moderate forecast group (Avg = 38.455) includes countries with relatively limited global cybersecurity contribution but stronger internal cybersecurity management capabilities (CSM > 3.5). The findings suggest that effective cyber crisis management partially compensates for lower international engagement and supports moderate competitiveness performance.

Highest forecast group (Avg = 42.828) includes countries with high levels of global cybersecurity contribution (GCC > 4.5). The results demonstrate that active participation in international cybersecurity initiatives, combined with relatively balanced internal cybersecurity capacities, is associated with the strongest competitiveness outcomes.

The findings emphasize that sustainable competitiveness in the digital economy depends on the balanced development of both international cybersecurity engagement and internal cybersecurity management capacities. Investments in cyber governance, crisis management, education, research, and international cooperation represent essential prerequisites for strengthening national competitiveness and economic resilience.

AUTHOR CONTRIBUTIONS

Conceptualization: Vitaliia Koibichuk, David Fülep, Oleksandr Kubatko, Andrii Skrylnyk, Kseniia Mohylna.
Data curation: Vitaliia Koibichuk, Alina Yefimenko, Andrii Skrylnyk, Kseniia Mohylna.
Formal analysis: Vitaliia Koibichuk, David Fülep, Oleksandr Kubatko, Alina Yefimenko.
Funding acquisition: David Fülep.
Investigation: Alina Yefimenko, Andrii Skrylnyk, Kseniia Mohylna.
Methodology: Vitaliia Koibichuk, Oleksandr Kubatko, Alina Yefimenko, Andrii Skrylnyk, Kseniia Mohylna.
Project administration: Oleksandr Kubatko.
Resources: David Fülep.
Software: David Fülep, Alina Yefimenko, Andrii Skrylnyk, Kseniia Mohylna.
Supervision: Vitaliia Koibichuk.
Validation: David Fülep, Alina Yefimenko, Andrii Skrylnyk, Kseniia Mohylna.
Visualization: Oleksandr Kubatko.

 http://dx.doi.org/10.21511/ppm.24(3).2026.22

Writing – original draft: Vitaliia Koibichuk, David Fülep, Oleksandr Kubatko, Alina Yefimenko, Andrii Skrylnyk, Kseniia Mohylna.
Writing – review & editing: Vitaliia Koibichuk, David Fülep, Oleksandr Kubatko, Alina Yefimenko, Andrii Skrylnyk, Kseniia Mohylna.

ACKNOWLEDGMENTS

The paper is prepared within the scientific research projects "Digital transformations to ensure civil protection and post-war economic recovery in the face of environmental and social challenges" (№0124U000549) and "Drivers and barriers to human capital transformation for a circular and green economy" (No. 0126U001080).

REFERENCES

1. Alzghoul, A., & Al-kasasbeh, O. (2024). The moderating role of information technology infrastructure in the relationship between fintech adoption and organisational competitiveness. *Investment Management and Financial Innovations, 21*(2), 155-166. https://doi.org/10.21511/imfi.21(2).2024.12
2. Annarelli, A., & Palombi, G. (2021). Digitalization capabilities for sustainable cyber resilience: A conceptual framework. *Sustainability, 13*(23), Article 13065. https://doi.org/10.3390/su132313065
3. Aria, M., Cuccurullo, C., & Gnasso, C. (2021). A comparison among interpretative proposals for Random Forests. *Machine Learning with Applications, 6,* Article 100094. https://doi.org/10.1016/j.mlwa.2021.100094
4. Arroyabe, M. F., Arranz, C. F., De Arroyabe, I. F., & de Arroyabe, J. C. F. (2024). Exploring the economic role of cybersecurity in SMEs: A case study of the UK. *Technology in Society, 78*. https://doi.org/10.1016/j.techsoc.2024.102670
5. Brangetto, P., & Kert-Saint Aubyn, M. (2015). *Economic aspects of national cyber security strategies.* Tallinn: The NATO Cooperative Cyber Defence Centre of Excellence. Retrieved from https://ccdcoe.org/uploads/2018/10/Economics-of-cybersecurity.pdf
6. Breiman, L., Friedman, J., Olshen, R. A., & Stone, C. J. (1984). *Classification and Regression Trees* (1st ed.). Chapman and Hall/CRC. https://doi.org/10.1201/9781315139470
7. Çifci, H., & Ergüner, E. (2025). Analysis of national cybersecurity strategies of G20: Objectives, latent themes, latest trends and comparisons. *Data & Policy, 7*. https://doi.org/10.1017/dap.2024.99
8. Classification Modeling in CART. (2019). *Selford Predictive Modeller. Classification Modeling in CART* (70 p.). Minitab, LLC. Retrieved from https://www.minitab.com/content/dam/www/en/uploadedfiles/content/products/spm/CART_Classification_Modeling.pdf
9. Dobrovolska, O., & Rozhkova, M. (2024a). Development of the country's sustainable cyberspace strategy to ensure the country's national security. *SocioEconomic Challenges, 8*(2), 197-214. https://doi.org/10.61093/sec.8(2).197-214.2024
10. Dobrovolska, O., & Rozhkova, M. (2024b). The impact of digital transformation on the anti-corruption and cyber-fraud system. *Business Ethics and Leadership, 8*(3), 231-252. https://doi.org/10.61093/bel.8(3).231-252.2024
11. e-Governance Academy Foundation. (n.d.). *National Cyber Security Index*. Retrieved from https://ncsi.ega.ee/ncsi-index/
12. Erixon, F., Guinea, O., & Pandya, D. (2024). *Securing Europe's future: Strengthening ICT competitiveness for economic and national security* (ECIPE Policy Brief, No. 22/2024). European Centre for International Political Economy (ECIPE). Retrieved from https://hdl.handle.net/10419/307451
13. European Commission. (n.d.a). *The Cybersecurity Strategy*. Retrieved from https://digital-strategy.ec.europa.eu/en/policies/cybersecurity-strategy
14. European Commission. (n.d.b). *The Digital Economy and Society Index (DESI): Shaping Europe's digital future.* Retrieved from https://digital-strategy.ec.europa.eu/en/policies/desi
15. Fernandez de Arroyabe, J. C., Arranz, N., Fernandez de Arroyabe, P., & Li, J. (2023). Cybersecurity resilience in SMEs: A machine learning approach. *Information Systems Management, 41*(2), 123-138. https://doi.org/10.1080/08874417.2023.2248925
16. Kalinichenko, L., Melnyk, L., Kubatko, O., Burlakova, I., Babych, K., & Pasko, T. (2024). Wiki communities' management tools in conditions of digitization. *Problems and Perspectives in Management, 22*(3), 303-313. http://doi.org/10.21511/ppm.22(3).2024.24
17. Kianpour, M., Kowalski, S., & Øverby, H. (2021). Systematically understanding cybersecurity economics: A survey. *Sustainability, 13*(24). https://doi.org/10.3390/su132413677
18. Koilo, V. (2024). Unlocking the sustainable value with digitalization: Views of maritime stakehold-

ers on business opportunities. *Problems and Perspectives in Management, 22*(1), 401-417. http://doi.org/10.21511/ppm.22(1).2024.33

19. Kolat, D., & Unver, N. (2025). The impact of economic growth on cybersecurity: Evidence from ICT development index. *International Journal of Eurasia Social Sciences, 16*(61). https://doi.org/10.70736/ijoess.1711
20. Korjonen-Kuusipuro, K., & Wojciechowski, A. (2025). Sense of security in the digital age. *Human Technology, 21*(1), 1-5. https://doi.org/10.14254/1795-6889.2025.21-1.0
21. Kosutic, D. (2021). *The impact of cybersecurity on competitive advantage*. Ecole de Management Grenoble. Retrieved from https://www.researchgate.net/publication/357826918_The_Impact_of_Cybersecurity_on_Competitive_Advantage
22. Kosutic, D., & Pigni, F. (2020). Cybersecurity: Investing for competitive outcomes. *Journal of Business Strategy*, 43(1), 28-36. https://doi.org/10.1108/JBS-06-2020-0116
23. Kuzior, A., Tiutiunyk, I., Zielińska, A., & Kelemen, R. (2024). Cybersecurity and cybercrime: Current trends and threats. *Journal of International Studies, 17*(2), 220-239. https://doi.org/10.14254/2071-8330.2024/17-2/12
24. Melnyk, L., Vasa, L., Singh, S., Kubatko, O., & Kalinichenko, L. (2025). Quasi-viral technologies as the drivers of the economy digital transformation towards sustainability. *HighTech and Innovation Journal, 6*(1), 183-200. https://doi.org/10.28991/HIJ-2025-06-01-013
25. Miethlich, B., Belotserkovich, D., Abasova, S., Zatsarinnaya, E., & Veselitsky, O. (2020). Digital economy and its influence on competitiveness of countries and regions. *Revista ESPACIOS, 41*(12), Article 20. Retrieved from https://www.revistaespacios.com/a20v41n12/a20v41n11p20.pdf
26. Morales-Sáenz, F., Medina-Quintero, J., & Reyna-Castillo, M. (2024). Beyond data protection: Exploring the convergence between cybersecurity and sustainable development in business. *Sustainability, 16*(14). https://doi.org/10.3390/su16145884
27. Morshed, A., & Khrais, L. T. (2025). Enhancing financial security through machine learning: Adoption challenges in Jordan's insurance fraud detection. *Insurance Markets and Companies, 16*(2), 85-95. https://doi.org/10.21511/ins.16(2).2025.07
28. Nosratabadi, S., Mosavi, A., Duan, P., Ghamisi, P., Filip, F., Band, S., Reuter, U., Gama, J., & Gandomi, A. (2020). Data science in economics: Comprehensive review of advanced machine learning and deep learning methods. *Mathematics, 8*(10). https://doi.org/10.3390/math8101799
29. Petroye, O., Lyulyov, O., Lytvynchuk, I., Paida, Y., & Pakhomov, V. (2020). Effects of information security and innovations on country's image: Governance aspect. *International Journal of Safety and Security Engineering, 10*(4), 459-466. https://doi.org/10.18280/ijsse.100404
30. Pollák, F., Kalamen, K., & Vavrek, R. (2026). Re-pricing risk in the digital economy: A multi-wave analysis of technology-sector volatility during COVID-19. *Investment Management and Financial Innovations, 23*(1), 124-139. http://doi.org/10.21511/imfi.23(1).2026.10
31. Safitra, M., Lubis, M., & Fukhrurroja, H. (2023). Counterattacking cyber threats: A framework for the future of cybersecurity. *Sustainability, 15*(18), Article 13369. https://doi.org/10.3390/su151813369
32. Shkolnyk, I., Tiutiunyk, I., Semenog, A., Kovalenko, Yu., & Pavlenko, L. (2025). Institutional, technological, and financial drivers of national cyber resilience under armed conflict and post-conflict recovery. *Problems and Perspectives in Management, 23*(4), 665-683. http://doi.org/10.21511/ppm.23(4).2025.45
33. The International Institute for Strategic Studies (IISS). (2023, September 7). *Cyber capabilities and national power volume 2*. Retrieved from https://www.iiss.org/research-paper/2023/09/cyber-capabilities-national-power-volume-2/
34. Vasiu, I., & Vasiu, L. (2018). Cybersecurity as an essential sustainable economic development factor. *European Journal of Sustainable Development, 7*(4), 171-178. https://doi.org/10.14207/ejsd.2018.v7n4p171
35. Vergara Cobos, E.B., Cakir, S., Mei-Zahav, H., & Berkay, B (2024). *The role of cybersecurity in economic performance* (Working Paper 193678). Washington, DC: World Bank. Retrieved from http://documents.worldbank.org/curated/en/099092324164526526
36. World Competitiveness Center. (2024). *World Competitiveness Ranking 2024: Rankings out of 67 countries*. Retrieved from https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-competitiveness-ranking/rankings/wcr-rankings/#_tab_Lis
37. World Economic Forum. (2023, January 18). *Global Cybersecurity Outlook 2023*. Geneva: World Economic Forum. Retrieved from https://www.weforum.org/publications/global-cybersecurity-outlook-2023/
38. Yarovenko, H., Bilovodska, V., Bylbas, R., Pankiv, O., Baghirzade, M., Niemi, O., & Djakons, D. (2025a). Digital readiness of European countries to combat corruption and cyber threats: Panel analysis. *Business Ethics and Leadership, 9*(2), 238-265. https://doi.org/10.61093/bel.9(2).238-265.2025
39. Yarovenko, H., Horbachova, O., Bylbas, R., & Latysh, D. (2025b). Digitalization as a socio-economic challenge: Modeling the impact on the level of cybercrime considering socio-economic, technological and institutional factors. *SocioEconomic Challenges, 9*(2), 282-315. https://doi.org/10.61093/sec.9(2).282-315.2025
40. Yarovenko, H., Hurochkina, V., Cugova, A., & Mohylna, K. (2026). Forecasting illicit practice impacts on economies of conflict countries: XGBoost approach. *Business Ethics and Leadership, 10*(1), 105-129. https://doi.org/10.61093/bel.10(1).105-129.2026

http://dx.doi.org/10.21511/ppm.24(3).2026.22

APPENDIX A

Table A1. Content essence of indicators used to develop the global competitiveness forecast

Source: Our elaboration based on WCR-Rankings – IMD, NCSI Ranking (e-Governance Academy Foundation, n.d.).

Indicator	Abbreviation	Measurement Scale, points	Indicator Description
World Competitiveness Ranking	WCR	ordinal ranking variable	Integral indicator determined based on integral values of subfactors: economic performance, government efficiency, business efficiency, infrastructure. For modeling purposes, the original WCR ranking was transformed into WCR* = 68 – WCR in order to ensure that higher transformed values correspond to higher competitiveness outcomes.
Cybersecurity policy	CP	0–15	Integral subfactor determined as the sum of five indicators, each measured on a scale from zero to three points: high-level cybersecurity leadership, cybersecurity policy development, cybersecurity policy coordination, national cybersecurity strategy, national cybersecurity strategy action plan.
Global cybersecurity contribution	GCC	0–6	Integral subfactor determined as the sum of three indicators: cyber diplomacy engagements (0–3 points), commitment to international law in cyberspace (0–1 point), contribution to international capacity building in cybersecurity (0–2 points).
Education and professional development	EPD	0–10	Integral subfactor determined as the sum of five indicators: cyber safety competencies in primary education (0–2 points), cyber safety competencies in secondary education (0–2 points), undergraduate cybersecurity education (0–2 points), graduate cybersecurity education (0–3 points), association of cybersecurity professionals (0–1 point)
Cybersecurity research and development	CRD	0–4	Integral subfactor determined as the sum of two indicators, each measured on a scale from zero to two points: cybersecurity research and development programs, cybersecurity doctoral studies.
Cybersecurity of critical information infrastructure	CCII	0–12	Integral subfactor determined as the sum of four indicators, each measured on a scale from zero to three points: identification of critical information infrastructure, cybersecurity requirements for operators of critical information infrastructure, cybersecurity requirements for public sector organizations, and competent supervisory authority.
Cybersecurity of digital enablers	CDE	0–12	Integral subfactor determined as the sum of six indicators, each measured on a scale from zero to two points: secure electronic identification, electronic signature, trust services, supervisory authority for trust services, cybersecurity requirements for cloud services, supply chain cybersecurity.
Cyber threat analysis and awareness raising	CTAAR	0–12	Integral subfactor determined as the sum of four indicators, each measured on a scale from zero to three points: cyber threat analysis, public cyber threat reports, public cybersecurity awareness resources, cybersecurity awareness raising coordination.
Protection of personal data	PPD	0–4	Integral subfactor determined as the sum of two indicators, each measured on a scale from zero to two points: personal data protection legislation, personal data protection authority.
Cyber incident response	CIR	0–14	Integral subfactor determined as the sum of five indicators: national incident response capacity (0–3 points), incident reporting obligations (0–3 points), cyber incident reporting tool (0–2 points), single point of contact for international cooperation (0–3 points), participation in international incident response cooperation (0–3 points).
Cybersecurity management	CSM	0–9	Integral subfactor determined as the sum of four indicators: cybersecurity management plan (0–2 points), national cybersecurity management exercises (0–3 points), participation in international cyber crisis exercises (0–2 points), operational crisis reserve (0–2 points).
Fight against cybercrime	FAC	0–16	Integral subfactor determined as the sum of six indicators: cybercrime offences in national law (0–3 points), procedural law provisions (0–3 points), ratification of or accession to the Convention on Cybercrime (0–2 points), cybercrime investigation capacity (0–3 points), digital forensics capacity (0–2 points), 24/7 contact point for international cybercrime (0–3 points).
Military cyber defense	MCD	0–6	Integral subfactor determined as the sum of three indicators, each measured on a scale from zero to two points: military cyber defense capacity, military cyber doctrine, military cyber defense exercises.

APPENDIX B

Table B1. Input data array for building a forecast of the global competitiveness level

Source: Our elaboration based on WCR-Rankings – IMD, NCSI Ranking (e-Governance Academy Foundation, n.d.).

Country	WCR	CP	GCC	EPD	CRD	CCII	CDE	CTAAR	PPD	CIR	CSM	FAC	MCD
Argentina	66	9	4	8	0	6	6	6	4	8	2	13	4
Australia	13	15	6	10	4	9	8	9	4	11	7	16	6
Austria	26	15	6	10	2	12	8	6	4	14	5	16	4
Bahrain	21	9	4	10	0	12	8	6	4	11	0	9	0
Belgium	18	12	6	10	4	12	10	12	4	14	7	16	4
Botswana	55	12	5	3	2	0	2	0	4	6	2	11	0
Brazil	62	6	4	6	1	0	1	4	4	3	1	4	6
Bulgaria	58	5	4	9	2	2	3	8	4	6	1	9	4
Canada	19	15	6	6	4	12	6	9	4	14	7	16	6
Chile	44	12	4	10	0	0	8	3	2	11	0	16	6
China	14	6	4	10	4	9	8	3	4	11	4	9	0
Colombia	57	2	2	6	2	0	1	7	4	3	1	9	4
Croatia	51	7	5	3	2	5	5	8	4	6	4	9	6
Cyprus	43	9	5	10	2	9	10	9	4	14	2	16	2
Czech Republic	29	15	6	10	4	12	12	12	4	14	9	16	4
Denmark	3	6	5	9	2	5	5	8	4	6	3	6	6
Estonia	33	12	6	10	2	9	10	12	4	14	7	16	4
Finland	15	7	5	9	5	4	0	9	4	5	3	9	6
France	31	6	4	8	3	4	6	8	4	4	3	9	6
Germany	24	7	5	9	3	5	6	8	4	6	4	9	4
Ghana	65	9	3	8	0	9	4	6	4	14	3	16	0
Greece	47	7	4	7	5	5	6	9	4	6	4	9	3
Hungary	54	7	5	9	6	5	2	7	4	6	1	9	4
Iceland	17	6	1	0	2	4	5	6	4	6	0	9	0
India	39	6	5	9	1	0	6	6	2	3	3	7	6
Indonesia	27	3	2	6	1	1	6	8	4	4	3	7	4
Ireland	4	12	4	8	0	12	12	9	4	12	7	11	2
Israel	22	4	4	6	3	1	1	6	4	4	4	9	6
Italy	42	12	4	10	4	12	10	9	4	14	5	16	6
Japan	38	7	4	9	3	2	2	2	4	3	3	9	1
Jordan	48	12	6	10	0	9	6	12	2	11	5	11	4
Kazakhstan	35	12	4	6	2	12	6	9	4	11	4	11	4
Korea Rep.	20	7	5	9	5	2	1	4	4	3	3	7	3
Kuwait	37	6	3	6	0	0	4	6	4	6	0	6	4
Latvia	45	15	3	8	2	12	8	12	4	9	4	16	2
Lithuania	30	12	3	10	2	12	12	9	4	11	7	16	4
Luxembourg	23	7	5	7	2	1	5	8	4	3	2	6	1
Malaysia	34	6	5	9	5	4	6	7	4	3	2	7	3
Mexico	56	3	4	6	0	6	2	3	4	8	2	6	2
Mongolia	61	0	1	4	1	0	0	2	1	0	1	4	0
Netherlands	9	12	4	10	2	9	10	9	4	14	5	13	6
New Zealand	32	9	6	8	0	3	4	9	4	11	2	8	2
Nigeria	64	15	0	4	2	6	8	3	4	11	0	13	4
Norway	10	2	5	9	3	0	5	8	4	3	0	9	4
Peru	63	0	1	6	2	4	4	7	4	6	1	9	4
Philippines	52	6	4	6	2	1	1	5	4	5	3	9	3
Poland	41	15	4	10	2	12	10	12	4	14	6	16	6
Portugal	36	12	3	10	2	12	8	9	4	14	5	16	6
Qatar	11	9	6	5	2	0	4	3	4	3	5	6	2
Romania	50	7	4	7	5	4	6	8	4	6	3	9	6
Saudi Arabia	16	12	5	6	2	12	8	3	4	9	2	6	2

http://dx.doi.org/10.21511/ppm.24(3).2026.22

Table B1 (cont.). Input data array for building a forecast of the global competitiveness level

Country	WCR	CP	GCC	EPD	CRD	CCII	CDE	CTAAR	PPD	CIR	CSM	FAC	MCD
Singapore	1	6	5	9	5	0	6	3	4	3	5	7	2
Slovak Republic	59	12	4	10	0	12	10	9	4	14	2	16	4
Slovenia	46	0	0	0	0	0	0	3	2	0	2	0	0
South Africa	60	1	0	4	1	0	1	5	4	3	0	9	0
Spain	40	6	5	9	3	5	5	9	4	4	3	9	6
Sweden	6	7	5	9	2	4	2	8	4	6	3	9	6
Switzerland	2	5	5	9	5	0	4	7	4	3	1	9	6
Thailand	25	6	5	8	1	1	3	5	4	6	3	4	4
Turkey	53	7	1	7	3	1	1	7	4	3	3	9	1
UAE	7	1	1	8	1	0	1	6	2	5	1	7	0
United Kingdom	28	9	6	10	4	6	6	6	4	11	6	16	6
USA	12	15	6	6	4	9	6	9	4	14	9	13	6
Venezuela	67	3	1	0	1	0	0	7	2	3	0	7	0

APPENDIX C

Table C1. The forecast values of competitiveness level for the 64 countries using the Score Data procedure in SPM software

Country	WCR*	RESPONSE*
Argentina	2	19.625
Australia	55	42.8276
Austria	42	42.8276
Bahrain	47	19.625
Belgium	50	42.8276
Botswana	13	42.8276
Brazil	6	19.625
Bulgaria	10	19.625
Canada	49	42.8276
Chile	24	19.625
China	54	38.4545
Colombia	11	19.625
Croatia	17	42.8276
Cyprus	25	42.8276
Czech Republic	39	42.8276
Denmark	65	42.8276
Estonia	35	42.8276
Finland	53	42.8276
France	37	19.625
Germany	44	42.8276
Ghana	3	19.625
Greece	21	38.4545
Hungary	14	42.8276
Iceland	51	19.625
India	29	42.8276
Indonesia	41	19.625
Ireland	64	38.4545
Israel	46	38.4545
Italy	26	38.4545
Japan	30	19.625
Jordan	20	42.8276
Kazakhstan	33	38.4545
Korea Rep.	48	42.8276

Table C1 (cont.). The forecast values of competitiveness level for the 64 countries using the Score Data procedure in SPM software

Country	WCR*	RESPONSE*
Kuwait	31	19.625
Latvia	23	38.4545
Lithuania	38	38.4545
Luxembourg	45	42.8276
Malaysia	34	42.8276
Mexico	12	19.625
Mongolia	7	19.625
Netherlands	59	38.4545
New Zealand	36	42.8276
Nigeria	4	19.625
Norway	58	42.8276
Peru	5	19.625
Philippines	16	19.625
Poland	27	38.4545
Portugal	32	38.4545
Qatar	57	42.8276
Romania	18	19,625
Saudi Arabia	52	42,8276
Singapore	67	42,8276
Slovak Republic	9	19,625
Slovenia	22	19,625
South Africa	8	19,625
Spain	28	42.8276
Sweden	62	42.8276
Switzerland	66	42.8276
Thailand	43	42.8276
Turkey	15	19.625
UAE	61	19.625
United Kingdom	40	42.8276
USA	56	42.8276
Venezuela	1	19.625

Note: Higher values of WCR* and RESPONSE* correspond to stronger competitiveness outcomes. The transformed indicators were calculated using the inverse transformation 68–x (meaning for the appropriate country), where 68 represents the total number of ranking positions plus one.

http://dx.doi.org/10.21511/ppm.24(3).2026.22

APPENDIX D

Source: Constructed by the authors with SPM software.

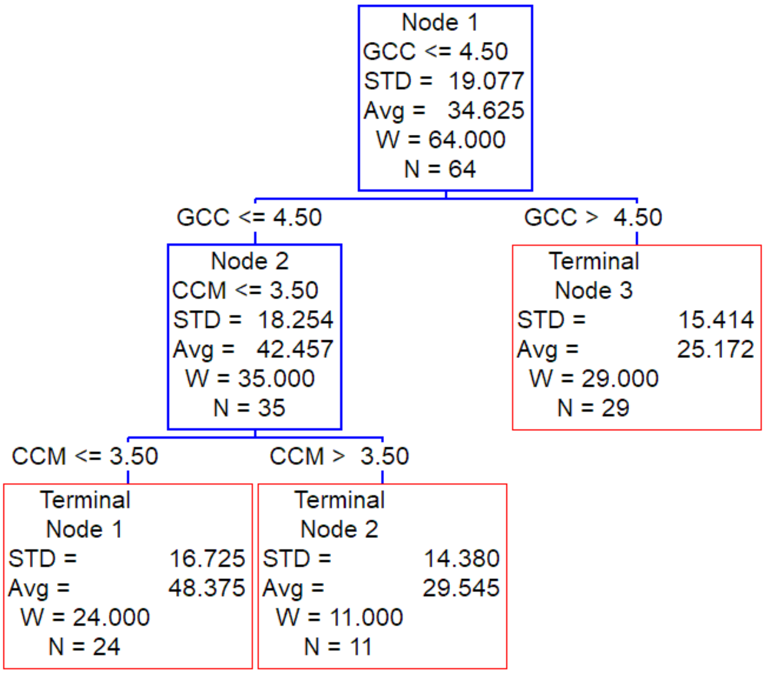

Figure D1. Regression tree of the influence of cybersecurity sub-factors on the level of country competitiveness

APPENDIX E

Table E1. Data for constructing QQ-plot

Sorted residuals	Theoretical quantiles	Sorted residuals	Theoretical quantiles
–105.375	–2.418	–29.1724	0.020
–94.375	–1.987	–27.375	0.059
–89.375	–1.762	–26.1724	0.098
–86.5455	–1.601	–24.375	0.138
–84.1724	–1.473	–22.5455	0.177
–82.1724	–1.366	–20.5455	0.217
–80.1724	–1.273	–19.1724	0.257
–78.375	–1.189	–17.375	0.298
–76.5455	–1.113	–16.1724	0.339
–74.1724	–1.043	–14.375	0.381
–71.375	–0.978	–13.1724	0.424
–68.5455	–0.917	–11.375	0.467
–67.1724	–0.858	–9.375	0.511
–65.1724	–0.803	–7.5455	0.556
–63.1724	–0.750	–6.375	0.602
–61.1724	–0.699	–4.5455	0.650
–59.375	–0.650	–3.375	0.699
–57.375	–0.602	–1.375	0.750
–56.1724	–0.556	–0.1724	0.803
–54.1724	–0.511	1.625	0.858
–51.5455	–0.467	2.8276	0.917
–50.1724	–0.424	4.4545	0.978
–48.1724	–0.381	5.625	1.043

Table E1. (cont.). Data for constructing QQ-plot

Sorted residuals	Theoretical quantiles	Sorted residuals	Theoretical quantiles
−46.1724	−0.339	7.625	1.113
−44.375	−0.298	9.4545	1.189
−41.375	−0.257	10.625	1.273
−40.1724	−0.217	11.8276	1.366
−38.1724	−0.177	13.625	1.473
−36.1724	−0.138	18.8276	1.601
−34.5455	−0.098	22.8276	1.762
−33.1724	−0.059	26.8276	1.987
−31.375	−0.020	28.8276	2.418

http://dx.doi.org/10.21511/ppm.24(3).2026.22