IMPACT OF DIGITAL DEVELOPMENT LEVEL ON NATIONAL CYBERSECURITY INDEX

Antun Fagarazzi[3]

UDC / UDK: 004.056
JEL classification / JEL klasifikacija: H56, L86, M15, O33
DOI: https://doi.org/10.22598/pi-be/2024.18.2.37
Preliminary communication / Prethodno priopćenje
Received / Primljeno: September 5, 2024 / 5. rujna 2024.
Accepted for publishing / Prihvaćeno za tisak: November 19, 2024 / 19. studenog 2024.

Summary

The integration of digital knowledge and information technology into all economic sectors is driven by the digital revolution and Industry 4.0. They also emerge as the primary driver of economic advancement across different nations. The main research goal of this paper is to analyse how the Digital Development Level influences the National Cybersecurity Index across different countries, as well as to determine the average Digital Development Level and the average National Cybersecurity Index value for all countries. A quantitative approach was employed in this research, utilizing secondary data. The analysis included one-way ANOVA, linear regression, correlation, and descriptive statistics. The study found a positive correlation between the Digital Development Level (DDL) and the National Cybersecurity Index (NCSI), as well as significant disparities between these variables. Qualitative factors, such as government policies, organizational culture, or international cooperation, are not accounted for in the analysis. Research results highlight the need for continued investments in both areas and underscore the importance of integrated policy approaches that address the complex challenges of the digital economy.

Keywords: *digital development level; national cybersecurity index; digital revolution; Industry 4.0.*

[3] Antun Fagarazzi, univ. mag. oec., ORCID iD: 0009-0009-8249-5679. E-mail: afagarazzi1@gmail.com

1. INTRODUCTION

The integration of digital knowledge and information technology into all economic sectors is driven by the digital revolution and Industry 4.0. Additionally, they emerge as the fundamental driver of economic advancement across various nations (Carlsson, 2004; Zhang & Chen, 2019; Tkachenko et al., 2019; Kwilinski, 2019; Kostetskyi, 2021). The real economy and digital technology are closely integrated to accelerate the reconstruction of a new economic development model and governance model by deeply incorporating digital technology, informatization, networking, and intelligence (Tapscott & Agnew, 2000; Linkov et al., 2018; Zhao et al., 2015; Korcsmaros et al., 2021). Currently, China's digital economy (DDE) is rapidly growing and maintains its position as a leading global digital economy powerhouse. The DDE is essential for driving China's economic growth, while economic growth continues to fuel the development of the DDE (Yin et al., 2019; Zhang & Chen, 2019; Jiang, 2020). The exploration of the digital development ecosystem (DDE) is being amplified by experts and scientific networks (Tapscott & Agnew, 2000; Korcsmaros et al., 2021; Yin et al., 2019). The fundamental dimensions of development are defined by them as they explore the links between economic, social, environmental, and digital development and anticipate the transformation of the economy due to digital development. Additionally, they are evaluating the best distribution of resources for DDE.

According to the United Nations Conference on Trade and Development (UNCTAD) Report (2019), the global market is dominated by China and the USA in terms of information technology development, with a combined share of over 40%. In addition, the modernization of economic infrastructure is being propelled by the implementation of digital technologies, which enable the establishment of forward-thinking innovation strategies. China has become a significant generator of high economic worth within the digital economy. The digital economy embodies a fresh type of economic activity that has developed due to progress in science and technology and the achievement of more advanced levels of economic progress. It indicates the path of reform and transformation in traditional industrial economics.

Almost every part of our daily lives is impacted by information and communication systems (Wegener, 2007). Cybercrime has adapted traditional scams for the digital age and created new offenses to exploit human naivety, software vulnerabilities, and vulnerable hardware, in order to make illegal profits. Norton reported that in 2010, the total costs of cybercrime, both direct and indirect, exceeded $338 billion (Whittaker, 2011), while McAfee (2014) suggested that the economic losses in Germany could reach as high as 1.6% of the gross domestic product (GDP).

Officials in the United States government have expressed worries about the potential occurrence of a "cyber Pearl Harbor" in the future (Bumiller & Shanker, 2012). There is a gap in policy and governance due to policymakers not staying current with the technology and the associated threat. Many developing countries have not acknowledged the risk, and this is especially notable in those areas (Lock-Teng Low et al., 2011).

Nowadays, cybersecurity has become a matter of national security with the potential to affect the daily lives of individual citizens (Klimberg, 2012).

The research problem lies in the lack of information about the connection between the Digital Development Level and the National Cybersecurity Index, as well as the average value of the Digital Development Level and the average value of the National Cybersecurity Index for all countries.

The aforementioned research problem allows defining the subject of research, theoretically and empirically analysing Digital Development Level and the National Cybersecurity Index in various countries.

Research questions

This paper will answer a series of research questions based on the problem and subject of research.

1. How does the Level of Digital Development influence the National Cybersecurity Index across different countries?
2. What is the average value of the Level of Digital Development and the average value of the National Cybersecurity Index for all countries?

The main research goal of this paper is to analyse how the Digital Development Level influences the National Cybersecurity Index across different countries, as well as to determine the average Digital Development Level and the average National Cybersecurity Index value for all countries.

The selection of the Digital Development Level (DDL) as an independent variable is based on its proven importance in enabling technological infrastructure and economic modernization (Tapscott & McQueen, 1996; Jorgenson et al., 2000). Previous studies, such as those by Oliner et al. (2008) and Greenstein and McDevitt (2011), emphasize the role of digitalization in boosting economic and institutional capacities, which indirectly strengthens cybersecurity. The National Cybersecurity Index (NCSI) is used as the dependent variable because it effectively measures a nation's preparedness against cybersecurity threats, as highlighted by McAfee (2014) and the European Commission (2013).

2. LITERATURE REVIEW

2.1. Digital economy

In 1996, the book "The Digital Economy: Promise and Peril in the Age of Networked Intelligence" by Tapscott & McQueen first introduced the idea of the digital economy. This concept was subsequently officially outlined in the US Department of Commerce's (1998) report "The Emerging Digital Economy." For over two decades, the worldwide digital economy has shown rapid growth and has become a key factor in driving the global economic recovery.

During the pandemic, China has successfully handled its economy by harnessing the impact of the digital economy. The digital economy has played a vital role in supporting COVID-19 containment measures and enabling the resumption of work, production, and education (Han et al., 2020). The digital economy has shown great potential for extensive applications and substantial growth by utilizing network and data space, in contrast to the traditional offline economy that relies on physical locations (Clifton et al., 2019).

The digital economy is the most vibrant, creative, and impactful form of economy, and it has become a central driving force for the national economy's growth (Guo, 2021). Following the pandemic, it is anticipated that the digital economy will play a crucial role in driving the high-quality growth of China's economy.

The digital economy is characterized by the exchange of goods and services using virtual methods, and it operates based on a distinct economic model. Its progress is intricately connected to the information and communication technology sector, resulting in the swift integration and evolution of related industries (Kim et al., 2002; Quah, 2002; Friedman, 2005). Data's emergence as a novel production factor, in addition to capital, labor, and land, represents a new economic and societal framework (Organisation for Economic Co-operation and Development, 2014). The digital economy offers the benefits of easy access to information, extensive interactions, and reduced costs associated with information and interaction (Barua et al., 1995; Barua et al., 1996; Choi et al., 1997). Studies on the global digital economy have advanced from the period of informatization and the internet to the present emphasis on the digital economy.

According to Roller and Waverman (2001), the widespread application of information and communication technology has the potential to significantly boost the economic development of specific regions. According to Antonelli (2003), the United States' total factor productivity has significantly improved as a result of the integration of information and communication technology (ICT). According to a study by Oliner et al. (2008), information technology played a significant role in the economic recovery that occurred between 1995 and 2000 after a review of US industry data. According to a 2011 study by Greenstein and McDevitt that examined the impact of broadband internet on the US GDP, the additional revenue it produced accounted for between 40 and 50 percent of the GDP. In a study by Jiménez et al. (2014), it was shown that the availability of the internet in Mexico positively impacted the country's economic growth.

The development of digital technologies like big data and artificial intelligence has caused academic circles to increasingly shift their focus to the digital economy. A nation's economic progress can be accelerated by the digital economy (Ivus & Boland, 2015; Jorgenson, 2016). Acemoglu and Restrepo (2018) enhanced the neoclassical model by proposing a cooperative relationship between machine intelligence and human labor. Their findings indicated that the adoption of machine intelligence might significantly accelerate economic growth at a rate of ten times or greater.

The focus of scholars shifted towards the progress of digital technology, and its positive impact on economic growth became more noticeable (Akimov et al., 2021; Kryshtanovych et al., 2021; Shpak et al., 2020; Vyshnevskyi, 2019; Molchanova, 2021; Trushkina, 2019). As per the findings of Jorgenson et al. (2000), the progress and enhancement of Internet products are facilitated by the availability of digital commodities and technologies. They suggest that Internet technology promotes economic advancement in accordance with the tenets of Moore's law and Metcalfe's law. 22 OECD country data samples were examined by Datta and Agarwal (2004) to demonstrate the beneficial impact of digital infrastructure on the fixed capital stock to GNP ratio. Thompson et al. (2013) stressed that the digital economy is defined by digital factors of production. By utilizing big data and artificial intelligence technologies, companies can lower expenses, shorten the supply chain, and enhance production efficiency, ultimately resulting in higher profits. Consequently, this prompts businesses to allocate a substantial portion of unused resources for autonomous research and development. In 2014, Turcan et al. suggested that the rise of networks changes the spread of social information, creating new possibilities for economic growth as information transmission speed and methods change. In his 2016 study, Pee examined B2C e-commerce and discovered that companies are using network platforms to directly involve consumers in the research and development of new products in the digital economy age. This enables easier communication and interaction with consumers, collecting valuable insights for improvement and creating a positive impact on the development of new products, ultimately improving the success rates of businesses. Teece (2018) drew a comparison between the digital economy and the traditional economy. He emphasized how the digital development environment has changed the traditional labour model and has provided a conducive environment for business expansion. This is achieved through enterprises embracing digital advancement via information technology and enhancing innovation capabilities to infuse new energy into enterprise development.

2.2. Cybersecurity

By addressing the digital security risks associated with the use of information and communication technologies, organizations, governments, and individuals can all achieve their development goals. This highlights the importance of building cybersecurity capacity. In minimizing the adverse effects of using information and computer technologies, this definition emphasizes how the government can improve its ability to achieve the required level of cybersecurity (Homburger, 2019).

Cybersecurity in France is considered to be the optimal condition for information systems that could be targeted by external threats, impacting the availability, integrity, or confidentiality of stored, processed, or transmitted data, as well as the services they offer (Da Silva, 2016).

The significance of safeguarding cyberspace, electronic data, information, and computer technologies that support it, along with the people who use it, is emphasized by Rossouw von Solms and Johan van Niekerk. This particular interpretation of "cybersecurity" sets it apart from the idea of "information security". The researchers point out distinct threats that pertain solely to cybersecurity, such as cyberbullying, a prevalent issue in modern society, and the security risks associated with smart home technologies that allow remote control and access (Sitdikova & Starodumova, 2019). Based on the data, the entertainment industry experiences the highest annual losses due to the potential unauthorized sharing of movies, music, and gaming apps, which directly infringes on the rights of copyright holders. Cyberterrorism primarily targets critical infrastructure, highlighting the significance of cybersecurity policy in safeguarding these assets (Rossouw von Solms, Johan van Niekerk, 2013). The broader scope of cybersecurity implies that it encompasses more issues than just information security. For instance, information security may involve unauthorized access, disclosure, and destruction of sensitive bank information by employees of banks and financial institutions (Klochko et al., 2016).

The classification put forward by scientists is quite thorough. Sharikov highlights three essential elements present in every cyberthreat: (1) sources, (2) goals, and (3) methods of carrying out cyberattacks. Therefore, it is crucial to consider all aspects of cyberthreats when creating a strong cybersecurity strategy (Sharikov, 2019).

Several countries have developed their national cybersecurity strategies (Falessi et al., 2012; Luiijf et al., 2013). Some underdeveloped countries' cybersecurity policy strategies provide useful perspectives, offering a wider framework for small island developing states and other growing economies. Small size and remote geography, traditionally seen as protective factors, do not shield against cyber threats (Ragnarsson & Bailes, 2010).

In 2010, the national cybersecurity strategy of the Republic of South Africa was published (Department of Communications, 2010; Luiijf et al., 2013). The creation of the National

Cybersecurity Advisory Council to supervise government policy and actions resulted from the policy, which is only twelve pages long (Department of Communications, 2010). The new body was collaborative across multiple agencies or ministries, with no specific agency or ministry designated as the primary leader. The strategy aimed to reduce cyber threats, establish international cooperation, build capacity, and encourage public-private collaboration (Phahlamohlaka et al., 2011).

The strategy fulfils the most basic requirements outlined in international guidelines. Despite this, it effectively promoted a distinct national goal of building trust in a secure information and communications technology environment (Luiijf et al., 2013). Tagert (2010) identified two main opposing approaches to national cybersecurity policy for developing African nations: one advocated for establishing a CERT as a crucial part of cybersecurity, while the other supported creating a legal framework for addressing cybercrime.

Tagert (2010) determined that Rwanda and Tunisia faced challenges with their limited technical capacity and lack of human resources, rendering existing approaches insufficient. He proposed that in these countries, customized approaches were required to enhance the technical capabilities and policy implementation skills of the government and private sector. Following this study, new international recommendations on national cybersecurity strategies have been issued by the ITU, OECD, European Union, and other organizations, which are more comprehensive and better suited for developing nations. Several international and regional organizations, such as ITU (Wamala, 2011), ENISA (Falessi et al., 2012), the European Union (European Commission, 2013), and OAS (2004), have issued recommendations for the development of national cybersecurity strategies. The private sector's participation in influencing national cybersecurity strategies is beginning to show.

3. METHODOLOGY AND DATA

A quantitative approach was taken in the following research, and secondary data were used. One-way ANOVA, linear regression and correlation were used to help answer the first research question. To fulfil the objective of responding to the second research question, descriptive statistics were used. The dataset was downloaded from the *e-Governance Academy Foundation data source (https://ncsi.ega.ee/ncsi-index/?order=-isd)*. Data was downloaded on August 8, 2023, and is updated daily. There were four attributes in the used data set. Countries without complete data for both indices were excluded to maintain data integrity. A sample of 155 nations was utilized after applying the stated condition to filter the data.

According to the e-Governance Academy Foundation (https://ncsi.ega.ee/methodology/), the following attributes are listed below:

- Digital Development Level (DDL) - The calculation of the DDL is based on the E-Government Development Index (EGDI) and Networked Readiness Index (NRI).
- The EGDI is made up of a weighted average of three normalized scores related to the three main aspects of e-government: (1) the scope and quality of online services (Online Service Index, OSI), (2) the advancement of telecommunication infrastructure (Telecommunication Infrastructure Index, TII), and (3) the foundational human capital (Human Capital Index, HCI). Each index is a comprehensive measure that can be individually extracted and examined (UN E-Government Knowledgebase, 2024).
- The DDL represents the average percentage that a country achieved out of the maximum value of both indexes.

The average percentage of the maximum values for EGDI and NRI is displayed in the DDL.

$$DDL = \frac{EGDI\ \% + NRI\ \%}{2}$$

National Cybersecurity Index (NCSI) - 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.

$$NCSI = \frac{Country\ Points\ X\ 100}{Maximum\ Points}$$

The nation is a representation of the nation or area that is examined in terms of its level of digitalization and cybersecurity.

Table 1. Shortened view of data on the National Index of Cybersecurity and data on the Level of Digital Development by country

Ranking	Country	Digital Development Level	National Cybersecurity Index
1.	Switzerland	82.93	75.32
2.	Denmark	82.68	84.42
3.	Korea (Republic)	82.23	68.83

4.	Nederland	81.86	83.12
5.	Sweden	81.51	84.42
6.	United States	81.05	64.94
7.	Norway	80.19	67.53
8.	Germany	80.01	90.91
9.	United Kingdom	79.96	89.61
10.	Singapore	79.93	71.43
11.	Japan	78.69	63.64
12.	Iceland	78.64	55.84
13.	Luxembourg	78.4	66.23
14.	Finland	78.35	85.71
15.	Australia	77.61	66.23
16.	France	77.29	84.42
17.	New Zealand	76.81	51.95
18.	Canada	75.96	70.13
19.	Austria	75.76	85.71
20.	Estonia	75.59	93.51

Source: https://ncsi.ega.ee/ncsi-index/?order=-isd

4. RESULTS OF EMPIRICAL RESEARCH

The data used to analyse the impact of the level of Digital Development and the National Cybersecurity Index can be found in Table 1.

Correlation

The main goal of this method is to investigate and identify whether there is a statistically significant relationship between the National Cybersecurity Index and the Level of Digital Development. The correlation matrix can be found in Figure 1.

Table 2. Correlation matrix

Attributes	Digital Development Level	National Cybersecurity Index
Digital Development Level	1	0.708
National Cybersecurity Index	0.708	1

The correlation between the National Cybersecurity Index (NCSI) and the Digital Development Level (DDL) is 0.708. The correlation value of 0.708 indicates a **strong**

positive correlation between the two variables. This means that there is a tendency for changes in the Level of Digital Development and the National Cybersecurity Index to take place in the same direction, i.e., when one of these indices increases, the other is likely to increase, and vice versa.

One-way ANOVA

This method aims to compare the Levels of Digital Development with different levels of the National Cybersecurity Index among countries. In this way, it is possible to identify whether there are persistent statistically significant differences in the Levels of Cybersecurity Index and the Levels of Digital Development.

Table 3. ANOVA Summary

ANVOA Summary					
Source	Degrees of Freedom DF	Sum of Squares SS	Mean Square MS	F-Stat	P-Value
Between groups	1	1757.0709	1757.0709	3.4443	0.0644
Within groups	308	157122.4844	510.1379		
Total	309	158879.5553			

Degrees of Freedom (DF):

- Between Groups (DF = 1): This indicates that there is one degree of freedom for the comparison between the groups. Since the comparison involves the Levels of Digital Development between two categories or groups of the National Cybersecurity Index (for example, low vs. high), this single degree of freedom is expected.
- Within Groups (DF = 308): The degrees of freedom within groups is 308, which is calculated based on the total number of observations (309) minus the number of groups (2). This reflects the variability within each group (variation in Digital Development Level within each category of the National Cybersecurity Index).
- Total (DF = 309): The total degrees of freedom is 309, which represents the total number of observations in the dataset minus 1.

Sum of Squares (SS):

- Between Groups (SS = 1757.0709): The Sum of Squares between groups represents the variability in the Levels of Digital Development that is explained by the differences in the National Cybersecurity Index groups. A higher value indicates more variability explained by the grouping.

- Within Groups (SS = 157122.4844): The Sum of Squares within groups captures the variability in the Levels of Digital Development that is not explained by the differences in the National Cybersecurity Index levels but by natural variation within each group.
- Total (SS = 158879.5553): The Total Sum of Squares combines the between-group and within-group variabilities and represents the overall variability in the dataset.

Mean Square (MS):

- Between Groups (MS = 1757.0709): The Mean Square between groups is obtained by dividing the Sum of Squares between groups by the degrees of freedom (DF = 1). It reflects the average variability explained by the group differences.
- Within Groups (MS = 510.1379): The Mean Square within groups is calculated by dividing the Sum of Squares within groups by the degrees of freedom within groups (DF = 308). This is a measure of the average variability within the groups.

F-Statistic (F = 3.4443): The F-statistic is the ratio of the Mean Square between groups to the Mean Square within groups (1757.0709 / 510.1379 = 3.4443). It tells us how much of the overall variability is explained by the group differences (in this case, the different levels of the National Cybersecurity Index) relative to the variability within groups. A larger F-statistic suggests that there is more between-group variability compared to within-group variability, which could indicate significant differences between the groups.

P-Value (P = 0.0644): The p-value tells us whether the observed differences between the groups are statistically significant. In this case, the p-value is 0.0644, which is just above the common significance level of 0.05. This means that while the differences in the Levels of Digital Development between the groups are suggestive, they are not statistically significant at the 0.05 level. There is a 6.44% chance that the observed differences are due to random variation rather than a true underlying difference between the groups.

Linear regression

The goal of linear regression is to model and understand the relationship between two variables – the National Cybersecurity Index (dependent) and the Digital Development Level (independent). A linear regression line has an equation of the form ***Y***

= a + bX. Linear regression is used to find the best linear function that best describes or predicts the values of one variable (National Cybersecurity Index) based on the values of another variable (Digital Development Level). The results of the linear regression can be found in Table 4.

Table 4. Linear regression summary

Best-fit values	
Slope	1.008 ± 0.08128
Y-intercept	-5.163 ± 4.420
X-intercept	5.123
1/Slope	0.9922
95% Confidence Intervals	
Slope	0.8485 to 1.167
Y-intercept	-13.83 to 3.5
X-intercept	-4.083 to 11.97
Goodness to Fit	
R square	0.5012
Sy.x	18.52
Is slope significantly non-zero?	
F	153.8
DFn,DFd	1.153
P Value	<0.0001
Deviation from horizontal?	Significant
Data	
Number of XY pairs	155
Equation	Y=1.008*X-5.163

Best-Fit Values:

- Slope (1.008 ± 0.08128): The slope of 1.008 indicates that for every unit increase in the Digital Development Level (X), the National Cybersecurity Index (Y) increases by approximately 1.008 units. The value of ±0.08128 represents the uncertainty or standard error of the slope estimate. This relatively small standard error suggests that the slope estimate is precise.
- Y-intercept (-5.163 ± 4.420): The Y-intercept is the point where the regression line crosses the Y-axis (when X = 0). The value of -5.163 suggests that when the Digital Development Level is zero, the predicted National Cybersecurity Index would be approximately -5.163 (which may not be meaningful in practical terms, as a cybersecurity index below zero is unrealistic, but it's important for the equation). The uncertainty of ±4.420 indicates a moderate variability in the Y-intercept estimate.

- X-intercept (5.123): This is the point where the regression line crosses the X-axis, which means that when the National Cybersecurity Index (Y) is zero, the Digital Development Level would be approximately 5.123. However, the range of possible X-intercepts from the confidence intervals (discussed below) suggests some uncertainty here.

95% Confidence Intervals:

- Slope (0.8485 to 1.167): This range indicates a 95% confidence that the true slope lies between 0.8485 and 1.167. Since this range does not include zero, it confirms that there is a statistically significant positive relationship between the Digital Development Level and the National Cybersecurity Index.
- Y-intercept (-13.83 to 3.5): The confidence interval for the Y-intercept is wide, ranging from -13.83 to 3.5, suggesting some uncertainty about the exact value when X = 0.
- X-intercept (-4.083 to 11.97): This wide range indicates uncertainty in predicting the exact point at which the National Cybersecurity Index would be zero. The range includes both negative and positive values, further highlighting the variability.

Goodness of Fit:

- R-squared (0.5012): R-squared indicates the proportion of variance in the National Cybersecurity Index that can be explained by the Digital Development Level. An R-squared value of 0.5012 means that 50.12% of the variation in the National Cybersecurity Index can be explained by the Digital Development Level. This is a moderate fit, suggesting that other factors beyond the Digital Development Level also play a role in determining cybersecurity preparedness.
- Sy.x (18.52): This is the standard error of the estimate, which measures the average distance that the observed values fall from the regression line. A Sy.x value of 18.52 suggests that, on average, the predicted National Cybersecurity Index values differ from the actual values by 18.52 units.

Is the Slope Significantly Non-zero?

- F-value (153.8): The F-statistic measures the overall significance of the regression model. A high F-value, such as 153.8, indicates that the model is statistically significant.
- Degrees of Freedom (DFn = 1, DFd = 153): These are the degrees of freedom associated with the F-test. DFn is the number of independent variables (1 in this

case, the Digital Development Level), and DFd is the number of data points minus the number of predictors (153).

- P-value (<0.0001): The p-value indicates the probability of observing these results if the null hypothesis (that the slope is zero) were true. A p-value of less than 0.0001 indicates that the slope is highly significant, allowing for the rejection of the null hypothesis with high confidence and leading to the conclusion that there is a statistically significant relationship between the two variables.
- Deviation from Horizontal (Significant): The results confirm that the regression line deviates significantly from a horizontal line, further supporting the conclusion that the slope is not zero.

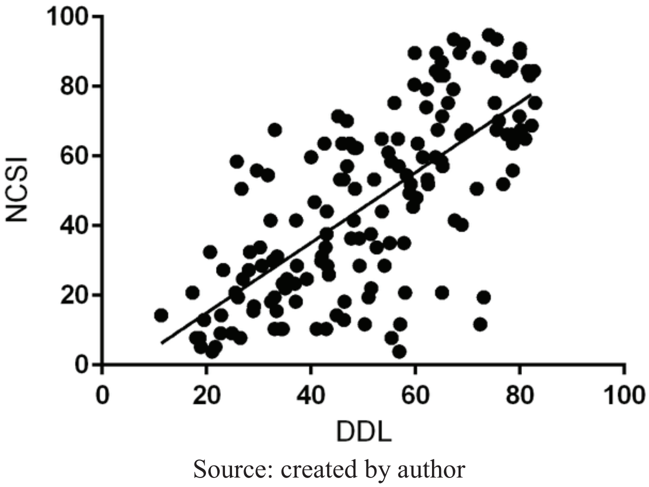
Data:

- Number of XY pairs (155): There are 155 pairs of data points used in the regression analysis, ensuring that the model is built on a robust sample size.

Equation of the Regression Line:

- Y = 1.008 * X - 5.163 This is the equation of the best-fit line, where Y (National Cybersecurity Index) can be predicted based on X (Digital Development Level).

Figure 1. Linear regression - graphical presentation



Source: created by author

Descriptive statistics

The goal of descriptive statistics is to get a better insight into the state of the Digital Development Level and the National Cybersecurity Index among different countries. By applying descriptive statistics, the results shown in Table 5 are obtained.

Table 5. Descriptive statistics – summary of results

Data summary				
Groups	N	Mean	Std. Dev.	Std. Error
Group 1	155	51.2134	18.3609	1.4748
Group 2	155	46.4519	26.1372	2.0994

Both groups consist of 155 observations (countries) each. This indicates that the sample size is the same for both groups, providing a balanced comparison in terms of the number of data points.

Mean:

- Group 1: The mean value is 51.2134, which represents the average value of the Digital Development Level for this group.
- Group 2: The mean value is 46.4519, representing the average value of the National Cybersecurity Index for this group.
- On average, Group 1 (Digital Development Level) has a higher mean score than Group 2 (National Cybersecurity Index), suggesting that, based on these sample means, countries generally have a relatively higher Digital Development Level compared to their National Cybersecurity Index.

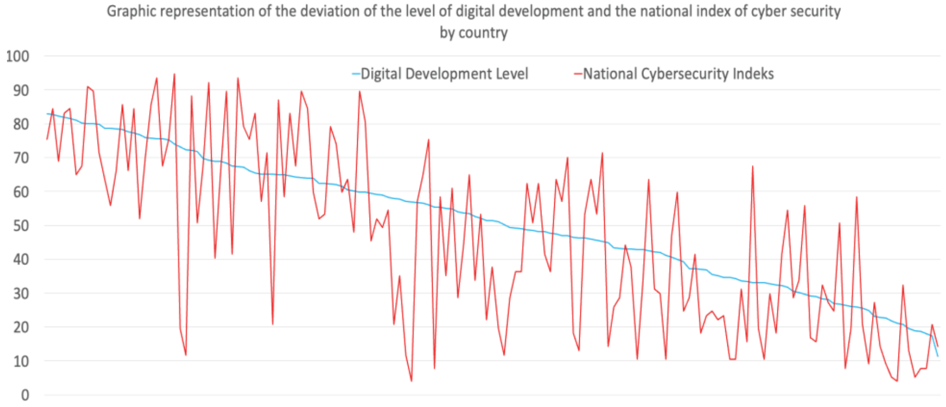
Standard Deviation (Std. Dev.):

- Group 1: The standard deviation is 18.3609, which measures how much the data points in Group 1 deviate from the mean on average. A higher standard deviation indicates greater variability within the Digital Development Level among countries.
- Group 2: The standard deviation is 26.1372, which suggests even greater variability in the National Cybersecurity Index within Group 2.
- The larger standard deviation in Group 2 indicates that the National Cybersecurity Index values are more spread out around the mean compared to the Digital Development Level in Group 1. This could mean that countries show more inconsistent results regarding National Cybersecurity Index than their Digital Development Level.

Standard Error (Std. Error):

- Group 1: The standard error is 1.4748, which provides an estimate of how much the sample mean is expected to deviate from the true population mean. A lower standard error indicates that the sample mean is a more accurate estimate of the population mean for the Digital Development Level.
- Group 2: The standard error is 2.0994, indicating a slightly less precise estimate of the population mean for the National Cybersecurity Index compared to Group 1.
- The standard errors suggest that the mean of Group 1 is estimated with more precision than that of Group 2. This could be due to the higher variability (standard deviation) in Group 2.

Figure 2. Graphic representation of the deviation of the level of digital development and the national index of cybersecurity by country



Source: created by author

5. DISCUSSION

This paper explores the dynamic relationship between the Digital Development Level and the National Cybersecurity Index, offering significant contributions to both theoretical and practical fields. The primary research goal was to assess the influence of Digital Development Level on the National Cybersecurity Index (NCSI) across countries. By applying statistical methods such as correlation and linear regression, the study found a positive correlation between the Digital Development Level (DDL) and National

Cybersecurity Index (NCSI), with a correlation coefficient of 0.708. It implies that countries with higher levels of Digital Development Level typically possess stronger National Cybersecurity Index. The linear regression analysis further confirmed that approximately 50% of the variance in the NCSI could be explained by the DDL.

The secondary goal of determining the average values of both the DDL and NCSI for the countries studied was also met. The results indicated that the average DDL was 51.21%, while the average NCSI was 46.45%, pointing to significant disparities in the Digital Development Level and National Cybersecurity Index between countries. Although the study reveals a strong correlation between DDL and NCSI, it is crucial to recognize the complexity of this relationship. Digital development can lead to increased cybersecurity risks as more systems become interconnected, creating new vulnerabilities. At the same time, improved cybersecurity can foster further digital growth by providing a safe environment for innovation. This two-way interaction suggests that future studies should explore whether cybersecurity acts as a mediator in the relationship between digital development and economic growth. Additionally, investigating sector-specific dynamics (e.g., finance, healthcare) could provide more granular insights into how digital and cybersecurity development influence each other.

This research makes several important theoretical contributions. The positive relationship between DDL and NCSI observed in the data corroborates existing research that suggests well-developed digital infrastructures contribute to improved cybersecurity capabilities (Homburger, 2019; Solms & Niekerk, 2013). However, it is essential to clarify that these studies do not explicitly argue that digital development automatically enhances cybersecurity. Instead, they emphasize the need for integrated cybersecurity strategies alongside digital development. The study builds upon the understanding that digital development—measured using indices such as the E-Government Development Index (EGDI) and Networked Readiness Index (NRI)—forms the foundation upon which nations can strengthen their cybersecurity capabilities. By integrating these indices into the analysis, the study provides a more nuanced framework for assessing the interplay between digital infrastructure and cybersecurity. However, the correlation observed in this study does not imply causation, meaning further research is required to investigate how specific aspects of digital development (e.g., investment in ICT, policy frameworks) directly impact cybersecurity.

The practical implications of this study are multifaceted, providing actionable insights for policymakers, businesses, and educational institutions. For policymakers, the findings suggest that prioritizing digital infrastructure development is critical not only for economic growth but also for enhancing cybersecurity capabilities. Countries that have limited digital development and poor cybersecurity ratings need to prioritize implementing broad policy changes that tackle both areas at the same time. International organizations such as the International Telecommunication Union (ITU) and the European Union (EU) can use these insights to help nations with underdeveloped digital systems allocate resources more effectively for building secure digital environments. From a business perspective, the study highlights the importance of cybersecurity as an integral part of digital transformation. Companies, particularly in industries like finance, healthcare, and critical infrastructure, should collaborate with governments to develop robust cybersecurity frameworks that align with national strategies. The results of the study also suggest that businesses in countries with high digital development may benefit from stronger national cybersecurity, which in turn could reduce risks to their operations. For educational institutions, particularly those involved in training future leaders in IT, economics, and cybersecurity, this research provides a valuable empirical foundation. The results can be incorporated into curricula to teach students about the importance of aligning digital development with cybersecurity strategies. The data-driven approach and use of international datasets provide a global perspective that can help students understand the interconnectedness of digital and security policies.

6. CONCLUSION

This paper successfully addresses its primary objective of exploring the relationship between the Digital Development Level and National Cybersecurity Level across a wide range of countries. The findings indicate a strong positive correlation between the two, suggesting that nations with higher levels of digital development are better positioned to secure their digital infrastructure. However, the study also points to significant gaps in both digitalization and cybersecurity capabilities globally, particularly among developing nations. These disparities highlight the need for continued investments in both areas, as well as the importance of integrated policy approaches that address the complex challenges of the digital economy.

Despite the study's insightful contributions, there are a few important limitations that should be noted. First, the research relies solely on secondary data, which may not capture the full complexity of the relationship between digital development and cybersecurity. Qualitative factors, such as government policies, organizational culture, or international cooperation, are not accounted for in the analysis but could play a significant role in shaping both digital and cybersecurity outcomes.

Additionally, while the correlation between digital development and cybersecurity is strong, the study does not establish a causal link. Future research could use more granular data or case studies to explore how specific investments in digital infrastructure (e.g., broadband access education in digital literacy) directly influence cybersecurity outcomes. Furthermore, exploring the impact of regional differences—such as the distinction between developed, emerging, and underdeveloped nations—could provide more context for the observed discrepancies in digital development and cybersecurity indices. While this study focuses on the relationship between digital development and cybersecurity, it is important to acknowledge that other factors could influence both. Geopolitical risks, such as regional conflicts or trade sanctions, could negatively impact both digital development and cybersecurity investments. Similarly, governance models, including the extent of regulatory frameworks and international cooperation, are crucial in shaping a country's approach to digitalization and security. Future research could benefit from incorporating these variables into the analysis to develop a more nuanced understanding of the interplay between digital and cybersecurity policies.

Another avenue for future research would be to investigate how different sectors within countries contribute to both digital developments and cybersecurity. For instance, industries such as finance, healthcare, and telecommunications may exhibit varying levels of maturity in terms of digital development and cybersecurity preparedness. This sectoral analysis could offer more targeted recommendations for improving cybersecurity in specific industries.

REFERENCES:

1. Acemoglu, D. and Restrepo, P. (2018). The race between man and machine: Implications of technology for growth, factor shares, and employment. *American Economic Review*, 108, pp. 1488–1542.s
2. Akimov, O., Karpa, M., Parkhomenko-Kutsevil, O., Kupriichuk, V., & Omarov, A. (2021). Entrepreneurship education of the formation of the e-commerce managers' professional qualities. *International Journal of Entrepreneurship*, *25*(S2), 1–8.
3. Antonelli, C. (2003). The digital divide: Understanding the economics of new information and communication technology in the global economy. *Information Economics and Policy*, 15, pp. 173–199.
4. Barua, A., Chellappa, R. and Whinston, A.B. (1995). Creating a collaboratory in cyberspace: Theoretical foundation and an implementation. *Journal of Organizational Computing and Electronic Commerce*, 5, pp. 417–442.
5. Barua, A., Chellappa, R. and Whinston, A.B. (1996). The design and development of Internet and Intranet-based collaboratories. *International Journal of Electronic Commerce*, 1, pp. 32–58.

6. Bumiller, E., & Shanker, T. (2012, October 11). Panetta warns of dire threat of cyberattack on U.S. The New York Times. Retrieved from www.nytimes.com
7. Carlsson, B. (2004). The Digital Economy: What is new and what is not? *Structural Change and Economic Dynamics*, *15*(3), 245–264. https://doi.org/10.1016/j.strueco.2004.02.001
8. Choi, S.Y., Stahl, D.O. and Whinston, A.B. (1997). *The Economics of Electronic Commerce*. Macmillan Technical Publishing: Indianapolis, Indiana, p. 626.
9. Clifton, N., Fuzi, A. and Loudon, G. (2019). Coworking in the digital economy: Context, motivations, and outcomes. *Futures*, 135, 102439.
10. Da Silva, M.F. (2016). Cyber Security vs. Cyber Defense – A Portuguese View On the Distinction. URL: https://www.academia.edu/23986861/CYBER_SECURITY_VS._CYBER_DEFENSE_A_PORTUGUESE_VIEW_ON_THE_ DISTINCTION
11. Datta, A., & Agarwal, S. (2004). Telecommunications and economic growth: A panel data approach. *Applied Economics*, *36*(15), 1649–1654. https://doi.org/10.1080/0003684042000218552
12. Department of Communications, Republic of South Africa (2010, February 19). Draft cybersecurity policy. Government Gazette No. 32963. Retrieved from http://www.pmg.org.za/files/docs/100219cybersecurity.pdf
13. e-Governance Academy Foundation. NCSI: National Cyber Security Index [Internet], available at: https://ncsi.ega.ee/ncsi-index/?order=-isd (Accessed on August 8, 2023)
14. e-Governance Academy Foundation. NCSI: National Cyber Security Index Methodology [Internet], available at: https://ncsi.ega.ee/methodology/ (Accessed on August 8, 2023)
15. European Commission. High Representative of the European Union for Foreign Affairs and Security Policy. (2013). Joint communication to the European Parliament, the Council, the European Economic and Social Committee and the Committee of the Regions. Cybersecurity strategy of the European Union: An open, safe and security cyberspace. Available at: http://ec.europa.eu/information_society/newsroom/cf/dae/document.cfm?doc_id=1667
16. Falessi, N., Gavrila, R., Klenstrup, M.R., & Moulinos, K. (2012). National cyber security strategies: Practical guide on development and execution. Retrieved from http://www.enisa.europa.eu/activities/ Resilience-and-

CIIP/national-cyber-security-strategies-ncsss/ national-cyber-security-strategies-an-implementation-guide

17. Friedman, T. (2005). *The World Is Flat*. Farrar, Straus and Giroux: New York, NY, USA, p. 488.
18. Greenstein, S. and McDevitt, R.C. (2011). The broadband bonus: Estimating broadband Internet's economic value. *Telecommunications Policy*, 35, pp. 617–632.
19. Guo, L. (2021). The impact mechanism of the digital economy on China's total factor productivity: An uplifting effect or a restraining effect? *South China Journal of Economics*, 40, pp.9–27.
20. Han, J., Sun, Y.W. and Chen, X. (2020). Analysis of the development path of China's digital economy in the post-pandemic era. *Comparative Economic Systems*, 5, pp.16–24.
21. Homburger, Z. (2019). The Necessity and Pitfall of Cybersecurity Capacity Building for Norm Development in Cyberspace. *Global Society*. https://doi.org/10.1080/13600826.2019.1569502
22. Ivus, O. and Boland, M. (2015). The employment and wage impact of broadband deployment in Canada. *Canadian Journal of Economics*, 48, pp. 1803–1830.
23. Jiang, X. (2020). Digital economy in the post-pandemic era. *Journal of Chinese Economic and Business Studies*, *18*(4), 333–339. https://doi.org/10.1080/14765284.2020.1855066
24. Jimenez, M., Matus, J.A. and Martinez, M.A. (2014). Economic growth as a function of human capital, Internet and work. *Applied Economics*, 46, pp. 3202–3210.
25. Jorgenson, A.K. (2016). Environment, development, and ecologically unequal exchange. *Sustainability*, 8, 227.
26. Jorgenson, D. W., Stiroh, K. J., Gordon, R. J., & Sichel, D. E. (2000). Raising the speed limit: US eco- nomic growth in the information age. *Brookings Papers on Economic Activity*, *31*(1), 125–235.
27. Kim, B., Barua, A. and Whinston, A.B. (2002). Virtual field experiments for a digital economy: A new research methodology for exploring an information economy. *Decision Support Systems*, 32, pp. 215–231.
28. Klimberg, A. (ed.) (2012). National cybersecurity framework manual. Tallinn, Estonia: NATO CCD COE Publication
29. Klochko, A.N., Kulish, A.N., Reznik, O.N. (2016). The social basis of criminal law protection of banking in Ukraine. *Russian Journal Of Criminology*. http://doi.org/10.17150/2500-4255.2016.10(4).790-800

30. Korcsmaros, E., Machova, R., Seben, Z., & Zsigmond, T. (2021). The regional innovations governance: Slovakia with regard to convergence criteria. *Marketing and Management of Innovations*, *1*, 170– 180. https://doi.org/10.21272/mmi.2021.1-13
31. Kostetskyi, P. (2021). Does digitalization lead to better transparency: Bibliometric approach. *Business Ethics and Leadership*, *5*(3), 102–107. https://doi.org/10.21272/bel.5(3).102-107.2021
32. Kryshtanovych, M., Akimova, L., Akimov, O., Kubiniy, N., & Marhitich, V. (2021). Modeling the process of forming the safety potential of engineering enterprises. *International Journal of Safety and Security Engineering*, *11*(3), 223–230. https://doi.org/10.18280/ijsse.110302
33. Kwilinski, A. (2019). Implementation of blockchain technology in accounting sphere. *Academy of Accounting and Financial Studies Journal*, *23*(2S), 1–6.
34. Linkov, I., Trump, B. D., Poinsatte-Jones, K., & Florin, M. V. (2018). Governance strategies for a sustain- able digital world. *Sustainability*, *10*(2), 440. https://doi.org/10.3390/su10020440
35. Lock-Teng Low, K., Fook Ong, S., & Aun Law, K. (2011). Sustainable ICT development: A perspective from ICT loops in developing nations. International Journal of Academic Research, 3(6), 92-97
36. Luiijf, E., Besseling, K., & Graaf, P. D. (2013). Nineteen national cyber security strategies. International Journal of Critical Infrastructures, 9(1), 3-31. DOI:10.1504/ICIS.2013.051608
37. McAfee (June, 2014). Net losses: Estimating the global cost of cybercrime. Retrieved from http://www.mcafee.com/us/ resources/reports/rp-economic-impact-cybercrime2.pdf
38. Molchanova, K. (2021). Organization of aviation enterprises' interaction based on the digital platform. *Virtual Economics*, *4*(1), 77–97. https://doi.org/10.34021/ve.2021.04.01(4)
39. Oliner, S.D., Sichel, D.E. and Stiroh, K.J. (2008). Explaining a productive decade. *Journal of Policy Modeling*, 30, pp. 633–673.
40. Organisation for Economic Co-operation and Development (2014). *Measuring the Digital Economy: A New Perspective*. OECD Publishing: Paris, France, pp. 45–49.
41. Organization of American States (2004). A comprehensive Inter-American cybersecurity strategy: A multidimensional and multidisciplinary approach to creating a culture of cybersecurity. AG/RES. 2004 (XXIV-0/04). Retrieved from: http://www.cicte.oas.org/Rev/En/Documents/ OAS GA/AGRES.%202004%20%28XXXIV-0-04%29_EN.pdf

42. Pee, L. G. (2016). Customer co-creation in B2C e-commerce: Does it lead to better new products? *Electronic Commerce Research*, *16*(2), 217–243. https://doi.org/10.1007/s10660-016-9221-z
43. Phahlamohlaka, L., Jansen van Vuuren, J., & Coetzee, C. (2011). Cybersecurity awareness toolkit for national security: An approach to South Africa's cyber security policy implementation. Proceedings of the South African Cyber Security Awareness Workshop (SACSAW 2011). Retrieved from http://www.csir.co.za/dpss/docs/SACSAWFinal_16Aug.pdf
44. Quah, D. (2002). *Digital Goods and the New Economy*. CEP Discussion Paper: London, UK, p. 563.
45. Ragnarsson, J. K., & Bailes, A.J. (2010). Iceland and cyber-threats. RANNSÓKNIR FÉLAGSVÍSINDUM XI, 60-65. Retrieved from http://skemman.is/stream/get/ 1946/7179/19284/1/STJbok-ritstyrt-heild.pdf#page=69
46. Roller, L.H. and Waverman, L. (2001). Telecommunications infrastructure and economic development: A simultaneous approach. *American Economic Review*, 91, pp. 909–923.
47. Rossouw von Solms, Johan van Niekerk (2013). From information security to cyber security. *Computer and Security.* Issue 38. P. 97–103.
48. Sharikov, P. (2019). Evolution of American Cyber Security Policies. *Mirovaya Ekonomika i Mezhdunarodnye Otnosheniya*. http://doi.org/10.20542/0131-2227-2019-63-10-51-58
49. Shpak, N., Kuzmin, O., Dvulit, Z., Onysenko, T., & Sroka, W. (2020). Digitalization of the marketing activities of enterprises: Case study. *Information*, *11*(2), 109. https://doi.org/10.3390/info11020109
50. Sitdikova, L.B.; Starodumova, S.J. (2019). Corporate agreement as a means of providing security in the course of entrepreneurship development, *Entrepreneurship and Sustainability Issues,* 7(1), 324-335. http://doi.org/10.9770/jesi.2019.7.1(24)
51. Tagert, A. (2010). Cybersecurity Challenges in Developing Nations. Unpublished dissertation, Carnegie Mellon University, Pittsburgh, PA. Retrieved from http://repository.cmu.edu/dissertations/22
52. Tapscott, D. and McQueen, R. (1996). The digital economy: Promise and peril in the age of networked intelligence. *Bambook*, 10, pp.69–71.
53. Tapscott, D., & Agnew, D. (2000). Governance in the digital economy. *Finance & Development*, *36*(4), 34–37.
54. Teece, D. J. (2018). Profiting from innovation in the digital economy: Enabling technologies, standards, and licensing models in the wireless world.

Research Policy, *47*(8), 1367–1387. https://doi.org/10.1016/j.respol.2017.01.015

55. Thompson, P., Williams, R., & Thomas, B. (2013). Are UK SMEs with active web sites more likely to achieve both innovation and growth? *Journal of Small Business and Enterprise Development*, *20*(4), 934–965. https://doi.org/10.1108/JSBED-05-2012-0067
56. Tkachenko, V., Kwilinski, A., Korystin, O., Svyrydiuk, N., & Tkachenko, I. (2019). Assessment of in- formation technologies influence on financial security of economy. *Journal of Security and Sustain- ability Issues*, *8*(3), 375–385. https://doi.org/10.9770/jssi.2019.8.3(7)
57. Trushkina, N. (2019). Development of the information economy under the conditions of global eco- nomic transformations: features, factors and prospects. *Virtual Economics*, *2*(4), 7–25. https://doi.org/10.34021/ve.2019.02.04(1)
58. Turcan, V., Gribincea, A., & Birca, I. (2014). Digital economy – a premise for economic development in the 20th century. *Economie si Sociologie: Revista Teoretico-Stiintifica*, *2*, 109–115.
59. UN E-Government Knowledgebase (2024). E-Government Development Index (EGDI) [Internet], available at: https://publicadministration.un.org/egovkb/en-us/About/Overview/-E-Government-Development-Index
60. United Nations Conference on Trade and Development. (2019). *Digital economy report 2019. Value creation and capture: Implications for developing countries*. UNCTAD. Retrieved January 20, 2022, from https://unctad.org/system/files/official-document/der2019_overview_en.pdf
61. Vyshnevskyi, O. (2019). Unity of digital and virtual economies within concept of Dataism. *Virtual Economics*, *2*(3), 7–21. https://doi.org/10.34021/ve.2019.02.03(1)
62. Wamala, F. (2011). The ITU national cybersecurity strategy guide. Geneva, Switzerland: International Telecommunications Union. Retrieved from www.itu.int
63. Wegener, H. (2007). Harnessing the perils in cyberspace: Who is in charge? Disarmament Forum 3, 45-52. Retrieved from http://www.unidir.org/pdf/articles/pdf-art2646.pdf
64. Whittaker, Z. (2011, September 7). Cybercrime costs $338 bn to global economy; More lucrative than drugs trade. ZDNet. Available at www.zdnet.com

65. Yin, Z., Gong, X., Guo, P., & Wu, T. (2019). What drives entrepreneurship in digital economy? Evidence from China. *Economic Modelling*, *82*, 66–73. https://doi.org/10.1016/j.econmod.2019.09.026
66. Zhang, M. L., & Chen, M. S. (2019). *China's digital economy: Opportunities and risks* (Working Paper 2019(016)). International Monetary Fund. https://doi.org/10.5089/9781484389706.001
67. Zhao, F., Wallis, J., & Singh, M. (2015). E-government development and the digital economy: A reciprocal relationship. *Internet Research*, *25*(5), 734–766. https://doi.org/10.1108/IntR-02-2014-0055

UTJECAJ RAZINE DIGITALNOG RAZVOJA NA NACIONALNI INDEKS KIBERNETIČKE SIGURNOSTI

Antun Fagarazzi

Sažetak

Integracija digitalnog znanja i informacijske tehnologije u sve gospodarske sektore potaknuta je digitalnom revolucijom i industrijom 4.0. Također se pojavljuju kao primarni pokretač ekonomskog napretka u različitim nacijama. Glavni cilj istraživanja ovog rada je analizirati kako razina digitalnog razvoja utječe na Nacionalni indeks kibernetičke sigurnosti u različitim zemljama, kao i odrediti prosječnu razinu digitalnog razvoja i prosječnu vrijednost Nacionalnog indeksa kibernetičke sigurnosti za sve zemlje. U ovom istraživanju korišten je kvantitativni pristup uz korištenje sekundarnih podataka. Analiza je uključivala jednosmjernu ANOVA-u, linearnu regresiju, korelaciju i deskriptivnu statistiku. Studija je otkrila pozitivnu korelaciju između razine digitalnog razvoja (DDL) i nacionalnog indeksa kibernetičke sigurnosti (NCSI), kao i značajne razlike između ovih varijabli. Kvalitativni čimbenici, kao što su vladine politike, organizacijska kultura ili međunarodna suradnja, nisu uzeti u obzir u analizi. Rezultati naglašavaju potrebu za kontinuiranim ulaganjima u oba područja i važnost integriranih pristupa politikama koji se bave složenim izazovima digitalnog gospodarstva.

Ključne riječi: *razina digitalnog razvoja; nacionalni indeks kibernetičke sigurnosti; digitalna revolucija; Industrija 4.0.*