Assessment of the Cybersecurity Efficiency of G20 Countries Using Data Envelopment Analysis

Mihraç KÜPELİ
Çankırı Karatekin University, Faculty of Science,
Department of Statistic
Çankırı, Türkiye
mihrackupeli@karatekin.edu.tr
0000-0001-5403-8512

Esra SÖĞÜT
Gazi University, Faculty of Technology,
Department of Computer Engineering Ankara, Türkiye
esrasogut@gazi.edu.tr
0000-0002-0051-2271

2024 17th International Conference on Information Security and Cryptology (ISCTürkiye) | 979-8-3315-3364-9/24/$31.00 ©2024 IEEE | DOI: 10.1109/ISCTRKIYE64784.2024.10779233

***Abstract*—With the rapid advancement of digital transformation, cybersecurity has emerged as a strategic priority for nations worldwide. Ensuring the secure participation of individuals, businesses, and governments in digital environments requires robust cybersecurity measures. However, measuring cybersecurity poses significant challenges due to the complexity of the issue and the limited availability of reliable data. This study addresses these challenges by employing Data Envelopment Analysis (DEA) to assess and rank the cybersecurity performance of G20 countries, utilizing existing cybersecurity indices such as the Global Cybersecurity Index (GCI) and the National Cyber Security Index (NCSI). The results indicate that Indonesia, France, India, and Japan exhibit efficient cybersecurity performance, while Mexico demonstrates the weakest performance among the G20 nations. This research provides valuable insights for policymakers and stakeholders to develop strategies aimed at enhancing national cybersecurity capabilities.**

Keywords—cyber security index, data envelopment analysis, efficiency, G20 countries

I. Introduction

With the rapid and effective spread of digital transformation, cybersecurity has become a strategic priority at both national and international levels. Today, the secure participation of individuals, businesses, and governments in digital environments depends on the presence of effective protection strategies against cyber threats. However, ensuring this secure environment requires measuring and managing cybersecurity, which involves complex and multifaceted challenges. Measuring cybersecurity takes place in an ecosystem where various actors have different incentives, data is limited, and methodological approaches vary. One of the challenges in measuring cybersecurity is that many actors in the ecosystem are reluctant to share the difficulties they face, the incidents they experience, or their levels of cybersecurity preparedness with malicious individuals [1]. Such situations create significant uncertainties in understanding the scope and impact of cybersecurity threats.

Measuring cybersecurity uncertainties can complement existing statistics to help predict emerging cybersecurity trends, develop more focused awareness programs, and build a more secure digital ecosystem [1]. However, measuring these uncertainties is not easy due to the lack of reliable data sources and the absence of data standards. Most existing data sources come either from official statistics or from private sector firms.

In both cases, data collection and reporting methods have various limitations due to different incentives and methodological approaches [1]. As a result, the challenges of measuring cybersecurity emphasize the need for more sophisticated and comprehensive measurement methods in this area. This study aims to evaluate the cyber security performance of G20 countries. This study employs Data Envelopment Analysis (DEA), a powerful methodology that can be used to rank a country's cybersecurity performance in comparison to other countries. To avoid uncertainties and gaps in the data, indices previously created for cybersecurity performance measurements are utilized in this study.

Chapter 2 of the study reviews related research in the literature. Chapter 3 presents the materials and methods employed in the study. The findings obtained are given in the next chapter. The fifth chapter presents the results of the study, comments, and suggestions for further studies.

II. Related Works

In this section, studies conducted to assess the cybersecurity performance of countries are examined. Due to the uncertainty of the variables that determine cybersecurity performance and the lack of available data for existing variables, the number of sources in the literature is limited. Nehrey et al. (2022) utilized the DEA methodology to determine the cybersecurity effectiveness of countries in Central Asia and Europe. Consistent with the nature of the methodology, Internet Users (IU), GDP per capita, Area, Digital Development Level (DDL), and Population density were used as input variables, while the Global Cybersecurity Index (GCI) and National Cybersecurity Index (NCSI) indices were employed as output variables. The study presented the results of analyzing existing indices that allow the evaluation of countries' cybersecurity levels and identify priority areas for the improvement of Ukraine's cybersecurity system [2].

Vevera et al. (2022) calculated an indicator called SECDIG for 11 Eastern European countries using the NCSI, the GCI, the Network Readiness Index (NRI), and the ICT Development Index (IDI). They proposed a multi-criteria approach utilizing the Complex Proportional Assessment (COPRAS) method for this calculation [3].

Radulescu et al. (2024) proposed a new method for calculating the Cyber Safety Score (CSS), which is simply

Authorized licensed use limited to: T.C. Cumhurbaskanligi Kutuphanesi. Downloaded on December 12,2024 at 22:09:11 UTC from IEEE Xplore. Restrictions apply.

the arithmetic mean of GCI, NCSI, and Cyber Security Exposure Index (CEI). In this study, multi-criteria methods such as VIKOR (Vise Kriterijumska Optimizacija I Kompromisno Resenje), Technique for Order of Preference by Similarity to Ideal Solution (TOPSIS), and COPRAS were used. The indices obtained in this study, along with the Cyber Safety Score (CSS), were compared for 15 European countries [4].

Although there are various indices created using different indicators in the context of cybersecurity, studies that provide a comprehensive evaluation of these indices at the country level are quite limited. Therefore, this study aims to contribute to the cybersecurity literature by evaluating the efficiency of countries.

III. Materials And Methods

A. Methodology

To determine the efficiency of Decision Making Units (DMU), Charnes et al. (1978) proposed a methodology called DEA. The fundamental concept of the methodology is the ratio of output to input. In cases with multiple inputs and/or outputs, this is extended to the ratio of weighted outputs to weighted inputs. The following equations were formulated by attempting to maximize this ratio [5].

$$E_k = min \frac{\sum_{i=1}^{m} v_i X_{ik}}{\sum_{r=1}^{p} u_r Y_{rk}}$$

$$\frac{\sum_{i=1}^{m} v_i X_{ij}}{\sum_{r=1}^{p} u_r Y_{rj}} \geq 1$$

$$u_r \geq \varepsilon \quad v_i \geq \varepsilon \quad j = 1, \ldots, n \quad r = 1, \ldots, p \quad i = 1, \ldots, m \qquad (1)$$

Here, u_r denotes the weight assigned to the r^{th} output for the k^{th} DMU, v_i denotes the weight assigned to the i^{th} input for the k^{th} DMU, Y_{rk} represents the r^{th} output produced by the k^{th} DMU, X_{ik} represents the i^{th} input used by the k^{th} DMU, Y_{rj} represents the r^{th} output produced by the j^{th} DMU, and X_{ij} represents the i^{th} input used by the j^{th} DMU. ε is defined as a very small positive number. The minimum possible value of the objective function is 1, and if this value equals 1, it indicates that the k^{th} Decision-Making Unit (DMU) is efficient. If the value is greater than 1, it indicates that the k^{th} DMU is not efficient. Equation (1) is referred to as the proportional model. The denominator of the objective function in this model is set equal to 1 and added to the constraints, resulting in the linear model shown in Equation (2).

$$E_k = min\left(\sum_{r=1}^{m} v_i X_{ik}\right)$$
$$\left(\sum_{r=1}^{p} u_r Y_{rk}\right) = 1$$
$$\left(\sum_{r=1}^{p} u_r Y_{rj}\right) - \left(\sum_{i=1}^{m} v_i X_{ij}\right) \leq 0$$
$$u_r \geq \varepsilon \quad v_i \geq \varepsilon$$
$$j = 1, \ldots, n \quad r = 1, \ldots, p \quad i = 1, \ldots, m \qquad (2)$$

B. Data

DEA is independent of the measurement units of inputs and outputs, making it highly flexible in the selection of desired inputs and outputs [5, 6]. However, despite this advantage of DEA, due to uncertainties in measuring cybersecurity, careful consideration is necessary when selecting variables (input and output). Various indicators are used in the literature as measures of cybersecurity, and it has become inevitable to conduct a comprehensive evaluation of these indicators, which are calculated using different variables. In this study, the Global Uncertainty Index (GUI) and Internet User (IU) were selected as the input variables, while the GCI, the NCSI, and the DDL indices were chosen as output variables.

The GUI was constructed using Economist Intelligence Unit (EIU) country reports for 143 countries [7]. This index reflects uncertainty related to economic and political developments. The global GUI index for the period from Q1 1990 to Q2 2024 is shown in Fig. 1. Significant events such as SARS, the Gulf War, the Euro debt crisis, Brexit 2016, the US elections, and the Covid-19 pandemic are associated with sudden increases in the index. In this study, the GUI index was used as an input. It will be concluded that DMUs achieving the maximum output while keeping this variable constant are leading countries in terms of cybersecurity performance.

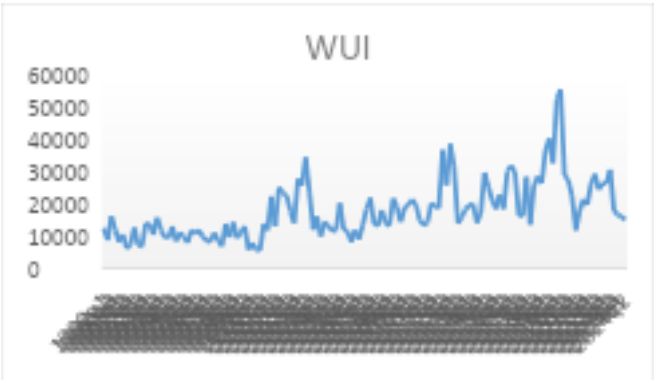


Fig. 1. The global GUI index for the period from Q1 1990 to Q2 2024 [8]

The IU represents the proportion of internet users in a country. In 2024, there are 5.35 billion internet users worldwide. This number is expected to reach 7.9 billion by 2029 [9]. The impact of this increase in internet usage on the field of cybersecurity is inevitable. Therefore, the proportion of internet usage was included as one of the input variables in this study.

The GCI is a reliable reference for measuring countries' commitment to cybersecurity at a global level and for raising awareness about the importance and various dimensions of the issue. Given the broad application of cybersecurity across many sectors and industries, each country's development or engagement level is assessed according to five pillars: Technical Measures, Legal

Authorized licensed use limited to: T.C. Cumhurbaskanligi Kutuphanesi. Downloaded on December 12,2024 at 22:09:11 UTC from IEEE Xplore. Restrictions apply.

Measures, Organizational Measures, Cooperation, and Capacity Building [10]. These are added together to calculate an overall score. A higher index indicates a higher level of reliability in the context of cybersecurity. Due to its significance as a cybersecurity indicator, the GCI index was selected as one of the output variables in this study.

The NCSI is a global, dynamic index that measures countries' preparedness for preventing cyber threats and managing cyber incidents. It focuses on the measurable aspects of cybersecurity implemented by central governments. This index is based on data collected from sources such as legitimate processes, official papers, and government websites. Due to its different focus and the variables it uses, it has a distinct ranking from the GCI index. For this reason, it was selected as one of the output variables indicating cybersecurity performance in this study.

The DDL is calculated according to Equation 3, using values from the E-Government Development Index (EGDI) and the NRI. It is essentially an indicator of the level of digitalization in countries. If this index is greater than the NCSI index, it can be inferred that the country's digitalization is ahead of its cybersecurity efforts. Conversely, if the DDL is less than or equal to the NCSI index, it can be said that the country's digitalization is on par with or behind its cybersecurity efforts.

$$DDL = \frac{NRI\,\%+EGDI\%}{2} \quad (3)$$

IV. Findings

To evaluate the cybersecurity efficiency of G20 countries, an output-oriented CCR DEA method was used. For this, two input variables and three output variables were selected. Table 1 presents the efficiency scores calculated using the DEA method and the rankings of the countries.

Table I
EFFICIENCY SCORES AND RANKINGS FOR COUNTRIES

Country	Efficiency Score	Rank
Türkiye	1.280	16
United States	1.074	8
Germany	1.024	7
Argentina	1.332	17
Australia	1.006	6
Brazil	1.218	13
United Kingdom	1.109	10
China	1.089	9
Indonesia	1	1
France	1	1
South Africa	1.355	18
India	1	1
Republic of Korea	1.123	11
Italy	1.001	5
Japan	1	1
Canada	1.141	12
Mexico	1.356	19
Russian Federation	1.246	15
Saudi Arabia	1.243	14
G20 mean	**1.137**	

According to the analysis, countries with an efficiency score of 1 are considered efficient. These countries are Indonesia, France, India, and Japan. Italy, with an efficiency score very close to these, is ranked fourth. The three countries with the lowest efficiency scores are Mexico, South Africa, and Argentina, respectively.

To become an efficient country, Argentina needs to increase its output by approximately 34% (1.332). Among the G20 countries, Türkiye is ranked 16th. If Türkiye aims to become efficient in terms of cybersecurity, it should target increasing its output by at least 28%. The average efficiency score of G20 countries is 1.137. If G20 countries increase their cybersecurity-related outputs by approximately 14%, they could become an efficient community.



Fig. 2. Comparison of countries' efficiency scores against the G20 average

Figure 2 shows the status of countries' efficiency scores compared to the G20 average. According to the provided graph, Türkiye, Argentina, Brazil, South Africa, Canada, Mexico, Russia, and Saudi Arabia have efficiency scores above the G20 average. To enhance their cybersecurity efficiency performance, these countries need to increase their outputs more compared to the community average.

Table II
CYBER SECURITY RANKINGS OF COUNTRIES

Country	GCI	NCSI	DDL	DEA
Türkiye	10	15	15	16
United States	1	11	2	8
Germany	12	1	3	7
Argentina	19	12	13	17
Australia	11	10	6	6
Brazil	13	16	14	13
United Kingdom	2	2	4	10
China	16	16	12	9
Indonesia	15	12	18	1
France	8	3	7	1
South Africa	18	19	17	18
India	9	9	19	1
Republic of Korea	4	8	1	11
Italy	14	5	9	5
Japan	6	12	5	1
Canada	7	7	8	12
Mexico	17	18	16	19
Russian Federation	5	6	10	15
Saudi Arabia	2	3	11	14

Table 2 shows the rankings of countries according to GCI, NCSI, DDL indexes and DEA method. The top three countries according to GCI index are United States, United

Authorized licensed use limited to: T.C. Cumhurbaskanligi Kutuphanesi. Downloaded on December 12,2024 at 22:09:11 UTC from IEEE Xplore. Restrictions apply.

Kingdom and Saudi Arabia. According to NCSI index, they are Germany, United Kingdom, France and Saudi Arabia. According to DDL, they are Republic of Korea, United States and Germany. According to DEA method, they are Indonesia, France, India and Japan. The last 3 countries according to GCI index are Mexico, South Africa and Argentina. According to NCSI index, they are Brazil, China, Mexico and South Africa. According to DEA method, they are Argentina, South Africa and Mexico. When these rankings are evaluated, Mexico is the country that is at the bottom of cyber security in all three techniques (GCI, NCSI, DEA). It is quite interesting that Saudi Arabia, which is in the top three according to GCI index, is among the last three countries according to DEA method. The reason for this situation is that the IU variable, which is used as an input in the DEA method and represents the rate of internet users in the country, is reported as 100% in the official statistics for Saudi Arabia. Since the DEA methodology aims for maximum output with minimum input, this high value in the input variable resulted in the country receiving a low efficiency score.

TABLE III
SPEARMAN CORRELATION COEFFICIENT

	GCI	NCSI	DDL	DEA
GCI	1	0.586	0.620	0.227
NCSI	0.586	1	0.579	0.380
DDL	0.620	0.579	1	0.269
DEA	0.227	0.380	0.269	1

Spearman correlation coefficients calculated between the rankings of GCI, NCSI, DDL indexes and DEA methodology are presented in Table 3. A moderately positive significant correlation was found between the rankings of GCI, NCSI and DDL indexes. There is no significant correlation between the rankings of DEA method and other indexes. As a result, a new cybersecurity performance ranking was created by using GCI, NCSI and DDL indexes with the DEA method.

V. CONCLUSION

Measuring cybersecurity and making comparisons on a global and national scale is quite challenging. This is because cybersecurity is both a highly complex issue and difficult to obtain data for its various components. Despite these challenges, the GCI was first established in 2014. Subsequently, the NCSI index was calculated, providing different indexes for the same countries. In this study, these indexes, which are indicators of cybersecurity, were used to evaluate the cybersecurity performance of G20 countries based on DEA methodology. The study revealed that four countries (Indonesia, France, India, and Japan) had efficient performance, while Mexico had the worst performance. This DEA-based study aims to guide strategies for improving countries' cybersecurity performance.

Using the references in the methodology, each country can define its specific strategy. Additionally, by using different indexes or indicators for input and output variables, the focus of the study can be altered. For example, the economic dimension of cybersecurity could also be included in the study. The scope of the study can be expanded to make comparisons between OECD, EU, or global countries. Since DEA is a data-driven method, changes in the scope, focus, or data sources of the study will completely alter the results and provide different perspectives.

REFERENCES

[1] OECD Report, "New perspectives on measuring cybersecurity", OECD Digital Economy Papers, No. 366, OECD Publishing, Paris, 2024, https://doi.org/10.1787/b1e31997-en.

[2] Nehrey, M., Voronenko, I., and Salem, A. B. M., "Cybersecurity Assessment: World and Ukrainian Experience", 12th International Conference on Advanced Computer Information Technologies (ACIT), pp. 335-340, 2022, September.

[3] Vevera, A. V., Cirnu, C. E., and Rădulescu, C. Z., "A multi-criteria approach for the calculation of a complex indicator of Cyber Security and Digital Development", Romanian Journal of Information Technology and Automatic Control, ISSN 1220-1758, vol. 32(4), pp. 19-32, 2022. https://doi.org/10.33436/v32i4y202202.

[4] Rădulescu, C. Z., Vevera, A. V., and Sandu, I. E., "Evaluation and analysis of a set of cyber security indices using multi criteria methods", Romanian Journal of Information Technology and Automatic Control, ISSN 1220-1758, vol. 34(1), pp. 45-58, 2024. https://doi.org/10.33436/v34i1y202405.

[5] Charnes, A., and Cooper, W. W., "Preface to topics in data envelopment analysis", Annals of Operations research, vol. 2(1), 59-94, 1984.

[6] Charnes, A., Cooper, W. W., Golany, B., Seiford, L., and Stutz, J., "Foundations of data envelopment analysis for Pareto-Koopmans efficient empirical production functions", Journal of Econometrics, vol. 30(1-2), 91-107, 1985.

[7] International Monetary Fund, "World Uncertainty Index (WUI): Global", 2024. [Online]. Available: https://worlduncertaintyindex.com.

[8] Ahir, H., Bloom, N., & Furceri, D. (2022). The world uncertainty index (No. w29763). NBER WORKING PAPER SERIES. National bureau of economic research, Cambridge, MA.

[9] Statista, "Number of internet and social media users worldwide as of July 2024", 2024. [Online]. Available: https://www.statista.com/statistics/617136/digital-population-worldwide/.

[10] The Telecommunication Development Sector, "Global Cybersecurity Index", 2024. [Online]. Available: https://www.itu.int/en/ITU-D/Cybersecurity/Pages/global-cybersecurity-index.aspx.

Authorized licensed use limited to: T.C. Cumhurbaskanligi Kutuphanesi. Downloaded on December 12,2024 at 22:09:11 UTC from IEEE Xplore. Restrictions apply.