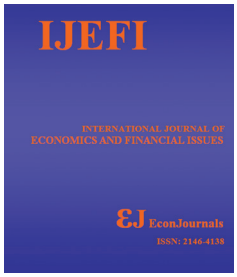

International Journal of Economics and Financial Issues

ISSN: 2146-4138

available at http: www.econjournals.com

International Journal of Economics and Financial Issues, 2025, 15(1), 24-31.

Digital Resilience of the Bucharest Nine and Ukraine

Diana Shkuropadska[1], Volodymyr Tokar[1]*, Olena Purdenko[1], Andrii Lotariev[2], Kyrylo Savchuk[3]

[1]State University of Trade and Economics, Kyiv, Ukraine, [2]KROK University, Kyiv, Ukraine, [3]European University, Kyiv, Ukraine.
*Email: v.tokar@knute.edu.ua

Received: 13 August 2024 **Accepted:** 13 November 2024 **DOI:** https://doi.org/10.32479/ijefi.17233

ABSTRACT

This study examines the digital resilience of the Bucharest Nine, an Eastern European NATO alliance, and Ukraine amidst the challenges of digital transformation. It aims to identify factors influencing their ability to manage cyber threats, digital divides, and socio-economic disparities resulting from rapid digitalization. Using a mixed-methods approach, integrating quantitative analysis and qualitative insights, the research computes an index of digital resilience based on cybersecurity measures, digital infrastructure quality, and socio-economic impacts. Findings reveal varying resilience levels, with some countries demonstrating robust cyber defenses and advanced digital infrastructures, while others lag due to weaker capacities and socio-economic constraints. Comprehensive policy frameworks and inclusive digital strategies are emphasized as critical for enhancing resilience. However, the study's focus on the Bucharest Nine and Ukraine may limit broader regional representation, and reliance on available data and potential biases in self-reported indices may affect comprehensiveness. Nonetheless, the insights can inform policymakers in developing targeted strategies to bolster digital resilience, emphasizing cybersecurity, bridging the digital divide, and promoting digital literacy and participation. This research contributes to understanding digital resilience by offering a comparative analysis of often overlooked geopolitical regions, combining various indicators to provide a holistic view of their digital landscapes.

Keywords: Bucharest Nine, Cybersecurity, Digital Competitiveness, Digital Resilience, Digital Skills, E-Participation
JEL Classifications: F52, H56, L86, R11

1. INTRODUCTION

In the contemporary era, digitalization stands as a defining characteristic of societal advancement, influencing how communities, economies, and governments operate on a global scale. However, the rapid integration of digital technologies brings with it a host of challenges that jeopardize both security and equity. The concept of digital resilience is especially relevant for the Bucharest Nine – a coalition comprising Eastern European NATO nations – and Ukraine. This region holds not only strategic importance but also faces significant cyber threats and digital disparities

Digital technology is crucial for the development agendas and will be vital in the coming years. This is particularly true for Ukraine's reconstruction and for boosting infrastructure, growth, and democratic values across the Eastern Neighbourhood. There is an increasing consensus on the importance of pairing infrastructure investments with the creation of a robust service layer, strong digital government foundations, and an active approach to skills development. This is happening in a scenario where dependence on a single technology supply source is becoming increasingly incompatible with the objectives of enhancing resilience and technological sovereignty (EU4Digital, 2022).

The reliance on technology and tech companies for financial services is making the financial sector more susceptible to cyber threats. The EU's Digital Operational Resilience Act (DORA), which was enacted on January 16, 2023 and will be enforced starting January 17, 2025, seeks to enhance the cyber security of financial institutions under the oversight of the 3 ESAs. Its goal is to ensure that Europe's financial industry can maintain its resilience amidst significant digital operational disruptions (EUR-Lex, 2022).

The imperative for digital resilience is underscored by the increasing volume of digital data and our growing reliance on information technology systems. As society becomes more dependent on digital infrastructures, it concurrently grows more vulnerable to cyberattacks. This vulnerability is manifested through various high-stakes risks including the loss of confidential information, the crippling of systems via malicious hacks, and the unsettling trend of ransom demands for the return of classified data. These incidents underscore the fragility of our digital frameworks and the pressing need for fortified cyber defenses.

Moreover, digitalization inadvertently contributes to widening the social gap through the phenomenon known as the digital divide. This divide separates those who have access to and can effectively utilize modern technologies from those who cannot, thereby engendering social inequalities and perpetuating a cycle of exclusion. This segregation based on digital access and literacy is a critical concern that requires comprehensive strategies to ensure inclusive technological empowerment.

Another significant risk posed by digital proliferation is the manipulation of digital media to spread disinformation. The ease with which false information can be disseminated online poses severe threats to political stability and social harmony, particularly in regions already susceptible to geopolitical tensions. The impact of such disinformation campaigns can erode trust in public institutions and undermine the integrity of democratic processes.

While the digital transformation of the economy holds considerable potential for spurring business development and enhancing living standards, it is not devoid of risks. The shift towards a digital economy involves complex challenges that can affect various facets of economic activity, from data privacy issues to the disruption of traditional industries. The promise of economic growth and innovation must therefore be balanced against these potential vulnerabilities to ensure a stable transition.

Additionally, the burgeoning demand for digital tools, technologies, and services escalates the requirements for data storage and energy, leading to increased carbon emissions globally. This environmental impact adds another layer of complexity to the digital transformation, as it contradicts the global imperative for sustainability.

Finally, a pervasive issue across the digital landscape is the low level of trust in digital technologies and services. Skepticism towards digital solutions can hinder their adoption across various sectors, from business to governance. In particular, the lack of trust and legitimacy in e-governance systems can significantly reduce citizen engagement in electronic services and procedures, thereby stalling progress toward digital democratization.

Delving deeper into the digital resilience of the Bucharest Nine and Ukraine, these multifaceted risks provide a backdrop against which the need for robust, inclusive, and secure digital strategies is starkly apparent. The journey towards digital resilience is complex and fraught with challenges, but it is also an essential undertaking for ensuring the security and prosperity of nations in the digital age.

2. LITERATURE REVIEW

The concept of digital resilience has become increasingly crucial as nations navigate through an array of cyber threats and technological disruptions. Significant contributions to the field come from a variety of studies that explore the intersection of digital technology, security, and socio-economic policies. Fleron, Pries-Heje, and Baskerville's research into Denmark's public sector digital transformation highlights the foundational elements of digital organizational resilience, such as digitalization strategy, inter-sectoral collaboration, and adaptive learning (Fleron et al., 2021). Their work provides a useful framework that could be adapted to analyze digital resilience in the Bucharest Nine and Ukraine, despite its primary focus on Denmark.

Furthermore, the role of digital policies in mitigating the impact of crises such as the COVID-19 pandemic is underscored by Motorga (2021), who examines how Romania's digital policy within the EU has targeted marginalized groups. This highlights the potential of digital strategies to enhance societal resilience by bridging digital divides and fostering inclusivity.

Studies by Seyawati et al. (2022) delve into digital resilience among adolescents, pointing out the essential skills needed to navigate online environments safely. Their findings on the protective factors that enhance digital resilience, such as critical thinking and respectful online behavior, are pivotal for informing policy aimed at strengthening cyber defenses among younger populations.

Gender disparities in the ICT sector also play a critical role in digital resilience, as outlined by Tokar et al. (2023) and Vinska et al. (2023). Their analyses reveal that promoting gender equality in ICT can significantly contribute to digital resilience by fostering diverse and innovative environments. These studies suggest that increasing female participation in STEM and ICT could be a strategic move to enhance digital resilience in the Bucharest Nine and Ukraine.

Despite the rich data on policy responses to economic and health crises, as discussed by Boiko et al. (2022), there is limited integration of these insights with digital resilience strategies. This points to a missed opportunity to leverage digital technologies in crisis management and resilience building. Regarding demographic challenges, Shkuropadska et al. (2024) emphasize the importance of demographic resilience illustrating that demographic stability is critical for sustained economic and digital resilience. This insight is particularly relevant for the Bucharest Nine and Ukraine, where digital divides might exacerbate existing demographic disparities.

Another critical area is the impact of migration on societal stability and resilience, as explored by Moldovan (2020). While migration is recognized as a factor that contributes to social capital and resilience, the specific digital aspects of this relationship remain underexplored. This gap suggests a need for further research into how migration influences digital infrastructure and cyber policies.

The specific challenges faced by the Bucharest Nine and Ukraine require tailored strategies. As noted by Goodwin et al. (2023), the

2022 Russian invasion of Ukraine tested the nation's resilience significantly. Their findings on national resilience, while focusing on social and psychological dimensions, inadvertently highlight the potential for digital tools to enhance communication and trust among citizens, thereby supporting resilience. This intersection of digital and traditional resilience mechanisms is crucial for understanding the broader scope of resilience strategies.

The literature reveals a significant gap in the contextual application of these concepts to the Bucharest Nine and Ukraine. The studies often lack a direct connection to the digital resilience strategies in these specific geopolitical contexts. For instance, the research by Datti and Kuppusamy (2023) discusses the role of digital resilience in national economic strategies but does not address the unique digital infrastructure challenges or cybersecurity threats faced by these countries.

Keudel and Huss (2023) analyze Ukraine's resilience through the lens of democratic processes. They discuss how local governance has played a pivotal role in sustaining democracy and statehood during the war, emphasizing the engagement of citizens and cooperation with non-state actors. This form of resilience, while primarily focusing on democratic mechanisms, hints at an underlying digital component given the significant role of information sharing and local governance in modern democratic systems. The decentralization reforms, which have strengthened political authority and fiscal autonomy, are also suggestive of a digital underpinning, facilitating efficient governance even under duress.

Duffield's work (Duffield, 2016) pivots to the broader implications of digital technologies in security governance, critiquing the rise of data informatics and remote management systems in humanitarian efforts. This shift towards a digital-first approach in governance and security has not only transformed operational modalities but also raised ethical and strategic concerns regarding surveillance and data privacy. Duffield's concept of "resilience of the ruins" particularly resonates within the context of the Bucharest Nine and Ukraine by suggesting that while digital tools can enhance governance, they also risk exacerbating vulnerabilities in already strained environments.

Șișu et al. (2022) address the impact of digitalization on organizational resilience, positing that the adoption of advanced IT systems and online business models has been crucial for companies during crises like the COVID-19 pandemic. This perspective is particularly relevant to the Bucharest Nine, where digital resilience is not just about countering external threats but also about internal organizational and societal stability. The emphasis on digital transformation and its role in enhancing adaptability suggests a roadmap for how nations and businesses in politically volatile regions might leverage technology for resilience.

Mehedintu and Soava (2022) delve into how investments in digital core and innovation foster resilience at the enterprise level. Their findings, based on a Romanian context, offer insights into how digital technologies can be strategically employed to bolster resilience. This is directly applicable to the broader discussions on digital resilience in the Bucharest Nine, where technological advancements can serve as a bulwark against both economic instability and external threats.

Kuppusamy (2022) discusses the broader societal and industrial changes driven by digital transformation, focusing on how strategic technology adoption is imperative for resilience. His analysis provides a framework for understanding the dynamic between digital transformation and resilience, which is critical for the Bucharest Nine and Ukraine. The ability of organizations to respond to disruptions through advanced digital practices is a key component of maintaining operational stability and security.

Overall, the literature suggests a complex interplay between digital transformation, democratic resilience, and organizational adaptability. Each piece highlights different aspects of how digital tools and strategies are integral to resilience in the face of geopolitical tensions and external threats. However, a gap remains in directly connecting these insights to specific digital strategies that could be implemented by the Bucharest Nine and Ukraine to enhance their digital resilience further, a critical area for future research and policy development.

3. METHODOLOGY

The methodology for assessing a country's digital resilience delineates key indicators, their thresholds, and a formula for calculating the integral index of digital resilience. This index mirrors a country's readiness and capacity to manage cyber threats, along with other risks affecting its information systems, economy, and national security.

To calculate the integral index of digital resilience, a process involves compiling a roster of indicators, establishing thresholds for them, standardizing the indicators, and computing the integral index. This index is based on 10 statistical indicators, with the most recent data utilized for indicators updated annually or facing significant reporting delays.

Indicators meeting predefined thresholds are considered sustainable; otherwise, they're labeled unsustainable. Normalizing the indicators entails adjusting them against these thresholds. Indicators surpassing or falling short of the thresholds are normalized to 0, while those aligning with them receive a normalized value of 1, thereby facilitating measurement on a scale from 0 to 1.

The integral index is calculated using the formula:

$$I_{d.r.} = \frac{\sum N_{x=1}}{\sum N_x} \cdot 100\%$$

Where:
$I_{d.r.}$ represents the integral index of digital resilience;
$N_{x=1}$ denotes the number of indicators with a normalized value of 1;
N_x signifies the total number of indicators.

Table 1 illustrates the relationship between the values of the integral index and the levels of national digital resilience.

4. RESULTS

The data presented in Table 2 provides a comparative view of the digital resilience among the Bucharest Nine countries – Bulgaria (BG), Estonia (EE), Latvia (LV), Lithuania (LT), Poland (PL), Romania (RO), Slovak Republic (SK), Hungary (HU), Czechia (CZ) – and Ukraine (UA). The Cybersecurity Index (2024) measures a country's preparedness against cyber threats and the robustness of its cybersecurity policies and infrastructure. The threshold value set for this index is 60. Estonia, Latvia, Lithuania, Poland, Slovak Republic, and Hungary all score impressively above the threshold, with Estonia at a remarkable 99. Such high scores suggest advanced cybersecurity frameworks capable of defending against sophisticated cyber threats. Lithuania and Latvia follow closely with scores of 98 and 97, respectively, indicating a robust cybersecurity stance in the Baltic region. Bulgaria, Romania, Czechia, and Hungary also perform well, with scores ranging from 74 to 92. Each of these countries shows a strong commitment to cybersecurity, ensuring they are well-prepared to handle potential cyber incidents. Ukraine, with a score of 65, barely meets the threshold. This suggests that while Ukraine has made progress in its cybersecurity efforts, there is still room for improvement, especially considering its geopolitical situation and associated cyber risks.

The Digital Quality of Life Index reflects the overall quality of digital infrastructure, including internet affordability, quality, e-government services, and digital government policies. The baseline for this index is set at 0.5. Estonia leads with an index of 0.7185, showcasing its strong digital environment, which is complemented by advanced digital public services and high internet quality. Lithuania and Romania are also notable performers with indices of 0.6957 and 0.6944, respectively, indicating a high quality of digital life that supports both citizens and technological developments. Latvia, Poland, and Czechia, with scores ranging from 0.6391 to 0.6613, exhibit good digital environments. These countries have invested significantly in improving their digital infrastructures, which is reflected in their above-average scores. Slovakia and Hungary are close to the threshold with scores of 0.6215 and 0.6149. These scores suggest that while there are quality digital services available, there is potential for further development to enhance the overall digital quality of life. Ukraine has the lowest score among the analyzed countries at 0.5295. While it meets the threshold, it indicates that Ukraine's digital quality of life could benefit significantly from enhanced internet services and better digital governance.

The Digital Skills Gap Index (2021) assesses the disparity between the digital skills required by employers and those available in the labor market. A score equal to or above 5 indicates a moderate to low skills gap conducive to economic growth and digital transformation. Bulgaria, Latvia, Lithuania, Poland, Slovakia, Hungary, and Czechia score between 5.0 and 5.6, indicating a fairly balanced digital skills landscape. These countries have effectively managed to align their educational outputs with market demands, ensuring a workforce that is relatively well-prepared to meet the challenges of a digital economy. Estonia stands out with a score of 7.0, suggesting an exemplary scenario where the education system significantly surpasses the digital skills demand of the job market. This could indicate a potential for Estonia to lead innovations and attract digital businesses seeking a skilled workforce. Romania and Ukraine, with scores of 4.7 and 4.8, respectively, are below the threshold, pointing towards a mismatch between the workforce's digital skills and the needs of employers. This gap may hinder their economic growth and digital innovation capabilities, necessitating targeted interventions in education and professional training.

Internet Speeds (2024) is a critical factor in the digital economy, affecting everything from business operations and innovation to user experience and access to digital services. The threshold for acceptable speeds is set at 100 Mbps. Lithuania, Poland, Romania, and Hungary show remarkable internet speeds exceeding this threshold, with Romania notably achieving 212.53 Mbps. Such speeds are indicative of advanced digital infrastructure that can support high-demand applications, fostering a competitive edge in technology and digital services. Latvia's internet speed closely meets the standard at 91.78 Mbps, suggesting adequate

Table 1: The interplay between the values of the integral index and the levels of national digital resilience

Levels of national digital resilience	Integral index values, %
High	≥90
Sufficient	(70; 90)
Medium	(50; 70)
Low	≤50

Source: Authors' own contribution

Table 2: Exploring indicators of digital resilience of the Bucharest nine and Ukraine

Indicator	Threshold value	BG	EE	LV	LT	PL	RO	SK	HU	CZ	UA
Cybersecurity index (2024)	≥60	67	99	97	98	94	76	92	91	74	65
Digital quality of life index (2023)	≥0.5	0.570	0.719	0.639	0.696	0.661	0.694	0.622	0.615	0.648	0.530
Digital skills gap index (2021)	≥5	5.0	7.0	5.4	5.8	5.6	4.7	5.1	5.2	5.5	4.8
Internet speeds (2024)	≥100	81.5	81.3	91.8	111.2	154.7	212.5	77.04	173.5	68.3	75.7
Information access index (2022)	≥6	7.6	9.3	8.4	9.5	8.1	8.3	8.9	7.2	8.3	8.0
World digital competitiveness index (2023)	≥50	50.7	84.8	66.4	77.2	66.5	58.3	58.3	58.3	79.4	54.0 (2021)
Digital readiness index (2021)	>0	+0.27	+1.57	+0.77	+0.88	+0.73	+0.35	+0.61	+0.36	+0.83	-0.13
ICT sector in the GDP (2022)	≥5	7.4	6.8	5.7	3.8	3.8	4.2	4.6	6.0	5.0	4.5
E-participation index (2022)	≥0.6	0.739	0.977	0.739	0.546	0.648	0.625	0.466	0.511	0.602	0.602
Climate change performance index (2024)	≥60	46.9	72.1	57.7	63	44.4	61.5	54.5	45.9	45.41	60.4 (2022)

Source: Authors' own elaboration based on (Bughin et al., 2019; CCPI, 2022; CISCO, 2021; DQL, 2023; EU Science Hub, 2024; European Commission, 2023; 2024; Eurostat Statistics Explained, 2020; FM Global, 2024; Fund for Peace, 2024; IMD World Competitiveness Center, 2024; Speedtest, 2024; Statista, 2020; 2022; Stevens Institute of Technology, 2023; UN E-Government Knowledgebase, 2022; Wiley, 2024; World Economic Forum, 2022)

infrastructure capable of supporting most modern digital demands. Bulgaria, Estonia, Slovak Republic, Czechia, and Ukraine have speeds ranging from 68.34 to 81.46 Mbps, below the set threshold. These countries might experience limitations in digital activities that require high bandwidth, such as streaming high-definition video, large-scale data processing, and online gaming. This could impact the user experience and might deter digital-intensive enterprises.

The Information Access Index (2022) evaluates the ease with which citizens can access digital information, which is crucial for informed citizenry and economic development. A threshold value of 6 indicates satisfactory access. Lithuania stands out with an impressive score of 9.5, suggesting that its citizens enjoy excellent access to information, facilitated by robust digital infrastructure and effective regulatory policies. Estonia follows closely with a score of 9.3, reinforcing its reputation as a highly digitalized nation where information access is prioritized. Latvia, Poland, Romania, Slovak Republic, Czechia, and Ukraine also score well, ranging from 8.0 to 8.9. These scores suggest a strong regional commitment to ensuring that citizens have substantial access to digital information, contributing to societal transparency and engagement. Bulgaria and Hungary, with scores of 7.6 and 7.2 respectively, while above the threshold, indicate room for improvement compared to their neighbors. Enhancing access could involve upgrading digital infrastructure, increasing digital literacy, and reducing regulatory barriers.

The World Digital Competitiveness Index (2023) measures a country's ability to adopt and explore digital technologies leading to transformation in government practices, business models, and society in general. The threshold for this index is set at 50. Estonia, with a score of 84.77, and Czechia, scoring 79.42, demonstrate exceptional digital competitiveness. These nations exhibit strong capabilities in technology infrastructure, regulatory frameworks, and future readiness, positioning them as leaders in digital innovation. Lithuania, Latvia, and Poland, with scores from 66.36 to 77.23, show significant digital competencies. Their strong performance suggests effective use of digital technologies in driving economic growth and enhancing competitive edges. Romania, Slovak Republic, and Hungary, each scoring around 58, meet the threshold, indicating they are competitive but still have areas to improve, especially in technology integration and innovation capacity. Bulgaria and Ukraine, with scores of 50.66 and 54 respectively, just surpass the threshold. These scores highlight the necessity for these countries to push for greater digital advancements and infrastructure improvements to keep pace with global and regional peers.

The Digital Readiness Index (2021) assesses how prepared countries are to participate in and benefit from digital economies and societies. A positive score indicates a country is better prepared relative to the baseline of zero. Estonia stands out with a significant positive score of +1.57, highlighting its advanced digital infrastructure and the effective integration of digital technologies in various sectors. This readiness facilitates innovation and competitiveness on a global scale. Lithuania and Latvia follow with scores of +0.88 and +0.77, respectively. These scores suggest a robust digital environment conducive to business operations and public services. Czechia also shows a strong performance with a score of +0.83, indicating a high level of digital integration into daily life and business activities. Poland, Slovakia, and Bulgaria show moderate digital readiness with scores around +0.73, +0.61, and +0.27. These countries are progressing towards greater digital integration, but the scores indicate a need for continued investment in technology and skills development to fully leverage digital opportunities. Romania and Hungary, with scores of +0.35 and +0.36 respectively, are slightly above zero, suggesting they have basic digital infrastructures in place but need significant enhancements to catch up with regional leaders. Ukraine is the only country with a negative score (−0.13), indicating it is less prepared compared to its peers. This highlights challenges in digital infrastructure and policy that could impede its participation in the digital economy.

The contribution of the ICT sector to GDP (2022) indicates the economic impact of digital technologies in a country. A threshold of 5% suggests a significant contribution by the sector to the national economy. Bulgaria leads with an ICT sector contribution of 7.4% to its GDP, reflecting a robust digital economy. Hungary also shows a strong performance with 6.0%, suggesting a substantial economic reliance on ICT. Estonia, Latvia, and Czechia have contributions ranging from 5.0% to 6.8%, indicating healthy digital economies that significantly drive national economic output. Lithuania, Poland, Romania, Slovak Republic, and Ukraine have contributions below 5%. Although these are below the threshold, they indicate growing ICT sectors. Lithuania and Poland, with contributions of 3.8%, and Ukraine, with 4.5%, particularly stand out for needing more focused growth in their digital sectors to boost their economic outputs.

The E-Participation Index measures how well governments enable information sharing, public participation in decision-making, and digital service provision. A threshold of 0.6 suggests a baseline for effective digital civic engagement. Estonia excels with an index of 0.9773, indicating an exemplary level of citizen engagement through digital platforms. This high score reflects Estonia's global reputation as a digital leader, especially in terms of government services and public participation. Bulgaria and Latvia, each scoring 0.7386, and Poland with 0.6477, demonstrate robust digital platforms that facilitate significant citizen involvement in governance. These scores suggest that these countries are effectively using digital tools to enhance civic participation and government transparency. Romania and Czechia, with scores just above the threshold at 0.6250 and 0.6023 respectively, along with Ukraine's identical score, indicate satisfactory levels of digital civic engagement. These countries have implemented adequate systems for e-participation but could benefit from further enhancements to reach the levels seen in Estonia. Lithuania, Slovak Republic, and Hungary, with scores from 0.4659 to 0.5455, fall below the threshold. These lower scores suggest these countries have significant room for improvement in integrating digital technologies into their civic engagement processes.

The Climate Change Performance Index (CCPI, 2022) rates how well countries are performing in addressing climate change

through their policies and actions. A score of 60 or higher indicates a proactive stance on climate initiatives. Estonia stands out with a score of 72.1, showcasing its leadership not only in digital realms but also in environmental policies. Lithuania also performs well with a score of 63, indicating effective and forward-looking climate policies. Romania and Ukraine, with scores of 61.5 and 60.4 respectively, meet the threshold, suggesting they are taking necessary steps to combat climate change, although there is still ample scope for further action. Latvia and Slovak Republic score close to the threshold with 57.7 and 54.5 respectively, indicating ongoing efforts towards better climate performance which could be enhanced with additional policies and initiatives. Bulgaria, Poland, Hungary, and Czechia, with scores ranging from 44.4 to 46.9, are significantly below the threshold. These scores reflect a need for more aggressive climate policies and initiatives to meet global standards and commitments.

Table 3 presents the integral index values and corresponding digital resilience levels for the Bucharest Nine countries and Ukraine. The data exhibits a predominant clustering of countries around specific resilience levels, providing an insightful glimpse into the region's digital preparedness and stability.

Estonia stands out with the highest integral index value at 90%, classified under a high digital resilience level. This indicates a robust digital infrastructure and effective policies in place, likely contributing to enhanced cybersecurity measures and technological advancements. Estonia's lead in the index could be attributed to its early and comprehensive adoption of digital solutions in governance and public services.

The majority of the countries listed – Latvia, Lithuania, Bulgaria, Poland, Czech Republic, Hungary, Romania, and Slovakia – show an integral index value of 80%, categorized as sufficient. This uniformity suggests a moderate but adequate level of digital resilience, indicating these nations have implemented necessary digital frameworks and security protocols to protect against common cyber threats and disruptions. However, this level also implies there is room for improvement, especially in coping with more sophisticated cyber challenges or in enhancing digital inclusivity.

Both Slovakia and Ukraine register lower at a medium digital resilience level with an index value of 60%. This positioning reflects a need for significant enhancements in their digital infrastructures. The medium classification hints at potential vulnerabilities in their digital ecosystems, which could hinder effective response to digital threats and limit digital transformation opportunities.

Table 3: Integral index values and digital resilience levels in the Bucharest Nine and Ukraine

Country	Integral index values, %	Digital resilience levels
Estonia	90	High
Latvia	80	Sufficient
Lithuania	80	Sufficient
Bulgaria	80	Sufficient
Poland	80	Sufficient
Czech Republic	80	Sufficient
Hungary	80	Sufficient
Romania	80	Sufficient
Slovakia	60	Medium
Ukraine	60	Medium

Source: Authors' own contribution

5. DISCUSSION

The findings concerning the high cybersecurity indices for countries like Estonia, Latvia, and Lithuania align with Fleron et al. (2021), who emphasized the significance of robust digital frameworks in enhancing organizational resilience. The remarkable score of 99 for Estonia in the Cybersecurity Index can be seen as a manifestation of the proactive digitalization strategies that these studies advocated for. Similar parallels can be drawn from the study by Seyawati et al. (2022), which highlighted the necessity of strong cybersecurity measures to foster digital resilience among adolescents—a demographic critical to long-term digital security.

However, the moderate performance of Ukraine, with a score just above the threshold, underscores a critical gap identified in the literature – specifically, the need for targeted digital policies that address the unique geopolitical and economic challenges faced by countries at greater risk. This is supported by Boiko et al. (2022), who suggested that the integration of digital strategies in crisis management could be instrumental in enhancing national resilience, a strategy that Ukraine might benefit from considerably.

The study's findings on the Digital Quality of Life Index, with Estonia leading, resonate with Motorga's (2021) insights on how digital policies can enhance societal resilience by improving digital inclusivity and infrastructure. The strong performances of countries like Romania and Lithuania also suggest that investments in digital infrastructure, as proposed by Shkuropadska et al. (2024), are pivotal in addressing demographic disparities and fostering economic growth through digital channels.

Nevertheless, the lower scores for Ukraine highlight a significant area for improvement. This mirrors the concerns raised by Datti and Kuppusamy (2023), who noted that failing to address infrastructural deficiencies could hinder a nation's ability to leverage digital technologies for economic and social resilience.

While the methodology employed in this study – using an integral index of digital resilience based on multiple indicators—is robust, there are notable limitations. Firstly, the reliance on quantitative data may overlook qualitative aspects such as user satisfaction, digital literacy, and the nuanced impacts of digital policies at the local level. These elements are crucial for a holistic understanding of digital resilience as suggested by Kuppusamy (2022), who argues that qualitative assessments can provide deeper insights into the societal impact of digital transformations.

Secondly, the study's scope is limited to the Bucharest Nine and Ukraine, potentially ignoring how regional interactions and external geopolitical pressures influence individual countries' digital resilience. This is particularly relevant given the ongoing

conflict in Ukraine, which poses unique challenges that are not fully encapsulated by the current indicators.

6. CONCLUSION

Examining the digital resilience of the Bucharest Nine countries – Bulgaria, Estonia, Latvia, Lithuania, Poland, Romania, Slovak Republic, Hungary, and Czechia – along with Ukraine utilizes a comprehensive methodology that integrates multiple indicators into an integral index of digital resilience. This index provides a nuanced understanding of each country's capabilities in managing cyber threats and safeguarding their information systems, economy, and national security.

From the results, it is evident that countries such as Estonia, Latvia, and Lithuania have achieved remarkably high levels of digital resilience. Estonia, in particular, stands out with an integral index value approaching 90%, reflecting its exceptional digital infrastructure and policies. This high level of digital resilience signifies Estonia's capability to effectively defend against sophisticated cyber threats and its advanced adoption of digital technologies in governance and public services.

The findings also highlight that while Bulgaria, Poland, Czechia, and Hungary perform well, their integral index values suggest that there is still room for improvement to reach the optimal resilience seen in leading nations. The near-uniform scores around 80% for many of the Bucharest Nine countries indicate a moderate but sufficient level of digital resilience, suggesting these countries possess the necessary digital frameworks and security protocols to mitigate common cyber risks.

Conversely, Ukraine, while making strides in improving its digital infrastructure, lags behind its peers, barely meeting the threshold in several indexes. This suggests an urgent need for targeted improvements, particularly in cyber security measures and digital quality of life, to elevate its overall digital resilience, especially given the ongoing geopolitical challenges it faces.

The value-added of this research is significant as it not only provides a clear benchmark of current digital resilience but also highlights the disparities among the countries in the region. This serves as a crucial tool for policymakers, helping them to identify areas needing strategic improvements and to prioritize investments in cybersecurity, digital infrastructure, and public services.

Policy implications arising from this research are profound. Governments are advised to enhance their digital frameworks and invest in robust cybersecurity measures tailored to the specific vulnerabilities identified through the resilience index. Additionally, there is a need for policy interventions to close the digital skills gap and improve internet quality, particularly in countries lagging behind their regional peers.

Future research directions should focus on longitudinal studies to track progress and the impact of policy changes on digital resilience. There is also a need for more granular research that can dissect the interplay between different indicators and digital resilience, providing deeper insights into how specific factors such as digital skills or e-participation contribute to the overall resilience of a nation.

Lastly, considering the dynamic nature of cyber threats and digital technologies, continuous updating of the indicators and thresholds used in calculating the integral index of digital resilience is essential. This will ensure that the assessment remains relevant and that countries can accurately measure their progress and adapt their strategies effectively. This research not only charts a path for current improvements but also sets the stage for sustained digital advancement and security in the region.

REFERENCES

Boiko, A., Umantsiv, Y., Cherlenjak, I., Prikhodko, V., Shkuropadska, D. (2022), Policy measures for economic resilience of Visegrad group and Ukraine during the pandemic. Problems and Perspectives in Management, 20(2), 71-83.

Bughin, J., Seong, J., Manyika, J., Hämäläinen, L., Windhagen, E., Hazan, E. (2019), Tackling Europe's Gap in Digital and AI. McKinsey and Company. Available from: https://www.mckinsey.com/featured-insights/artificial-intelligence/tackling-europes-gap-in-digital-and-ai [Last accessed on 2024 Feb 14].

CCPI. (2022), Climate Change Performance Index 2024: Ranking and Results. Available from: https://ccpi.org/wp-content/uploads/ccpi-2022-results-1.pdf [Last accessed on 2024 Feb 14].

CISCO. (2021), Digital Readiness Index. Available from: https://www.cisco.com/c/m/en_us/about/corporate-social-responsibility/research-resources/digital-readiness-index.html#/[Last accessed on 2024 Feb 14].

Datti, L.C., Kuppusamy, M. (2022), A conceptual argument on the digital resilience capability within the developing and developed countries. International Journal of Advanced Business Studies, 1(1), 10-19.

DQL. (2023), Digital Quality of Life Index. Available from: https://surfshark.com/dql2023 [Last accessed on 2024 Feb 14].

Duffield, M. (2016), The resilience of the ruins: Towards a critique of digital humanitarianism. Resilience, 4(3), 147-165.

EU Science Hub. (2024), ICT Sector Analysis 2022. Available from: https://joint-research-centre.ec.europa.eu/predict/previous-predict-editions/ict-sector-analysis-2022_en [Last accessed on 2024 Feb 14].

EU4Digital. (2022), Building Digital Resilience: How New Technologies can Support Rebuilding Ukraine and Strengthen Digital Transformation in Eastern Neighbouring Countries. Acvailable from: https://eufordigital.eu/building-digital-resilience-how-new-technologies-can-support-rebuilding-ukraine-and-strengthen-digital-transformation-in-eastern-neighbouring-countries [Last accessed on 2024 Feb 14].

EUR-Lex. (2022), Regulation (EU) 2022/2554 of the European Parliament and of the Council of 14 December 2022 on Digital Operational Resilience for the Financial Sector and Amending Regulations (EC) No 1060/2009, (EU) No 648/2012, (EU) No 600/2014, (EU) No 909/2014 and (EU) 2016/1011 (Text with EEA Relevance). Available from: https://eur-lex.europa.eu/eli/reg/2022/2554/oj [Last accessed on 2024 Feb 14].

European Commission. (2023), Shaping Europe's Digital Future. Available from: https://digital-strategy.ec.europa.eu/en/library/cardinal-points-digital-decade-report-2023 [Last accessed on 2024 Feb 14].

European Commission. (2024), DESI 2022 Composite Index. Availble from: https://digital-decade-desi.digital-strategy.ec.europa.eu/datasets/desi-2022/charts/desi-composite?indicator=desi_sliders&

breakdownGroup=desi&period=2022&unit=pc_desi_sliders [Last accessed on 2024 Feb 14].

Eurostat Statistics Explained. (2020), ICT sector-Value Added, Employment and R and D. 2020. Available from: https://ec.europa.eu/eurostat/statistics-explained/index.php?title=ict_sector_-_value_added,_employment_and_r%26D [Last accessed on 2024 Feb 14].

Fleron, B., Pries-Heje, J., Baskerville, R. (2021), Digital Organizational Resilience: A History of Denmark as a Most Digitalized Country. Proceedings of the 54th Hawaii International Conference on System Sciences. p. 2400-2409. Available from: http://hdl.handle.net/10125/70907; https://www.fmglobal.com/research-and-resources/tools-and-resources/resilienceindex/explore-the-data [Last accessed on 2024 Feb 14].

FM Global. (2024), FM Global Resilience Index. Available from: https://www.fmglobal.com/research-and-resources/tools-and-resources/resilienceindex/explore-the-data [Last accessed on 2024 Feb 14].

Fund for Peace. (2024), Information Access Index. Available from: https://www.fundforpeace.org/SRI/about.html [Last accessed on 2024 Feb 14].

Goodwin, R., Hamama-Raz, Y., Leshem, E., Ben-Ezra, M. (2023), National resilience in Ukraine following the 2022 Russian invasion. International Journal of Disaster Risk Reduction, 85, 103487.

IMD World Competitiveness Center. (2024), World Digital Competitiveness Ranking. Available from: https://www.imd.org/centers/wcc/world-competitiveness-center/rankings/world-digital-competitiveness-ranking [Last accessed on 2024 Feb 14].

Keudel, O., Huss, O. (2023). 'Der Beitrag lokaler Selbstverwaltungsbehörden zur demokratischen Resilienz der Ukraine. Ukraine-Analysen, 287, 11-17.

Kuppusamy, M. (2022), Digital resilience capability for pervasive digital transformation: A framework notation. International Journal of Advanced Business Studies, 1(1), 20-26.

Mehedintu, A., Soava G. (2022), 'A structural framework for assessing the digital resilience of enterprises in the context of the technological revolution 4.0'. Electronics, 11(15), 2439.

Moldovan, I.D. (2020), Resilience and social change-Romania after 1989. Research and Science Today, 2(20), 79-91.

Motorga, M.E. (2021), The digital single market, social media, the digital educational system, romania, and the European Union: A critical view. Political Studies Forum, 2(1), 61-84.

Seyawati, R., Mareza, L., Hamka, M. (2022), Digital resilience: Opportunities and threats for adolescents in a virtual world. Acta Informatica Malaysia, 6(2), 67-71.

Shkuropadska, D., Lebedeva, L., Shtunder, I., Ozhelevskaya, T., Khrustalova, V. (2024), The impact of demographic resilience on the economic development of countries (on the example of the Visegrad Group countries). Financial and Credit Activity Problems of Theory and Practice, 1(54), 552-563.

Șișu, J.A., Năstase, M., Tîrnovanu, A., Mujaya, J., Ito, S. (2022), Resilience Through Digitalization in Organizations. Proceedings of the 16th International Management Conference "Management and Resilience Strategies for a Post-Pandemic Future. p322-330. Available from: https://conferinta.management.ase.ro/archives/2022/pdf_IMC_2022/2_8.pdfhttps://www.fmglobal.com/research-and-resources/tools-and-resources/resilienceindex/explore-the-data/? [Last accessed on 2024 Feb 14].

Speedtest. (2024), Speedtest Global Index. Available from: https://www.speedtest.net/global-index [Last accessed on 2024 Feb 14].

Statista. (2020), Share of the Information, Communications, and Technology (ICT) Sector in the Gross Domestic Product (GDP) in Central and Eastern Europe (CEE) in 2020, by Selected Country. Available from: https://www.statista.com/statistics/1393918/cee-share-of-ict-sector-in-gdp [Last accessed on 2024 Feb 14].

Statista. (2022), Employment in the Information and Communications Technology (ICT) Industry as a Share of Total Employment in Central and Eastern Europe (CEE) in 2022, by country. Available from: https://www.statista.com/statistics/1385205/cee-ict-share-of-employment-by-country [Last accessed on 2024 Feb 14].

Stevens Institute of Technology. (2023), Countries Ranked by Internet Privacy. Available from: https://online.stevens.edu/info/countries-ranked-by-internet-privacy [Last accessed 2024 Feb 14].

Tokar, V., Tyshchenko, D., Franchuk, T., Makoiedova, V., Lotariev, A. (2023), Using Cluster Analysis for Revealing Gender Equality Patterns in EU ICT Education and Employment. Journal of Theoretical and Applied Information Technology, 101(16), 50893-50904.

UN E-Government Knowledgebase. (2022), E-Participation Index. Available from: https://publicadministration.un.org/egovkb/en-us/data-center [Last accessed on 2024 Feb 14].

Vinska, O., Harbuza, T., Teslenko, N., Tokar, V. (2022), Gender dimension of the European Union's communication ecology problems in high-technology sectors. Explore Business, Technology Opportunities and Challenges After the Covid-19 Pandemic. Vol. 495. ICBT. Berlin: Lecture Notes in Networks and Systems. p1303-1315.

Wiley. (2024), The Digital Skills Gap Index. Available from: https://dsgi.wiley.com/global-rankings [Last accessed on 2024 Feb 14].

World Economic Forum. (2022), The Cyber Resilience Index: Advancing Organizational Cyber Resilience. Available from: https://www.weforum.org/publications/the-cyber-resilience-index-advancing-organizational-cyber-resilience [Last accessed 2024 Feb 14].