T. Kijek, P. Bolibok, A. Matras-Bolibok, *Innovation and cybersecurity resilience in Central and Eastern Europe: An empirical analysis*,
„Yearbook of the Institute of East-Central Europe", 23 (2025), issue 3, pp. 195–216,
DOI: https://doi.org/10.36874/RIESW.2025.3.10

*Tomasz Kijek**
*Piotr Bolibok***
*Anna Matras-Bolibok****

Innovation and cybersecurity resilience in Central and Eastern Europe: An empirical analysis

Innowacyjność a cyberbezpieczeństwo w Europie Środkowo-Wschodniej. Analiza empiryczna

ABSTRACT:
The paper aims to investigate the relationship between economic innovativeness and cybersecurity performance in the context of Central and Eastern European Countries (CEECs). Using a panel dataset for eleven CEECs over the 2014–2024 period, the empirical approach combines the Global Cybersecurity Index by the International Telecommunication Union, the European Innovation Scoreboard Summary Innovation Index, and an originally developed composite ICT Innovation Performance Index based on patent activity, R&D sector performance, and firm-level innovation metrics. The model is estimated using a Tobit regression with random effects, controlling for GDP per capita and tertiary education attainment. The results support the developed hypotheses, suggesting that general innovativeness is negatively associated with cybersecurity performance, whereas ICT-sector-specific innovation

* Dr hab. Tomasz Kijek – prof. UMCS, Department of Microeconomics and Applied Economics, Maria Curie-Sklodowska University, Poland, ORCID: https://orcid.org/0000-0002-0134-4943, e-mail: tomasz.kijek@umcs.pl.
** Dr Piotr Bolibok – Department of Economic Policy and Banking, The John Paul II Catholic University of Lublin, Poland, ORCID: https://orcid.org/0000-0002-5649-181X, e-mail: piotr.bolibok@kul.pl.
*** Dr Anna Matras-Bolibok – Department of Microeconomics and Applied Economics, Maria Curie-Sklodowska University, Poland, ORCID: https://orcid.org/0000-0001-9646-4472, e-mail: anna.matras@umcs.pl.

performance improves national cybersecurity resilience. These findings offer relevant implications for the innovation policies and digitalisation strategies of CEECs. In this light, innovation policy should prioritise investments in cybersecurity R&D and cross-sectoral technology transfer mechanisms that strengthen digital resilience. As digital transformation accelerates, these policy dimensions become not only complementary but also essential for sustainable, innovation-led growth in the region.

KEYWORDS:
cybersecurity, innovation, innovativeness, ICT, CEECs

STRESZCZENIE:
Celem artykułu jest analiza zależności między innowacyjnością gospodarki a poziomem bezpieczeństwa cybernetycznego w krajach Europy Środkowo-Wschodniej (EŚW). Do analizy wykorzystano zbiór danych panelowych obejmujący 11 krajów EŚW w latach 2014–2024, zawierający wskaźniki Global Cybersecurity Index opracowany przez International Telecommunication Union, Summary Innovation Index Europejskiego Rankingu Innowacyjności oraz autorsko skonstruowany syntetyczny Indeks Innowacyjności Sektora ICT, oparty na aktywności patentowej, działalności sektora B+R oraz aktywności innowacyjnej przedsiębiorstw. Model oszacowano za pomocą regresji tobitowej z efektami losowymi oraz zmiennymi kontrolnymi: PKB per capita i odsetkiem ludności z wykształceniem wyższym. Rezultaty empiryczne potwierdzają postawione hipotezy, wykazując, że ogólna innowacyjność gospodarki jest negatywnie skorelowana z poziomem cyberbezpieczeństwa, natomiast innowacyjność sektora ICT wzmacnia odporność cybernetyczną na poziomie krajów. Uzyskane wyniki niosą istotne implikacje dla polityk innowacyjnych oraz strategii cyfryzacji gospodarek krajów EŚW. W ich świetle polityka innowacyjna powinna w sposób priorytetowy wspierać inwestycje w B+R w obszarze cyberbezpieczeństwa oraz rozwijać mechanizmy międzysektorowego transferu technologii, wzmacniając odporność cyfrową. W warunkach postępującej transformacji cyfrowej, wspomniane wymiary polityki stają się nie tylko komplementarne, lecz również kluczowe dla zapewnienia trwałego, innowacyjnego wzrostu gospodarczego w regionie.

SŁOWA KLUCZOWE:
cyberbezpieczeństwo, innowacje, innowacyjność, ICT, EŚW

Introduction

Innovation is widely recognized as a cornerstone of economic progress[1]. By accelerating productivity, enhancing competitiveness, and opening new markets, it constitutes a key driver of sustainable long-run growth. With the rise of the digital age, innovation processes across nearly all sectors have become increasingly intertwined with information and communication technologies (ICT). On the one hand, ongoing digitalisation is fundamentally transforming the mechanisms behind technological and organisational advancement, as data emerge as crucial inputs to innovation activities[2]. On the other hand, the outputs of these activities are not only supported by ICT but often heavily dependent on its functionalities.

This trajectory, however, entails significant risks. As economies adopt digital technologies and embed advanced innovations across sectors, they become increasingly vulnerable to cybersecurity threats[3]. Paradoxically, the very processes that drive modernisation can also expose national infrastructures to digital vulnerabilities.

This paper argues that while general innovativeness tends to expand the digital attack surface, ICT-specific innovation – particularly in cybersecurity – plays a vital role in mitigating these threats. Recognising and managing this paradox is essential for fostering sustainable and secure development.

A particularly compelling context for an empirical investigation of the links between innovation and cybersecurity at the national level is provided by the post-transition economies of Central and Eastern Europe (CEECs). First, because their development trajectories – aimed at closing the innovation gap with more advanced economies – have been increasingly reliant on

1 R.M. Solow, *A Contribution to the Theory of Economic Growth*, "The Quarterly Journal of Economics" 1956, vol. 70, no. 1, pp. 65–94. DOI: 10.2307/1884513.

2 OECD, *Innovation policies in the digital age*, 2018, https://www.oecd.org/en/publications/innovation-policies-in-the-digital-age_eadd1094-en.html.

3 D. Botha-Badenhorst, *Navigating the Intersection of Innovation and Cybersecurity: A Framework*, "European Conference on Research Methodology for Business and Management Studies" 2023, vol. 22, no. 1, DOI: 10.34190/ecrm.22.1.1490.

digital technologies[4]. Second, in recent years, they have faced heightened cybersecurity threats, particularly from Russia[5].

This paper offers several original contributions. First, drawing on the existing literature, it identifies and examines the key linkages between innovation and cybersecurity from the perspective of economics and related disciplines. Second, it contributes to the literature on the development patterns and innovation dynamics of CEECs. Third, using a panel dataset covering eleven CEECs over the period 2014–2024, it hypothesises and demonstrates that while the overall level of innovativeness is negatively associated with cybersecurity performance, the growing innovative capacity of the ICT sector has a positive effect on national cybersecurity outcomes.

The remainder of the paper is structured as follows. Section 2 provides a comprehensive review of the theoretical and empirical literature on the relationship between innovation and cybersecurity. Section 3 outlines the methodological framework and data selection procedures. Section 4 presents and discusses the empirical findings. Finally, Section 5 concludes with a summary of the main results, policy implications, and directions for future research.

Literature review

Mapping the innovation–cybersecurity nexus: A bibliometric analysis

To investigate the general linkages between innovation and cybersecurity in the literature within the fields of "Social Sciences", "Business, Management and Accounting" and "Economics, Econometrics and Finance", we conduct a bibliometric analysis using VOSViewer® software applied to a sample of peer-reviewed scientific sources, including articles, books, book chapters, and conference papers, extracted from the Scopus database, using a query that contained both terms "innovation" and "cybersecurity" in title, abstract, or keywords. The query returned 675 sources meeting the above criteria. Next, we performed a co-occurrence clustering analysis for 51 keywords that

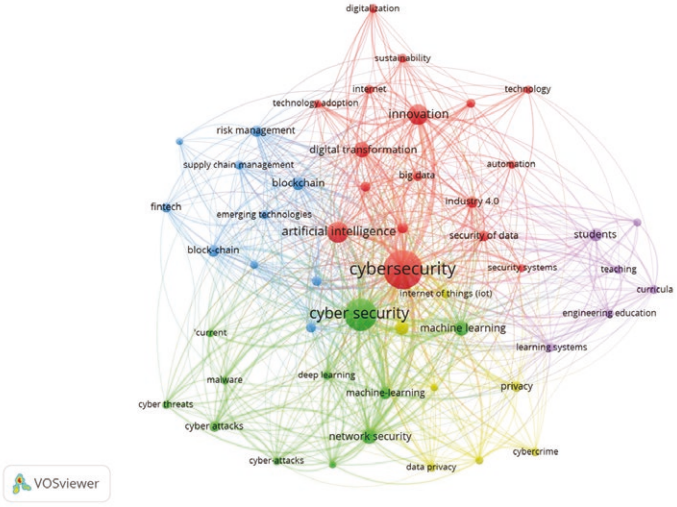
[4] M. Tutak, J. Brodny, *Technological progress in central and eastern Europe: Digitalization and business innovation leaders and outsiders*, "Journal of Open Innovation: Technology, Market, and Complexity" 2024, vol. 10, no. 4, 100404, DOI: 10.1016/j.joitmc.2024.100404.

[5] *Eastern Europe's Cyber Reckoning: Russia's Digital Threat Is Forcing a Strategic Shift*, Inkstick, 9 June 2025, https://inkstickmedia.com/eastern-europes-cyber-reckoning-russias-digital-threat-is-forcing-a-strategic-shift/.

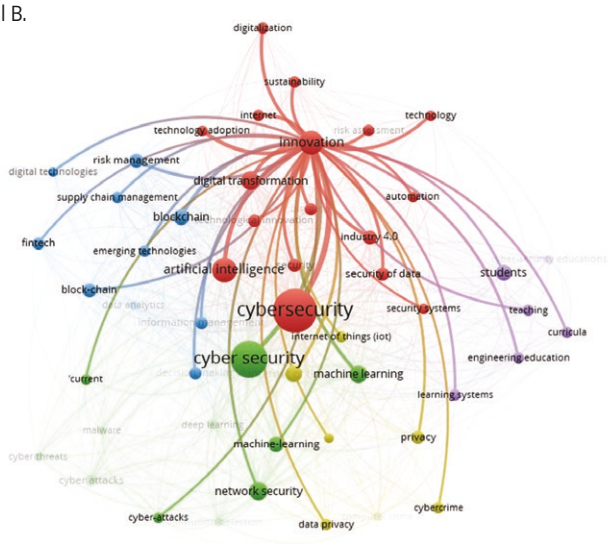
appeared at least ten times in the examined sample. The results of clustering are presented in Figure 1. Panel A presents the complete network of linkages between the selected keywords, whereas Panel B highlights the linkages involving the term "innovation".

Figure 1. Linkages between innovation and cybersecurity in the relevant literature

Panel A.



Panel B.



Source: Own elaboration using the VOSViewer' software.

The VOSViewer' algorithm identified five broad literature clusters interlinked predominantly via issues related to cybersecurity. The largest cluster (marked in Figure 1 in red) focuses on various economic dimensions of the interplay between innovation and cybersecurity, covering the issues related to artificial intelligence, technology adoption, digital transformation, automation, industry 4.0, data security, and sustainability. The second cluster (green) encompasses the issues related to network security and specific cybersecurity threats on the one hand, and machine learning on the other. The third cluster (blue) centres on blockchain technology and its applications in financial services, risk management, or supply chain management. The fourth cluster covers issues related to the internet-of-things, data privacy, and cybercrime. Finally, the last cluster (violet) represents the educational dimension of the investigated relationship.

Economy innovativeness and cyber risk exposure

Increasing innovation capacity enables economies to develop and adopt new, more efficient technologies across key sectors. While this process is critical for fostering economic growth, it also leads to greater systemic complexity and interconnectedness. In turn, as demonstrated by Perrow, the more complex and coupled systems become, the more prone they are to cascading failures resulting from localised disruptions[6].

As justly noted by Li, in a fragmented global landscape, regulating rapidly advancing technologies becomes increasingly complex and challenging[7]. In contrast to earlier industrial revolutions, contemporary technological shifts are progressing at an unparalleled speed, rapidly outpacing existing governance frameworks and intensifying both regulatory imbalances and geopolitical tensions. The growing securitisation of technology at the national level, coupled with the lack of binding international frameworks, impedes effective global cooperation and accelerates an unregulated "technological arms race".

[6] C. Perrow, *Normal Accidents: Living with High-Risk Technologies*, updated ed., Princeton University Press, 1999, https://press.princeton.edu/books/paperback/9780691004129/normal-accidents.

[7] J. Li, *Governing High-Risk Technologies in a Fragmented World: Geopolitical Tensions, Regulatory Gaps, and Institutional Barriers to Global Cooperation*, "Fudan Journal of the Humanities and Social Sciences" 2025, DOI: 10.1007/s40647-025-00445-4.

Tackling these governance challenges necessitates multilateral engagement, the establishment of legally binding agreements, and the creation of independent regulatory institutions equipped with enforcement powers. In the absence of coordinated global action, unchecked technological diffusion risks amplifying security threats, widening global disparities, and undermining trust in both national and international regulatory systems.

Cybersecurity is frequently described as an area marked by substantial market failures. One contributing factor is that investments made by individual firms in enhancing their cybersecurity often generate positive externalities, benefiting not only the firm itself but also its clients and supply chain partners. When there are no mechanisms in place to distribute the associated costs among these beneficiaries, such externalities tend to lead to insufficient investment in cybersecurity. This underinvestment provides a justification for government intervention. Additionally, the presence of information asymmetries – where consumers cannot accurately assess the security features of products or services – can also distort market outcomes[8].

As argued by Carr, the intersection of technological innovation and cybersecurity at the national level often creates a uniquely challenging landscape for public–private partnership[9]. On the one hand, policymakers often hesitate to assert state authority by mandating stricter cybersecurity regulations, while on the other, private sector entities are equally reluctant to accept responsibility or liability for national digital security. This structural imbalance, in turn, complicates collaborative efforts and raises important questions about the governance of cybersecurity in innovation-driven economies. It also reflects the well-known discrepancy between the socially optimal level of R&D investments and the actual quantity supplied by private, profit-maximising firms[10].

A strategic dimension of innovation-led vulnerabilities in the context of cybersecurity is discussed by Kello, who posits that with the emergence of

[8] OECD, *New perspectives on measuring cybersecurity*, OECD Publishing, 2024, https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/new-perspectives-on-measuring-cybersecurity_6069c1b9/b1e31997-en.pdf.

[9] M. Carr, *Public–private partnerships in national cyber-security strategies*, "International Affairs" 2016, vol. 92, no. 1, pp. 43–62, DOI: 10.1111/1468-2346.12504.

[10] J.E. Stiglitz, S.J. Wallsten, *Public-Private Technology Partnerships: Promises and Pitfalls*, "American Behavioral Scientist" 1999, vol. 43, no. 1, pp. 52–73, DOI: 10.1177/00027649921955155.

cyberspace, information "is no longer just a source of power; it has become force itself" (p. 5)[11], as technological advances render innovative economies more vulnerable to various forms of digital threats, including state-sponsored cyber operations.

Another contributing factor is that fast-paced innovation often outstrips the capacity of institutions to regulate it. In this context, Bada, Sasse, and Nurse[12] investigate the reasons for the failure of cybersecurity awareness campaigns, arguing that technological adoption is frequently unaccompanied by effective behavioural change or sufficient improvements in security literacy.

A report by the European Union Agency for Cybersecurity demonstrates that, apart from the public administration and government sector, cybersecurity incidents tend to be concentrated in technologically advanced and innovative industries, such as digital services, banking, and finance, suggesting that concentrations of technological activity may exacerbate national cyber risk[13].

Moreover, a recent study by Xu highlights the role of cybersecurity governance in promoting corporate innovation through reducing precautionary saving, improving reputation, and providing risk-taking incentives[14].

Simultaneously, the continuing digitalisation of economies introduces new platforms for various forms of cyberattacks and security breaches. Contemporarily, this issue becomes a vital challenge for nearly every sector and industry, ranging from energy, manufacturing, and logistics, through finance and healthcare, to national defence, and even agriculture.

According to Botha-Badenhorst, innovation and cybersecurity have concurrently become integral to contemporary business practices, and their intersection has gained ever more prominence in recent years. As firms increasingly adopt digital processes and technology-driven business

[11] L. Kello, *The Virtual Weapon and International Order*, Yale University Press, 2017, DOI: 10.2307/j.ctt1trkjd1.

[12] M. Bada, A.M., Sasse, J.R.C. Nurse, *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?*, arXiv:1901.02672, 2019, DOI: 10.48550/arXiv.1901.02672.

[13] European Union Agency for Cybersecurity. *ENISA threat landscape 2022: July 2021 to July 2022*, 2022, DOI: 10.2824/764318.

[14] J. Xu, *Cybersecurity governance and corporate innovation: Evidence from Chin*a, "Finance Research Letters" 2025, vol. 82, 107619, DOI: 10.1016/j.frl.2025.107619.

models, cybersecurity risks have, therefore, emerged as a pervasive and critical concern[15].

As smart manufacturing gradually strengthens its position as a major technology trend, the related production systems, embedding both data and critical equipment, become increasingly attractive targets for cyber-attacks. In comparison to traditional settings, smart manufacturing is likely more susceptible not only to direct but also indirect cyber-attacks, as they are usually parts of larger ecosystems, combining diverse hardware- and software-related components and agents within an intricate network of interdependencies[16].

Unanticipated systemic vulnerabilities may also be introduced by inter-sectoral innovation spillovers. As innovations from one sector can be repurposed or misapplied in others without adequate safeguards, individual organisations and even entire sectors of the economy may become exposed to chains of unforeseen threats[17].

Taddeo and Floridi highlight the ethical and security externalities resulting from the widespread deployment of AI and big data technologies, which are typically adopted more rapidly in innovative economies, often without robust governance[18]. On the one hand, the source of these challenges lies in the very essence of AI, which gradually becomes a distinct form of autonomous and self-learning agency. On the other hand, the fact that AI is fuelled by data, results in a wide array of problems related to data governance, in terms of access, privacy, ownership and consent.

---

15 D. Botha-Badenhorst, *Navigating the Intersection of Innovation and Cybersecurity: A Framework*, "European Conference on Research Methodology for Business and Management Studies" 2023, vol. 22, no. 1, Article 1, DOI: 10.34190/ecrm.22.1.1490.

16 F. Maggi et al., *Smart Factory Security: A Case Study on a Modular Smart Manufacturing System*. "Procedia Computer Science" 2021, vol. 180, pp. 666–675, DOI: 10.1016/j.procs.2021.01.289.

17 J. Fell et al., *Towards a framework for assessing systemic cyber risk*, 2022, https://www.ecb.europa.eu/press/financial-stability-publications/fsr/special/html/ecb.fsrart202211_03~9a8452e67a.en.html.

18 M. Taddeo, L. Floridi, *How AI can be a force for good*, "Science" 2018, vol. 361, no. 6404, pp. 751–752, DOI: 10.1126/science.aat5991.

ICT sector innovation as a driver of cybersecurity resilience

The theoretical and empirical evidence discussed in the previous subsection suggests that increasing the overall innovativeness of an economy may make cybersecurity management at the national level more challenging. By contrast, the innovativeness of the ICT sector itself (likely due to a higher awareness of cyber threats and greater availability of human and capital resources) can be expected to exert a positive influence on a country's cybersecurity performance.

Innovativeness of the ICT sector, particularly in the area of cybersecurity, creates tools and capabilities to counter digital threats. As demonstrated by Radanliev et al.[19], innovative adoption of machine learning (ML) and artificial intelligence (AI) enhances predictive cyber risk analytics and strengthens the related capacities at the country level. It is worth noting that, in recent years, artificial intelligence and machine learning have become increasingly integral to cybersecurity, enabling the automation of threat detection, analysis, and response processes. Traditional rule-based security systems often fall short when confronted with sophisticated threat actors who continuously develop new tactics and techniques. Advanced ML approaches – including supervised, unsupervised, and deep learning – equip cyber defence mechanisms with the capability to identify normative behavioural patterns within vast datasets and to detect deviations that may indicate malicious activity. Given the rapidly evolving nature of cyber threats, AI-based solutions provide essential advantages such as adaptability, rapid response, and scalability, making them vital components in contemporary cybersecurity strategies[20].

Recent research by the UK Department for Science, Innovation and Technology (DSIT) and the Home Office reveals that cybersecurity-specialised ICT companies report significantly fewer successful cyberattacks than those

[19] P. Radanliev et al., *Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains*, "Cybersecurity" 2020, vol. 3, no. 13, DOI: 10.1186/s42400-020-00052-8.

[20] A.A. Mustaphaa et al., *Current Trends and Innovations in Cybersecurity Technologies: A Comprehensive Review*, "Journal of Scientific and Engineering Research" 2024, vol. 11, no. 5, pp. 100–112.

operating in other sectors, which may be attributed to proactive defence mechanisms and security-by-design practices[21].

Cybersecurity innovations developed within the ICT sector often generate positive externalities for other sectors. For example, secure cloud infrastructure and threat intelligence platforms serve as public goods for the financial, public health, and defence sectors. Notably, an effective identity federation framework that integrates on-premises directory services with cloud-based platforms is essential for authenticating users and managing their access to cloud resources. Inadequately defined or overly permissive access controls can lead to significant privacy risks, particularly in cases of credential compromise. To mitigate such threats, the implementation of multi-factor authentication, well-defined access policies, and periodic audits of user permissions is crucial[22].

As the global interconnectedness of the digital environment creates strong interdependencies across various entities and sectors of the economy, unsurprisingly, most dimensions of digital security risk management require cooperation and cannot be successfully addressed by isolated parties. This is particularly relevant to the implementation of innovative security and preparedness measures developed in the ICT sector[23].

In today's digital economy, the market success of companies in almost every sector strongly hinges on their ability to follow and implement innovative ICT solutions for data security and cyber-attack protection[24].

Research design

The theoretical and empirical evidence available in the relevant literature reveals complex and multidimensional linkages between innovativeness

[21] The Department for Science, Innovation and Technology, & The Home Office, *Cyber security breaches survey 2025*, 2025, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025.

[22] A.A. Mustaphaa et al., op. cit.

[23] OECD, *Digital Security Risk Management for Economic and Social Prosperity*, 2015, https://www.oecd.org/en/publications/digital-security-risk-management-for-economic-and-social-prosperity_9789264245471-en.html.

[24] R. Hristev, M. Veselinova, *ICT for Cyber Security in Business*, "IOP Conference Series: Materials Science and Engineering" 2021, vol. 1099, no. 1, 012035, DOI: 10.1088/1757-899X/1099/1/012035.

and cybersecurity at the country level. On the one hand, cybersecurity is undoubtedly a technology-driven phenomenon, and thus its development is expected to be positively related to the innovative capacity of a given country, especially within the ICT sector. On the other hand, almost all new products and processes today involve the use of digital technologies, which also makes them more vulnerable to cybersecurity threats[25] (European Union Agency for Cybersecurity, 2022). Therefore, it is possible that increasing innovativeness may expose economies to a wider range of cybersecurity challenges.

The above ambiguities allow us to formulate the following set of research hypotheses:

- H1: *The overall level of innovativeness is negatively related to cybersecurity performance at the country level.*
- H2: *The innovativeness of the ICT sector is positively related to cybersecurity performance at the country level.*

The research is focused on the Central and Eastern European Countries (CEECs). For the purposes of the present study, we follow the OECD methodology[26], which classifies the following countries as part of this group: Albania, Bulgaria, Croatia, the Czech Republic, Estonia, Hungary, Latvia, Lithuania, Poland, Romania, the Slovak Republic, and Slovenia. However, due to limited data availability, we decided to drop Albania from the final sample.

Regarding the data collection procedures, we use the Global Cybersecurity Index developed by the International Telecommunication Union[27] as a proxy for cybersecurity performance at the country level. Since ITU publishes the index irregularly, in the present study, we extracted data from the 2014, 2017, 2020, and 2024 editions to ensure approximately equal time intervals between observations. Additionally, data from the 2014 and 2017 editions have been recalculated according to the methodology employed in the most recent editions.

[25] European Union Agency for Cybersecurity, *ENISA threat landscape 2022: July 2021 to July 2022*, 2022, DOI: 10.2824/764318.

[26] OECD, *OECD Glossary of Statistical Terms*, OECD Publishing, 2008, DOI: 10.1787/9789264055087-en.

[27] International Telecommunication Union, *Global Cybersecurity Index 2024*, 2025, https://www.itu.int/epublications/publication/global-cybersecurity-index-2024.

To proxy for country innovation performance, we use the Summary Innovation Index (SII) from the European Innovation Scoreboard[28] for the respective years.

To assess the ICT sector innovation performance at the country level, we employ a composite index based on the Hellwig taxonomic measure of development[29]. To construct the index, we use the following measures of innovative performance:

- the number of patent applications in the ICT-related technologies[30] to the European Patent Office per 1 million inhabitants,
- the number of patents granted by the European Patent Office in the ICT-related technologies per 1 million inhabitants,
- business R&D expenditure in the ICT sector[31] per inhabitant,
- the number of R&D researchers employed in the business ICT sector,
- and the percentage of innovation active enterprises in the ICT sector.

The data on the first two indicators were extracted from the European Patent Office website[32]. The remaining measures were obtained from the Eurostat database[33]. The gaps in the dataset have been filled using the regression imputation technique.

The first step in the calculation of the composite ICT index innovation involves the construction of the matrices of standardised indicators

[28] European Commission, *European Innovation Scoreboard*, 2025, https://research-and-innovation.ec.europa.eu/statistics/performance-indicators/european-innovation-scoreboard_en.

[29] E. Roszkowska, *A Comprehensive Exploration of Hellwig's Taxonomic Measure of Development and Its Modifications – A Systematic Review of Algorithms and Applications*, "Applied Sciences" 2024, vol. 14, no. 21, DOI: 10.3390/app142110029.

[30] Audio-visual technology, telecommunications, digital communication, basic communication processes, computer technology, IT methods for management, and semiconductors.

[31] Section J of the NACE Rev. 2 classification (European Commission, *NACE Rev. 2: Statistical classification of economic activities in the European Community*, EC Publications Office, 2008).

[32] European Patent Office, *Data to download*, epo.org, 2025, https://www.epo.org/en/about-us/statistics/data-download.

[33] Eurostat, *Ec.europa.eu/eurostat/databrowser/view/RD_P_BEMPOCCR2/default*, 2025, https://ec.europa.eu/eurostat/databrowser/view/RD_P_BEMPOCCR2/default; Eurostat, *[rd_e_berdindr2] BERD by NACE Rev. 2 activity*, 2025, https://ec.europa.eu/eurostat/databrowser/view/rd_e_berdindr2/default/table?lang=en;

Eurostat, *[sbs_ovw_act] Enterprises by detailed NACE Rev. 2 activity and special aggregates*, 2025, https://ec.europa.eu/eurostat/databrowser/view/sbs_ovw_act/default/table?lang=en.

representing the particular dimensions of each country's innovation performance in the individual years of the examined period:

$$Z_t = \begin{bmatrix} z_{11,t} & z_{12,t} & \cdots & z_{1k,t} \\ z_{21,t} & z_{22,t} & \cdots & z_{2k,t} \\ \vdots & \vdots & \ddots & \vdots \\ z_{n1,t} & z_{n2,t} & \cdots & z_{nk,t} \end{bmatrix} \quad (1)$$

where:

- $z_{ij,t} = \frac{x_{ij,t} - \overline{x_{j,t}}}{s_{j,t}}$ – the standardised value of indicator j for country i in year t,
- $x_{ij,t}$ – the value of indicator j for country i in year t,
- $\overline{x_{j,t}}$ – the mean value of indicator j in year t,
- $s_{j,t}$ – the standard deviation of indicator j in year t,
- $k = 5$ – the number of indicators,
- $n = 11$ is the total number of countries in the sample.

The Hellwig taxonomic measure of development is based on the Euclidean distance of each country from a benchmark, representing a hypothetical "ideal" object (country), exhibiting the best performance in each of the analysed dimensions in a given year. Since all the selected measures of innovative performance are stimulants, such an "ideal" object in year t ($R_{o,t}$) can be defined as:

$$R_{0,t} = [z_{01,t} \quad z_{02,t} \quad \cdots \quad z_{0k,t}], \text{ where } z_{0j,t} = \max_i \{z_{ij,t}\} \quad (2)$$

The composite index of country i's innovative performance in the ICT sector in year t (hereinafter referred to as) is given by the following formula:

$$CICTIPI_{i,t} = 1 - \frac{d_{i0,t}}{d_{0,t}} \quad (3)$$

where:

$$d_{i0,t} = \left[\sum_{j=1}^{k} \left(z_{ij,t} - z_{0j,t} \right)^2 \right]^{\frac{1}{2}} \quad (4)$$

is the Euclidean distance of country i from the benchmark, and

$$d_{0,t} = \overline{d_{0,t}} + 3S_{0,t} \tag{5}$$

$$\overline{d_{0,t}} = \frac{1}{n}\sum_{i=1}^{n} d_{i0,t} \tag{6}$$

$$S_{0,t} = \left[\frac{1}{n}\sum_{i=1}^{n}\left(d_{i0,t} - \overline{d_{0,t}}\right)^2\right]^{\frac{1}{2}} \tag{7}$$

In formula (5), we use three standard deviations ($S_{0,t}$) from the mean distance ($\overline{d_{0,t}}$), which is recommended in cases where there are very large differences in values of particular indicators across the examined sample.

CICTIPI takes values between 0 and 1, inclusive. Higher values indicate a smaller distance from the 'ideal' object, and thus better innovative performance in the ICT sector. The index allows countries to be ranked on the basis of the distance from the benchmark (from the worst to the best ICT sector innovation performance), as well as enables their classification into groups of similar levels of infrastructure development.

To investigate the impact of innovativeness on cybersecurity performance and test the formulated research hypotheses, we develop a panel regression model using SII and *CICTIPI* as the main explanatory variables and the natural log of *per capita* GDP in purchasing power standard (*lnGDPpc*), and the percentage of population with tertiary education attainment (*TEA*) as control variables:

$$GCI_{i,t} = \beta_0 + \beta_1 SII_{i,t} + \beta_2 CICTP_{i,t} + \beta_3 lnGDPpc_{i,t} + \beta_4 TEA_{i,t} + \varepsilon_{i,t} \tag{8}$$

where:

- $GCI_{i,t}$ – Global Cybersecurity Index for country *i* in year *t*,
- $SII_{i,t}$ – Summary Innovation Index for country *i* in year *t*,
- $CTIPI_{i,t}$ – Composite ICT Innovative Performance Index for country *i* in year *t*,
- $GDPpc_{i,t}$ – natural log of GDP *per capita* in PPS for country *i* in year *t*,
- $TEA_{i,t}$ – percentage of population aged 25–35 with tertiary education attainment,

- β_0 – constant term,
- $\beta_1, \beta_2\ \beta_3, \beta_4$ – regression parameters,
- $\varepsilon_{i,t}$ – error term.
- Following the formulation of first hypothesis of the present study (*H1*) we expect the value of parameter to be negative. All the other parameters are expected to take positive values, as increases in the corresponding explanatory variables should strengthen cybersecurity performance at the country level.

Since our response variable (GCI) may only take values between 0 and 100 (inclusive), we estimate the model's parameters using a Tobit regression with random effects, designed specifically for censored outcomes. All calculations were carried out using the STATA/SE® 14 statistical package.

Results

The key descriptive statistics of the variables employed in the regression are given in Table 1.

Table 1. Descriptive statistics of the employed variables

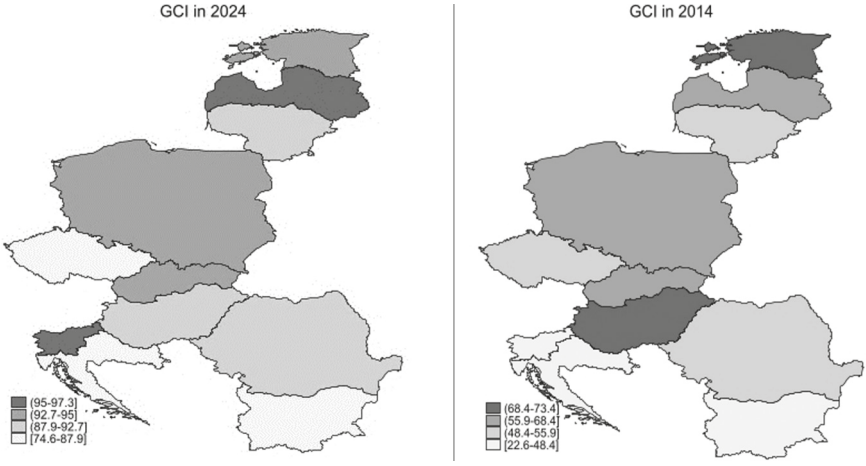
Variable	Min	Max	Mean	Median	SD	Skewness	Kurtosis
$GCI_{i,t}$	22.630	99.480	71.778	73.885	19.731	-0.442	2.326
$SII_{i,t}$	0.150	0.580	0.345	0.350	0.104	0.135	2.379
$CTIPI_{i,t}$	0.188	0.998	0.488	0.475	0.169	1.327	5.550
$GDPpc_{i,t}$	9.465	10.496	10.041	10.028	0.248	-0.086	2.445
$TEA_{i,t}$	23.200	58.200	38.168	38.500	8.238	0.465	2.974

Source: Own elaboration.

The analysis of the Global Cybersecurity Index (GCI) between 2014 and 2024 for CEECs (Figure 2) reveals a clear upward trajectory in cybersecurity commitment and infrastructure development. Countries such as Slovenia and Lithuania exhibited particularly significant advancements. Slovenia improved from a GCI score of 22.63 in 2014 to 96.48 in 2024, marking the most substantial increase (a gain of 73.85 points). This suggests the implementation of extensive cybersecurity reforms, likely encompassing legal, technical, organisational, and capacity-building measures. Similarly, Bulgaria, Croatia, and Romania recorded impressive improvements of approximately

25 to 43 points, further indicating enhanced national efforts to align with international cybersecurity standards and frameworks. The Czech Republic, Hungary, Latvia, Poland, and Slovakia also reported notable increases, with 2024 GCI values exceeding 80 across the board. This cohort represents a broader regional trend in CEECs toward comprehensive cybersecurity modernisation, possibly influenced by EU directives and increasing cyber threat exposure. Notably, the average GCI score for these countries rose from approximately 54.26 in 2014 to 89.26 in 2024, underscoring a robust regional progression over the decade.

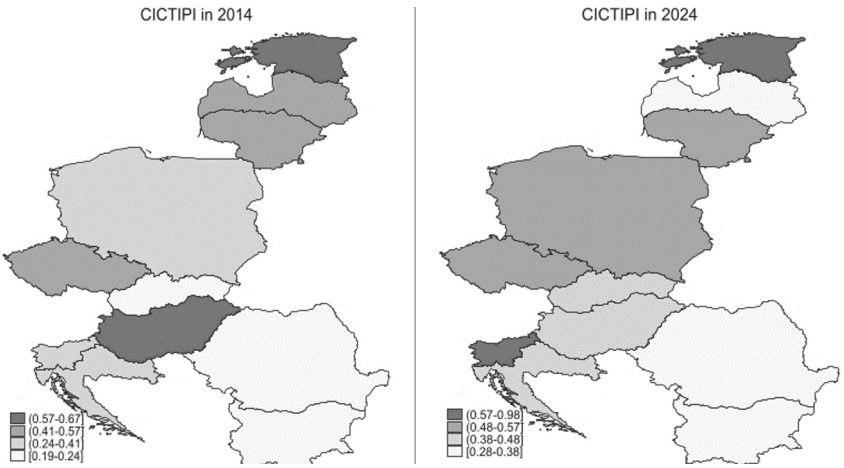
Figure 2. Spatial distribution of Global Cybersecurity Index in 2014 and 2024



Source: Own elaboration.

The analysis of the Composite ICT Innovative Performance Index (CICTP) for the years 2014 and 2024 indicates that several countries experienced noticeable improvements in ICT-related innovation (Figure 3). Estonia showed the most dynamic growth, with the index increasing from 0.61 to 0.98, while Slovenia, Poland, and Lithuania also recorded steady progress. Bulgaria, Romania, Slovakia, and Croatia saw more moderate but positive changes. In contrast, Hungary and Latvia experienced a decline in their innovation performance over the period. The Czech Republic remained largely stable, with its index value showing minimal variation. These patterns suggest a generally upward trend among most countries, albeit with clear disparities in the pace and sustainability of ICT innovation development.

Figure 3. Spatial distribution of Composite ICT Innovative Performance Index in 2014 and 2024



Source: Own elaboration.

The estimation results of the employed regression model are presented in Table 2.

Table 2. Results of Tobit panel regression model estimation

Variable	Coefficient estimate/ value	Standard error	z-statistic	p-value	95%-confidence interval		VIF
$cons.$	-590.215	112.096	-5.27	0.000	-809.920	-370.511	
SII	-119.689	38.890	-3.08	0.002	-195.912	-43.466	3.62
$CICTIPI$	55.450	0.580	2.97	0.003	18.90424	91.995	2.23
$lnGDPpc$	67.020	0.998	5.70	0.000	43.973	90.067	1.89
TEA	0.086	10.496	0.30	0.763	-0.472	0.644	1.23
Log likelihood	-178.180						
Wald x^2	42.87			0.000			
σ_u	0.000	7.893	0.00	1.000	-15.469	15.469	
σ_e	13.882	1.480	9.38	0.000	10.982	16.783	
ρ	0.000	0.000			0.000	1.000	
n	44						

Source: Own elaboration.

The estimation results indicate that the overall constructed model is statistically significant, as suggested by the Wald X^2 test. Except for , all regression coefficient estimates are statistically significant. Moreover, the relatively low

values of variance inflation factors (VIFs) do not suggest any significant problems with multicollinearity. Since is zero, the panel-level variance component is unimportant, and the panel estimator does not differ from the pooled estimator.

In line with our expectations, the estimate of coefficient is negative, implying that in the examined sample of CEECs, more innovative economies are on average more exposed to cybersecurity challenges, thus supporting the first hypothesis of the present study. On the one hand, this result suggests that stronger innovative performance may create a wider cyber attack surface. On the other hand, it is also likely that more innovative countries become prime targets for such attacks. Simultaneously, a positive estimate of coefficient suggests that better innovative performance of the very ICT sector improves cybersecurity at the country level, which in turn supports our second research hypothesis. This finding is in line with the conclusions drawn by Fagarazzi[34], whose research shows that countries with more advanced digital infrastructure tend to achieve higher scores on the National Cybersecurity Index. Consistent with our expectations, the coefficient estimates for the control variables employed in the model (and) are positive, suggesting that higher levels of national income and better education attainment generally foster cybersecurity at the country level. Somewhat surprisingly, however, the impact of the latter variable has turned out to be statistically insignificant which suggests that more educated societies may not necessarily be more resilient to cybersecurity threats.

Conclusions

The results of our study call for a differentiated understanding of the effects of innovation on cybersecurity. General economic innovativeness, while desirable for growth and competitiveness, can unintentionally amplify systemic cyber risks. In contrast, ICT-sector innovation, especially when oriented toward cybersecurity, constitutes a form of digital resilience capital. In this context, innovation policy in CEECs should prioritise investments in cybersecurity R&D and cross-sectoral technology transfer mechanisms that

[34] A. Fagarazzi, *Impact of digital development level on national cybersecurity index*, "Poslovna izvrsnost – Business Excellence" 2024, vol. 18, no. 2, pp. 37–62, DOI: 10.22598/pibe/2024.18.2.xy.

strengthen digital resilience. Furthermore, innovation funding programmes should include incentives promoting secure-by-design technologies, especially in sectors with heightened exposure to cyber threats, such as finance, logistics, energy, and public administration. Given the regional context, CEECs would also benefit from closer cooperation within the Visegrád Group and the European Union, harmonising regulatory approaches and sharing best practices. In particular, such initiatives should build on existing frameworks, including the V4's Central European Cyber Security Platform and the EU's recent Directive on measures for a high common level of cybersecurity across the Union. Building an innovation ecosystem that enhances cybersecurity requires not only technological advancement but also institutional coordination, regulatory foresight, and transnational alignment. As digital transformation accelerates, these policy dimensions become not just complementary but essential for sustainable innovation-led growth in the region.

The main limitation of our study lies in its focus on the specific context of CEECs. Consequently, future research could empirically examine the relationship between innovation and cybersecurity on a broader international scale to determine whether the identified patterns are universal or context-specific. Depending on data availability, future studies could also consider using different cybersecurity metrics or incident statistics, broader sets of control variables, and more frequent or granular data to verify the robustness of the results discussed in this paper. In particular, they may attempt to explore the role of institutional quality and the effectiveness of the rule of law in shaping the linkages between innovativeness and cybersecurity resilience. Moreover, a particularly promising direction for further scientific inquiry is the empirical assessment of the trade-offs between overall innovation intensity and cybersecurity vulnerability, preferably using cross-national panel data and comparative sectoral analyses.

References:

Bada M., Sasse A.M., Nurse J.R.C., *Cyber Security Awareness Campaigns: Why do they fail to change behaviour?*, arXiv:1901.02672, 2019, DOI: 10.48550/arXiv.1901.02672.

Botha-Badenhorst D., *Navigating the Intersection of Innovation and Cybersecurity: A Framework*, "European Conference on Research Methodology for Business and Management Studies" 2023, vol. 22, no. 1, DOI: 10.34190/ecrm.22.1.1490.

Carr M., *Public–private partnerships in national cyber-security strategies*, "International Affairs" 2016, vol. 92, no. 1, pp. 43–62, DOI: 10.1111/1468-2346.12504.

Eastern Europe's Cyber Reckoning: Russia's Digital Threat Is Forcing a Strategic Shift, Inkstick, https://inkstickmedia.com/eastern-europes-cyber-reckoning-russias-digital-threat-is-forcing-a-strategic-shift/.

European Commission, *European Innovation Scoreboard*, 2025m https://research-and-innovation.ec.europa.eu/statistics/performance-indicators/european-innovation-scoreboard_en.

European Commission, *NACE Rev. 2: Statistical classification of economic activities in the European Community*, EC Publications Office, 2008.

European Patent Office, *Data to download*, epo.org, 2025, https://www.epo.org/en/about-us/statistics/data-download.

European Union Agency for Cybersecurity, *ENISA threat landscape 2022: July 2021 to July 2022*, 2022, DOI: 10.2824/764318.

Eurostat, *Ec.europa.eu/eurostat/databrowser/view/RD_P_BEMPOCCR2/default*, 2025, https://ec.europa.eu/eurostat/databrowser/view/RD_P_BEMPOCCR2/default.

Eurostat, *[rd_e_berdindr2] BERD by NACE Rev. 2 activity*, 2025, https://ec.europa.eu/eurostat/databrowser/view/rd_e_berdindr2/default/table?lang=en.

Eurostat, *[sbs_ovw_act] Enterprises by detailed NACE Rev. 2 activity and special aggregates*, 2025, https://ec.europa.eu/eurostat/databrowser/view/sbs_ovw_act/default/table?lang=en.

Fagarazzi A., *Impact of digital development level on national cybersecurity index*, "Poslovna izvrsnost - Business Excellence", 2024, vol. 18, no. 2, pp. 37-62, DOI: 10.22598/pi-be/2024.18.2.xy.

Fell J., de Vette N., Gardó S., Klaus B., Wendelborn J., *Towards a framework for assessing systemic cyber risk*, 2022, https://www.ecb.europa.eu/press/financial-stability-publications/fsr/special/html/ecb.fsrart202211_03~9a8452e67a.en.html.

Hristev R., Veselinova M., *ICT for Cyber Security in Business*, "IOP Conference Series: Materials Science and Engineering" 2021, vol. 1099, no. 1, 012035, DOI: 10.1088/1757-899X/1099/1/012035.

International Telecommunication Union, *Global Cybersecurity Index 2024*, 2025, https://www.itu.int/epublications/publication/global-cybersecurity-index-2024.

Kello L., *The Virtual Weapon and International Order*, Yale University Press, 2017, DOI: 10.2307/j.ctt1trkjd1.

Li J., *Governing High-Risk Technologies in a Fragmented World: Geopolitical Tensions, Regulatory Gaps, and Institutional Barriers to Global Cooperation*, "Fudan Journal of the Humanities and Social Sciences" 2025,DOI: 10.1007/s40647-025-00445-4.

Maggi F., Balduzzi M., Vosseler R., Rösler M., Quadrini W., Tavola G., Pogliani M., Quarta D., Zanero S., *Smart Factory Security: A Case Study on a Modular Smart Manufacturing System*, "Procedia Computer Science" 2021, vol. 180, pp. 666–675, DOI: 10.1016/j.procs.2021.01.289.

Mustaphaa A.A., Alhassanb R.J., Ashic T.A., *Current Trends and Innovations in Cybersecurity Technologies: A Comprehensive Review*, "Journal of Scientific and Engineering Research" 2024, vol. 11, no. 5, pp. 100–112.

OECD, *Digital Security Risk Management for Economic and Social Prosperity*, 2015, https://www.oecd.org/en/publications/digital-security-risk-management-for-economic-and-social-prosperity_9789264245471-en.html.

OECD, *Innovation policies in the digital age*, 2018, https://www.oecd.org/en/publications/innovation-policies-in-the-digital-age_eadd1094-en.html.

OECD, *OECD Glossary of Statistical Terms*, OECD Publishing, 2008, DOI: 10.1787/9789264055087-en.

OECD, *New perspectives on measuring cybersecurity*, OECD Publishing, 2024. https://www.oecd.org/content/dam/oecd/en/publications/reports/2024/06/new-perspectives-on-measuring-cybersecurity_6069c1b9/b1e31997-en.pdf.

Perrow C., *Normal Accidents: Living with High-Risk Technologies*, updated edition, Princeton University Press, 1999, https://press.princeton.edu/books/paperback/9780691004129/normal-accidents.

Radanliev P., De Roure D., Page K., Nurse J.R.C., Mantilla Montalvo R., Santos O., Maddox L., Burnap P., *Cyber risk at the edge: Current and future trends on cyber risk analytics and artificial intelligence in the industrial internet of things and industry 4.0 supply chains*, "Cybersecurity" 2020, vol. 3, no. 13, DOI: 10.1186/s42400-020-00052-8.

Roszkowska E., *A Comprehensive Exploration of Hellwig's Taxonomic Measure of Development and Its Modifications – A Systematic Review of Algorithms and Applications*, "Applied Sciences" 2024, vol. 14, no. 21, DOI: 10.3390/app142110029.

Solow R.M., *A Contribution to the Theory of Economic Growth*, "The Quarterly Journal of Economics" 1956, vol. 70, no. 1, pp. 65–94, DOI: 10.2307/1884513.

Stiglitz J.E., Wallsten S.J., *Public-Private Technology Partnerships: Promises and Pitfalls*, "American Behavioral Scientist" 1999, vol. 43, no. 1, pp. 52–73, DOI: 10.1177/00027649921955155.

Taddeo M., Floridi L., *How AI can be a force for good*, "Science" 2018, vol. 361, no. 6404, pp. 751–752, DOI: 10.1126/science.aat5991.

The Department for Science, Innovation and Technology, & The Home Office, *Cyber security breaches survey 2025*, 2025, https://www.gov.uk/government/statistics/cyber-security-breaches-survey-2025/cyber-security-breaches-survey-2025.

Tutak M., Brodny J., *Technological progress in central and eastern Europe: Digitalization and business innovation leaders and outsiders*, "Journal of Open Innovation: Technology, Market, and Complexity" 2024, vol. 10, no. 4, 100404, DOI: 10.1016/j.joitmc.2024.100404.

Xu J., *Cybersecurity governance and corporate innovation: Evidence from China*, "Finance Research Letters" 2025, vol. 82. 107619, DOI: 10.1016/j.frl.2025.107619.