Geliş/Received: 05.04.2025 | Revizyon/Revised: 20.08.2025 |Kabul/Accepted: 13.10.2025 | Erken Görünüm/Early View: 30.11.2025

Research Article | Araştırma Makalesi

LOPCOW-MARCOS yaklaşımıyla BRICS ülkelerinde siber güvenlik değerlendirmesi

Tayfun Öztaş | Doç.Dr, Pamukkale Üniversitesi, toztas@pau.edu.tr, 0000-0001-8224-5092

Corresponding author/Sorumlu yazar: Tayfun Öztaş

Öz

Dijitalleşmenin bir sonucu olarak sanal ortamda paylaşılan veri miktarında büyük bir artış yaşanmaktadır. Ancak kişisel verilerin çalınması, fidye yazılımı saldırıları, kimlik avı saldırıları, sistem açıkları gibi siber güvenlik riskleri; ekonomik, yasal, hizmet kesintileri ve itibar kaybı gibi sonuçlar doğuran olaylara yol açabilmektedir. Bu nedenle, siber güvenlik ile ilgili faaliyetler ulusal düzeyde, stratejik ve bütüncül bir yaklaşımla yürütülmek zorundadır. Stratejik bir planlama konusu olarak siber güvenlik, uluslararası düzeyde ilgi gören bir araştırma alanıdır. Bu çalışmada BRICS ülkelerinin siber güvenlik performanslarını karşılaştırmak için Uluslararası Telekomünikasyon Birliği'nin (International Telecommunication Union) Küresel Siber Güvenlik Endeksi (Global Cybersecurity Index) verilerinden faydalanılarak, LOPCOW ve MARCOS yöntemleriyle bir analiz yapılmıştır. Yapılan hesaplamalarda en önemli kriterin "İş birliği ölçümleri" olduğu belirlenirken; Birleşik Arap Emirlikleri, Endonezya ve Mısır'ın en iyi performans gösteren ülkeler olduğu tespit edilmiştir. Önerilen LOPCOW-MARCOS yaklaşımının kriter ağırlıklarındaki değişimlere karşı hassasiyetini ölçmek için beş farklı senaryo ile yürütülen duyarlılık analizinde yöntemin tutarlı sonuçlar ürettiği görülmüştür. Ayrıca önerilen yaklaşımın sonuçlarının güvenirliği TOPSIS, MABAC, MAIRCA, ARAS ve CoCoSo yöntemleriyle karşılaştırmalı analiz yapılarak test edilmiştir. Bulgular, önerilen yaklaşımın TOPSIS yöntemiyle çok güçlü bir ilişkiye (ρ=0,9876), diğer yöntemler ile tam uyuma sahip olduğunu göstererek güvenilir sonuçlar verdiğini doğrulamaktadır.

Anahtar Kelimeler: Dijitalleşme, Siber Güvenlik, ÇKKV, BRICS Ülkeleri **JEL Kodları:** D70, P47

Cybersecurity assessment in BRICS countries using the LOPCOW–MARCOS approach

Abstract

There has been a dramatic increase in the volume of data shared in virtual environment as a result of digitalization. However, cybersecurity risks such as personal data breaches, ransomware, phishing attacks, and system vulnerabilities may lead to incidents with economic, legal, service outage, and loss of reputation consequences. Therefore, cybersecurity-related activities must be carried out at the national level with a strategic and holistic approach. As a strategic planning issue, cybersecurity is a prominent field of research at the international level.In this study, the cybersecurity performance of BRICS countries is analyzed using data from the International Telecommunication Union's Global Cybersecurity Index through the LOPCOW and MARCOS methods. The analysis identified "Cooperation measures" as the most significant criterion, with the United Arab Emirates, Indonesia, and Egypt emerging as the top-performing countries. A sensitivity analysis conducted using five different scenarios to test the proposed LOPCOW-MARCOS approach revealed that the method yields consistent results despite variations in criterion weights. The reliability of the proposed methodology has been tested through comparative analysis including TOPSIS, MABAC, MAIRCA, ARAS and CoCoSo methods. The findings confirm that the proposed approach provides reliable results by showing that it has a very strong correlation with the TOPSIS method (ρ=0.9876) and fully consistent with other methods.

Keywords: Digitalization, Cybersecurity, MCDM, BRICS Countries **JEL Codes:** D70, P47

Extended Summary

With the advent of digitalization, computers, mobile devices, and the internet have become inseparable elements of daily life. As technological advancements and digital transformation continue to reshape modern interactions, the volume of data shared among individuals, institutions, and organizations has naturally increased. While this shift has led to benefits such as improved operational efficiency and reduced costs, it has also raised significant concerns regarding the secure storage and management of shared data (Craigen et al., 2014, p. 13). The growing reliance on digital platforms, especially after the Covid-19 pandemic, which accelerated the adoption of remote work—has substantially expanded the amount of data exchanged in virtual environments. As a consequence, cybersecurity issues have surged in both frequency and impact (Yusif and Hafeez-Baig, 2021, p. 492). Increasing

How to cite this article / Bu makaleye atıf vermek için:
Öztaş, T. (2026). LOPCOW-MARCOS yaklaşımıyla BRICS ülkelerinde siber güvenlik değerlendirmesi. *KOCATEPEİİBFD, 28*(1), 21-37.
https://doi.org/10.33707/akuiibfd.1670493

cyberattacks have become a serious threat with the potential to disrupt operations, cause financial loss, and erode public trust (Almeida, 2025, p. 1).

This study aims to compare the cybersecurity performance of BRICS countries by applying a Multi-Criteria Decision-Making (MCDM) methodology. Cybersecurity indices, which are developed based on specific methodologies by specialized organizations, evaluate the performance of countries or sectors (alternatives) across several key dimensions (criteria). In this context, the Global Cybersecurity Index (GCI) provided by the International Telecommunication Union (ITU) is used as the primary data source for the analysis. The weights of the evaluation criteria were calculated using the LOPCOW (Logarithmic Percentage-Change-driven Objective Weighting) method, while the final ranking of countries was established through the MARCOS (Measurement of Alternatives and Ranking according to Compromise Solution) method. By adopting this approach, the study aims to contribute to the growing body of international research on cybersecurity, a field of increasing strategic importance. The integration of LOPCOW and MARCOS methodologies applied together for the first time in cybersecurity performance evaluation represents a novel and original contribution to the existing literature.

A review of the literature reveals a limited number of studies that systematically compare the cybersecurity performance of countries, indicating that this area remains underexplored and holds considerable research potential. Most of the existing studies rely on the AHP (Analytical Hierarchy Process) and TOPSIS (Technique for Order of Preference by Similarity to Ideal Solution) methods, including their fuzzy variants, to determine criteria weights and rank alternatives. Other approaches such as Entropy, BWM (Best Worst Method), DEMATEL (Decision-Making Trial and Evaluation Laboratory), and VIKOR (Vise Kriterijum-ska Optimizacija I Kompromisno Resenje) are also occasionally used. The present study distinguishes itself by employing LOPCOW and MARCOS, thereby highlighting their applicability in the context of national cybersecurity assessments and reinforcing the study's originality. Both the research problem and the methodology aim to fill a meaningful gap in literature.

The proposed methodology involves four stages. In the first stage, the importance levels (weights) of the selected criteria were determined using the LOPCOW method. In the second stage, the BRICS countries were ranked using the MARCOS method based on the previously calculated weights. In the third stage, a sensitivity analysis was performed to verify the robustness of the LOPCOW-MARCOS results to changes in criteria weights under five different scenarios. In the final stage, a comparative analysis was conducted to test the reliability of the LOPCOW-MARCOS results by benchmarking them against rankings generated by five widely used MCDM techniques: TOPSIS, MABAC (Multi Attributive Border Approximation Area Comparison), ARAS (Additive Ratio Assessment), MAIRCA (Multi-Attributive Ideal-Real Comparative Analysis), and CoCoSo (Combined Compromise Solution).

Based on the LOPCOW analysis, the most important criterion was "Cooperation Measures" ($w_5 = 0.2390$), followed by "Legal Measures" ($w_1 = 0.2267$), "Organizational Measures" ($w_3 = 0.1978$), and "Capacity Development Measures" ($w_4 = 0.1910$). "Technical Measures" ($w_2 = 0.1455$) was identified as the least significant. These differences in importance highlight key areas for improvement and can guide decision-makers in prioritizing efforts. Improvements in highly weighted criteria are expected to yield more substantial benefits in overall performance. Based on the MARCOS analysis, the United Arab Emirates (A1), Indonesia (A4), and Egypt (A9) demonstrated the highest benefit function values and shared the top positions. India (A7), Brazil (A2), Russia (A10), and China (A3) followed in the rankings. Meanwhile, South Africa (A6), Ethiopia (A5), and Iran (A8) were identified as the lowest-performing countries in terms of cybersecurity.

A structured sensitivity analysis was performed by systematically varying the weight of criteria under five different scenarios. The results confirmed that the ranking outcomes remained largely stable, indicating the model's reliability and resistance to changes in criteria weights. To validate the reliability of the ranking results, a comparative analysis was conducted using the same criteria weights derived from LOPCOW and applying them to the TOPSIS, MABAC, ARAS, MAIRCA, and CoCoSo methods. The correlation between the LOPCOW-MARCOS results and the TOPSIS method was found to be very strong ($\rho = 0.9876$), while complete consistency was observed with the other methods. The results support the reliability and effectiveness of the LOPCOW-MARCOS methodology in assessing the cybersecurity performance of BRICS countries.

As with any research, this study has certain limitations and opens avenues for future investigation. Since the analysis is based on data from 2024, the findings are specific to that year. Including data from multiple years could allow for the examination of temporal trends in national cybersecurity performance. Moreover, expanding the dataset to cover different dimensions of cybersecurity or incorporating alternative indices could enhance the comprehensiveness of the evaluation. Future studies may also benefit from combining objective data with expert judgment, integrating subjective insights into the weighting process to enrich the analysis further.

Giriş

Dijitalleşme ile bilgisayarlar, mobil cihazlar ve internet günlük hayatın ayrılmaz bir parçası haline gelmiştir. Teknolojik gelişmelerin ve dijitalleşmenin hayatımıza getirdiği yenilikler ile kişiler, kurum ve kuruluşlar arasında veri paylaşımı da doğal olarak artmıştır. İşlem kolaylığı ve maliyetlerdeki düşüşler gibi olumlu iyileşmelere karşın paylaşılan bilgilerin, verilerin güvenli bir şekilde saklanıp saklanmadığı önemli bir husus haline gelmiştir. Craigen vd. (2014, s. 13) tarafından siber güvenliğin çok boyutlu olması nedeniyle kısa ve genel kabul görmüş bir tanımın olmadığı belirtilmektedir. Buna karşın, Türk Dil Kurumu (TDK) siber güvenliği, "Bilişim sistemlerinde kişiler ve kurumlar arasında oluşturulan iletişim ortamının ve elektronik ortamda paylaşılan bilgilerin bütünlüğünün ve gizliliğinin korunması durumu" şeklinde tanımlamaktadır.

Kurum ve kuruluşların hizmetlerini giderek artan şekilde elektronik ortamda sunmaya başlaması, özellikle Covid-19 pandemisi sonrası iş hayatında bir dönüşüm yaratan uzaktan çalışmanın yaygınlaşması gibi faktörler sanal ortamda paylaşılan veri miktarını artırmış ve bunun sonucunda da siber güvenlik ile ilgili sorunlarda büyük bir artış yaşanmıştır (Yusif ve Hafeez-Baig, 2021, s. 492). Artan siber saldırılar kurum ve kuruluşların faaliyetlerinin devamlılığını etkileme, finansal kayıp ve kamuoyunda güven kaybı gibi ciddi sonuçları olabilen bir problem haline gelmiştir (Almeida, 2025, s. 1). Siber saldırıların kaynağının, zamanının ve nasıl gerçekleşeceğinin bilinememesi nedeniyle siber güvenlik, kurum ve kuruluşlar için yüksek riskli bir hale gelmektedir (Yusif ve Hafeez-Baig, 2021, s. 490). Dünya Ekonomik Forumu (World Economic Forum) tarafından siber güvenliğin kısa dönemli küresel riskler arasında dördüncü sırada yer aldığı belirtilmektedir (World Economic Forum, 2024, s. 8). Siber güvenliğin kurum ve kuruluşların ötesine geçerek küresel bir risk olarak değerlendirilmesi, bu hususun bireylerin ya da kurumların inisiyatifine bırakılamayacak kadar önemli olduğunu göstermektedir.

Siber güvenlikle ilgili riskler, öngörülemez olması nedeniyle tamamen ortadan kaldırılamamaktadır (Bodin vd., 2018, s. 528). Bu nedenle kurum ve kuruluşlar tarafından önemli miktarda personel istihdamı ve yatırımlar yapılmaktadır (AlDaajeh ve Alrabaee, 2024, s. 1; Nelson ve Wang, 2024, s. 66). Böylelikle yatırım, istihdam ve personelin eğitimi yoluyla risklerin azaltılması planlanmaktadır (Shaikh ve Siponen, 2024, s. 1109). Ancak siber güvenlik alanında istihdam edilecek personel sayısının talebe yetmemesinin iş gücü piyasasında önemli bir açık oluşturduğu da bilinmektedir (Almeida, 2025, s. 1; Catota vd., 2019, s. 2).

Bir kuruluşun siber güvenlik açısından önlem alması tek başına yeterli değildir. Örneğin tedarik zincirindeki herhangi bir paydaşın yeterli siber güvenlik tedbirleri almaması nedeniyle müşteri verilerinin sızmasına yol açabilmektedir (Song vd., 2024, s. 1). Bu nedenle siber güvenlik, bilgi işlemle ilgili bir departmanın ya da bir yöneticinin sorumlu olamayacağı kadar karmaşık ve çok boyutlu bir konudur. Siber güvenlik risklerinin yol açabileceği sorunlar nedeniyle, ülkeler daha geniş bir bakış açısıyla ulusal siber güvenlik stratejileri oluşturmaktadır (Proudfoot vd., 2024, s. 2). Örneğin, Türkiye'de 2024-2028 dönemi için Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, 7 Eylül 2024'te Resmî Gazete'de yayımlanmıştır (T.C. Ulaştırma ve Altyapı Bakanlığı, 2024).

Siber güvenlik, küresel düzeyde önem taşıdığından, çeşitli kuruluşlar tarafından ülkeler veya sektörler düzeyinde siber güvenlik düzeylerini ölçen endeksler oluşturulmaktadır. Oluşturulan bu endeksler sayesinde, ülkeler veya sektörler arasında karşılaştırma yapmak, zaman içindeki gelişmeleri takip etmek mümkün hale gelmektedir. Bu endekslerden bazıları şunlardır: ITU'nun Küresel Siber Güvenlik Endeksi (Global Cybersecurity Index-GCI) (ITU, 2024a), Cisco'nun Siber Güvenlik Hazırlık Endeksi (Cisco Cybersecurity Readiness Index) (Cisco, 2024), e-Yönetişim Akademisi Vakfı'nın (e-Governance Academy Foundation) Ulusal Siber Güvenlik Endeksi (National Cyber Security Index-NCSI) (e-Governance Academy Foundation, 2025), Avrupa Birliği Siber Güvenlik Ajansı'nın (European Union Agency For Cybersecurtiy) ENISA Tehdit Görünümü Raporu (ENISA Threat Landscape) (ENISA, 2024).

Bu çalışmanın temel amacı, BRICS ülkelerinin siber güvenlik performanslarını Çok Kriterli Karar Verme (ÇKKV) yöntemlerini kullanarak karşılaştırmaktır. Siber güvenlik endeksleri, belirli metodolojilere dayalı olarak çeşitli kriterler altında ülkelerin veya sektörlerin performanslarını değerlendirmektedir. Bu bağlamda çalışmada GCI (ITU, 2024a) verisi kullanılarak çok kriterli bir değerlendirme gerçekleştirilmiştir. Çalışmada öncelikle kriterlerin ağırlıklarını nesnel biçimde hesaplamak amacıyla LOPCOW yöntemi kullanılmıştır. LOPCOW yöntemi, karar vericilerin kişisel önyargılarından bağımsız olarak kriterlerin ağırlık değerlerinin hesaplanmasına imkân sağlamaktadır. Yöntemin logaritma temelli yapısı kriter değerleri belirlenirken her bir kriterin taşıdığı bilgi miktarını hesaplayarak, daha çok bilgi içeren kriterlere daha yüksek kriter değerleri atayabilmektedir. Ayrıca LOPCOW yönteminin sade hesaplama yapısı, hesaplama karmaşıklığını azaltarak uygulama kolaylığı sağlamaktadır. Ülkelerin sıralanmasında ise MARCOS yöntemi tercih edilmiştir. Bu yöntem, ideal ve ideal olmayan çözümleri dikkate alarak göreli fayda dereceleri üzerinden dengeli bir değerlendirme sunmaktadır. Yöntemin çok sayıda kriter ve alternatifle çalışabilmesi karar vericiler için karmaşık problemleri ele alabilme avantajını sağlamaktadır. Bu çerçevede önerilen LOPCOW–MARCOS bütünleşik yaklaşımı, öznel etkilerden arındırılmış, veri odaklı ve güvenilir bir değerlendirme mekanizması sunmaktadır. Literatürde ilk kez siber güvenlik performans analizi için kullanılan bu metodoloji, alan yazına önemli bir katkı sağlamayı hedeflemektedir. Yapılan analiz ile şu sorulara yanıt aranmıştır:

- BRICS ülkelerinin siber güvenlik performanslarını belirleyen en önemli ve en az önemli kriterler hangileridir?
- BRICS ülkeleri, siber güvenlik performansı açısından birbirlerinden ne ölçüde farklılık göstermektedir?
- LOPCOW-MARCOS metodolojisi kriter ağırlıklarındaki değişimlere ne kadar duyarlıdır?
- LOPCOW–MARCOS metodolojisi, siber güvenlik performanslarının değerlendirilmesinde ne derece güvenilirdir ve diğer ÇKKV yöntemleriyle karşılaştırıldığında nasıl bir konumda yer almaktadır?

Çalışmanın sonraki bölümleri şu şekilde organize edilmiştir: Literatür taraması bölümünde, siber güvenlik alanında yürütülen ÇKKV metodolojisine sahip çalışmalar ve bu çalışmada benimsenen yöntemleri içeren çalışmalar değerlendirilmiştir. Yöntem bölümünde kriter ağırlığı hesaplama ve ülkeleri sıralamada kullanılan ÇKKV yöntemlerinin teorik altyapıları ve hesaplama adımları ayrıntılı olarak açıklanmıştır. Uygulama bölümünde, BRICS ülkeleri için çalışmada benimsenen yaklaşımla sayısal analiz gerçekleştirilmiş ve bulgular ortaya konulmuştur. Ayrıca önerilen metodolojinin kriter ağırlıklarındaki değişimlere hassasiyetini ve güvenirliğini incelemek amacıyla duyarlılık analizine ve karşılaştırmalı analize yer verilmiştir. Sonuç bölümünde ise bulgular literatürle ilişkilendirilerek tartışılmış, çalışmanın sınırlılıkları ile gelecekteki çalışmalar ile ilgili bazı çıkarımlarda bulunulmuştur.

1. Literatür Taraması

Çalışmanın bu kısmında, ÇKKV metodolojisini kullanan siber güvenlik ile ilgili araştırmalara ilişkin literatür taramasına ilişkin bilgilere yer verilmiştir. Yapılan incelemelerde, araştırmacıların siber güvenlik ile ilgili çok sayıda problemin çözümünde ÇKKV yöntemlerinden faydalandığı tespit edilmiştir. Çalışmalara belirli kategoriler altında gruplanarak yer verilmiştir.

Endüstri 4.0'ın siber güvenlik boyutuna odaklanan çalışmalar şu şekildedir: Alamri vd. (2024), sağlık nesnelerin internetine yönelik olarak blok zincir tabanlı kimlik yönetim sistemlerini değerlendirmek amacıyla Delphi ve SMART (Simple Multi-Attribute Rating Technique) tekniklerini kullanmış ve bir siber güvenlik risk yönetimi çerçevesi sunmuştur. Andrade vd. (2022), nesnelerin interneti sistemlerindeki güvenlik risklerini değerlendirmek amacıyla Bayes Ağları ve BWM metodolojisinden yararlanmıştır. Torbacki (2021), Endüstri 4.0 bileşenlerini sürdürülebilir kalkınma, karbon ayak izinin azaltılması ve döngüsel ekonomi bağlamında incelemiş; DEMATEL, ANP (Analytic Network Process) ve PROMETHEE II (Preference Ranking Organization Method for Enrichment Evaluation) yöntemlerini bir araya getirerek hibrit bir model önermiştir.

Kritik altyapılar ve bunlara yönelik siber güvenlik kapsamında odaklanan çalışmalara ilişkin bulgular şu şekildedir: Pourmadadkar vd. (2024), sağlık sektöründe siber direncin arttırılarak kritik altyapının korunmasını sağlamak amacıyla Hata Türü Etkileri ve Analizi ile Bulanık TOPSIS yöntemini kullanarak bir araştırma gerçekleştirmiştir. Zhang vd. (2024), güç sistemlerindeki iletişim ağlarının güvenliğini değerlendirmek amacıyla Entropi ve TOPSIS yöntemlerini kullanarak bir analiz gerçekleştirmiştir. Bouramdane (2023), akıllı şebekelerle ilgili siber güvenlik kararlarına yardımcı olmak ve kaynak tahsisini optimize etmek için bir AHP yaklaşımı önermiştir. AbdelMouty ve Abdel-Monem (2023), güç yönetim ve kontrol sistemlerinde kullanılan iletişim ağlarının siber güvenlik risklerini belirlemek amacıyla aralık değerli Nötrosofik EDAS (Evaluation Based on Distance from Average Solution) yönteminden yararlanmıştır. Priyadarshini vd. (2021), enerji sektöründe bulut bilişim ve akıllı şebekeler gibi teknolojilerin güvenlik açıklarına odaklanarak kritik altyapılara yönelik riskleri AHP yöntemiyle değerlendirmiştir.

Kurumsal siber güvenlik risklerinin değerlendirilmesine ilişkin literatürde yer alan bazı çalışmalar şunlardır: Tanaji ve Roychowdhury (2024), ulaştırma sistemlerinde bağlantılı ve otonom araçların siber güvenlik açıklarını belirlemek ve sistem kırılganlıklarını sıralamak için BWM ve Nötrosofik VIKOR yöntemlerini kullanmıştır. Sukumar vd. (2023), çevrimiçi perakende sektöründe faaliyet gösteren küçük ve orta ölçekli işletmeler (KOBİ) için siber güvenlik risk analizine yönelik SWARA (Step-Wise Weight Assessment Ratio Analysis) ve BWM yöntemlerine dayalı bir karar destek modeli geliştirmiştir. Tusher vd. (2022), otonom gemicilikteki siber güvenlik risklerini değerlendirmek amacıyla BWM yöntemini kullanmıştır.

Son yıllarda siber güvenlik performansına yönelik yapılan çalışmalar şu şekildedir: Panigrahi vd. (2024), siber saldırı tespit modellerinin performansını karşılaştırmak amacıyla AHP, TOPSIS, VIKOR, Entropi ve makine öğrenmesi algoritmalarına dayalı hibrit sistemler geliştirmiştir. Küpeli ve Söğüt (2024), GCI ve NCSI verilerini kullanarak G20 ülkelerinin siber güvenlik etkinliklerini Veri Zarflama Analizi (VZA) ile ölçmüştür. Radulescu vd. (2024), altı farklı indeksten elde edilen verileri birlikte kullanarak Doğu Avrupa ülkelerinin siber güvenlik seviyelerini TOPSIS yöntemiyle ölçmüştür. Candan ve Toklu (2022), Eurostat verilerini kullanarak Avrupa Birliği üyelerinin sürdürülebilir siber güvenlik performanslarını Bulanık SMART ve ARAS yöntemleriyle karşılaştırmıştır. Bruggemann vd. (2022), GCI metodolojisinin KOBİ'lerin siber güvenlik farkındalıklarını artırmak için kullanılabileceğini öne sürmüş ve Hasse diyagramlarıyla analiz yapmıştır. Altıntaş (2022), GCI verilerini kullanarak G7 ülkelerinin siber güvenlik performanslarını Entropi-MABAC yöntemleriyle kıyaslamıştır.

ÇKKV metodolojisini kullanarak siber güvenlik ile ilgili yukarıda ele alınan araştırma problemlerinden farklı olarak Kostelić (2025), çalışanların siber güvenlik risklerini analiz etmek için AHP ve TOPSIS yöntemlerinden faydalanarak bir çerçeve ortaya koymuştur.

Alhakami (2024), Suudi Arabistan'ın siber güvenlik politikalarına öneriler geliştirmek için Bulanık AHP, Bulanık DEMATEL ve Bulanık TOPSIS yöntemleriyle siber güvenlik yeterliliklerini belirlemiştir. Kaur vd. (2024), tedarik zincirinin siber güvenliğini artırabilmek amacıyla siber dayanıklılık kriterleri kapsamında tedarikçi seçimi için karma tam sayılı programlama modelinden yararlanmıştır. Ahasan vd. (2023), oltalama saldırılarının tespiti için doğal dil işleme, makine öğrenme algoritmaları ve Bulanık ÇKKV metodolojisini bir araya getirerek bir model önermiştir. Polireddi ve Sekhar (2023), finansal sistemlerin siber saldırılara karşı savunmasızlığını Bulanık TOPSIS yöntemiyle analiz etmiştir. Abushark vd. (2022), siber saldırı tespit sistemleri için makine öğrenmesi temelli bir yaklaşımla Bulanık AHP ve Bulanık TOPSIS yöntemleriyle bir değerlendirme yapmıştır. Alharbi vd. (2021), saldırı tespit sistemlerini Tereddütlü (Hesitant) Bulanık AHP ve Tereddütlü Bulanık TOPSIS yöntemlerini makine öğrenme algoritmalarıyla birlikte kullanarak analiz etmiştir. Ansari vd. (2020), sağlık sektörü için güvenli yazılım geliştirme sürecinde en uygun güvenlik gereksinimlerini Bulanık TOPSIS yöntemiyle belirlemiştir. Noor vd. (2020), en uygun siber tehdit zekâsı hizmet sağlayıcısını seçmek için AHP yöntemini kullanmıştır.

LOPCOW yöntemini kullanarak kriter ağırlıklarını belirleyen çalışmalara ilişkin literatür taraması sonuçları Tablo 1'de özetlendiği gibidir.

Tablo 1. LOPCOW Yöntemine İlişkin Literatür Taraması Bulguları

Yazar(lar)	Yöntem(ler)	Ele Alınan Problem
D. Zhang (2025)	LOPCOW, ERUNS	Metin analiz aracı seçimi
Abacıoğlu vd. (2025)	LOPCOW, MEREC, CoCoSo, CRADIS, EDAS, MABAC, MAIRCA, MARCOS	Yeşil üniversitelerin sıralanması
Ecer vd. (2025)	Aralık değerli nötrosofik LOPCOW, MARCOS	Tedarikçi seçimi
Ji vd. (2025)	LOPCOW, WASPAS	Teknoloji seçimi
Çelebi Demirarslan vd. (2024)	MEREC, LOPCOW, MPSI, MAIRCA	Ülkelerin yaşam kalitelerinin karşılaştırılması
Öztaş ve Öztaş (2024)	LOPCOW, MAIRCA	Ülkelerinin inovasyon performans analizi
Yavuz (2024)	LOPCOW, TOPSIS	Finansal performans analizi
Işık vd. (2024)	LOPCOW, CRITIC, ALWAS	Şehirlerin sürdürülebilirlik performanslarının analizi
Ulutaş vd. (2024)	Gri LOPCOW, Gri PSI, Gri MACONT	Lojistik hizmet sağlayıcısı seçimi
Simic vd. (2023)	Nötrosofik LOPCOW, ARAS	Teknoloji seçimi
Ulutaş vd. (2023)	LOPCOW, PSI, MEREC, MCRAT	Malzeme seçimi
Ersoy (2023)	LOPCOW, RSMVC	Finansal performans analizi
Ecer ve Pamucar (2022)	LOPCOW, DOBI	Sürdürülebilirlik performans analizi

ERUNS (Evaluation Based on Relative Utility and Nonlinear Standardization), **MEREC** (Method Based on The Removal Effects of Criteria), **CRADIS** (Compromise Ranking of Alternatives from Distance to Ideal Solution), **WASPAS** (Weighted Aggregated Sum Product Assessment), **MPSI** (Modified Preference Selection Index Method), **CRITIC** (Criteria Importance Through Inter-Criteria Correlation), **ALWAS** (Aczel-Alsina Weighted Assessment), **PSI** (Preference Selection Index), **MACONT** (Mixed Aggregation by Comprehensive Normalization Technique), **MCRAT** (Multiple Criteria Ranking By Alternative Trace), **RSMVC** (Ranking The Solutions Based On The Mean Value Of Criteria), **DOBI** (Dombi Bonferroni)

Tablo 1 incelendiğinde, LOPCOW yönteminin yakın zamanda literatüre kazandırılmış bir yöntem olmasına rağmen son yıllarda artan şekilde araştırmacıların ilgisini çektiği görülmektedir. Yeryüzündeki kaynakların gelecek kuşaklara aktarılabilmesi endişesiyle ortaya çıkan sürdürülebilirlik odaklı çalışmalar (Abacıoğlu vd., 2025; Ecer ve Pamucar, 2022; Işık vd., 2024) en çok ilgi gören alan olarak göze çarpmaktadır. Performans analizi (Çelebi Demirarslan vd., 2024; Ersoy, 2023; Öztaş ve Öztaş, 2024; Yavuz, 2024) LOPCOW yönteminin kullanıldığı bir diğer önemli çalışma alanı olarak belirlenmiştir. Tedarikçi ve hizmet sağlayıcı seçimi (Ecer vd., 2025; Ulutaş vd., 2024) ile teknoloji ve malzeme seçimi (Ji vd., 2025; Simic vd., 2023; Ulutaş vd., 2023; D. Zhang, 2025) araştırmacılar tarafından diğer önemli çalışma alanları olarak değerlendirilmiştir.

Son yıllarda MARCOS yöntemiyle yürütülmüş araştırmalara ilişkin literatür bulguları Tablo 2'de özetlenmiştir. Tablo 2, MARCOS yönteminin sürdürülebilirlik (Ghoushchi vd., 2023; Kumar vd., 2024; Stević vd., 2020), insani kalkınma ve adaletli kaynak dağıtımı (Aycın vd., 2024; Jamili vd., 2024), performans ölçümü (Işık vd., 2025; Torkayesh ve Torkayesh, 2021), madencilik (Roshanravan vd., 2025), iş güvenliği (Tayebi vd., 2025), malzeme seçimi (Abas vd., 2023), yüklenici/tedarikçi seçimi (Karbassi Yazdi vd., 2022; Mohammed Abdelkader vd., 2023) gibi konularda kullanıldığını göstermektedir. Ayrıca, Tablo 2'de yer alan bulgular MARCOS yönteminin diğer ÇKKV yöntemleriyle de başarıyla entegre edilebildiğini göstermektedir.

Tablo 2. MARCOS Yöntemine İlişkin Literatür Taraması Bulguları

Yazar(lar)	Yöntem(ler)	Ele Alınan Problem
Roshanravan vd. (2025)	BWM, MARCOS	Mineral potansiyeli modelleme
Tayebi vd. (2025)	Nötrosofik MARCOS	Muhtemel iş kazalarını sıralama
Işık vd. (2025)	Bulanık LBWA, Bulanık LMAW, MARCOS	Banka performansı değerlendirme
Aycın vd. (2024)	MEREC, MARCOS	Ülkelerin kadınlar açısından insani kalkınma seviyelerini karşılaştırma
Kumar vd. (2024)	CRITIC, Entropi, MEREC, MARCOS	Yenilenebilir enerji kaynaklarının potansiyelini değerlendirme
Jamili vd. (2024)	MEREC, MARCOS, CODAS, MAIRCA	Kaynak dağıtımını ölçme

Tablo 2. Devam.

Mohammed Abdelkader vd. (2023)	Bulanık ANP, CoCoSo, WISP, MARCOS, WASPAS, MARCOS	Proje yüklenicisi belirleme
Abas vd. (2023)	WISP, MARCOS, TOPSIS	Malzeme seçimi
Ghoushchi vd. (2023)	SWARA, MARCOS	Sürdürülebilir ulaşım sistemi seçimi
Karbassi Yazdi vd. (2022)	BWM, Gri MARCOS	Enerji sektörü için tedarikçi sözleşmesi seçimi
Torkayesh ve Torkayesh (2021)	LBWA, MARCOS	Ülkelerin bilgi ve iletişim teknoloji düzeylerini karşılaştırma
Stević vd. (2020)	MARCOS	Sürdürülebilir tedarikçi seçimi

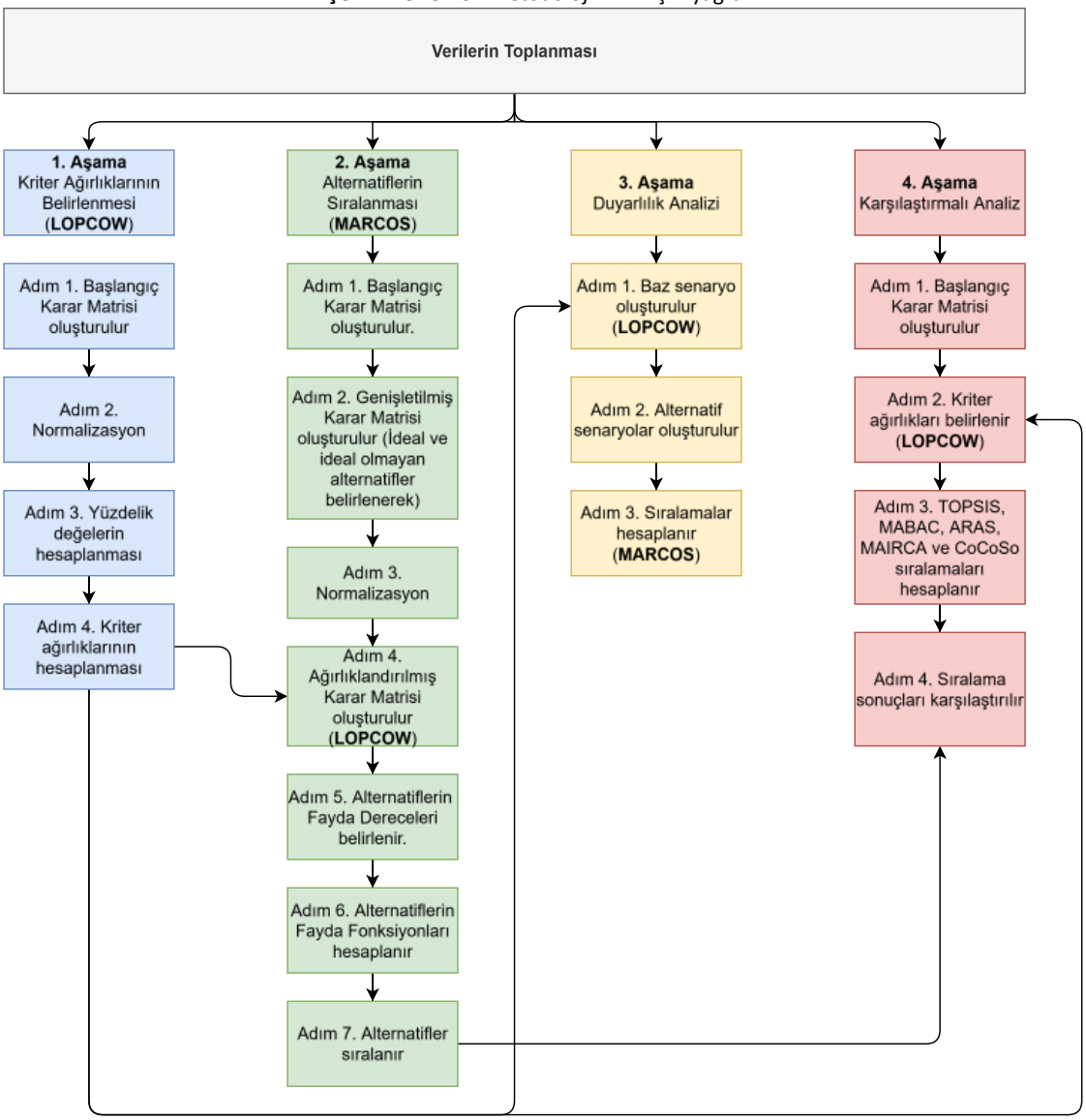
LBWA (Level Based Weight Assessment), **LMAW** (Logarithm Methodology of Additive Weights), **CODAS** (Combinative Distance Based Assessment), **WISP** (Weighted Sum Product)

Literatürde siber güvenlik alanında bulunan karar verme problemlerini ÇKKV metodolojisiyle ele alan çok sayıda çalışma bulunmaktadır. Bu çalışmalar; Endüstri 4.0, kurumsal siber risk yönetimi, kritik altyapıların güvenliği, siber güvenlik performans analizi, tedarik zinciri, çalışanların siber riskleri ve en uygun siber saldırı tespit sistemlerinin seçimi gibi önemli konulara odaklanmaktadır. Ancak ülkelerin siber güvenlik performanslarını karşılaştıran çalışmaların azlığı, bu alanın henüz yeterince araştırılmadığını ve önemli bir potansiyel taşıdığını göstermektedir. Literatürdeki çalışmaların büyük bir kısmında AHP ve TOPSIS yöntemleri ile bu yöntemlerin bulanık uzantılarının, kriter ağırlıklarının belirlenmesi ve alternatiflerin sıralanmasında kullandığı tespit edilmiştir. Bu yöntemler dışında Entropi, BWM, DEMATEL ve VIKOR yöntemlerinin de tercih edildiği görülmektedir. Bu durum, çalışmada kullanılan LOPCOW ve MARCOS yöntemlerinin ülkelerin siber güvenlik performanslarını ölçmek için uygun olduğunu ve çalışmanın özgün yönünü ortaya koyduğunu göstermektedir. Hem ele alınan problemin hem de kullanılan metodolojinin literatürde önemli bir boşluğu dolduracağı öngörülmektedir.

2. Metodoloji

Bu çalışmada BRICS ülkelerinin siber güvenlik performanslarını karşılaştırmak için dört aşamalı bir metodolojik yaklaşım benimsenmiştir. Metodolojinin ilk aşamasında, analize dahil edilen kriterlerin önem düzeylerini (ağırlıklarını) belirlemek amacıyla LOPCOW yöntemi kullanılmıştır. İkinci aşamada, BRICS ülkeleri, ilk aşamada elde edilen kriter ağırlıkları kullanılarak MARCOS yöntemi ile sıralanmıştır. Metodolojinin üçüncü aşamasında, önerilen modelin kriter ağırlıklarındaki değişimlere hassasiyetini incelemek için beş senaryo altında duyarlılık analizi gerçekleştirilmiştir. Metodolojinin dördüncü ve son aşamasında ise, LOPCOW-MARCOS yaklaşımının ortaya koyduğu sonuçların güvenirliği, TOPSIS, MABAC, ARAS, MAIRCA ve CoCoSo yöntemleriyle karşılaştırmalı analiz yoluyla test edilmiştir. Çalışmada benimsenen metodolojiye ilişkin akış diyagramı Şekil 1'de sunulmuştur. Bu bölümün geri kalan kısmında, LOPCOW ve MARCOS yöntemlerinin hesaplama adımları ayrıntılı biçimde sunulmuştur.

Şekil 1. Önerilen Metodolojinin Akış Diyagramı



2.1. LOPCOW Yöntemi

LOPCOW yöntemi kriter ağırlıklarını objektif şekilde belirlemek için kullanılan en yeni ÇKKV yöntemlerinden biridir. Ele alınan problem verisinde negatif değerler olması durumunda da kriter ağırlığı hesaplayabilmesi, LOPCOW yönteminin en önemli avantajlarından biridir (Ecer ve Pamucar, 2022, s. 4).

Ecer ve Pamucar (2022, ss. 4-5) tarafından önerilen LOPCOW yöntemi ile kriter ağırlığı hesaplayabilmek için izlenmesi gereken adımlar sırasıyla aşağıda sunulmuştur:

Adım 1. Ele alınan problem için Başlangıç Karar Matrisi (BKM) Eşitlik (1)'de gösterildiği gibi oluşturulur. Bu matriste m adet alternatif, n adet kriter bulunur.

$$BKM = \begin{bmatrix} x_{11} & \cdots & x_{1n} \\ \vdots & \ddots & \vdots \\ x_{m1} & \cdots & x_{mn} \end{bmatrix} \quad (1)$$

Adım 2. Her bir kriter farklı birimde ölçülebildiği için BKM elemanlarının normalize edilerek $[0,1]$ arasındaki değerlere dönüştürülmesi gerekmektedir. Bu dönüşüm işlemi kriterlerin fayda yönlü ya da maliyet yönlü olmasına göre sırasıyla Eşitlik (2) ya da Eşitlik (3)'e göre yapılır.

$$\hat{x}_{ij} = \frac{x_{ij} - x_{min}}{x_{max} - x_{min}} \text{ (Fayda yönlü kriterler için)} \quad (2)$$

$$\hat{x}_{ij} = \frac{x_{max} - x_{ij}}{x_{max} - x_{min}} \text{ (Maliyet yönlü kriterler için)} \quad (3)$$

Adım 3. Her bir kriter için yüzdelik değerleri (YD) Eşitlik (4) yardımıyla hesaplanır. Veri büyüklüğünden kaynaklanan boşluğu (farkları) ortadan kaldırmak için, her bir kriterin standart sapmalarının yüzdesi olarak ortalama kare değeri hesaplanır.

$$YD_{ij} = \left| \ln\left(\frac{\sqrt{\frac{\sum_{i=1}^{m} \hat{x}_{ij}^2}{m}}}{\sigma} \right) . 100 \right| \quad (4)$$

Burada, m alternatif sayısını; σ ise standart sapmayı göstermektedir.

Adım 4. Her bir kriter için YD_{ij} değerlerine bağlı olarak Eşitlik (5) ile ağırlık değeri hesaplanır.

$$w_j = \frac{YD_{ij}}{\sum_{i=1}^{n} YD_{ij}} \quad (5)$$

2.2. MARCOS Yöntemi

Alternatifler ile referans değerler (ideal ve ideal olmayan alternatifler) arasındaki ilişkiye dayanan MARCOS yöntemi, Stević vd. (2020) tarafından literatüre kazandırılmıştır.

MARCOS yöntemi ile sıralama yapabilmek için izlenmesi gereken hesaplama adımları sırasıyla şu şekildedir (Stević vd., 2020, ss. 3-5):

Adım 1. m adet alternatif ve n adet kriterden oluşan BKM, Eşitlik (1)'de gösterildiği şekilde oluşturulur.

Adım 2. BKM, ideal ve ideal olmayan alternatifler eklenerek Eşitlik (6)'da verilen Genişletilmiş Karar Matrisi (GKM), oluşturulur. İdeal ve ideal olmayan alternatifler belirlenirken Eşitlik (7) ve Eşitlik (8)'de gösterildiği gibi kriterin fayda ya da maliyet yönlü olması dikkate alınır. Kriterin özelliğine göre en iyi olan ideal alternatif (AI); en kötü olan ise ideal olmayan alternatif (AAI) olarak belirlenir. Örneğin, fayda yönlü bir kriter için ideal alternatif (AI) en yüksek değere sahip alternatif olarak seçilirken; maliyet yönlü bir kriter için ise en düşük değere sahip alternatif olarak seçilir. Bunun tam tersi de geçerlidir.

$$GKM = \begin{matrix} AAI \\ A_1 \\ \vdots \\ A_m \\ AI \end{matrix} \begin{bmatrix} x_{aa1} & \cdots & x_{aan} \\ x_{11} & \cdots & x_{1n} \\ \vdots & \ldots & \vdots \\ x_{m1} & \ddots & x_{mn} \\ x_{ai1} & \cdots & x_{ain} \end{bmatrix} \quad (6)$$

$AAI = \min_i x_{ij}$ fayda yönlü kriterler için ($\max_i x_{ij}$ maliyet yönlü kriterler için) (7)

$AI = \max_i x_{ij}$ fayda yönlü kriterler için ($\min_i x_{ij}$ maliyet yönlü kriterler için) (8)

Adım 3. GKM'nin elemanları fayda ya da maliyet yönlü olmalarına göre Eşitlik (9) ve Eşitlik (10)'da gösterildiği gibi normalize edilerek $[0,1]$değerlere dönüştürülür.

$\hat{x}_{ij} = \frac{x_{ai}}{x_{ij}}$ (Maliyet yönlü kriterler için) (9)

$\hat{x}_{ij} = \frac{x_{ij}}{x_{ai}}$ (Fayda yönlü kriterler için) (10)

Adım 4. Normalize edilen GKM'nin elemanları, Eşitlik (11)'de gösterildiği gibi kriter ağırlıkları (w_j) ile çarpılarak Ağırlıklandırılmış Karar Matrisi (AKM) elde edilir.

$$v_{ij} = \hat{x}_{ij} \times w_j \quad (11)$$

burada, $v_{ij} \in AKM$.

Adım 5. Alternatiflerin fayda dereceleri (K_i) hesaplanır. Eşitlik (12) ve Eşitlik (13) yardımıyla ideal ve ideal olmayan alternatiflere göre fayda derecesi hesaplanır.

$$K_i^- = \frac{S_i}{S_{aai}} \quad (12)$$

$$K_i^+ = \frac{S_i}{S_{ai}} \quad (13)$$

burada, $S_i = \sum_{j=1}^{n} v_{ij}$ $(i = 1,2, \ldots m)$.

Adım 6. Her bir alternatifin fayda fonksiyonu $f(K_i)$ belirlenir. Bu değer, ideal çözüm ile ideal olmayan çözüm arasındaki uzlaşmayı ifade eder. Fayda fonksiyonu, Eşitlik (14) ile hesaplanır.

$$f(K_i) = \frac{K_i^+ + K_i^-}{1 + \frac{1-f(K_i^+)}{f(K_i^+)} + \frac{1-f(K_i^-)}{f(K_i^-)}} \quad (14)$$

burada, $f(K_i^+)$ ideal çözümün; $f(K_i^-)$ ise ideal olmayan çözümün fayda fonksiyonlarını ifade eder. Bu fayda fonksiyonları Eşitlik (15) ve Eşitlik (16)'da gösterildiği gibi hesaplanır.

$$f(K_i^+) = \frac{K_i^-}{K_i^+ + K_i^-} \quad (15)$$

$$f(K_i^-) = \frac{K_i^+}{K_i^+ + K_i^-} \quad (16)$$

Adım 7. Alternatifler fayda fonksiyonuna göre yüksek değerden düşük değere doğru sıralanır. Burada en yüksek fayda fonksiyonu değerine sahip olan alternatif, en iyi alternatif olarak belirlenir.

3. Sayısal Uygulama

Siber güvenlik, dijital ortamda paylaşılan her türlü bilgiyi kapsamaktadır. Bilgi paylaşımının tarafları, siber güvenlikle ilgili yeterli bilince sahip olmaz ya da gerekli önlemleri almazsa hukuki, finansal ya da itibar kaybına yol açan durumlara neden olabilmektedir. Siber güvenlik ile ilgili risklerin geniş kitleleri etkileyebilecek potansiyele sahip olması nedeniyle, konuya küresel perspektiften yaklaşmak faydalı olacaktır. Bu çalışmada, ülkelerin siber güvenlik performanslarının karşılaştırılmasını sağlayacak çok kriterli bir karar verme metodolojisinin önerilmesi amaçlanmaktadır. Önerilen metodoloji ile ülkelerin mevcut durumları ortaya konabilecek ve karar vericiler için potansiyel iyileştirme alanları tespit edilebilecektir.

Ülkelerin siber güvenlik performanslarını karşılaştırmak için ITU (2024a) tarafından yayımlanan Global Cybersecurity Index (GCI) 2024 verileri kullanılmıştır. Bu endeks, beş kategori altında yirmi göstergeye ilişkin veriler toplayarak nihai bir skor üretmektedir. Bu çalışmada kriter olarak kullanılan kategorilere ilişkin bilgilere Tablo 3'te yer verilmiştir. Her bir kriter 0 ile 20 arasında bir değere sahiptir.

Tablo 3. Analizde Kullanılan Kriterlere İlişkin Bilgiler

Kriter	İlgi Konusu	Yönü
K1-Yasal ölçümler	Siber suç ve siber güvenlik ile ilgili kanunları ölçer	Fayda
K2- Teknik ölçümler	Ülkeye ya da sektöre özgü teknik kabiliyetlerin uygulanışını ölçer	Fayda
K3-Organizasyonel ölçümler	Ulusal stratejileri ve siber güvenliği uygulayan kurumları ölçer	Fayda
K4-Kapasite geliştirme ölçümleri	Siber güvenlik kapasitesini geliştirecek farkındalık kampanyaları, eğitimler ve teşvikleri ölçer	Fayda
K5-İş birliği ölçümleri	Kurumlar, firmalar ve ülkeler arasındaki iş birliğini ölçer	Fayda

Kaynak: (ITU, 2024b, s. 2)

Bu çalışmada üyeliği Türkiye'nin de gündeminde bulunan BRICS ülkelerinin siber güvenlik performansları karşılaştırmalı olarak analiz edilmiştir. BRICS ülkeleri, dünya ekonomisindeki payının yüksekliği, dünya nüfusunun önemli bir bölümünü barındırması ve küresel internet kullanıcı popülasyonundaki yüksek oranları (Jiang ve Belli, 2025: 10) nedeniyle tercih edilmiştir. Analize dahil edilen ülkelere (alternatifler) ilişkin bilgiler Tablo 4'te sunulmuştur.

Tablo 4. Analize Dahil Edilen Ülkeler

Ülkeler ve Gösterimleri	
A1-Birleşik Arap Emirlikleri	A6-Güney Afrika
A2-Brezilya	A7-Hindistan
A3-Çin	A8-İran
A4-Endonezya	A9-Mısır
A5-Etiyopya	A10-Rusya

Kaynak: (BRICS Portal)

Kriter ağırlığı hesaplama ve alternatifleri sıralamak için LOPCOW ve MARCOS yöntemleri için gerekli BKM Tablo 5'te gösterildiği gibi oluşturulmuştur.

Tablo 5. Başlangıç Karar Matrisi (BKM)

	K1	K2	K3	K4	K5
A1	20	20	20	20	20
A2	20	20	17,29	19,09	20
A3	20	17,14	18,34	18,46	17,7
A4	20	20	20	20	20
A5	18,83	14,37	12,12	15,33	15,69
A6	20	18,57	14,84	12,84	20
A7	20	20	18,49	20	20
A8	17,79	14,49	16,72	10,27	6,25
A9	20	20	20	20	20
A10	20	16,59	20	18,77	16,77

Kaynak: (ITU, 2024b)

Tablo 5 incelendiğinde, BRICS ülkelerinin en yüksek performansı K1-Yasal ölçümler kriterinde (ortalama değeri 19,66), en düşük performansı ise K4-Kapasite geliştirme ölçümleri kriterinde (ortalama değeri 17,48) sergilediği tespit edilmiştir. Ayrıca, K1-Yasal ölçümler kriterinin en düşük değişkenliğe sahip kriter olduğu (standart sapma değeri 0,75); K5-İş birliği ölçümleri kriterinin ise en yüksek değişkenliğe sahip olan kriter olduğu (standart sapma değeri 4,32) tespit edilmiştir.

Hesaplama sürecinin ilk aşamasında, Tablo 5'te yer alan başlangıç karar matrisi kullanılarak LOPCOW yöntemiyle kriter ağırlıkları hesaplanırken, öncelikle Eşitlik (2) veya Eşitlik (3) yardımıyla karar matrisi normalize edilmiş ve ardından Eşitlik (4) kullanılarak yüzdelik değerler hesaplanmıştır. Hesaplanan normalize edilmiş karar matrisi (NKM) ve yüzdelik değerler bir arada olacak şekilde Tablo 6'da verilmiştir.

Tablo 6'daki normalize karar matrisi, veri setindeki tüm kriterlerin fayda yönlü olmasından dolayı yalnızca Eşitlik (2) kullanılarak elde edilmiştir. Aynı tabloda yer alan yüzdelik değerler, Eşitlik (5) yardımıyla kriterler ağırlıklarının hesaplanmasında kullanılmıştır. Elde edilen kriter ağırlıkları Tablo 7'de sunulmuştur.

Tablo 6. NKM ve Yüzdelik Değerler

	$\boldsymbol{NKM}$				
	K1	**K2**	**K3**	**K4**	**K5**
A1	1,0000	1,0000	1,0000	1,0000	1,0000
A2	1,0000	1,0000	0,6561	0,9065	1,0000
A3	1,0000	0,4920	0,7893	0,8417	0,8327
A4	1,0000	1,0000	1,0000	1,0000	1,0000
A5	0,4706	0,0000	0,0000	0,5200	0,6865
A6	1,0000	0,7460	0,3452	0,2641	1,0000
A7	1,0000	1,0000	0,8084	1,0000	1,0000
A8	0,0000	0,0213	0,5838	0,0000	0,0000
A9	1,0000	1,0000	1,0000	1,0000	1,0000
A10	1,0000	0,3943	1,0000	0,8736	0,7651
	Yüzdelik Değerler				
	K1	**K2**	**K3**	**K4**	**K5**
	97,8031	62,7600	85,3070	82,4059	103,1088

Tablo 7. Kriterlere Ait Ağırlık Değerleri

$\boldsymbol{w_1}$	$\boldsymbol{w_2}$	$\boldsymbol{w_3}$	$\boldsymbol{w_4}$	$\boldsymbol{w_5}$
0,2267	0,1455	0,1978	0,1910	0,2390

Tablo 7'deki sonuçlar, K5-İş birliği ölçümleri kriterinin en yüksek ağırlığa ($w_5 = 0{,}2390$) sahip olduğunu ortaya koymaktadır. Bu kriteri sırasıyla K1-Yasal ölçümler ($w_1 = 0{,}2267$), K3-Organizasyonel ölçümler ($w_3 = 0{,}1978$) ve K4-Kapasite geliştirme ölçümleri ($w_4 = 0{,}1910$) kriterleri izlemektedir. K2-Teknik ölçümler ($w_2 = 0{,}1455$) kriteri ise en düşük öneme sahip kriter olarak belirlenmiştir. Bu bulgular çalışmanın birinci araştırma sorusuna doğrudan yanıt niteliğindedir. Kriterlerin önem düzeylerindeki farklılıklar, karar vericilerin hangi alanlara öncelik vermeleri gerektiğine dair yol gösterici olacaktır. Özellikle yüksek önem düzeyine sahip kriterlere odaklanılarak yapılacak iyileştirmelerin, genel performans üzerinde daha belirgin ve olumlu etkiler yaratması beklenmektedir.

Hesaplamanın ikinci aşamasında, LOPCOW yöntemiyle elde edilen kriter ağırlıkları kullanılarak, BRICS ülkeleri MARCOS yöntemiyle sıralanmıştır. Ülkeler sıralanırken öncelikle Eşitlik (7) ve Eşitlik (8) yardımıyla GKM oluşturulmuştur. Bu matris, Eşitlik (9) ve Eşitlik (10) yardımıyla normalize edilmiştir. Hesaplanan GKM ve NKM Tablo 8'de sunulmuştur.

Tablo 8'de sunulan GKM'de AAI değerleri, tüm kriterlerin fayda yönlü olması nedeniyle, Eşitlik (7) kullanılarak minimum değerli alternatifler üzerinden, AI değerleri ise Eşitlik (8) kullanılarak maksimum değerli sahip alternatifler üzerinden hesaplanmıştır. Normalizasyon işlemi, kriterlerin tamamının fayda yönlü olması nedeniyle Eşitlik (10) kullanılarak gerçekleştirilmiştir.

LOPCOW yöntemiyle hesaplanan ve Tablo 7'de sunulan kriter ağırlıkları kullanılarak, AKM Eşitlik (11) yardımıyla oluşturulmuştur. Devamında, alternatifler için Eşitlik (12) ve Eşitlik (13) kullanılarak göreli fayda dereceleri, Eşitlik (14) yardımıyla da fayda fonksiyonları hesaplanmıştır. Bu fayda fonksiyonları değerleri kullanılarak da alternatiflerin nihai sıralamaları elde edilmiştir. Elde edilen sonuçlar Tablo 9'da sunulmuştur.

Tablo 8. GKM ve NKM

	$\boldsymbol{GKM}$					$\boldsymbol{NKM}$				
	K1	K2	K3	K4	K5	K1	K2	K3	K4	K5
AAI	17,79	14,37	12,12	10,27	6,25	0,8895	0,7185	0,6060	0,5135	0,3125
A1	20	20	20	20	20	1,0000	1,0000	1,0000	1,0000	1,0000
A2	20	20	17,29	19,09	20	1,0000	1,0000	0,8645	0,9545	1,0000
A3	20	17,14	18,34	18,46	17,7	1,0000	0,8570	0,9170	0,9230	0,8850
A4	20	20	20	20	20	1,0000	1,0000	1,0000	1,0000	1,0000
A5	18,83	14,37	12,12	15,33	15,69	0,9415	0,7185	0,6060	0,7665	0,7845
A6	20	18,57	14,84	12,84	20	1,0000	0,9285	0,7420	0,6420	1,0000
A7	20	20	18,49	20	20	1,0000	1,0000	0,9245	1,0000	1,0000
A8	17,79	14,49	16,72	10,27	6,25	0,8895	0,7245	0,8360	0,5135	0,3125
A9	20	20	20	20	20	1,0000	1,0000	1,0000	1,0000	1,0000
A10	20	16,59	20	18,77	16,77	1,0000	0,8295	1,0000	0,9385	0,8385
AI	20	20	20	20	20	1,0000	1,0000	1,0000	1,0000	1,0000

Tablo 9. Fayda Fonksiyonları ve Sıralamalar

	$\boldsymbol{K^-}$	$\boldsymbol{K^+}$	$\boldsymbol{f(K^-)}$	$\boldsymbol{f(K^+)}$	$\boldsymbol{f(K)}$	**Sıra**
A1	1,6699	1,0000	0,3745	0,6255	0,8168	1
A2	1,6107	0,9645	0,3745	0,6255	0,7878	5
A3	1,5373	0,9206	0,3745	0,6255	0,7519	7
A4	1,6699	1,0000	0,3745	0,6255	0,8168	1
A5	1,2888	0,7717	0,3745	0,6255	0,6304	9
A6	1,4532	0,8702	0,3745	0,6255	0,7108	8
A7	1,6450	0,9851	0,3745	0,6255	0,8046	4
A8	1,0774	0,6452	0,3745	0,6255	0,5270	10
A9	1,6699	1,0000	0,3745	0,6255	0,8168	1
A10	1,5444	0,9248	0,3745	0,6255	0,7554	6

Tablo 9'da sunulan sonuçlara göre, Birleşik Arap Emirlikleri (A1), Endonezya (A4) ve Mısır (A9) en yüksek fayda fonksiyonu değerlerine sahip olmaları nedeniyle ilk sırayı paylaşmıştır. Sıralamada Hindistan (A7), Brezilya (A2), Rusya (A10) ve Çin (A3) sonraki pozisyonlara yerleşmiştir. Güney Afrika (A6), Etiyopya (A5) ve İran (A8) ise en düşük fayda fonksiyonu değerlerini alarak listenin son üç sırasında konumlanmıştır. Bu bulgu, çalışmanın ikinci araştırma sorusunu yanıtlamakta ve BRICS ülkeleri arasında siber güvenlik performansları açısından farklılıklar olduğunu ortaya koymaktadır.

3.1. Duyarlılık Analizi

ÇKKV yöntemlerinin ürettiği sıralama sonuçları, kriter ağırlıklarındaki değişikliklerden doğrudan etkilenmektedir. Bu nedenle, duyarlılık analizleri ile geliştirilen ÇKKV metodolojilerinin sağlamlıklarını, kriter ağırlıklarındaki değişimlere ne derecede duyarlı olduklarını tespit etmek mümkündür. Bu amaçla çalışmada beş senaryo altında duyarlılık analizi gerçekleştirilmiştir. Senaryolara ait kriter ağırlıkları Tablo 10'da sunulmuştur.

Tablo 10. Duyarlılık Analizine İlişkin Senaryolar ve Kriter Ağırlıkları

Senaryo	$\boldsymbol{w_1}$	$\boldsymbol{w_2}$	$\boldsymbol{w_3}$	$\boldsymbol{w_4}$	$\boldsymbol{w_5}$
Senaryo 1	0,2267	0,1455	0,1978	0,1910	0,2390
Senaryo 2	0,2053	0,1318	0,1792	0,1730	0,3107
Senaryo 3	0,2331	0,1496	0,2034	0,1964	0,2175
Senaryo 4	0,2151	0,1892	0,1877	0,1812	0,2268
Senaryo 5	0,2000	0,2000	0,2000	0,2000	0,2000

Tablo 10'da yer alan senaryoların özellikleri şu şekildedir:

Senaryo 1, LOPCOW yöntemiyle hesaplanan kriter ağırlıklarından oluşmaktadır ve diğer senaryolar bu baz senaryo üzerinden elde edilmiştir.

Senaryo 2, baz senaryodaki en önemli kriterin (K5) değerinin %30 arttığı, diğer kriterlerin ağırlıklarının ise %9,42 azaldığı senaryodur (Örnek olarak bu senaryodaki kriter ağırlıklarının değişim oranı şu şekilde hesaplanmaktadır: Senaryoda ağırlığı değiştirilen kriterin değerine bağlı olarak diğer kriterlerin alabileceği toplam değer bulunur $(1 - (0{,}2390 * 1{,}3) = 0{,}6893)$ ve bu kriterlerin baz senaryoda sahip olduğu toplam değere $(0{,}2267 + 0{,}1455 + 0{,}1978 + 0{,}1910 = 0{,}7610)$ bölünür. Elde edilen oran $(0{,}9058)$ ile baz senaryodaki kriter ağırlığı çapılarak yeni kriter değeri ($w_1 = 0{,}2267$ * 0,9058 = 0,2053) hesaplanır).

Senaryo 3, baz senaryodaki en önemli kriterin (K5) ağırlığının %30 azaldığı, diğer kriterlerin ağırlıklarının ise %2,83 arttığı senaryodur.

Senaryo 4, baz senaryodaki en düşük önemli kriterin (K2) ağırlığının %30 arttığı, diğer kriterlerin ağırlığının %5,11 azaldığı senaryodur.

Senaryo 5 ise bütün kriterlerin eşit öneme $(0{,}20)$ sahip olduğu durumdur.

Oluşturulan senaryolar altında elde edilen duyarlılık analizi sonuçları Tablo 11'de verildiği gibidir.

Tablo 11. Duyarlılık Analizi Sonuçları

	Senaryo1	***Senaryo2***	***Senaryo3***	***Senaryo4***	***Senaryo5***
A1	1	1	1	1	1
A2	5	5	5	5	5
A3	7	6	7	7	7
A4	1	1	1	1	1
A5	9	9	9	9	9
A6	8	8	8	8	8
A7	4	4	4	4	4
A8	10	10	10	10	10
A9	1	1	1	1	1
A10	6	7	6	6	6

Duyarlılık analizi sonucunda beş farklı senaryo oluşturulmuş ve kriter ağırlıklarındaki değişimlerin MARCOS yönteminin sıralama sonuçlarına etkisi incelenmiştir. Analiz sonuçlarına göre A1, A4 ve A9 numaralı ülkeler tüm senaryolarda ilk sırayı paylaşmıştır. A5, A6, A7 ve A8 numaralı alternatiflerin sıralamalarında da herhangi bir değişiklik gözlemlenmemiştir. Yalnızca A3 ve A10 numaralı alternatiflerin, Senaryo 2'de sırasıyla bir basamak yükseldiği (A3) ve bir basamak düştüğü (A5) tespit edilmiştir. Bu durum, A3'ün K5 kriteri açısından daha avantajlı, A10'un ise daha zayıf olduğunu ortaya koymaktadır. Elde edilen bulgular, çalışmada önerilen metodolojinin kriter değişimlerine karşı sağlamlığını ve istikrarlı sonuçlar ürettiğini göstermektedir. Böylece, çalışmanın üçüncü araştırma sorusuna yanıt verilmiş ve önerilen metodolojinin kriter ağırlıklarındaki değişimlere karşı düşük hassasiyet gösterdiğini sonucuna ulaşılmıştır.

3.2. Karşılaştırmalı Analiz

Bu çalışmada, BRICS ülkelerinin siber güvenlik performanslarını karşılaştırmak amacıyla LOPCOW ve MARCOS yöntemlerini bütünleşik biçimde kullanan bir yaklaşım benimsenmiştir. Ülkelerin performanslarını karşılaştırmada kullanılan yöntemlerin sonuçlarını doğrulamak ve sıralama sürecinin güvenirliğini test etmek amacıyla karşılaştırmalı analiz yapılmıştır. Karşılaştırmalı analiz, literatürde yaygın biçimde kullanılan TOPSIS, MABAC, ARAS, MAIRCA ve CoCoSo yöntemleriyle yürütülmüştür. Karşılaştırmalı analizde, LOPCOW yöntemiyle elde edilen kriter ağırlıkları esas alınmıştır. Karşılaştırmalı analiz sonucunda elde edilen sıralama sonuçları Tablo 12'de sunulmuştur.

Tablo 12. Karşılaştırmalı Analiz Sonuçları

	MARCOS	**TOPSIS**	**MABAC**	**ARAS**	**MAIRCA**	**CoCoSo**
A1	1	1	1	1	1	1
A2	5	5	5	5	5	5
A3	7	6	7	7	7	7
A4	1	1	1	1	1	1
A5	9	9	9	9	9	9
A6	8	8	8	8	8	8
A7	4	4	4	4	4	4
A8	10	10	10	10	10	10
A9	1	1	1	1	1	1
A10	6	7	6	6	6	6
ρ	1	0,9876	1	1	1	1

Tablo 12 incelendiğinde, BRICS ülkelerinin siber güvenlik performanslarının sıralanmasında LOPCOW ve MARCOS yöntemlerinin, literatürde yaygın şekilde kullanılan TOPSIS, MABAC, ARAS, MAIRCA ve CoCoSo gibi ÇKKV yöntemleriyle uyumlu sonuçlar verdiği görülmektedir. Bu yöntemlerden yalnızca TOPSIS, A3 ve A10 alternatiflerinin sıralamalarında farklılık göstermiştir. Bu durum, tablonun son satırında yer alan ve çalışmada kullanılan LOPCOW-MARCOS metodolojisi ile karşılaştırma amacıyla hesaplanan Spearman korelasyon katsayısı (ρ) değerlerine de yansımıştır. LOPCOW-MARCOS metodolojisi ile TOPSIS yöntemi arasında 0,9876 değerinde çok güçlü bir korelasyon bulunduğu; diğer yöntemlerle ise tam uyum sağlandığı sonucuna varılmıştır. Dolayısıyla, LOPCOW-MARCOS yaklaşımıyla ülkelerin siber güvenlik performans karşılaştırmalarının yapılabileceği ortaya konmuştur. Bu bulgu, çalışmanın dördüncü araştırma sorusuna yanıt teşkil etmektedir.

Sonuç

Dijitalleşmenin günlük hayatın ayrılmaz bir parçası haline gelmesiyle, bireylerin ve kurumların maruz kaldığı siber tehditlerin sayısı ve etkisi önemli ölçüde artmıştır. Özellikle pandemi dönemiyle birlikte çevrim içi ortamda yürütülen işlemlerin artarak kalıcı hale gelmesi, siber saldırıların yalnızca bireyleri değil, aynı zamanda kamu ve özel kurumları da hedef aldığını göstermiştir. Bu nedenle, siber güvenlik bir kişinin ya da bir departmanın sorumluluğunda olan teknik bir konu olmaktan çıkmış; ulusal güvenlik, ekonomik istikrar ve kamu hizmetlerinin sürekliliği açısından stratejik öneme sahip bir konu haline gelmiştir. Dolayısıyla, ülkelerin siber güvenlik performanslarının bütüncül yaklaşımlarla ölçülmesi, iyileştirmeye açık alanların tespit edilmesi ve bu alanlara yönelik politikaların geliştirilmesi kritik bir gereklilik haline gelmiştir.

Bu çalışmada, ITU (2024a) tarafından geliştirilen GCI verilerinden faydalanılarak BRICS ülkeleri için dört aşamalı bir siber güvenlik performans karşılaştırması yapılmıştır. Çalışmanın temel amacı, BRICS ülkelerinin siber güvenlik performanslarını ÇKKV yöntemleriyle objektif şekilde değerlendirmek ve karşılaştırmalı analizler sunmaktır. Stratejik öneme sahip olan ve kalkınmanın bir göstergesi olan siber güvenlik performans analizi için beş kriter (Yasal ölçümler, Teknik ölçümler, Organizasyonel ölçümler, Kapasite geliştirme ölçümleri ve İş birliği ölçümleri) altında on alternatif (Birleşik Arap Emirlikleri, Brezilya, Çin, Endonezya, Etiyopya, Güney Afrika, Hindistan, İran, Mısır ve Rusya) analize dahil edilmiştir. İlk aşamada, kriterlerin önem düzeylerini (ağırlıklarını) objektif bir şekilde belirleyebilmek için LOPCOW yönteminden yararlanılmıştır. Yapılan analizler sonucunda K5-İş birliği ölçümleri kriterinin en yüksek öneme sahip kriter olduğu; K2-Teknik ölçümler kriterinin ise en düşük öneme sahip kriter olduğu tespit edilmiştir. Araştırmanın ikinci aşamasında, ilk aşamada elde edilen kriter ağırlıkları kullanılarak MARCOS yöntemiyle BRICS ülkeleri için sıralama yapılmıştır. BRICS ülkelerinin nüfus, ekonomi ve internet kullanıcı sayısı açısından dünya üzerinde önemli bir paya sahip olmaları bu ülkeler grubunun temel seçim nedeni olmuştur. Yapılan hesaplamalar sonucunda Birleşik Arap Emirlikleri (A1), Endonezya (A4) ve Mısır (A9) ülkeleri rakiplerine göre daha iyi performans göstererek ilk sırayı paylaşmışlardır. Bu bulgu, söz konusu ülkelerin GCI'da küresel düzeyde rol modeli olarak gösterilen ülkeler (ITU, 2024b: 24) arasında yer almasıyla uyumlu bir sonuçtur. Bu ülkelerin ilk sırayı paylaşmaları, ulusal düzeyde benimsenen siber güvenlik politikaları, dijital dönüşüm ve altyapı yatırımları, uluslararası iş birlikleri, siber güvenlik insan kaynağının eğitimi gibi nedenlere bağlıdır. İran (A8) ise son sırayı alarak BRICS ülkeleri arasında en düşük siber güvenlik performansını göstermiştir. İran'ın yaptırımlar nedeniyle uluslararası alanda izole durumda olması ve altyapı ile personel eğitiminin yetersizliği, en düşük performansı sergilemesinin temel nedenleri arasında görülmektedir. Küpeli ve Söğüt (2024) tarafından GCI indeksi kullanılarak G20 ülkeleri için yapılan VZA sonucunda Endonezya ve Hindistan'ın ilk sırayı paylaşarak yüksek verimliliğe sergilediği tespit edilmiştir. Bu çalışmada ise Endonezya ve Hindistan'ın sırasıyla birinci ve dördüncü sıraları alarak üst sıralarda yer alma eğiliminde olduğu doğrulanmaktadır. Altıntaş (2022) tarafından elde edilen bulgularda Teknik ve Organizasyonel ölçümler en yüksek önem düzeyine sahip kriterler olarak belirlenmiştir. Buna karşılık, bu çalışmada Teknik ölçümler (K2) en düşük, Organizasyonel ölçümler (K3) ise üçüncü en önemli kriter olarak belirlenmiştir. Bu farklılıklar, ağırlıklandırmada kullanılan Entropi ve LOPCOW yöntemlerinin veri yapısına duyarlılığı ve kriterler arası varyasyonlara yaklaşım biçimiyle ilişkilidir. Üçüncü aşamada, kriter ağırlıklarındaki değişimin etkisini ölçmek için beş senaryo oluşturularak duyarlılık analizi yapılmıştır. Analiz sonucunda en yüksek ve en düşük performans gösteren ülkelerin sıralamalarında herhangi bir değişim gözlenmemiştir. Sıralamalarda kısmi değişimin yalnızca belirli ülkelere özgü ve sınır düzeyde olduğu tespit edilmiştir. Bu durum, önerilen modelin kriter ağırlıklarındaki değişimlere karşı dayanıklı olduğunu ve karar vericiler için istikrarlı, güvenilir sonuçlar üretebildiğini göstermektedir. Araştırmanın dördüncü ve son aşamasında, LOPCOW-MARCOS metodolojik yaklaşımının ortaya koyduğu sonuçların güvenirliğini test etmek amacıyla, literatürde yaygın şekilde kullanılan TOPSIS, MABAC, ARAS, MAIRCA ve CoCoSo yöntemleriyle karşılaştırmalı bir analiz gerçekleştirilmiştir. Analiz sonucunda, kullanılan yaklaşımın güvenilir sonuçlar ürettiği ve siber güvenlik alanında kullanılabileceği ortaya konmuştur.

Her ne kadar bu çalışma BRICS ülkelerine odaklanmış olsa da siber güvenliğe ilişkin politika önerileri genel geçer nitelikte olup tüm ülkeler için yol gösterici olabilir. Siber güvenlik çok boyutlu ve karmaşık bir olgu olduğundan, ülkelerin siber saldırılara karşı dirençli hale gelebilmeleri için stratejik adımlar atmaları gerekmektedir. Ülkelerin öncelikle ulusal siber güvenlik stratejilerini gözden geçirerek çağın gerekliliklerine uygun güncellemeler yapması gerekmektedir. Siber tehditler dünyanın herhangi bir yerinden kaynaklanabildiği için, uluslararası iş birliklerinin güçlendirilmesi ve ülkeler arasında bilgi paylaşımının sağlanması önem taşımaktadır. Siber güvenlik hem kamu hem de özel kurumları tehdit ettiğinden, çok sayıda yetişmiş uzmana ihtiyaç duyulmaktır. Bu nedenle, ülkelerin siber güvenlikle ilgili eğitim programlarını yaygınlaştırması ve üniversitelerle iş birliğini artırması gerekmektedir. Kamu hizmetlerinin sürdürülebilirliğinin sağlanabilmesi için, kritik altyapıların siber dayanıklılığının arttırılması ve penetrasyon testleriyle düzenli olarak denetlenmesi gerekmektedir. Bireylerin siber güvenliğe ilişkin farkındalığını arttırmak için ise bilinçlendirme ve eğitim programları düzenlenmelidir. Tüm bu stratejilerin bütüncül bir şekilde uygulanması, ülkelerin uzun vadede sürdürülebilir bir siber güvenlik kapasitesi geliştirmesine olanak tanıyacaktır.

Her çalışmada olduğu gibi, bu çalışmada da bazı sınırlılıkları ve bu sınırlılıkların giderilmesiyle gelecekte yürütülebilecek yeni çalışma konuları bulunmaktadır. Çalışmada 2024 yılına ait veriler kullanıldığı için, yapılan çıkarımlar yalnızca bu yıla özgüdür. Farklı yıllara ait verilerin de analize dahil edilmesi durumunda, ülkelerin performanslarındaki zamana bağlı değişim ölçülebilecektir. Çalışmada kullanılan veri setinin, siber güvenliğin farklı boyutlarını ölçecek şekilde genişletilmesi ya da farklı endeks verilerinin analize dahil edilmesi, ülkelerin siber güvenlik performanslarını daha güçlü bir şekilde ölçmeye imkân verecektir. Benzer şekilde, siber güvenlik alanında uzman kişilerin değerlendirmelerini dikkate alarak objektif yaklaşım ile subjektif bakış açılarını bir araya getiren bir metodolojik yaklaşımın benimsenmesi ve bu yaklaşımla kriter ağırlıklarının hesaplanması, analizi zenginleştirecektir.

This research article has been licensed with Creative Commons Attribution - Non-Commercial 4.0 International License. Bu araştırma makalesi, Creative Commons Atıf - Gayri Ticari 4.0 Uluslararası Lisansı ile lisanslanmıştır.

Yazar Katkıları

Yazar, çalışmayı tek başına hazırladığını beyan etmiştir.

Teşekkür Beyanı

Yazar(lar), çalışma için teşekkür beyanında bulunmamışlardır.

Destek Beyanı

Yazar(lar), çalışma için herhangi bir destekleyen beyanında bulunmamışlardır.

Çıkar Çatışması

Yazar(lar), çalışma için herhangi bir çıkar çatışması beyanında bulunmamışlardır.

Etik Beyanı

Yazar(lar), çalışma için Etik Kurul Onayı alınması gerekmediğini beyan etmişlerdir.

Kaynakça

Abacıoğlu, S., Ayan, B. ve Pamucar, D. (2025). The race to sustainability: Decoding green university rankings through a comparative analysis (2018–2022). *Innovative Higher Education*, *50*(1), 241-275. https://doi.org/10.1007/s10755-024-09734-4

Abas, M., Habib, T., Noor, S., Zimon, D. ve Woźniak, J. (2023). Application of multi-criteria decision-making methods in the selection of additive manufacturing materials for solid ankle foot orthoses. *Journal of Engineering Design*, *34*(8), 616-643. https://doi.org/10.1080/09544828.2023.2247859

AbdelMouty, A. M. ve Abdel-Monem, A. (2023). Neutrosophic MCDM methodology for assessment risks of cyber security in power management. *Neutrosophic Systems with Applications*, *3*, 53-61. https://doi.org/10.61356/j.nswa.2023.18

Abushark, Y. B., Khan, A. I., Alsolami, F., Almalawi, A., Alam, M. M., Agrawal, A., Kumar, R. ve Khan, R. A. (2022). Cyber security analysis and evaluation for intrusion detection systems. *Computers, Materials & Continua*, *72*(1), 1765-1783. https://doi.org/10.32604/cmc.2022.025604

Ahasan, M. A. Al, Hu, M. ve Shahriar, N. (2023). OFMCDM/IRF: A phishing website detection model based on optimized fuzzy multi-criteria decision-making and improved random forest. *2023 Silicon Valley Cybersecurity Conference (SVCC)*, 1-8. https://doi.org/10.1109/SVCC56964.2023.10165344

Alamri, B., Richardson, I. ve Crowley, K. (2024). Cybersecuriy risk management and evaluation framework of blockchain identity management systems in HIoT: Experts evaluation. *IEEE Access*, *12*, 144652-144683. https://doi.org/10.1109/ACCESS.2024.3468379

AlDaajeh, S. ve Alrabaee, S. (2024). Strategic cybersecurity. *Computers & Security*, *141*, 103845. https://doi.org/10.1016/j.cose.2024.103845

Alhakami, W. (2024). Enhancing cybersecurity competency in the Kingdom of Saudi Arabia: a fuzzy decision-making approach. *Computers, Materials & Continua*, *79*(2), 3211-3237. https://doi.org/10.32604/cmc.2023.043935

Alharbi, A., Seh, A. H., Alosaimi, W., Alyami, H., Agrawal, A., Kumar, R. ve Khan, R. A. (2021). analyzing the impact of cyber security related attributes for intrusion detection systems. *Sustainability*, *13*(22), 12337. https://doi.org/10.3390/su132212337

Almeida, F. (2025). Comparative analysis of EU-based cybersecurity skills frameworks. *Computers & Security*, *151*, 104329. https://doi.org/10.1016/j.cose.2025.104329

Altıntaş, F. F. (2022). G7 Ülkelerinin siber güvenlik performanslarının analizi: Entropi tabanlı MABAC yöntemi ile bir uygulama. *Güvenlik Bilimleri Dergisi*, *11*(1), 263-286. https://doi.org/10.28956/gbd.1109776

Andrade, R., Ortiz, I., Cazares, M., Navas, G. ve Sánchez-Pazmiño, M. I. (2022). Defining cyber risk scenarios to evaluate IoT systems. *Games*, *14*(1), 1. https://doi.org/10.3390/g14010001

Ansari, M. T. J., Al-Zahrani, F. A., Pandey, D. ve Agrawal, A. (2020). A fuzzy TOPSIS based analysis toward selection of effective security requirements engineering approach for trustworthy healthcare software development. *BMC Medical Informatics and Decision Making*, *20*(1), 236. https://doi.org/10.1186/s12911-020-01209-8

Aycın, E., Cercı, M. ve Sonugelen, E. (2024). An evaluation of women's human development level using multi criteria decision-making methods: a case study of OECD countries. *Economic Computation and Economic Cybernetics Studies and Research*, *58*(4/2024), 109-128. https://doi.org/10.24818/18423264/58.4.24.07

Bodin, L. D., Gordon, L. A., Loeb, M. P. ve Wang, A. (2018). Cybersecurity insurance and risk-sharing. *Journal of Accounting and Public Policy*, *37*(6), 527-544. https://doi.org/10.1016/j.jaccpubpol.2018.10.004

Bouramdane, A. A. (2023). Cyberattacks in smart grids: challenges and solving the multi-criteria decision-making for cybersecurity options, including ones that incorporate artificial intelligence, using an analytical hierarchy process. *Journal of Cybersecurity and Privacy*, *3*(4), 662-705. https://doi.org/10.3390/jcp3040031

BRICS portal. *The BRICS chairmanship.*18 Mart 2025 tarihinde https://infobrics.org/ adresinden edinilmiştir.

Bruggemann, R., Koppatz, P., Scholl, M. ve Schuktomow, R. (2022). Global cybersecurity index (GCI) and the role of its 5 pillars. *Social Indicators Research*, *159*(1), 125-143. https://doi.org/10.1007/s11205-021-02739-y

Candan, G. ve Toklu, M. C. (2022). Evaluating security performances of EU countries in the context of sustainable development using fuzzy SMART and ARAS approaches. *Environment, Development and Sustainability*, *26*(1), 1645-1671. https://doi.org/10.1007/s10668-022-02779-5

Catota, F. E., Morgan, M. G. ve Sicker, D. C. (2019). Cybersecurity education in a developing nation: the Ecuadorian environment. *Journal of Cybersecurity*, *5*(1), tyz001. https://doi.org/10.1093/cybsec/tyz001

Cisco. (2024). *2024 Cisco cybersecurity readiness index*. 07 Mart 2025 tarihinde https://newsroom.cisco.com/c/r/newsroom/en/us/a/y2024/m03/cybersecurity-readiness-index-2024.html#methodology adresinden edinilmiştir.

Craigen, D., Diakun-Thibault, N. ve Purse, R. (2014). Defining cybersecurity. *Technology Innovation Management Review*, *4*(10), 13-21. https://doi.org/10.22215/timreview/835

Çelebi Demirarslan, P., Sönmez Çakır, F. ve Akansel, I. (2024). Ranking the quality of life indexes by years in Asian countries using multi-criteria decision-making methods. *Asia-Pacific Journal of Regional Science*, *8*(3), 911-942. https://doi.org/10.1007/s41685-024-00350-w

Ecer, F. ve Pamucar, D. (2022). A novel LOPCOW-DOBI multi-criteria sustainability performance assessment methodology: An application in developing country banking sector. *Omega*, *112*, 102690. https://doi.org/10.1016/j.omega.2022.102690

Ecer, F., Tanrıverdi, G., Yaşar, M. ve Görçün, Ö. F. (2025). Sustainable aviation fuel supplier evaluation for airlines through LOPCOW and MARCOS approaches with interval-valued fuzzy neutrosophic information. *Journal of Air Transport Management*, *123*, 102705. https://doi.org/10.1016/j.jairtraman.2024.102705

e-Governance Academy Foundation. (2025). *National cyber security index-NCSI*. 07 Mart 2025 tarihinde https://ncsi.ega.ee/ adresinden edinilmiştir.

ENISA. (2024). *ENISA threat landscape 2024*. 07 Mart 2025 tarihinde https://www.enisa.europa.eu/publications/enisa-threat-landscape-2024 adresinden edinilmiştir.

Ersoy, N. (2023). BIST perakende ticaret sektöründe LOPCOW-RSMVC modeli ile performans ölçümü. *Sosyoekonomi*, *31*(57), 419-436. https://doi.org/10.17233/sosyoekonomi.2023.03.20

Ghoushchi, S. J., Ab Rahman, M. N. A., Soltanzadeh, M., Rafique, M. Z., Hernadewita, H., Marangalo, F. Y. ve Ismail, A. R. (2023). Assessing sustainable passenger transportation systems to address climate change based on MCDM methods in an uncertain environment. *Sustainability*, *15*(4), 3558. https://doi.org/10.3390/su15043558

Işık, Ö., Shabir, M., Demir, G., Puska, A. ve Pamucar, D. (2025). A hybrid framework for assessing Pakistani commercial bank performance using multi-criteria decision-making. *Financial Innovation*, *11*(1), 38. https://doi.org/10.1186/s40854-024-00728-x

Işık, Ö., Shabir, M. ve Moslem, S. (2024). A hybrid MCDM framework for assessing urban competitiveness: A case study of European cities. *Socio-Economic Planning Sciences*, *96*, 102109. https://doi.org/10.1016/j.seps.2024.102109

ITU. (2024a). *Global cybersecurity index - ITU*. 07 Mart 2025 tarihinde https://www.itu.int/hub/publication/d-hdb-gci-01-2024/ adresinden edinilmiştir.

ITU. (2024b). *Global cybersecurity index 2024 5th Edition*. 06 Mart 2025 tarihinde https://www.itu.int/epublications/publication/global-cybersecurity-index-2024 adresinden edinilmiştir.

Jamili, A., Imani Shamloo, J. ve Dargahi, F. (2024). Spatial analysis and integrated multi-criteria decision making methods; a model to evaluate justice in the distribution ff urban services in Tehran. *International Journal of Urban Sciences*, 1-26. https://doi.org/10.1080/12265934.2024.2438184

Ji, L., Zhang, D., Wang, Z., Liu, M., Sun, M., Zhang, H., Kraiem, N. ve Anjum, M. (2025). Paradigm shift in implementing smart technologies for machinery optimisation in manufacturing using decision support system. *Alexandria Engineering Journal*, *114*, 526-542. https://doi.org/10.1016/j.aej.2024.11.106

Jiang, M. ve Belli, L. (2025). Introduction: Contesting digital sovereignty: Untangling a complex and multifaceted concept. In M. Jiang ve L. Belli (Ed.), *Digital Sovereignty in the BRICS Countries: How the Global South and Emerging Power Alliances Are Reshaping Digital Governance* (ss. 1-38). Cambridge University Press. https://doi.org/10.1017/9781009531085.002

Karbassi Yazdi, A., Tan, Y., Spulbar, C., Birau, R. ve Alfaro, J. (2022). An approach for supply chain management contract selection in the oil and gas industry: combination of uncertainty and multi-criteria decision-making methods. *Mathematics*, *10*(18), 3230. https://doi.org/10.3390/math10183230

Kaur, H., Gupta, M. ve Singh, S. P. (2024). Integrated model to optimize supplier selection and investments for cyber resilience in digital supply chains. *International Journal of Production Economics*, *275*, 109338.

https://doi.org/10.1016/j.ijpe.2024.109338

Kostelić, K. (2025). TOPSIS-based framework for evaluating employee cybersecurity risk. *Croatian operational research review*, *16*(1), 31-44. https://doi.org/10.17535/crorr.2025.0003

Kumar, S., Arzaghi, E., Baalisampang, T., Abaei, M. M., Garaniya, V. ve Abbassi, R. (2024). A risk-based multi-criteria decision-making framework for offshore green hydrogen system developments: Pathways for utilizing existing and new infrastructure. *Sustainable Production and Consumption*, *46*, 655-678. https://doi.org/10.1016/j.spc.2024.03.020

Küpeli, M. ve Söğüt, E. (2024). Assessment of the cybersecurity efficiency of G20 countries using data envelopment analysis. *2024 17th International Conference on Information Security and Cryptology (ISCTürkiye)*, 1-4. https://doi.org/10.1109/ISCTrkiye64784.2024.10779233

Mohammed Abdelkader, E., Zayed, T., El Fathali, H., Alfalah, G., Al-Sakkaf, A. ve Moselhi, O. (2023). An integrated multi-criteria decision making model for the assessment of public private partnerships in transportation projects. *Mathematics*, *11*(16), 3559. https://doi.org/10.3390/math11163559

Nelson, A. ve Wang, S. (2024). The importance of cybersecurity disclosures in customer relationships. *Journal of Corporate Accounting & Finance*, *35*(3), 66-74. https://doi.org/10.1002/jcaf.22695

Noor, U., Anwar, Z., Altmann, J. ve Rashid, Z. (2020). Customer-oriented ranking of cyber threat intelligence service providers. *Electronic Commerce Research and Applications*, *41*, 100976. https://doi.org/10.1016/j.elerap.2020.100976

Öztaş, T. ve Öztaş, G. Z. (2024). Innovation performance analysis of G20 countries: A novel integrated LOPCOW-MAIRCA MCDM approach including the covid-19 period. *Verimlilik Dergisi*, *Productivity for Innovation (SI)*, 1-20. https://doi.org/10.51551/verimlilik.1320794

Panigrahi, G. R., Sethy, P. K., Behera, S. K., Gupta, M., Alenizi, F. A., Suanpang, P. ve Nanthaamornphong, A. (2024). Analytical validation and integration of cic-bell-dns-exf-2021 dataset on security information and event management. *IEEE Access*, *12*, 83043-83056. https://doi.org/10.1109/ACCESS.2024.3409413

Polireddi, N. S. A. ve Sekhar, K. R. (2023). Improved fuzzy-based MCDM–TOPSIS model to find and prevent the financial system vulnerability and hazards in real time. *Soft Computing*, 1-8. https://doi.org/10.1007/s00500-023-08318-2

Pourmadadkar, M., Lezzi, M. ve Ardebili, A. A. (2024). Investigating cyber risks in a surgical process for healthcare cyber resilience. *2024 IEEE International Conference on Cyber Security and Resilience (CSR)*, 575-580. https://doi.org/10.1109/CSR61664.2024.10679428

Priyadarshini, I., Kumar, R., Sharma, R., Singh, P. K. ve Satapathy, S. C. (2021). Identifying cyber insecurities in trustworthy space and energy sector for smart grids. *Computers & Electrical Engineering*, *93*, 107204. https://doi.org/10.1016/j.compeleceng.2021.107204

Proudfoot, J. G., Cram, W. A. ve Madnick, S. (2024). Weathering the storm: examining how organisations navigate the sea of cybersecurity regulations. *European Journal of Information Systems*, 1-24. https://doi.org/10.1080/0960085X.2024.2345867

Radulescu, C. Z., Radulescu, M., Vevera, A. V. ve Boncea, R. (2024). Extended group TOPSIS method with application for cybersecurity. *2024 10th International Conference on Control, Decision and Information Technologies (CoDIT)*, 1768-1773. https://doi.org/10.1109/CoDIT62066.2024.10708191

Roshanravan, B., Kreuzer, O. P. ve Buckingham, A. (2025). BWM-MARCOS: A new hybrid MCDM approach for mineral potential modelling. *Journal of Geochemical Exploration*, *269*, 107639. https://doi.org/10.1016/j.gexplo.2024.107639

Shaikh, F. A. ve Siponen, M. (2024). Organizational learning from cybersecurity performance: effects on cybersecurity investment decisions. *Information Systems Frontiers*, *26*(3), 1109-1120. https://doi.org/10.1007/s10796-023-10404-7

Simic, V., Dabic-Miletic, S., Tirkolaee, E. B., Stević, Ž., Ala, A. ve Amirteimoori, A. (2023). Neutrosophic LOPCOW-ARAS model for prioritizing industry 4.0-based material handling technologies in smart and sustainable warehouse management systems. *Applied Soft Computing*, *143*, 110400. https://doi.org/10.1016/J.ASOC.2023.110400

Song, J. M., Wang, T., Yen, J.-C. ve Chen, Y.-H. (2024). Does cybersecurity maturity level assurance improve cybersecurity risk management in supply chains? *International Journal of Accounting Information Systems*, *54*, 100695. https://doi.org/10.1016/j.accinf.2024.100695

Stević, Ž., Pamučar, D., Puška, A. ve Chatterjee, P. (2020). Sustainable supplier selection in healthcare industries using a new MCDM method: Measurement of alternatives and ranking according to compromise solution (MARCOS). *Computers & Industrial Engineering*, *140*, 106231. https://doi.org/10.1016/j.cie.2019.106231

Sukumar, A., Mahdiraji, H. A. ve Jafari-Sadeghi, V. (2023). Cyber risk assessment in small and medium-sized enterprises: A multilevel decision-making approach for small e-tailors. *Risk Analysis*, *43*(10), 2082-2098. https://doi.org/10.1111/risa.14092

Tanaji, B. A. ve Roychowdhury, S. (2024). BWM integrated VIKOR method using Neutrosophic fuzzy sets for cybersecurity risk assessment of connected and autonomous vehicles. *Applied Soft Computing*, *159*, 111628. https://doi.org/10.1016/j.asoc.2024.111628

Tayebi, A., Abbasianjahromi, H. ve Aghakarimi, M. (2025). Using a hybrid method to assess the consequence of hazards on the project success factors. *Engineering, Construction and Architectural Management*. https://doi.org/10.1108/ECAM-08-2023-0806

T.C. Ulaştırma ve Altyapı Bakanlığı. (2024). *Ulusal siber güvenlik stratejisi ve eylem planı (2024-2028) yayımlandı*. 07 Mart 2025 tarihinde https://hgm.uab.gov.tr/duyurular/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2024-2028-yayimlandi adresinden edinilmiştir.

Torbacki, W. (2021). A hybrid MCDM model combining DANP and PROMETHEE II methods for the assessment of cybersecurity in industry 4.0. *Sustainability*, *13*(16), 8833. https://doi.org/10.3390/su13168833

Torkayesh, A. E. ve Torkayesh, S. E. (2021). Evaluation of information and communication technology development in G7 countries: An integrated MCDM approach. *Technology in Society*, *66*, 101670. https://doi.org/10.1016/j.techsoc.2021.101670

Tusher, H. M., Munim, Z. H., Notteboom, T. E., Kim, T. E. ve Nazir, S. (2022). Cyber Security Risk Assessment in Autonomous Shipping. *Maritime Economics & Logistics*, *24*(2), 208-227. https://doi.org/10.1057/s41278-022-00214-0

Türk Dil Kurumu (TDK). *Güncel Türkçe sözlük*. 07 Mart 2025 tarihinde https://sozluk.gov.tr/ adresinden edinilmiştir.

Ulutaş, A., Balo, F. ve Topal, A. (2023). Identifying the most efficient natural fibre for common commercial building insulation materials with an integrated PSI, MEREC, LOPCOW and MCRAT model. *Polymers*, *15*(6), 1500. https://doi.org/10.3390/polym15061500

Ulutaş, A., Topal, A., Görçün, Ö. F. ve Ecer, F. (2024). Evaluation of third-party logistics service providers for car manufacturing firms using a novel integrated grey LOPCOW-PSI-MACONT model. *Expert Systems with Applications*, *241*, 122680. https://doi.org/10.1016/j.eswa.2023.122680

World Economic Forum. (2024). *The global risks report 2024, 19th Edition*. 07 Mart 2025 tarihinde www.weforum.org adresinden edinilmiştir.

Yavuz, İ. (2024). Analysis of the financial performance of airline companies in star alliance in the period 2018-2022 using LOPCOW-TOPSIS methods. *Ege Akademik Bakis (Ege Academic Review)*, *24*(4), 531-562. https://doi.org/10.21121/eab.20240404

Yusif, S. ve Hafeez-Baig, A. (2021). A conceptual model for cybersecurity governance. *Journal of Applied Security Research*, *16*(4), 490-513. https://doi.org/10.1080/19361610.2021.1918995

Zhang, D. (2025). Applying multi-criteria decision-making to text analysis for optimizing engineering knowledge management. *Alexandria Engineering Journal*, *117*, 648-661. https://doi.org/10.1016/j.aej.2025.01.028

Zhang, P., Wei, Y., Zhang, Y., Zhu, Y. ve Zhang, H. (2024). Security evaluation of power communication coupling system for new power system. *2024 International Conference on Artificial Intelligence and Power Systems (AIPS)*, 491-496. https://doi.org/10.1109/AIPS64124.2024.00107