DOI: 10.55643/ser.3.53.2024.572

Vitaliia Koibichuk
Candidate of Economy Sciences, Associate Professor of the Economic Cybernetics Department, Sumy State University, Sumy, Ukraine;
ORCID: 0000-0002-3540-7922

Kateryna Slavhorodska
Student of the Economic Cybernetics Department, Sumy State University, Sumy, Ukraine;
ORCID: 0009-0005-3941-9100

Anastasiia Samoilikova
Candidate of Economy Sciences, Senior Lecturer of the Department of Financial Technologies and Entrepreneurship, Sumy State University, Sumy, Ukraine;
e-mail: a.samoilikova@biem.sumdu.edu.ua
ORCID: 0000-0001-8639-5282
(Corresponding author)

Tetyana Mayboroda
Candidate of Economy Sciences, Associate Professor of the Oleg Balatskyi Department of Management, Sumy State University, Sumy, Ukraine;
ORCID: 0000-0002-4547-5822

Artem Artyukhov
D.Sc. in Economics, Associate Professor of the Research Institute of Trade and Sustainable Business, University of Economics in Bratislava, Bratislava, Slovakia;
ORCID: 0000-0003-1112-6891

Received: 12/07/2024
Accepted: 18/09/2024
Published: 30/09/2024

THE INTERCONNECTION OF THE COUNTRY'S CYBER SECURITY AND INNOVATION POTENTIAL DURING INNOVATION TRANSFER AND IMPLEMENTATION

ABSTRACT

The article is devoted to the investigation of the relationship between innovation and cyber security in the context of forecasting and reducing risks related to cyber security during the implementation of innovations. The purpose of the study is to confirm and model the interconnection between the levels of innovation development and cyber security of the country. The work describes the concept of innovation risk and the importance of cyber security in the modern world as one of the important factors in overcoming innovation risks. The current state of cyber security was analysed based on various indices, and the impact of cyber threats on innovation processes was investigated based on a sample from 26 countries of the world. This made it possible to identify leaders and outsiders in this field, as well as trends in the development of cyber security in dynamics. It is well-founded that cyber security is a key factor for the development and implementation of innovations. To confirm the existing relationship between cyber security and innovation, the multiple correlation coefficient was calculated, and an econometric model was built using the built-in functions of MS Excel (the estimation of the model parameters was carried out using the method of least squares using the built-in "Data Analysis" package of the MS spreadsheet editor Excel for a multivariable linear model). The significance of the model was confirmed by the coefficient of determination, Fisher's test, and the level of significance of the p-value. The results of the study can be used to develop effective cyber defence strategies and contribute to the stable development of technologies in the face of growing cyber threats.

Keywords: business, cyber indices, digital transformation, government, information society, innovation, risk management

JEL Classification: D81, L86, O32

INTRODUCTION

Innovation is a key engine of economic and social progress, but its implementation is accompanied by numerous risks, especially cyber risks, which can lead to significant losses and negative consequences. The transfer and implementation of innovations, the development of which will allow countries to strengthen their competitive positions, is becoming an urgent problem in the modern information society.

The rapid development of technology and global digital transformation are creating unprecedented opportunities for innovation. However, in parallel with this, the number of cyber security threats is also increasing, which can significantly affect the success of innovation projects. Since innovation activity is accompanied by a high degree of risk, it is necessary to learn how to manage it and reduce its level.

Innovation risk is defined as the probability of an adverse situation or a deviation of the actual result from the planned during the implementation of innovation activity (at each of its stages during the development, implementation and use of innovations), which may cause unplanned losses arising from the investment of funds by the enterprise in the production of new goods or the provision of services, in the development of new equipment and technology, when investing in the development of management innovations that will not give the desired effect (Fishchenko & Khalaimova, 2011).

DOI: 10.55643/ser.3.53.2024.572

Given that innovation risks and cyber risks are closely related, cyber risks can have a significant impact on the success of innovation projects. Innovation often leads to the development of new products, services and technologies that provoke new vulnerabilities against cyber-attacks. Attackers can exploit these vulnerabilities to introduce system crash tools, etc.

For the implementation of innovations at enterprises to become more attractive, it is necessary to increase the level of cyber security and create conditions for its stable development. The unpredictability of cyber-attacks and their potential consequences for business, society and the state require the development of effective mechanisms for forecasting and risk management.

Thus, the study of cyber threat detection systems can contribute to the development of a complex threat forecasting model. The importance of the research lies, firstly, in the detailed analysis of the nature of innovations and the risks associated with their implementation, and secondly, in the development of a methodology for assessing and mitigating these risks with the help of cyber security. This includes integrating cyber threat and vulnerability data into innovation planning and forecasting processes, enabling adaptive risk management models to be created.

Therefore, the issue of developing an integrated approach to ensure the safe and effective implementation of innovation technologies, taking into account the dynamics and complexity of modern cyber threats, is an urgent issue in the context of creating effective cyber protection strategies, increasing the sustainability of innovation projects and ensuring the sustainable development of technologies in the face of the growth of cyber threats.

LITERATURE REVIEW

Separately, the issue of transfer and implementation of innovations and the issue of cyber security in the conditions of digital transformation and the formation of the information society are quite relevant and widely represented in the scientific literature. However, in their interrelationship, these issues still remain insufficiently researched.

Kia et al. (2024) concluded that all approaches in this context can be divided into two general categories: 1) approaches that aim to predict cyber incidents and risks in a specific individual system or network (Buczak & Guven, 2016; Khodabakhsh et al., 2020; Salfner et al., 2010; Sentuna et al., 2021); 2) approaches that explore the concept of cyber risk regardless of whether they focus on any specific application, system, or network ecosystem (Kia et al., 2024; Subroto & Apriyana, 2019). The ability to predict cyberattacks will significantly limit the socio-economic consequences of such events.

Other scholars pay attention to the issue of the interdependence of the level of cyber security and innovation development. A key result is that firms can effectively counter the negative consequences of cyber risks through innovation. Whether firms facing higher levels of cyber risk demonstrate greater innovativeness. In order to quantify the mechanisms considered in the work, an analysis was conducted on whether firms with increased cyber risk apply innovative practices related to cyber security. The growing threat of cybercrime is also driving innovation in security measures and systems, leading to technological advancements and potential long-term growth as security measures are developed in-house at digitally savvy companies. In fact, the risk of cybercrime motivates companies working with large volumes of data to actively implement digital innovations, which subsequently increases productivity in various aspects of their operations (Gomes et al., 2023a; Gomes et al., 2023b).

The work by Del Giorgio Solfa (2022) was devoted to assessing the impact of cyber security on digital operations and innovation. The results confirmed a significant positive relationship between cybersecurity and digital operations.

In this context, attention is also drawn to the new challenges of artificial intelligence, which consist of the balance between innovation and security. To remain competitive, organizations must encourage innovation, including the use of artificial intelligence as a business enabler. However, focusing solely on AI capabilities without addressing the associated cyber risks leaves organizations vulnerable. Cyber leaders are coming to a conclusion about the importance of security integration in innovative projects (Axon & Bouckaert, 2024).

Petroye et al. (2020) studied the impact on the image of the country of various informational factors in the economic, social, political, innovative and technological spheres, placing a special emphasis on intangible factors - informational influences, the development of technologies and innovations.

Lattanzio & Ma (2023) reasoned that the growth of cyber threats is changing corporate innovations and strategies. In particular, firms exposed to cyber threats are filing for simpler patents to accelerate their innovation cycle. This ultimately causes a significant decrease in companies' return on investment in research and development.

Aranha (2023) also investigated the impact of cybersecurity on innovation and strategy. Cyber threats can have a significant impact on innovation, especially in the tech industry: loss of intellectual property, damage to reputation, financial losses, compliance and regulatory fines, cyber security spending, difficulty in attracting customers and investors, etc.

Wang et al. (2024) considered the impact of cyber security risks on corporate innovation activities. Based on textual analysis and machine learning to estimate firms' prior cybersecurity risk for a sample of US companies, it was proven that cybersecurity risk is negatively associated with corporate innovation.

Despite the existing significant scientific output on the issues of innovation development and national security, including cyber security, the issue of empirical confirmation of relationships, modelling and impact assessment between the studied indicators remains relevant and requires further scientific development and clarification.

AIMS AND OBJECTIVES

The purpose of the study is to confirm and model the relationship between the levels of innovative development and cyber security in the country.

METHODS

In order to build a model that determines the impact of cyber security on the innovation potential of countries, a comprehensive analysis of the current state of cyber security was carried out, where cyber indexes were studied, which provide an assessment of the level of cyber security in different countries of the world. The indicators of the Global Innovation Index, which provides an assessment of the innovation potential of the countries of the world, were also studied.

26 countries were taken for analysis. It includes USA, China, UK, Australia, Netherlands, France, Germany, Ukraine, Canada, North Korea, Spain, Japan, Singapore, New Zealand, Israel, Sweden, Saudi Arabia, Switzerland, Turkey, Egypt, Estonia, India, Italy, Malaysia, Lithuania, and Brazil. Such a composition of countries was chosen due to the fact that they represent different levels of economic development, geographical regions and political systems. This approach makes it possible to identify general trends and specific features of the impact of cyber security on innovation in different contexts. In addition, the sample includes leading countries in the field of innovation (USA, China, Israel), as well as countries with different levels of cyber security development (Ukraine, India), which allows us to compare their experience and identify best practices.

A comparative analysis of current state of cyber security was conducted on the basis of the National Cyber Power Index (NCPI) 2022 (Voo et al., 2022), the Global Cyber Security Index (GCI) 2020 (ITU, 2021; European Commission, n.d.b), the Cybersecurity Exposure Index (CEI) 2020 (PasswordManagers.co, n.d.), and the Cyber Defence Index (CDI) 2022 (European Commission, n.d.a).

Analysis of the NCPI allows us to measure the cyber capabilities of the countries of the world. The NCPI is measured by the Belford Centre, a Centre for Science and International Affairs at the John F. Kennedy School of Government at Harvard University. The Belford Centre was created to protect the nation's infrastructure from cyberattacks and combat conflicts in cyberspace. The definition of the cyber power index is carried out in the context of 7 national goals, using 32 indicators of intentions and 27 indicators of capabilities of the analysed countries. The national targets that the NCPI has identified for surveillance of cyber-harassed countries are as follows: 1) observation and monitoring of internal groups; 2) strengthening and improvement of national cyber defence; 3) control and manipulation of the information environment; 4) collection of foreign intelligence in the interests of national security; 5) commercial benefit or promotion of the growth of domestic industry; 6) destruction or disabling of the enemy's infrastructure and potential; 7) definition of international cyber norms and technical standards (Voo et al., 2022).

The NCPI measures the effectiveness of government strategy, crime response and countermeasures, defence capabilities, resource allocation, private sector participation, workforce effectiveness, and cybersecurity innovation. The assessment is simultaneously a measurement of the proven strength and potential, as well as the effectiveness of using these opportunities by the government of each country participating in the rating (Voo et al., 2022).

In turn, the analysis of the indicator of the current version of the GCI allows to compare the level of cyber security of different countries, to identify countries that are leading or lagging behind in the field of cyber security, to identify trends in the development of cyber security in dynamics, to assess the impact of cyber security on innovation activity thanks to

DOI: 10.55643/ser.3.53.2024.572

the assessment of the level of cyber security of the countries of the world based on 5 main components (legal, technical, organizational, potential of human resources, level of awareness) (ITU, 2021).

Analysis of the CEI is also important. It calculates a country's level of vulnerability to cybercrime on a scale of 0 to 1. The higher the score, the higher the level of vulnerability. To identify countries that are most and least prone to cybercrime, data was collected on the five most common types of cyberattacks on endpoints and cloud services, as well as the level of commitment to cyber security in countries around the world. These data provide the most up-to-date information on which countries are most vulnerable, least vulnerable, and which are in between (PasswordManagers.co, n.d.).

In addition, one of the main indicators for analysing the current state of cyber security is the CDI. It measures the extent to which the world's 20 largest and most digitally advanced economies have implemented technologies and digital practices to counter cyberattacks, and how effectively their governments and political structures promote the cybersecurity of digital transactions (European Commission, n.d.a).

Also, to analyse the relationship between the state of cyber security and innovation potential, the indicator of the Global Innovation Index was considered. It was prepared under the overall leadership of WIPO Director General Daren Tan, the WIPO IP and Innovation Ecosystems Sector led by Marco Aleman, Deputy Director General, and the Department of Economics and Data Analysis led by Karsten Fink, Chief Economist. The Global Innovation Index (GII) is a comprehensive indicator that measures the innovative potential and performance of countries in various fields. The index is developed and published annually by the World Intellectual Property Organization (WIPO) in cooperation with other international organizations and institutions. Its calculation uses data from a wide range of sources, including economic statistics, indicators of scientific and technical development, level of education, infrastructure, access to information and communication technologies, business environment and other factors (Dutta et al., 2022). In carrying out the research, it will help to assess how the innovative activity of countries correlates with the level of cyber security, which will allow to identify weak points and potential risks, as well as to develop strategies to increase the efficiency of innovation processes by strengthening cyber security.

To confirm the existing relationship between cyber security and innovation, the multiple correlation coefficient was calculated and an econometric model was built using the built-in functions of MS Excel (the estimation of model parameters according to the main indicators of cyber security and innovation development was carried out using the method of least squares using the built-in package "Data analysis" of the MS Excel table editor as for the usual multivariate linear model). The significance of the model was confirmed by the coefficient of determination, the Fisher test and the level of significance of the p-value.

RESULTS

Firstly, a comparative analysis of the current state of cyber security was conducted with the help of indices: the National Cyber Security Index and the Cyber Defence Index. The results of the analysis of 26 countries are presented in Figure 1.

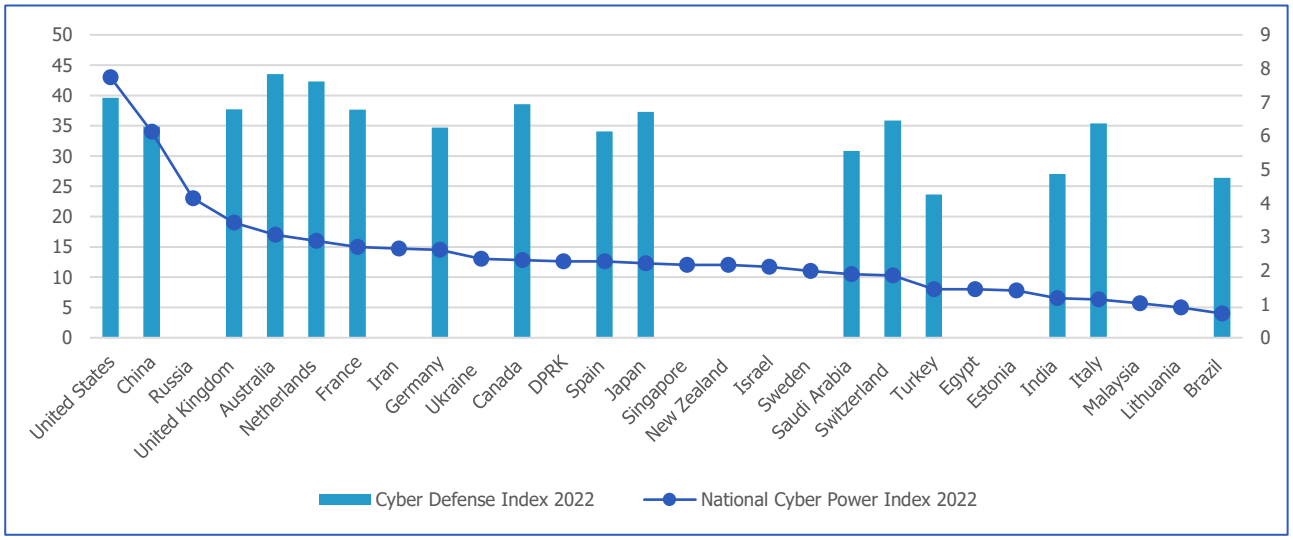

Figure 1. The results of the comparative analysis of the current state of cyber security. *(Source: built by the authors based on (Voo et al., 2022; European Commission, n.d.a))*

Based on the data in Figure 1, it can be said that the high values of the NCPI indicate significant potential in cyberspace. The USA (43) and China (34) have the highest values, indicating their considerable cyber power. Countries with a high NCPI usually invest in innovative technologies and cyber defence, which contributes to their innovation development. In addition, the CDI country scores indicate that Australia (7.83), the Netherlands (7.61), and the United States (7.13) have high CDI values, indicating their effective cyber defences. A high level of cyber defence contributes to stable innovative development, as it reduces the risks associated with cyber threats. In general, effective cyber defences and high cyber strength are critical to the innovative development of countries, as they reduce the risks associated with cyber threats and allow them to focus on technological progress.

Given that the Global Cybersecurity Index (GCI) provides a detailed cross-section of a country's cybersecurity, covering legal, technical, and organizational aspects, human capital potential, and cybercrime levels, it is an indispensable tool for exploring the relationship between cybersecurity and innovation. So, it is appropriate to investigate its data by country. The corresponding data collection results are presented in Figure 2.

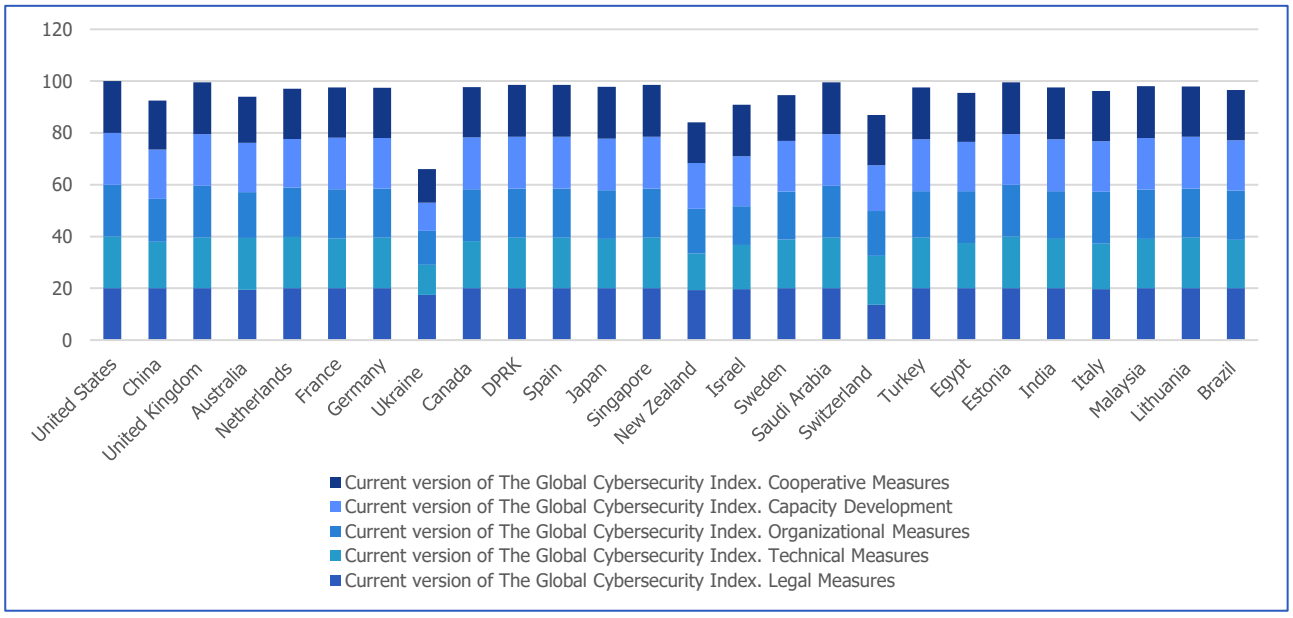

Figure 2. The results of comparative analysis of the GCI blocks. *(Source: built by the authors based on (European Commission, n.d.b))*

Based on the data in Figure 2, it can be concluded that the overall GCI score shows the overall state of cyber security in the country. The USA has the highest score (100), indicating its leading role in global cyber security. The UK (99.54) also scores highly, confirming its strong position in cyber security. The Legal Measures indicator shows that all countries have maximum scores (20), which indicates a high level of legal measures in the field of cyber security. The Technical Measures indicator presents high results for the USA (20), and the UK (19.54), but Ukraine (11.6) with lower scores may face technical challenges in the field of cyber security. The Organizational Measures indicator shows high scores in the USA (20), the UK (20), and Israel (15.02), but Ukraine (13.06) has lower scores, which may indicate a need to improve organizational structures. In addition, the Capacity Development indicator evaluates measures for the development of potential in the field of cyber security. The USA (20), the UK (20), and Canada (20) demonstrate the highest level of capacity development, while Ukraine (10.94) needs further capacity development. In the Cooperative Measures indicator, the United States (20), the UK (20), and Canada (19.41) demonstrate a high level of cooperation, but Ukraine (12.97) has lower scores, which may indicate insufficient international cooperation. The high overall GCI scores for countries like the USA, and the UK reflect their comprehensive approach to cyber security, including legal, technical, institutional measures and international cooperation. Legal measures are a strength of most countries, providing a solid legal framework to combat cyber threats. Some countries, such as Ukraine, may need to improve technical and organizational measures to provide better protection against cyber threats. Capacity building and international cooperation are critical to long-term cybersecurity, especially for low-performing countries. Effective cyber security and cooperation at the international level contribute to innovation development, as they ensure the protection of technological innovations and reduce the risks of cyber threats.

Whereas the CEI focuses on countries' vulnerabilities to cyberattacks, providing a quantitative assessment of risk, the GCI offers a broader view, assessing various aspects of cybersecurity, including legal, technical and organizational measures.

DOI: 10.55643/ser.3.53.2024.572

Comparing these two indices allows you to get a more complete picture of cyber threats and identify weak points in the cyber defence of different countries. The CEI data analysis is presented in Figure 3.

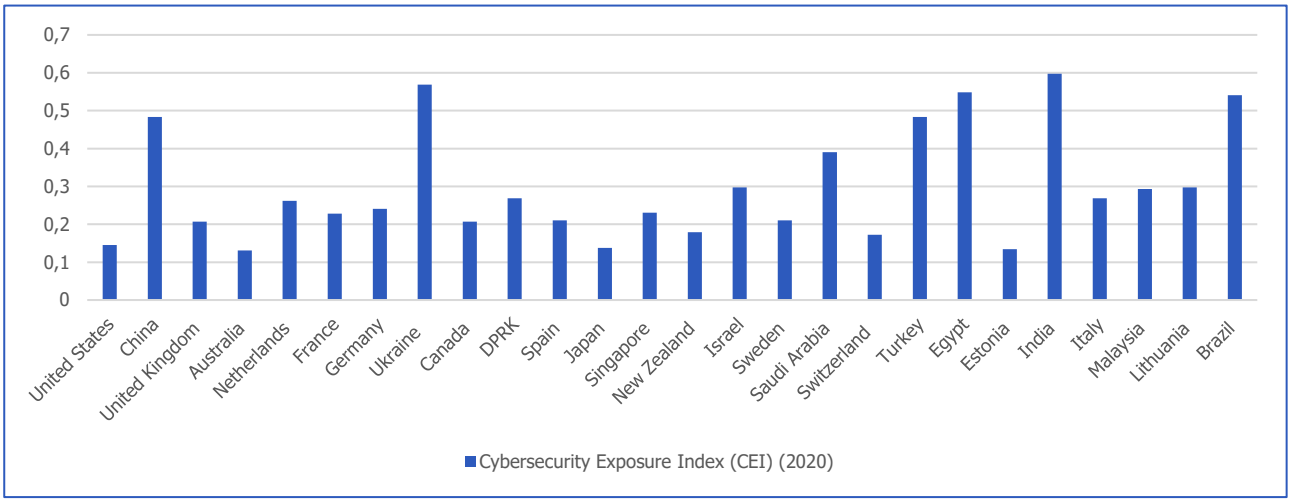

Figure 3. The results of the cross-country analysis of CEI. *(Source: built by the authors based on (PasswordManagers.co, n.d.))*

Based on the data in Figure 3, Australia (0.131), Japan (0.138), USA (0.145), and New Zealand (0.179) have the lowest CEI values. This indicates their high level of cyber security and relatively low risk of cyber-attacks. India (0.597), Ukraine (0.569), and Brazil (0.541) show the highest levels of vulnerability, indicating the need to strengthen cyber security measures. In general, the CEI data shows that countries with high index values have a higher risk of cyber threats and need to improve their cyber security systems. Countries with low CEI scores may be more vulnerable to cyber-attacks.

Comparing the two indicators analysed above, countries with a low CEI (low vulnerability), such as the USA (0.145), Japan (0.138), and Australia (0.131), have high overall GCI scores, indicating strong cybersecurity. Estonia (CEI 0.134), despite low vulnerability, has a high overall GCI score (99.48), highlighting its well-developed cybersecurity. India (0.597), Ukraine (0.569), and Brazil (0.541) have high CEI values, indicating high vulnerability. However, India (GCI 97.49) and Brazil (GCI 96.6) score high on the GCI, which may indicate that they are already taking steps to strengthen cybersecurity. Ukraine shows the lowest overall GCI score (65.93), which may explain its high CEI (0.569). In general, countries with high GCI scores have low CEI values, indicating that strong cybersecurity (according to the GCI) reduces vulnerability (according to the CEI). Meanwhile, countries with high CEI have significant differences in GCI scores, which may indicate that their cybersecurity efforts are not yet fully reflected in their actual security.

To evaluate the innovation development of 26 countries, the data of the Global Innovation Index was analysed. The relevant results are presented in Figure 4.

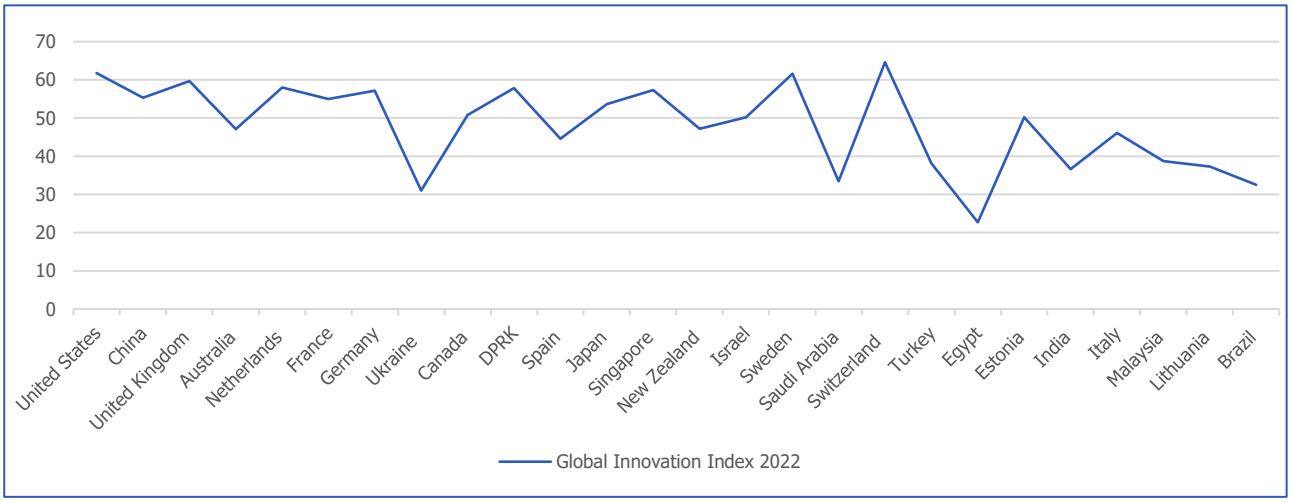

Figure 4. The results of the cross-country analysis of GII. *(Source: built by the authors based on (Dutta et al., 2022))*

From the data in Figure 4, it was concluded that high values of the GII indicate a high level of innovation activity. The USA (61.8), Switzerland (64.6), Sweden (61.6) and the UK (59.7) have the highest scores, indicating their leadership innovation potential. China (55.3) and France (55) also score highly, highlighting their strong innovation economies. Ukraine (31) has lower indicators, which may indicate certain difficulties in the development of innovations.

Overall, effective cybersecurity is a factor in promoting innovation, providing a secure environment for the development of new technologies, and protecting intellectual property.

When conducting a comparative analysis on the level of cyber security and innovation, it is worth noting that the USA, Switzerland, and Sweden have high scores in both the Global Innovation Index and the Global Cyber Security Index). This shows that advanced cyber security promotes innovation, ensuring the protection of intellectual property and creating a safe environment for the development of new technologies. The UK and the Netherlands also score highly in both indices, underscoring the importance of cyber security in supporting innovation. Ukraine has a low Global Innovation Index (31) and a high Cyber Exposure Index (0.569), highlighting the need to improve cyber security to stimulate innovation. Canada (50.8), Israel (50.2), and Japan (53.6) have a high level of cybersecurity, but their innovation scores do not reach the level of the leaders. This may indicate that, despite strong cybersecurity, other factors such as research funding, regulatory barriers, or insufficient support for startups may be affecting their innovation capacity. So, countries with high GII and GCI scores show that strong cyber security is a key condition for innovation. These countries invest in protecting their digital infrastructure, which allows for the safe introduction of new technologies and the development of startups. Countries with low GII scores and high CEI values face cybersecurity challenges that can hinder their innovative development. Investing in cybersecurity can help these countries improve their innovation performance. Countries with high cybersecurity scores but an average GII have the potential to improve innovation performance by increasing research funding, supporting startups, and overcoming regulatory barriers.

So, based on data analysis, cyber security is a key factor for the development and implementation of innovations in the modern world. Innovation, as a rule, involves the development of new technologies and systems, which are often the target of cyber-attacks. Cybersecurity, on the other hand, protects these innovations, allowing them to grow and thrive. Thus, innovation drives the development of cyber threats, and cyber security is a prerequisite for successful innovation. It is an interactive process where the development of one aspect affects the development of another.

To confirm the existing relationship between cyber security and innovation, an econometric model was developed using the built-in functions of MS Excel. In order to confirm the connection between cyber security and innovation, as well as to establish the existing correlation, the coefficient of multiple correlation was calculated:

$$r = \frac{\sum_{i-1}^{n}(y_i-\overline{y})(\hat{y_i}-\overline{\hat{y}})}{\sqrt{\sum_{i-1}^{n}(y_i-\overline{y})^2}\sqrt{\sum_{i=1}^{n}(\hat{y_i}-\overline{\hat{y}})^2}} \quad (1)$$

where y_i is the actual (statistical) value of cyber security; $\hat{y_i}$ – calculated cyber security values.

Using standard MS Excel built-in functions, the correlation coefficient between cybersecurity and innovation was determined to be 0.49. Therefore, the conducted research revealed a strong correlation between the level of cyber security and the amount of innovation. This means that increasing the security level of information systems has a positive effect on the innovative activity of countries.

To analyse the relationship between cyber security and innovation, the main indicators in these two areas were selected - the NCPI and the GII (Table 1). These indicators are key to understanding how the level of cyber security affects innovation and vice versa.

The selected cyber security index became the basis for determining the impact on innovative development based on a pairwise regression: $y_t = \beta_0 + \beta_1 x_1 + \varepsilon$, where β_j are the parameters of the model for the independent variable; x_1 – innovation index; ε is the stochastic component of the model.

Table 1. Initial data for building an econometric model based on the main indices of cyber security and innovation. *(Source: generalized by the authors based on (Voo et al., 2022; Dutta et al., 2022))*

Country	National Cyber Power Index 2022	Global Innovation Index 2022
United States	43	61.8
China	34	55.3
United Kingdom	19	59.7
Australia	17	47.1

DOI: 10.55643/ser.3.53.2024.572

Netherlands	16	58
France	15	55
Germany	14.5	57.2
Ukraine	13	31
Canada	12.8	50.8
DPRK	12.6	57.8
Spain	12.6	44.6
Japan	12.3	53.6
Singapore	12	57.3
New Zealand	12	47.2
Israel	11.7	50.2
Sweden	11	61.6
Saudi Arabia	10.5	33.4
Switzerland	10.3	64.6
Turkey	8	38.1
Egypt	8	22.70
Estonia	7.8	50.2
India	6.5	36.6
Italy	6.3	46.1
Malaysia	5.7	38.7
Lithuania	5	37.3
Brazil	4	32.5

Estimation of the parameters of the model according to the main indicators of cyber security and innovation was carried out using the method of least squares using the built-in package "Data analysis" of the spreadsheet editor MS Excel as for the usual multivariable linear model (Figure 5).

Summarizing the results

Regression statistics	
Multiple R	0.49872375
R-square	0.24872538
Normalized R square	0.21742227
Standard error	7.49079937
Observations	26

Analysis of variance

	df	*SS*	*MS*	*F*	*The signifi-cance of F*			
Regression	1	445.8501969	445.8501969	7.945708582	0.009504171			
Residual	24	1346.689803	56.11207513					
Total	25	1792.54						
	Coefficients	*Standard error*	*t-statistics*	*P-value*	*The bottom 95%*	*The top 95%*	*The bottom 95%*	*The top 95%*
Y-section	-5.0095563	6.590354127	-0.760134614	0.454577144	-18.6113787	8.592266	-18.6114	8.592266
Change X1	0.377116154	0.133801531	2.818813329	0.009504171	0.101008751	0.653314	0.101009	0.653314

Figure 5. Results of calculations in the "Data Analysis" package for the distribution-lag model.

Given the above, the estimated equation of which has the form:

$$y_{i=} - 5{,}0095562 + 0{,}37716153x_1 + \varepsilon\,. \qquad (2)$$

The built econometric model is adequate, since the coefficient of determination R2=0.24 (Figure 4), while 24.8 % of changes in innovations depend on changes in cyber security. The model is statistically significant according to Fisher's test and p-value.

Therefore, the correct assessment of risks related to cyber security is an integral part of the successful implementation of new innovative projects.

The study shows that cyber risks and innovation risks are closely related. The implementation of new technologies and services often reveals new vulnerabilities that can be used by attackers to steal intellectual property or destroy systems. Thus, the development of cyber risk prediction models can help in innovation risk management.

DISCUSSION

The econometric model (2) demonstrates that cyber security is a significant factor influencing the level of innovation. By regulating the level of cyber security, it is possible to directly influence the innovative activity of the economy. This model can be used as a basis for the development of effective measures to improve cyber security, which, in turn, minimizes risks for innovative projects and stimulates their development.

Petroye et al. (2020) thanks to correlation and cluster analysis, also determined interdependencies between some indicators, connected with informational influences, the development of technologies and innovations, however different from those studied in this article.

Innovation creates new opportunities for development but also opens new vectors for cyber-attacks. On the other hand, cyber security is a necessary condition for the successful implementation of innovations, as it ensures the protection of intellectual property and critical infrastructure.

The available annual statistical data on the level of cyber security and innovation development allow for a detailed analysis of the relationships between various variables, such as technological achievements, the amount of investment in innovation, the frequency of cyber threats, and other factors that affect the dynamics of these two areas. This data will be used to develop a model that will help predict the behaviour of the technology market and determine effective strategies for managing security and stimulating innovation.

DOI: 10.55643/ser.3.53.2024.572

The results of the analytical and empirical research will contribute to the further development of a model for forecasting innovation risks related to cyber security of countries, which will allow companies and organizations to assess the risks of cyber-attacks at the early stages of innovative projects and develop effective measures for cyber security and identify ways to overcome risks in forecasting innovations.

CONCLUSIONS

The analysis of the relationship between the state of cyber security and innovation potential made it possible to draw conclusions about how cyber security affects the innovation activity of countries. The economic, social and political consequences of high and low levels of cyber security and innovation potential of countries around the world were explored during the study of this relationship and influence on each other. It has been confirmed that cyber security is a key factor for the development and implementation of innovations in the modern world. Innovation, as a rule, involves the development of new technologies and systems, which are often the target of cyber-attacks. Cybersecurity, on the other hand, protects these innovations, allowing them to grow and thrive. Thus, innovation drives the development of cyber threats, and cyber security is a prerequisite for successful innovation. It is an interactive process where the development of one aspect affects the development of another.

Existing cyber defence models and methods emphasize the importance of quickly identifying and responding to new vulnerabilities to minimize the negative effects of cyber threats. The analysis of the cyber security index and the global innovation index shows the importance of integrating cyber security in the process of planning and implementing innovations. Countries with high levels of cyber security typically also demonstrate high levels of potential for innovation. This shows that investing in cyber security not only protects against risk but also promotes innovation. For example, the USA and China have a high cyber security index, which helps them support and develop innovative technologies. Effective cyber defence strategies must be integrated into all phases of innovation. This includes the use of specialized monitoring systems, analysis of large volumes of data with the help of artificial intelligence, methods of detecting signature attacks, regular analysis of vulnerabilities and development of new protection policies. As a result, improving cyber security will contribute to the successful implementation of innovative projects, increase their resistance to cyber threats and ensure the stable development of technologies.

Therefore, based on the conducted analysis, it is possible to propose ways to overcome the risks of introducing innovations by strengthening the level of cyber security of countries:

1. Strategic directions such as integration of cyber security into the innovation strategy; inclusion of cyber security in the early stages of development of innovation products and services; conducting regular cyber security risk assessments for new projects; development of response plans for cyber security incidents.
2. Investments in cyber security technologies: use of modern intrusion detection and data protection systems; application of artificial intelligence methods for threat analysis; regular updating of software and operating systems.
3. State support, namely the creation of a favourable legislative environment, development of clear and understandable laws regulating cyber security and financing of research in the field of cyber security, and training of personnel.

The model of overcoming the risks of innovation with the help of cyber security requires a comprehensive approach that includes not only technical measures but also a change in the culture of the organization and cooperation with external partners. It is important to understand that cyber security is not a static state, but an ongoing process that requires constant adaptation to new threats. The proposed ways of overcoming innovation risks are universal and can be adapted to the specific needs of each organization.

ADDITIONAL INFORMATION

AUTHOR CONTRIBUTIONS

All authors have contributed equally.

FUNDING

This research was funded by the Ministry of Education and Science of Ukraine and performed the results of the project «Business-Education-Science Coopetition: Institutional and Economic Models of Innovation Transfer for National Security and Sustainable Development» (№ 0122U000772).

CONFLICT OF INTEREST

The Authors declare that there is no conflict of interest.

REFERENCES

1. Aranha, V. (2023). The Impact of Cybersecurity on Tech Industry Innovation and Strategy. Retrieved from https://medium.com/coinmonks/the-impact-of-cybersecurity-on-tech-industry-innovation-and-strategy-f32c26cc13d3
2. Axon, L., & Bouckaert, J. (2024). The new AI imperative is about balancing innovation and security. WEF Centre for Cybersecurity. Retrieved from https://www.weforum.org/agenda/2024/09/why-the-new-ai-imperative-is-balancing-innovation-and-security/
3. Buczak, A. L. & Guven, E. (2016). A survey of data mining and machine learning methods for cyber security intrusion detection. *IEEE Communications Surveys & Tutorials, 18*(2), 1153-1176. https://doi.org/10.1109/COMST.2015.2494502
4. Del Giorgio Solfa, F. (2022). Impacts of Cyber Security and Supply Chain Risk on Digital Operations: Evidence from the Pharmaceutical Industry. *International Journal of Technology, Innovation and Management (IJTIM), 2*(2), 18-32. Retrieved from https://www.aacademica.org/del.giorgio.solfa/412.pdf
5. Dutta, S., Lanvin, B., León, L. R., & Wunsch-Vincent, S. (2022). Global Innovation Index 2022. What is the future of innovation driven growth? WIPO, 15th Edition, 226 p. Retrieved from https://www.wipo.int/edocs/pubdocs/en/wipo-pub-2000-2022-en-main-report-global-innovation-index-2022-15th-edition.pdf
6. European Commission (n.d.a). Cyber Defence Index 2022. Composite Indicators and Scoreboards. Retrieved from https://composite-indicators.jrc.ec.europa.eu/explorer/explorer/indices/cdfi/cyber-defense-index
7. European Commission (n.d.b). Global Cybersecurity Index. Composite Indicators and Scoreboards. Retrieved from https://composite-indicators.jrc.ec.europa.eu/explorer/explorer/indices/GCI/global-cyber-security-index
8. Fishchenko, O. M., & Khalaimova, A. V. (2011). Osoblyvosti otsinyuvannya innovatsiynykh ryzykiv. *Marketing and innovation management, 2*(4), 53–57. Retrieved from https://mmi.sumdu.edu.ua/wp-content/uploads/mmi/volume-2-issue-4-part-2/mmi2011_4_2_52_57.pdf
9. Gomes, O., Mihet, R., & Rishabh, K. (2023a). Cyber Risk-Driven Innovation in the Modern Data Economy. Retrieved from https://www.tse-fr.eu/sites/default/files/TSE/documents/conf/2024/digital/mihet.pdf
10. Gomes, O., Mihet, R., & Rishabh, K. (2023b). Data Risk, Firm Growth, and Innovation. Swiss Finance Institute Research Paper, 23-86. http://dx.doi.org/10.2139/ssrn.4559921
11. ITU (2021). Global Cybersecurity Index 2020. Measuring commitment to cybersecurity. Retrieved from https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf
12. Khodabakhsh, A., Yayilgan, S.Y., Abomhara, M., Istad, M., & Hurzuk, N. (2020). Cyber-risk identification for a digital substation. Proceedings of the 15th international conference on availability, reliability and security, 1-7. https://doi.org/10.1145/3407023.3409227
13. Kia, A. N., Murphy, F., Sheehan, B., & Shannon, D. (2024). A cyber risk prediction model using common vulnerabilities and exposures. *Expert Systems with Applications, 237* (B), art. 121599. https://doi.org/10.1016/j.eswa.2023.121599
14. Lattanzio, G., & Ma, Yu. (2023). Cybersecurity risk and corporate innovation. *Journal of Corporate Finance, 82*, art. 102445. https://doi.org/10.1016/j.jcorpfin.2023.102445
15. PasswordManagers.co (n.d.). Cybersecurity Exposure Index (CEI) 2020. Retrieved from https://passwordmanagers.co/cybersecurity-exposure-index/#europe
16. Petroye, O., Lyulyov, O., Lytvynchuk, I., Kozar, Yu., & 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
17. Salfner, F., Lenk, M., & Malek, M. (2010). A survey of online failure prediction methods. *ACM Computing Surveys, 42*(3), 10. https://doi.org/10.1145/1670679.1670680
18. Sentuna, A., Alsadoon, A., Prasad, P., Saadeh, M., & Alsadoon, O. H. (2021). A novel enhanced naïve bayes posterior probability (ENBPP) using machine learning: Cyber threat analysis. *Neural Processing Letters, 53*(1), 177-209. https://doi.org/10.1007/s11063-020-10381-x
19. Subroto, A., & Apriyana, A. (2019). Cyber risk prediction through social media big data analytics and statistical machine learning. *Journal of Big Data, 6*(1), 1-19. https://doi.org/10.1186/s40537-019-0216-1

DOI: 10.55643/ser.3.53.2024.572

20. Voo, J., Hemani, I., & Cassidy, D. (2022). National Cyber Power Index 2022. Report. Retrieved from https://www.belfercenter.org/sites/default/files/pantheon_files/files/publication/CyberProject_National%20Cyber%20Power%20Index%202022_v3_220922.pdf

21. Wang, J., Ho, C. Ye. (C), & Shan, Yu. G. (2024). Does cybersecurity risk stifle corporate innovation activities? *International Review of Financial Analysis, 91*, art. 103028. https://doi.org/10.1016/j.irfa.2023.103028

Койбічук В., Славгородська К., Самойлікова А., Майборода Т., Артюхов А.

ВЗАЄМОЗВ'ЯЗОК КІБЕРБЕЗПЕКИ ТА ІННОВАЦІЙНОГО ПОТЕНЦІАЛУ КРАЇНИ ПІД ЧАС ТРАНСФЕРУ ТА ВПРОВАДЖЕННЯ ІННОВАЦІЙ

Стаття присвячена дослідженню взаємозв'язку між інноваціями й кібербезпекою в контексті прогнозування та зменшення ризиків, пов'язаних із кібербезпекою під час упровадження інновацій. Метою дослідження є підтвердження та моделювання взаємозв'язку між рівнями інноваційного розвитку й кібербезпеки країни. У роботі охарактеризовано поняття інноваційного ризику та важливості кібербезпеки в сучасному світі, як одного з важливих факторів подолання інноваційних ризиків. Проаналізовано сучасний стан кібербезпеки на основі різних індексів і досліджено вплив кіберзагроз на інноваційні процеси на основі вибірки з 26 країн світу. Це дозволило виявити лідерів та аутсайдерів у цій царині, а також тенденції розвитку кібербезпеки в динаміці. Обґрунтовано, що кібербезпека є ключовим фактором для розвитку та впровадження інновацій. Для підтвердження наявного взаємозв'язку між кібербезпекою й інноваціями було розраховано коефіцієнт множинної кореляції та побудовано економетричну модель за допомогою вбудованих функцій MS Excel (оцінювання параметрів моделі здійснене з допомогою методу найменших квадратів із використанням вбудованого пакета «Аналіз даних» табличного редактора MS Excel для багатофакторної лінійної моделі). Значущість моделі підтверджено за коефіцієнтом детермінації, критерієм Фішера та рівнем значущості p-value. Результати дослідження можуть бути використані для розробки ефективних стратегій кіберзахисту та сприяти стабільному розвиткові технологій в умовах зростання кіберзагроз.

Ключові слова: бізнес, інновації, інформаційне суспільство, кіберіндекси, ризик-менеджмент, уряд, цифрова трансформація

JEL Класифікація: D81, L86, O32