JOURNAL OF POST-QUANTUM CRYPTOGRAPHY AND SYSTEMS

RESEARCH ARTICLE

Volume 01, Issue 01, 2026

Measuring National Cybersecurity Preparedness: A Comparative Analysis Using the Global Cybersecurity Index

R. R. K. Sharma[1*], Niraj K. Vishvakarma[2]

[1*]Department of Management Studies, Indian Institute of Technology, Kanpur, India. Email: rrkiitk@gmail.com
[2]Indian Institute of Information Technology, Lucknow, India. Emailnirajkumar.v@gmail.com

ABSTRACT

As the dependency on technology infrastructure increases, so does the necessity for strong cyber-preparedness frameworks at the national level. This paper examines a comparative approach to global cybersecurity readiness through the use of the Global Cybersecurity Index (GCI) from 2020 to 2024. A quantitative research methodological approach is applied, with the combination of descriptive and distributional statistics, as well as clustering methods, to analyze the cybersecurity preparedness among 194 nations. It was found that there was an increase in the global cybersecurity capacity, reflected by the improved GCI score and a lower number of poorly prepared countries. The pillar analysis revealed that the progress made was mainly as a result of improvements in terms of organizational, legal, and cooperation factors, and on the other hand, there was moderate progress in technical skills and capacity building in addition to human capital development. The findings also showed that there was clear persistence when it came to ranking at the global level, but there were instances of high mobility for some countries. The clustering analysis showed that there were different clusters of countries based on their high, medium, and low preparedness levels, showing that there were structural differences in terms of cybersecurity developments.

Keywords: cybersecurity preparedness, Global Cybersecurity Index, comparative analysis, cyber resilience, national security, clustering analysis

1. Introduction

National-level cyber readiness has become an important determinant that plays an integral role in determining the economic stability, security, and resilience of states operating in a globalized environment. Given that technology is developing at an alarming rate today, and there have been many cyberattacks against different nations, the need for implementing holistic approaches for ensuring that the information infrastructure is protected from any vulnerabilities has become crucial. In this regard, it has become essential to evaluate the cybersecurity capacity of different countries, as a method of identifying their strengths and weaknesses, which will then help to find ways of mitigating the identified issues. Cybersecurity indices such as Global Cybersecurity Index (GCI) and National Cybersecurity Index (NCSI) provide multidimensional evaluations of the degree of national readiness that encompasses factors such as lawfulness, technological capacity, organization, and collaboration. The cybersecurity indices serve as indicators and mechanisms as well as means for policy alignment and promoting international collaboration. However, there exist divergences in terms of approaches, scope, and data sources that might result in inconsistencies in evaluation of the indices and therefore create concerns regarding their validity and credibility (Alguliyev et al., 2025). Various scholarly studies analyzing cybersecurity indices have demonstrated their pros and cons, such as being able to capture global tendencies and dynamism of cybersecurity environments (Kravets, 2019).

Preparedness to cyber attacks is very much related to cyber resiliency and readiness, in general. As the necessity to analyze cybersecurity measures becomes more apparent, more factors are taken into account in the process. Thus, such aspects of security and preparedness as institutional and governmental preparedness, human resource development, among others, can all play a crucial role when analyzing cybersecurity. One such example is the creation of the National Cyber Resilience Index, which demonstrates the importance of more dynamic measurement instruments to incorporate both aspects of prevention and response (Ndibe, 2024). Furthermore, some scientific studies proposed the implementation of a vulnerability-based model for measuring preparedness in critical infrastructure sectors (Karabacak et al., 2016).

Comparative studies of national cybersecurity strategies have shown considerable diversity in terms of how countries manage their cybersecurity governance systems. These differences may stem from the different legal, institutional, and policy structures that exist between countries, which may affect the degree to which cyber threats are effectively managed by governments. Comparative studies on several national cybersecurity strategies show that while some nations employ a holistic or integrated strategy for managing cybersecurity, other countries have adopted a piecemeal or reactive approach (Odebade & Benkhelifa, 2023; Shafqat & Masood, 2016).

Regional perspectives also add to these dynamics. For instance, studies on the Euro-Mediterranean area show the importance of cooperation and policy alignment in improving cybersecurity preparedness, but at the same time demonstrate the enduring disparities between advanced and developing nations (Gorenšek & Trivunčević, 2025). Comparisons of individual countries like Pakistan and Indonesia also showcase how national differences shape their cybersecurity effectiveness despite having comparable development patterns (Sadat et al., 2025). Additionally, cross-national investigations of cybersecurity indexes together with data security mechanisms provide a clearer picture of the interrelated nature of cyber issues (Weng & Wu, 2024).

However, despite the emergence of many scientific works related to national cybersecurity preparedness, there are still a number of gaps in the empirical investigation of this area of study. Firstly, existing literature mainly concentrates either on index analysis or on national strategy analysis without any quantitative comparisons between different countries. Secondly, considering the constantly changing character of cybersecurity problems, one can state the need for the regular updating of methodologies used for measuring national cybersecurity preparedness. The following work will try to fill some gaps in the current scientific discussion on the topic of cybersecurity.

The following research paper will contribute to the literature review through its attempt to analyze national cybersecurity preparedness with the use of the Global Cybersecurity Index. Through the comparison of different countries, it will be possible to determine the main factors affecting the development of national cybersecurity strategies.

2. Methodology

2.1 Research Design

The research makes use of the quantitative cross-comparative methodology, which will allow comparing differences in the level of cybersecurity preparedness among different nations and changes in national preparedness during 2020-

2024. A two-period panel is the analytical design used in the paper, which helps not only to compare nations' capabilities but also to trace the dynamics of cybersecurity development within the particular nation during the period under discussion. Descriptive statistics, correlation, and cluster analysis will be used for studying global trends, internal linkages within the developed index, and grouping of nations into clusters according to their cybersecurity preparedness. As the time frame is not extensive enough to make some conclusions concerning causality, the comparative approach should prevail in the study.

2.2 Data Sources

The empirical research will be conducted using the Global Cybersecurity Index (GCI), which was developed by the International Telecommunication Union. The database comprises 194 countries observed during two periods: 2020 and 2024. Thus, a total number of 388 cases is provided, which is an ideal example of a balanced panel. The GCI presents an aggregate indicator of the national readiness to ensure cybersecurity by means of five sub-indicators: legal measures, technical measures, organizational measures, capacity development, and cooperation (Rameez, 2026). Each sub-indicator presents particular components of national cybersecurity ecosystems, such as regulations, institutional capacities, technical infrastructure, human resource development, and international cooperation. The dataset is free from any inconsistencies because every country is mentioned only once per year in the database, and no duplications have been revealed during validation. However, there is a problem related to the absence of the sub-indicator that covers the topic of child online protection in the dataset of 2024.

2.3 Variable Specification

The main dependent variable used is the overall score in the GCI scale as a continuous measure with values varying from 0 to 100. It signifies the total level of preparedness concerning the cybersecurity of nations. Other explanatory variables that will be used are the five-pillar scores. They include the legal score, technical score, organizational score, capacity development score, and the cooperative score. These pillars are elements of the composite index but are studied separately for their contribution and interactions within. In addition, other derived variables are created for the purpose of analyzing the temporal nature of the phenomenon. Change in preparedness is computed by subtracting the 2020 GCI score from the 2024 GCI score.

2.4 Analytical Framework

To begin the research, descriptive statistics should be used for the given data set in order to estimate the distribution of cyber readiness on the international scale. Indicators of centralization and dispersion for both years will be calculated. The comparison of the mean, median, and distribution of scores within specific intervals will enable estimating the shifts in distribution patterns. The first stage establishes the general trajectory of cybersecurity evolution on the international scale. The time-series evolution will be estimated through the pair comparisons method. To evaluate the shifts in countries' scores, we will have to calculate the difference between the scores of 2024 and 2020.

The analysis of correlations aims at investigating the inner construction of the index. Pearson correlation coefficients will be calculated for the general score and each pillar, as well as for all the pillars in pairs, revealing possible interrelations. In addition, Spearman's rank correlation will be calculated to measure the stability of the hierarchy within the two time periods and reveal any tendencies concerning the persistence of the global ranking. Clustering procedures are implemented to detect latent types of cybersecurity preparedness among nations. Specifically, a k-means clustering algorithm will be employed to separate countries according to the similarity of their cybersecurity characteristics in terms of the scores received for the four pillars.

In addition, distributional analysis is used to analyze issues of inequality and convergence. Analysis of changes at both the bottom end and the top end of the distribution will help identify whether there is an increase or decrease in gaps between nations across the globe.

2.5 Robustness and Sensitivity Considerations

Several ways are employed in order to ensure that the analysis is reliable. Firstly, the omission of the missing

technical sub-indicator in 2024 guarantees that there will be no distortions when comparing the results. Secondly, clustering results are tested through various means to validate the consistency of country classifications. Lastly, sensitivity to outliers is determined by analyzing their effects on general trends.

3. Results

3.1 Global Trends in Cybersecurity Preparedness

According to the results obtained, there has been a significant improvement in global cybersecurity readiness since 2020 up to 2024. Indeed, the GCI scores for 2024 have an average score of 65.79 compared to an average score of 51.71 in 2020. This corresponds to an average improvement of 14.08 in the GCI score. In addition, the median of the GCI scores in 2024 has gone up considerably from 50.52 to 70.40. Thus, the change in the distribution of the scores is depicted in Figure 1.

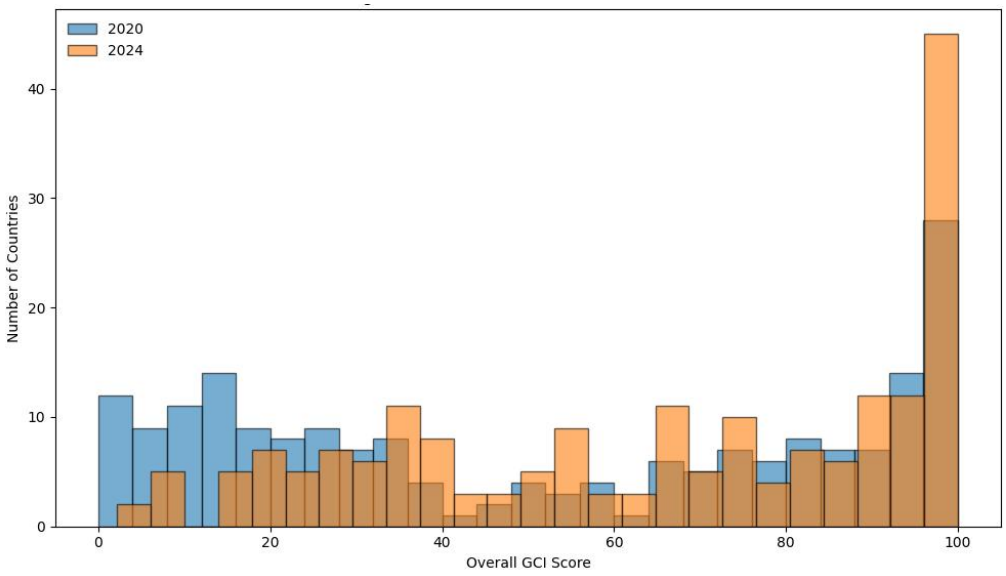

Figure 1: Global Distribution of GCI Scores

The whole distribution of the scores has been shifted upwards, and at the same time, there is a compression of the bottom tail. Countries having very low levels of readiness (scores less than 20) have dropped drastically from 55 to 14. On the other hand, the number of top-performers has also increased; the number of countries that scored above 90 has gone up from 45 to 65. Countries scoring the highest score, i.e., 100, have also gone up from 1 to 12. These trends reflect an international pattern of convergence wherein countries are not only coming out of low-capacity states but also increasing in numbers to approach the highest value of the index. The overall distributions and central tendencies of cybersecurity readiness for various countries are reflected in Table 1.

Table 1: Descriptive Statistics of GCI and Pillars (2020 vs 2024)

Variable	Mean 2020	Mean 2024	Median 2020	Median 2024	Std. Dev. 2020	Std. Dev. 2024
Overall GCI Score	51.71	65.79	50.52	70.39	35.29	29.71
Legal Score	12.80	16.08	13.53	18.18	6.78	4.91
Technical Score	9.64	11.40	10.37	14.44	7.82	7.61
Organizational Score	9.45	13.43	8.77	15.78	7.47	6.57
Capacity Development	9.40	11.39	8.28	12.11	7.74	7.04
Cooperative Score	10.41	13.49	11.07	14.28	7.39	5.94

3.2 Pillar-Level Performance

All five indicators of GCI display a positive change on average over the period of research, although the level of the change differs from one dimension to another. The maximum level of change is displayed by the organizational indicators, seconded by legal and cooperative measures. Measures related to capacity development and technical aspects also demonstrate positive changes; however, these changes are relatively lower compared to others. Figure 2 provides a comparative analysis of the five dimensions of cyber readiness.

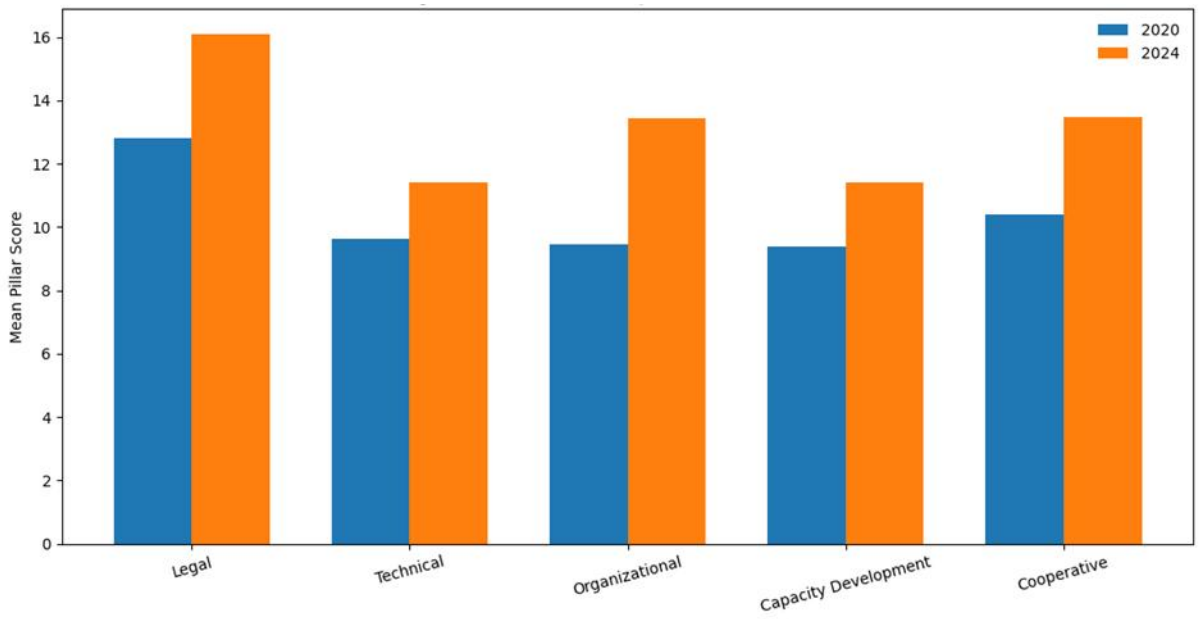

Figure 2: Pillar Score Comparison

Organizational scores increased by about four points, which is an indication of general improvement in terms of national cybersecurity policies, coordination mechanisms, and governance structures. Scores for laws and regulations also saw marked increases, which could be attributed to the adoption of more cybersecurity laws and regulations. The category that saw the greatest improvement was cooperative measures, which could mean greater cooperation on the international scene in matters related to cybersecurity. These changes are shown in Table 2.

Table 2: Pillar-wise Changes in Cybersecurity Preparedness

Pillar	Mean 2020	Mean 2024	Absolute Change
Legal	12.80	16.08	+3.28
Technical	9.64	11.40	+1.76
Organizational	9.45	13.43	+3.97
Capacity Development	9.40	11.39	+1.99
Cooperative	10.41	13.49	+3.07

Technical measures, which have improved to some extent, were the least enhanced compared to the other four pillars. This is an indication that while much effort has been made to set up policies and structures, improvements in technical capacity remain relatively slow. Capacity building has improved moderately because of gradual developments in terms of skills acquisition.

3.3 Country-Level Changes

The vast majority of nations have shown improvements in their respective GCI ratings. Of the total 194 countries, 172 countries showed improvement in their ratings from 2020 to 2024, whereas only 22 countries have displayed

deterioration. This is further proof of the trend observed, which was a global improvement in the country ratings on cybersecurity.

Some countries made huge jumps up in their ratings due to several factors, such as organizational development, implementation of policies, etc. Examples of nations that have registered gains of over 50 points include Eswatini, Ecuador, Togo, Vanuatu, and the Democratic Republic of Congo. Table 3 provides some of the variations found at the national level on cybersecurity.

Table 3: Countries with Largest Improvements and Declines (2020–2024)

Country	GCI 2020	GCI 2024	Change
Eswatini	18.23	79.43	+61.20
Ecuador	26.30	87.11	+60.81
Togo	33.19	90.06	+56.87
Vanuatu	12.88	69.29	+56.40
Congo, Dem. Rep.	5.30	56.75	+51.46
Andorra	26.38	76.50	+50.12
Ethiopia	27.74	76.51	+48.76
Malawi	36.83	80.42	+43.59
Bhutan	18.34	60.77	+42.42
Mozambique	24.18	66.07	+41.88

On the contrary, there was a decline in scores for a few countries. Notably, these were North Macedonia, Iran, Latvia, and Kuwait. It would be best to view such declines not as worsening capacity but as movements downward when compared to a generally upward-trending global setting regarding cybersecurity capability. Such declines might result from lagging improvements in comparison to other countries.

3.4 Ranking Dynamics

However, despite all the changes, the relative position of the states was practically unchanged. The Spearman correlation of ranks in 2020 and 2024 is 0.917, demonstrating a rather stable structure of the global hierarchy by cybersecurity readiness levels. In addition, the Pearson correlation of the total score for two years is also 0.910.

Nevertheless, some changes in ranks were noticed in some states. There were several states that managed to significantly rise their positions, surpassing 50 spots, whereas there were states with negative dynamics, which also had a considerable shift. This fact proves that even though the overall structure does not change, each state can be flexible regarding its position in the hierarchy and change it fast enough depending on how quickly it develops. The internal relationships between the components of the GCI are presented in Table 4.

Table 4: Correlation Matrix (2024)

Variable	Overall	Legal	Technical	Organizational	Capacity	Cooperative
Overall GCI	1.000	0.870	0.950	0.927	0.951	0.916
Legal	0.870	1.000	0.777	0.772	0.775	0.757
Technical	0.950	0.777	1.000	0.847	0.897	0.829
Organizational	0.927	0.772	0.847	1.000	0.844	0.806
Capacity Development	0.951	0.775	0.897	0.844	1.000	0.847
Cooperative	0.916	0.757	0.829	0.806	0.847	1.000

3.5 Top and Bottom Performers

The list of countries with the highest level of cybersecurity preparedness included Finland, the UAE, the UK, Saudi Arabia, South Korea, and Italy, among others, scoring 100 in GCI in 2024. The countries in question demonstrate an

advanced level of preparedness characterized by the availability of all necessary legal measures, highly developed technical measures, good coordination between institutions, and international collaboration.

Countries like Eritrea, the Central African Republic, and Yemen, at the other end of the distribution, were noted to have scored low levels. Countries like those mentioned have limited institutional preparedness and poor technical measures, coupled with low international interaction in relation to cybersecurity. Low performers such as those noted above indicate continued disparities in terms of cybersecurity developments around the world, despite overall advancements. Figure 3 shows the distribution of changes in cybersecurity preparedness.

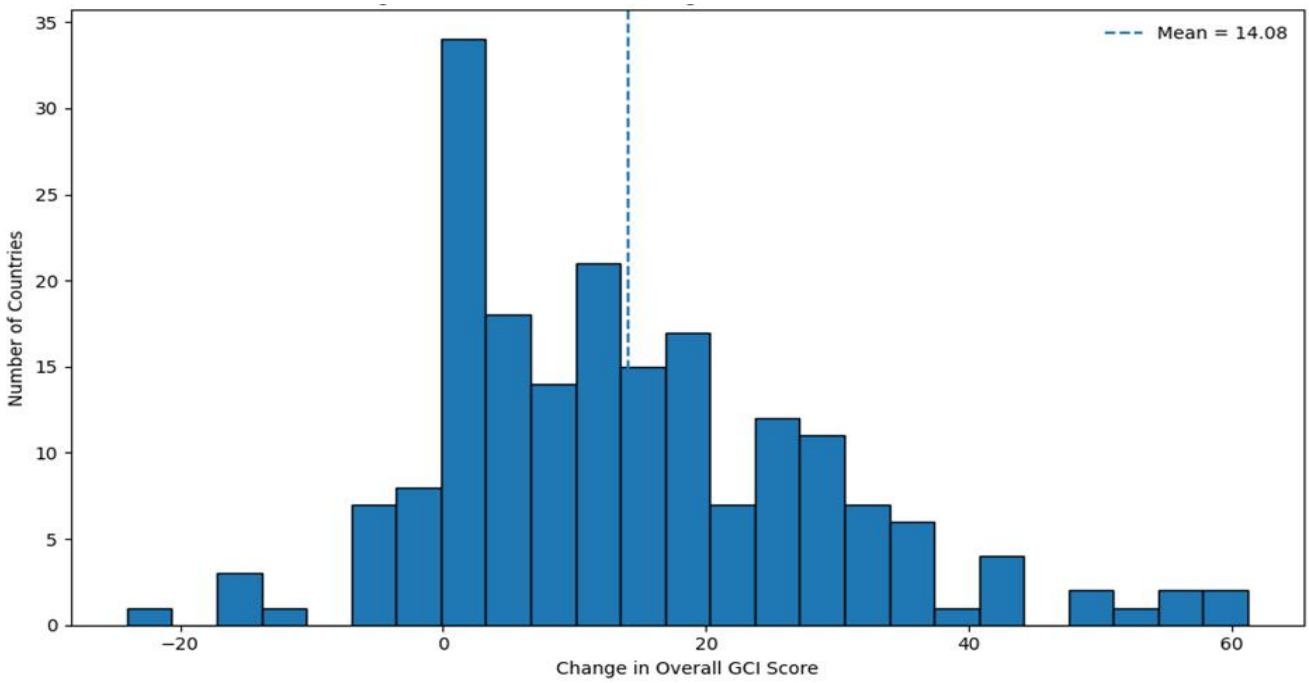

Figure 3: Change Distribution (ΔGCI)

3.6 Internal Structure of the Index

It has been found that there exists a significant correlation between the total score obtained in the GCI and each of the five dimensions considered. Dimensions of capacity development and technical measures have been observed to have the greatest correlation with the total score; thus, these two dimensions seem to play the most significant role in shaping overall preparedness levels. Other dimensions of organizational/cooperative and legal measures correlate significantly with the total score.

Significant correlations among pillars imply that the phenomenon of cybersecurity readiness is a multi-dimensional one, and any improvement achieved in one dimension can have an effect on other dimensions. This multi-dimensional nature of the concept can justify viewing the GCI as a holistic indicator of the level of cybersecurity readiness of a country rather than the sum of several unrelated dimensions. Table 5 summarizes the classification of nations into different groups of cyber readiness.

Table 5: Cluster Characteristics (2024)

Cluster	Mean GCI	Legal	Technical	Organizational	Capacity	Cooperative
Low Preparedness	29.18	10.89	2.57	5.62	3.18	6.92
Medium Preparedness	71.40	17.50	12.64	15.29	11.88	14.09
High Preparedness	96.88	19.87	19.02	19.40	19.13	19.46

3.7 Distributional Patterns and Convergence

The findings from distributional analysis reveal a decline in disparities between nations when it comes to cybersecurity readiness. About this, the contraction in the lower tail of the distribution and the elevation in the median of the distribution indicate that many nations have managed to establish a threshold level of readiness. Conversely, the clustering towards the upper end of the distribution may signal an element of saturation among nations at the upper end.

This implies that there is some partial convergence since the lower-performing nations are catching up, while those that perform relatively better become similar. However, cross-national ranking dynamics are depicted in Figure 4 below, showing both the persistence of the existing hierarchy and changes in some nations.

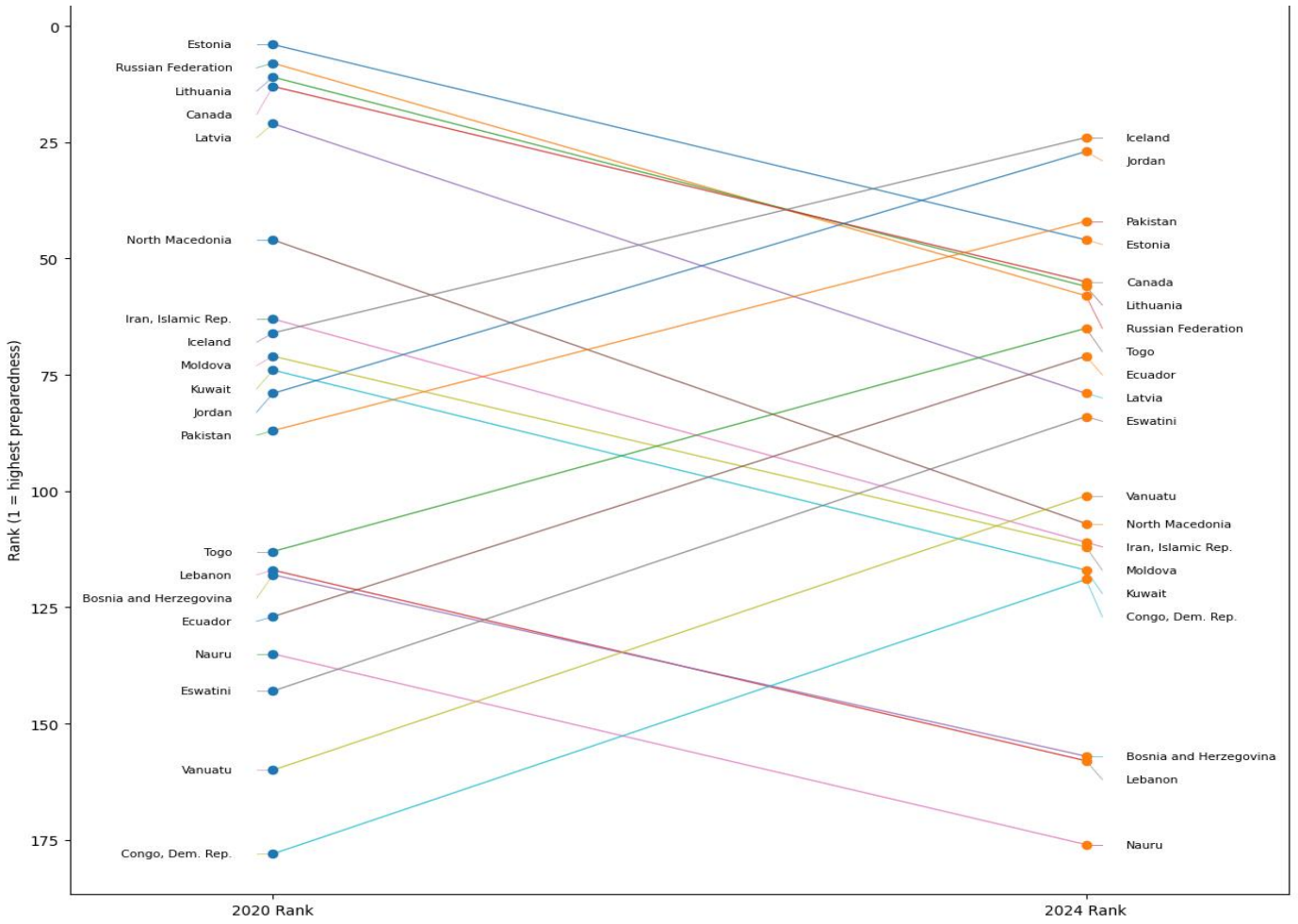

Figure 4: Rank Change Plot

The findings provide evidence that there has been a worldwide trend of better cybersecurity readiness from 2020 through 2024. There are improvements all around due to developments in institutional, regulatory, and international relations aspects. Although improvements in technical ability and talent development have taken place, they are behind other aspects such as institutional and policy-related components.

There seems to be a tendency of convergence on the worldwide stage as indicated by a decline in the number of countries having a low ability level. Rank correlation is still strong, indicating that the global ranking structure has not changed much. Ceiling effects within high-ranking countries indicate deficiencies in the measurement approach used in assessing cybersecurity ability.

4. Discussion

The findings gathered from this research have provided more insight into the evolution of national cybersecurity preparedness and the factors that drive the process. The rise in global GCI values from 2020 to 2024 has been driven by the trend toward cybersecurity institutionalization in states. This conclusion correlates with earlier research on the subject, which shows that state-level readiness is becoming more and more dependent on the process of planning and organization rather than technology (Bruggemann et al., 2022).

On the other hand, the slow growth of the capacity/technical category also indicates certain internal challenges in applying such policies in practice. This conclusion matches the existing literature, according to which technical readiness, including the creation of infrastructure and availability of workforce, requires both persistence and time (Bahuguna et al., 2020). Following the same logic, the maturity model of cybersecurity suggests that while there may not be any problems in building the structure of governance, achieving higher technical complexity and sophistication requires time (Karabacak et al., 2016).

The close relationship that exists between the GCI overall scores and its individual components is evidence of the fact that cybersecurity preparedness is indeed a multi-dimensional variable. According to prior studies, cybersecurity readiness should include all the factors, such as legal, technical, organizational, and cooperation aspects, in order to be effective (Khudyntsev et al., 2021). The very inter-dependence of these dimensions that we see in this study is additional proof of the validity of the use of composite indices such as GCI for measuring the complexities of the national cybersecurity environment (Bruggemann et al., 2022). This inter-dependence also creates the risk of redundancy.

Furthermore, the cluster analysis presents some additional empirical support for the presence of structural differences in the preparedness of countries to cyber threats on a global level. High-preparedness clusters include countries that display well-balanced progress in all three pillars. This indicates that the countries have a well-developed system of government, technical infrastructure, and international relations. On the other hand, countries that belong to low-preparedness clusters are lacking progress in several areas, specifically in technical and capacity-building pillars. This result is supported by resilience-based approaches to cybersecurity assessments, which emphasize the necessity of building a comprehensive capability to improve CIIs (Kulugh et al., 2022).

The findings of the rank consistency, along with the presence of selective mobility for some countries, suggest that although the world order in terms of cybersecurity readiness has remained unchanged to an extent, there are chances for quick progress. This is consistent with the existing literature on factors that determine cyber readiness, wherein good governance, economic development, and institutions have been found to play crucial roles (Makridis & Smeets, 2019). The nations that exhibited significant progress during this research have probably leveraged policy instruments in this regard. Regional and sectoral factors are also important aspects to consider in relation to this research evidence. There is evidence from research that examines specific sectors, for instance, the use of eHealth, which indicates that cybersecurity readiness can be affected by sector-specific needs and conditions (Burke et al., 2019). The connection between cybersecurity readiness and the digital economy also highlights the impact of technological and economic progress in contributing to effective national cybersecurity (Chen et al., 2023).

In addition, there are some implications regarding the methodology in connection with the article being considered. While the adoption of composite indices enables one to compare countries and obtain some benefits from benchmarking, this methodological approach has several limitations. For instance, prior research indicated that index construction could prove difficult due to weighting methods, data access, and national variations (Yarovenko et al., 2020). The presence of ceiling effects in relation to countries that have achieved excellent results in the research implies that current indices are rather inefficient for evaluating prepared countries.

Furthermore, the findings of this study contribute to the ongoing debate concerning cybersecurity resilience by illustrating the need for a more holistic and dynamic viewpoint in relation to national preparedness in this area. In light of the ongoing developments associated with the domain of cyber threats, traditional approaches to their evaluation might turn out to be ineffective. This means that the adoption of resilience-based approaches that consider both preventative and adaptive capacities could serve as a fruitful research direction for future endeavors in this field (Kulugh et al., 2022).

5. Conclusion

This research offers a detailed comparative evaluation of the national cybersecurity readiness levels based on the Global Cybersecurity Index for 194 countries in 2020 and 2024. The results of the analysis show that there is a general improvement in cybersecurity capabilities on a worldwide scale in terms of an increase in the total score as well as a decrease in the number of low-level countries. This is mainly attributable to the evolution in the areas of organizational framework, legislation, and international collaboration, suggesting the focus on institution-based policies within cybersecurity. However, the analysis shows several issues. Moreover, there is stability found in the global ranking of countries. This implies that although progress may be made by all countries, differences and inequalities still exist structurally between different countries. Clustering analysis shows the presence of three categories of nations based on their level of cybersecurity preparedness. Thereby, the study brings out the significance of the use of a comprehensive strategy in managing cybersecurity. Measurement frameworks have been called for to overcome some shortcomings in the existing metrics, including ceiling effects and issues related to comparability.

References

1. Kravets, V. (2019). Comparative analysis of the cybersecurity indices and their applications. Theoretical and Applied Cybersecurity, 1(1).
2. Gorenšek, T., & Trivunčević, R. (2025). Cybersecurity Readiness in the Euro-Mediterranean: A Comparative Review of Literature on National Strategies and Global Indices. Journal of Criminal Justice and Security, 1-32.
3. Ndibe, O. S. (2024). National Cyber Resilience Index: A Data-Driven Framework for Measuring Preparedness. Journal of Computational Analysis and Applications, 33(1A), 729-750.
4. Alguliyev, R., Nabiyev, B., & Dashdamirova, K. (2025). Comparative Analysis of Global Cybersecurity Indices in the Context of the Formation of Cyber Sovereign States. BOOK OF SELECTED PAPERS, 147.
5. Voronenko, I., Nehrey, M., Laptieva, A., Babenko, V., & Rohoza, K. (2022). National cybersecurity: assessment, risks and trends. International Journal of Embedded Systems, 15(3), 226-238.
6. Odebade, A. T., & Benkhelifa, E. (2023). A comparative study of national cybersecurity strategies of ten nations. arXiv preprint arXiv:2303.13938.
7. Shafqat, N., & Masood, A. (2016). Comparative analysis of various national cybersecurity strategies. International Journal of Computer Science and Information Security, 14(1), 129-136.
8. Weng, Y., & Wu, J. (2024). Fortifying the global data fortress: a multidimensional examination of cyber security indexes and data protection measures across 193 nations. International Journal of Frontiers in Engineering Technology, 6(2), 13-28.
9. Sadat, A., Lawelai, H., Younus, M., & Nurmandi, A. (2025). Comparative analysis of National Cyber Security Index: A case study of Pakistan and Indonesia. Kasetsart Journal of Social Sciences, 46(1), 460101-460101.
10. Karabacak, B., Yildirim, S. O., & Baykal, N. (2016). A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness. International Journal of Critical Infrastructure Protection, 15, 47-59.
11. Rameez, M. (2026). Global cybersecurity index dataset (2020–2024). Kaggle. https://www.kaggle.com/datasets/mr1rameez/global-cybersecurity-index-dataset-2020-2024

12. Karabacak, B., Yildirim, S. O., & Baykal, N. (2016). A vulnerability-driven cyber security maturity model for measuring national critical infrastructure protection preparedness. International Journal of Critical Infrastructure Protection, 15, 47-59.
13. Makridis, C. A., & Smeets, M. (2019). Determinants of cyber readiness. Journal of Cyber Policy, 4(1), 72-89.
14. Bahuguna, A., Bisht, R. K., & Pande, J. (2020). Country-level cybersecurity posture assessment: Study and analysis of practices. Information Security Journal: A Global Perspective, 29(5), 250-266.
15. Yarovenko, H. M., Kuzmenko, O. V., & Stumpo, M. (2020). Strategy for determining country ranking by level of cybersecurity.
16. Khudyntsev, M., Davydiuk, A., Lebid, O., Trofymchuk, O., & Zhylin, A. (2021). Cybersecurity Indices: Review and Classification. CPITS II (1), 117-126.
17. Burke, W., Oseni, T., Jolfaei, A., & Gondal, I. (2019, January). Cybersecurity indexes for eHealth. In Proceedings of the australasian computer science week multiconference (pp. 1-8).
18. Bruggemann, R., Koppatz, P., Scholl, M., & Schuktomow, R. (2022). Global cybersecurity index (GCI) and the role of its 5 pillars. Social Indicators Research, 159(1), 125-143.
19. Kulugh, V. E., Mbanaso, U. M., & Chukwudebe, G. (2022). Cybersecurity resilience maturity assessment model for critical national information infrastructure. SN computer science, 3(3), 217.
20. Chen, X., Wang, T., Lin, X., Hinde, D. E., Yan, Q., & Zeljana, Z. (2023). The potential of the digital economy: A comparative assessment of key countries' cybersecurity. International Journal of Education and Humanities, 11(1), 1-7.