Eskişehir Osmangazi Üniversitesi
Sosyal Bilimler Dergisi
Kasım 2024(3), 745-760
DOI: 10.17494/ogusbd.1485362

Endüstri 5.0'a Geçişte Siber Güvenlik: Yeni Sanayileşen Ülkeler Üzerine Bir İnceleme

Zafer DURAN[1]

Endüstri 5.0'a Geçişte Siber Güvenlik: Yeni Sanayileşen Ülkeler Üzerine Bir İnceleme

Öz

Bu çalışmanın amacı, yeni sanayileşen ülkelerin siber güvenlik düzeylerini derinlemesine değerlendirerek, bu ülkelerin Endüstri 5.0'a geçişlerini güvenli bir biçimde gerçekleştirmelerine yönelik içgörüler sunmaktır. Endüstri 5.0, kişiselleştirilmiş ürün ve hizmetlerin sürdürülebilir bir biçimde sunulmasını sağlayarak dijital dönüşümde yeni bir aşamayı temsil etmekte, ancak bu süreçte ortaya çıkan siber güvenlik riskleri işletmeler için önemli tehditler oluşturmaktadır. İşletmeler bu risklere karşı gerekli önlemleri alsalar da siber güvenliğin etkin bir şekilde sağlanabilmesi ülkelerin benimsediği politikalarla yakından ilişkilidir. Bu nedene ülkelerin siber güvenliğe ilişkin yaklaşımları, Endüstri 5.0'a geçiş sürecini önemli ölçüde şekillendirmektedir. Bu bağlamda, Entropi tabanlı MABAC yöntemiyle yapılan değerlendirme, organizasyonel önlemlerin yeni sanayileşen ülkeler için en kritik siber güvenlik göstergesi olduğunu ve Malezya'nın bu ülkeler arasında siber güvenlik düzeyi bakımından lider konumda olduğunu ortaya koymuştur.

Anahtar Kelimeler: Endüstri 5.0, Siber güvenlik, Yeni sanayileşen ülkeler, Entropi, MABAC

Cybersecurity in the Transition to Industry 5.0: A Study on Newly Industrializing Countries

Abstract

The aim of this study is to provide insights for newly industrialized countries to safely transition to Industry 5.0 by conducting an in-depth evaluation of their cybersecurity levels. Industry 5.0 represents a new stage in digital transformation by enabling the sustainable delivery of personalized products and services; however, the cybersecurity risks that arise during this process pose significant threats to businesses. Although companies take necessary precautions against these risks, the effective provision of cybersecurity is closely related to the policies adopted by countries. For this reason, countries' approaches to cybersecurity significantly shape the transition to Industry 5.0. In this context, the evaluation conducted using the Entropy-based MABAC method revealed that organizational is the most critical cybersecurity indicators for newly industrialized countries, and Malaysia holds a leading position among these countries in terms of cybersecurity levels.

Keywords: Industry 5.0, Cybersecurity, New industrializing countries, Entropy, MABAC

Makale Türü: Araştırma Makalesi

Paper Type: Research Article

[1] Öğr. Gör. Dr., Alanya Alaaddin Keykubat Üniversitesi, Gazipaşa Mustafa Rahmi Büyükballı Meslek Yüksekokulu, İşletme Yönetimi Programı, zafer.duran@alanya.edu.tr, https://orcid.org/0000-0002-7227-4196

Makale Gönderim Tarihi: 16.5.2024
Makale Kabul Tarihi: 30.9.2024

1. Giriş

Endüstri 5.0, Endüstri 4.0'ın attığı temel üzerine inşa edilen ve siber-fiziksel sistemler ile insan odaklı teknolojilerin entegrasyonunu vurgulayan endüstriyel evrimin bir sonraki aşamasını temsil etmektedir (Cotta vd., 2023). Endüstriyel evrimin bu yeni aşaması insan aklı ve bilişsel bilgi işlem arasındaki iş birliğine vurgu yaparken, otomasyonu da insanın fiziksel, duyusal ve bilişsel kapasitelerinin ek bir artırımı olarak görmektedir (Leng vd., 2022). Bu bağlamda Endüstri 5.0, üretim alanındaki insan görevlerini, çalışanlara fayda sağlayacak şekilde köklü bir şekilde yeniden yapılandırarak insanları tekrar üretim süreçlerine dahil etmektedir (Longo vd., 2020). Bu sayede insanların bilişsel yeteneklerini makinelerin verimliliği ile birleştirerek daha esnek, uyarlanabilir ve sürdürülebilir bir ekosistemi mümkün hale getirmektedir.

Endüstri 5.0, verimlilik ve üretkenliğin ötesine geçen bir paradigma değişimi sağlayarak endüstrinin topluma katkısını vurgulamaktadır (Maddikunta vd., 2022; Sverko vd., 2022; Gervasi vd., 2022). Endüstri 5.0 sürecinde otomasyonlar, cihazlar ve sistemler çalışma ortamına entegre edilerek robotlar, makineler ve insanlar arasındaki iş birliği artırılmaktadır (Güdek, 2023). Bu dönüşüm, insan unsurunun endüstriyel fiziksel ve kültürel çevrelerle karmaşık bir şekilde bütünleşen akıllı siber-fiziksel sosyo-teknik sistemleri yapılandırarak Endüstri 5.0'a geçişte önemli bir rol üstlenmesine neden olmaktadır. Bu bağlamda, Endüstri 5.0'ın insan merkezli yaklaşımı, endüstriyel dönüşümde insan faktörünün önemini vurgulayarak daha sürdürülebilir ve etkili bir endüstriyel geleceğin inşasına katkı sağlamaktadır (Leng vd., 2022).

Endüstri 5.0, üretim süreçlerini tek bir merkezde toplamaktan ziyade farklı coğrafi konumlardaki tesislere paylaştıran dağıtılmış üretim anlayışı ile karakterize edilmektedir (Raja Santhi ve Muthuswamy, 2023). Bu anlayış değer zincirinin uçtan uca kontrolünü hiç olmadığı kadar mümkün kılarak özelleştirilmiş üretim sistemlerinin önünü açmaktadır (Ahmed vd., 2024). Böylece hiper kişiselleştirilmiş ürün ve hizmetlerin sürdürülebilir bir şekilde sunumu olanaklı hale gelmektedir. Zira Endüstri 5.0, tekrarlayan ve monoton görevleri robotlara/makinelere; eleştirel düşünme gerektiren görevleri ise insanlara atayarak hem kaliteyi artırmakta hem de üretim süreçlerini müşteri ihtiyaçları ve pazar değişiklikleri doğrultusunda koordine edebilmektedir.

Endüstri 5.0, daha esnek ve otonom sistemlerin uygulanması yoluyla işletmeleri bireysel müşterilere özel deneyimler sunma konusunda güçlendiren bir yaklaşıma sahiptir (Ahmed vd., 2024). Ancak, bu yaklaşım, iş modellerini dönüştürerek değer zinciri boyunca tasarım aşamasından satış sonrası hizmetlere kadar köklü değişikliklere neden olmaktadır. Dolayısıyla değer zincirinin tüm yönlerini etkileyen çeşitli zorlukları da beraberinde getirmektedir. Bu zorluklar arasında, özellikle veri toplama ve işleme süreçlerindeki güvenlik, mahremiyet ve etik konular önemli bir yer tutmaktadır (Maddikunta vd., 2022). Bu nedenle, Endüstri 5.0'ın başarılı bir şekilde uygulanabilmesi için bu alanlardaki sorunlara yönelik etkili çözümlerin geliştirilmesi ve uygulanması büyük önem arz etmektedir. Bu bağlamda siber güvenlik, Endüstri 5.0'ın potansiyel avantajlarını koruma ve güvenlik risklerini en aza indirme noktasında kritik bir konu olarak öne çıkmaktadır. Zira Endüstri 5.0'ın sunduğu esneklik ve kişiselleştirilmiş deneyimler, önemli hacimlerde hassas verinin işlenmesini gerektirmekte ve dolayısıyla siber güvenlik risklerine karşı duyarlılığı artırmaktadır.

Endüstri 5.0'ın teknolojik temeli, birbirine bağlı seriler, siber-fiziksel sistemler, yapay zekâ nesnelerin interneti ve endüstriyel internetten oluşmaktadır (Corallo vd., 2022). Bu teknolojik enstrümanların bir arada kullanımı üretim süreçlerini optimize ederek işletmelere önemli avantajlar sağlamaktadır. Ancak çeşitli sistem ve süreçlerin birbirine internet ağları ile bağlı olması, herhangi bir güvenlik açığı veya arızası durumunda dalgalanma etkisiyle geniş çapta sorunlara neden olabilmektedir. Özellikle siber saldırılar, bu karmaşık ve birbirine bağlı sistemlerin zayıf noktalarını hedef alarak ciddi sorunlara neden olabilmektedir. Keza Endüstri 5.0 enstrümanlarının birbirine

karmaşık bir ağ yapısıyla bağlı olması ve kısmi bağımsızlığı, bilgisayar korsanlarının potansiyel olarak verilere erişmesine veya bunları sistemin verimliliğine saldırmak için kullanmasına olanak tanıyan kanallar oluşturmaktadır (Czeczot vd., 2023). Bu bağlamda her ne kadar kimlik doğrulama, şifreleme, erişim kontrolü ve veri gizliliği gibi geleneksel güvenlik önlemleri mevcut olsa da tüm paydaşların endüstriyel dönüşüme tam anlamıyla uyum sağlamamış olması, Endüstri 5.0'a geçiş sürecinde araştırmacıların ve uygulayıcıların dikkatlerini siber güvenlik konusuna çekmektedir.

Endüstriyel süreçler giderek daha fazla birbirine bağlı hale geldikçe verilerin, donanımların, sistemlerin ve ağların korunması da giderek daha önemli hale gelmektedir. Bu bağlamda, ülkelerin siber güvenlik konusunda benimsedikleri tutum ve yaklaşımlar, Endüstri 5.0'a geçişi etkileyen kritik bir faktör olarak ön plana çıkmaktadır. Zira düzenleyici çerçeveler ve Ar-Ge yatırımlarından uluslararası iş birliği ve insan sermayesi gelişimine kadar, ülkelerin siber güvenlik sorunlarını ele alırken yaptıkları seçimler, Endüstri 5.0'a geçişin yörüngesini şekillendirmektedir. Bu nedenle günümüzde ülkelerin Endüstri 5.0'ın karmaşıklığı içinde yol alırken siber güvenliğe yönelik proaktif, işbirlikçi ve ileri görüşlü tutum ve yaklaşımları benimsemeleri, endüstriyel inovasyon ve üretkenliğin geleceğini korumak için kaçınılmaz bir gereklilik haline gelmektedir. Nitekim kapsamlı ve dayanıklı siber güvenlik çerçevelerinin oluşturulması, endüstriyel tesislerin siber tehditlere karşı dayanıklılığını artırabilecek en etkili adımlardan biridir. Dolayısıyla Endüstri 5.0'a başarılı bir geçiş yaparak ekonomik ve sosyal kalkınmada fırsat yakalamak isteyen ülkelerde siber güvenlik düzeyinin izlenmesi ve geliştirilmesi hayati bir önem taşımaktadır.

Ülkelerin siber güvenlik düzeylerinin değerlendirilmesi çok yönlü ve karmaşık bir süreçtir. Uluslararası Telekomünikasyon Birliği, ülkelerin siber güvenlik seviyelerini değerlendirmek için bir çerçeve oluşturmak amacıyla 2015 yılında Küresel Siber Güvenlik Endeksi'ni (KSGİ) geliştirerek bu probleme bir çözüm sunmaya çalışmıştır. KSGİ ülkelerin siber tehditlere karşı daha hazırlıklı olmaları ve siber güvenlik alanındaki güçlü ve zayıf yönlerini tespit etmeleri için bilgi sunarken değerlendirme işleminde indikatörlerin önem derecelerini göz ardı ettiği için eleştirilmektedir. Bu çalışmada KSGİ verileri, Entropi ve MABAC yöntemleriyle değerlendirilerek KSGİ'nin sağladığı bilgiler daha nitelikli hale getirmeye çalışılmıştır. Bu bağlamda Endüstri 5.0'a geçişte büyük potansiyele sahip yeni sanayileşen ülkelere odaklanılarak çalışmadan elde edilecek kazanımların en üst düzeye çıkarılması hedeflenmiştir. Siber güvenlik ihlallerinin ekonomik hasar, üretim kaybı, yaralanma ve hatta ölüm gibi büyük olumsuz etkilere neden olabileceği (Corallo vd., 2022) göz önünde bulundurulduğunda elde edilen sonuçların araştırmacı ve uygulayıcılara kıymetli içgörüler sunacağı düşünülmektedir.

2. Literatür

Endüstri 5.0, siber-fiziksel sistemlerin, nesnelerin internetinin ve endüstriyel internetin birleşimini temsil etmekte ve yüksek düzeyde birbirine bağlı ve otomatikleştirilmiş sistemlerle karakterize edilmektedir. Bu birbirine bağlılık, siber tehditlere karşı artan güvenlik açıklarını beraberinde getirmektedir. Bununla birlikte siber uzayın birbirine bağlı doğası ve karmaşıklığı, Endüstri 5.0 paradigması için siber güvenliği oldukça önemli bir konu haline getirmektedir. Nitekim son dönemde yapılan araştırmalar, siber güvenliğin araştırmacılar arasında giderek daha fazla ilgi gören bir konu olduğunu ortaya koymaktadır. Bu bağlamda çalışma kapsamında büyük veri tabanlarında kapsamlı bir tarama gerçekleştirilmiş ve öne çıkan çalışmalara ilişkin hususlar, aşağıda belirtilmiştir.

Literatür incelendiğinde, siber güvenlikle ilgili yapılan çalışmaların genellikle işletme bazlı olduğu gözlemlenmiştir. Endüstriyel dönüşümün siber güvenlik yönüne odaklanıldığı için bu çalışmalar arasından sadece endüstri 5.0'a geçiş süreciyle ilgili olanları detaylı bir şekilde irdelenmiştir. Bu bağlamda Ahmed vd. (2024), Endüstri 5.0'ın temel siber güvenlik zorluklarını değerlendirdikleri çalışmalarında, Grafik Teorisi ve Matris Yaklaşımını kullandıkları görülmüştür. Araştırmacılar değerlendirmelerinin sonucunda Endüstri 5.0 teknolojilerinin avantajlarından tam olarak

yararlanabilmek için güçlü siber güvenlik programlarının geliştirilmesi ve siber risklerin azaltılmasının önemini vurgulamışlardır. Benzer şekilde Rajabion (2023) Endüstri 5.0'a geçişte ağları, programları ve sistemleri dijital saldırılara karşı korumada siber güvenliğin önemini araştırdığı çalışmasında finans, bilgi, uygulamalar gibi değerli kaynakların siber tehditlerden korunmasında sağlam siber güvenlik önlemlerinin gerekliliğini ortaya koymuştur. Kumar ve Mallipeddi (2022) ise siber güvenliğin operasyonlar ve tedarik zinciri yönetimi üzerindeki etkisini inceledikleri çalışmada kuruluşların Endüstri 5.0'a geçişte gelişmiş teknolojiler nedeniyle yeni risklerle karşı karşıya kaldığını ve bu risklerle başa çıkabilmek için siber güvenliğe yönelik sağlam stratejilere ihtiyaç duyduklarını öne sürmüşlerdir.

Endüstri 5.0'a geçiş sürecinde ulusal tutum ve yaklaşımlar, bu dönüşümün yönetilmesi ve etkilerinin dengelenmesi açısından kritik bir öneme sahiptir. Bu nedenle araştırmacılar, son zamanlarda ülkelerin siber güvenlik durumlarına odaklanan çalışmalar da gerçekleştirmektedir. Bu bağlamda Bustamante vd. (2018) Ekvador için siber güvenlik ve siber savunma modeli geliştirebilmek adına siber güvenliğe ilişkin dünya çapındaki durumu incelemişlerdir. KSGİ doğrultusunda gerçekleştirmiş oldukları analizler, G8 ülkelerinin Siber Güvenlik/Siber Savunma ve Siber Savaş alanlarında en hazırlıklı ve olgun görünen ülkeler olduğunu, Ekvador'un ise yalnızca kapasite geliştirme ve iş birliği konularında olumlu bir tutum sergilediğini; diğer KSGİ indikatörlerinde ise son derece kısıtlı kaldığını gözler önüne sermiştir. Benzer şekilde Maisikeli (2020), Birleşik Arap Emirlikleri'nde siber güvenlik algısı ve risklerini gelişmiş ülkelerle karşılaştırdığı çalışmasında, siber risk davranışının gelişmiş ülkelerle benzer seviyede olduğunu ancak dijital olgunluk, internete erişim ve siber güvenlik farkındalığının diğer gelişmiş ülkelere kıyasla düşük olduğunu ortaya koymuştur. Bu nedenle BAE'de siber güvenlik farkındalık programının agresif bir şekilde desteklenmesi gerektiğini savunmuştur. Peter (2017) spesifik bir şekilde Afrika'nın en iyi 12 gelişmekte olan ekonomisinin siber direncini izlemek ve karşılaştırmak amacıyla bir çalışma gerçekleştirmiştir. Yapmış olduğu analizler sonucunda Sudan, Gana, Libya, Zimbabwe, Cezayir ve Angola olmak üzere altı ülkenin kritik sistemlerinden ödün verilmesi riskiyle karşı karşıya olduğunu; Mısır, Kenya, Nijerya, Tunus, Fas ve Güney Afrika olmak üzere diğer altı ülkenin siber tehditlere karşı nispeten daha hazır durumda olduklarını öne sürmektedir. Bununla birlikte Peter çalışmasında siber tehditlere karşı dayanıklılığın gelişen değerlendirme kriterleri kullanılarak periyodik olarak yapılması gerektiğini özellikle belirtmiştir. Odebade ve Benkhelifa (2023) ise seçilmiş on ülkenin ulusal siber güvenlik stratejilerini karşılaştırarak güvenlik yaklaşımlarındaki benzerlikleri ve farklılıkları belirlemeye çalışmıştır. Araştırmalarının sonucunda, "Siber Güvenlik" terimine ilişkin ortak bir anlayış olmamasına rağmen ülkelerin kritik varlıkların korunması, araştırma ve geliştirme taahhüdü, gelişmiş ulusal ve uluslararası iş birliği konularında benzerliklere sahip olduğunu tespit etmişlerdir. Ayrıca, ülkelerin benimsediği ulusal siber güvenlik stratejilerinin güçlü ve zayıf yönlerini ortaya koyarak, siber güvenlik stratejilerini geliştirmeyi veya güncellemeyi planlayan ülkelere içgörüler sağlamışlardır.

Literatür taraması sırasında ülkelerin siber güvenlik düzeylerini değerlendirmeye yönelik yapılan çalışmaların oldukça sınırlı olduğu fark edilmiştir. Yarovenko vd. (2020), Ulusal Siber Güvenlik Endeksi verilerini kullandıkları çalışmada TOPSIS, VIKOR ve MAAM yöntemleriyle ülkeleri siber güvenlik düzeyleri doğrultusunda değerlendirerek sıralamışlardır. Çalışmalarının sonucunda Estonya ve Çek Cumhuriyeti tüm indikatörlerde sahip oldukları ideale yakın değerler nedeniyle en yüksek derecelere sahip olurken Güney Sudan tüm yöntemlerle yapılan hesaplamalarda en düşük derece sahip ülke olmuştur. Ülkelerin siber güvenlik performanslarını değerlendiren bir başka çalışma, Altıntaş (2022) tarafından gerçekleştirilmiştir. G7 ülkelerinin siber güvenlik performanslarının analiz edildiği bu çalışmada KSGİ verilerinden yararlanılarak ülkeler çok kriterli karar verme yöntemleri kullanılarak sıralanmıştır. Sıralama işleminin sonucunda ABD ilk sırada alırken İtalya sonuncu olmuştur. Vavera vd. (2022) ise Doğu Avrupa ülkelerinin siber güvenlik ve dijital kalkınma performanslarını değerlendirmek için ulusal ve uluslararası dört farklı indeksi bir araya getirmişlerdir. Bu çalışmada, Doğu Avrupa ülkeleri

COPRAS yöntemi kullanılarak sıralanmış ve siber güvenlik ile dijital kalkınma tedbirlerini destekleyebilecek çeşitli öneriler sunulmuştur.

Siber güvenlik, giderek dijitalleşen dünyanın en önemli konularından biri olarak görülmektedir. Bu durum araştırmacıları siber güvenlikle ilgili pek çok konuda araştırma yapmaya yöneltmektedir. Ancak yukarıda da bahsedildiği üzere ülkelerin siber güvenlik düzeylerini konu edinen çalışmalar oldukça sınırlıdır. Dolayısıyla ülkelerin siber güvenlik performanslarını ölçmek için güvenilir metrikler öneren ve performansları değerlendiren çalışmalara olan ihtiyaç, belirgin bir şekilde görülmektedir. Bu çalışma, Endüstri 5.0'a geçiş sürecinde büyük bir potansiyele sahip olan yeni sanayileşmiş ülkelerin siber güvenlik düzeylerini değerlendirerek ülkelere önemli içgörüler sunmanın yanı sıra literatürdeki bu sınırlılığın giderilmesine de katkı sağlamayı amaçlamaktadır. Odaklanılan ülkelerin kendine özgü özellikleri, çalışmanın kapsamını derinleştirirken özgünlüğünü de artırmaktadır. Ayrıca bu ülkelerin karşılaştırılması, her birinin benimsediği siber güvenlik yaklaşımının sağladığı avantajların daha iyi anlaşılmasına olanak tanımaktadır.

3. Yöntem

Bu bölümde çalışmada kullanılan veri setine ve değerlendirme işleminde yararlanılan yöntemlere yer verilmiştir. Bu bağlamda ilk olarak araştırmada kullanılan veriler, ardından da yararlanılan yöntemler açıklanmıştır. Çalışma, Araştırma ve Yayın Etiğine uygun bir şekilde gerçekleştirilmiştir.

3.1. Veri

Çalışma kapsamında yeni sanayileşen ülkelerin siber güvenlik düzeyleri, KSGİ verileri doğrultusunda değerlendirilmiştir. KSGİ, 2014 yılından bu yana Birleşmiş Milletler' in bilgi ve iletişim teknolojilerinden sorumlu uzmanlık kuruluşu olan Uluslararası Telekomünikasyon Birliği tarafından yayınlanan bir indekstir. Bu indeks, ülkelerin siber güvenliğe ilişkin yeteneklerini ve hazırlıklarını ölçmektedir. Bu bağlamda ülkelerin siber güvenlik yönetimine ilişkin gelişim düzeyini değerlendirmek için kapsamlı bir araç görevi görmektedir. Ülkelerin siber güvenlik çabalarını kıyaslamalarına, iyileştirme alanlarını belirlemelerine ve genel siber güvenlik duruşlarını geliştirmeye yönelik çalışmalarına olanak tanır. KSGİ'yi oluşturan indikatörlere ve çalışma kapsamında atanmış olan kodlarına, Tablo 1'de yer verilmiştir.

Tablo 1. KSGİ indikatörleri ve kodları

İndikatörler	KOD
Yasal önlemler	C1
Teknik önlemler	C2
Organizasyonel önlemler	C3
Kapasite geliştirme tedbirleri	C4
İşbirlikçi önlemler	C5

Hata! Başvuru kaynağı bulunamadı.'den anlaşılacağı üzere KSGİ, ülkelerin siber güvenlik s tratejilerini ve yaklaşımlarını beş ana indikatör ile ele almaktadır: yasal önlemler, teknik önlemler, organizasyonel önlemler, kapasite geliştirme tedbirleri ve işbirlikçi önlemler. Yasal önlemler indikatörü, siber uzayda yasa dışı faaliyetleri belirleyen mevzuatın oluşturulması ve bu mevzuatın uygulanması için gerekli araçların tanımlanmasını kapsamaktadır. Ayrıca, ulusal paydaşlar için siber güvenlik temellerinin oluşturulması ve uluslararası yükümlülüklerle uyumluluğun sağlanması için prosedürleri ele almaktadır. Teknik önlemler indikatörü, siber güvenlik riskleri ve olaylarıyla başa çıkmak için ulusal düzeyde etkili mekanizmalar ve kurumsal yapıların durumunu incelemektedir. Benzer şekilde organizasyonel önlemler indikatörü de ülkelerdeki siber güvenliği ele alan yönetişim ve koordinasyon mekanizmalarına odaklanmaktadır. Bu indikatör aynı zamanda siber güvenliğin en üst düzeyde yürütülmesinin ve

sürdürülmesinin sağlanması, çeşitli ulusal kuruluşlara ilgili rol ve sorumlulukların atanması ve bunların ulusal siber güvenlik duruşundan sorumlu kılınması gibi hususları ele almaktadır. Kapasite geliştirme tedbirleri indikatörü ise ülkelerin siber güvenlik çalışmalarını ayrıntılandırarak bilgi birikimini ve olanaklarını artırarak siber güvenlik direnci oluşturabilme kapasitesini irdelemektedir. Son olarak işbirlikçi önlemler indikatörü, ülkelerin siber riskler ve olaylarla başa çıkabilmek için diğer paydaşlarla yapmış olduğu iş birliklerinin performansını yansıtmaktadır.

KSGİ, ülkelerin siber tehditlere karşı ne kadar hazır olduklarını, riskleri nasıl yönettiklerini ve bu alanda ne kadar ilerleme kaydettiklerini gösteren uluslararası tek ölçüm araçlarıdır. Bu nedenle çalışma kapsamında ülkelerin siber güvenlik düzeylerini değerlendirmek için KSGİ indikatörleri kullanılmıştır. Bu bağlamda çalışmanın odaklandığı yeni sanayileşmiş ülkelerin KSGİ indikatörlerine ilişkin skorları, Tablo 2'de sunulmuştur.

Tablo 2. Yeni sanayileşen ülkelerinin KSGİ indikatörlerine ilişkin skorları

Ülkeler	C_1	C_2	C_3	C_4	C_5
Brezilya	20,00	18,73	18,98	19,48	19,41
Çin	20,00	17,94	16,63	19,04	18,91
Endonezya	18,48	19,08	17,84	19,48	20,00
Filipinler	20,00	13,00	11,85	12,74	19,41
Güney Afrika	16,82	15,85	12,50	15,37	17,93
Hindistan	20,00	19,08	18,41	20,00	20,00
Malezya	20,00	19,08	18,98	20,00	20,00
Meksika	15,61	17,90	14,70	16,13	17,34
Tayland	19,11	15,57	17,64	16,84	17,34
Türkiye	20,00	19,54	17,96	20,00	20,00

Kaynak: (International Telecommunication Union, 2020)

3.1. Araştırmada Kullanılan Yöntemler

Çalışma kapsamında, ülkelerin siber güvenlik düzeylerine ilişkin indikatörleri ağırlıkları Entropi yöntemiyle belirlenmiş, ülkelerin görece sıralamaları ise MABAC yöntemiyle gerçekleştirilmiştir. Böylece iki farklı yöntemin bir araya getirilerek değerlendirme daha hassas bir şekilde yapılmaya çalışılmıştır. Çalışmada kullanılan bu yöntemler aşağıda detaylı bir şekilde açıklanmıştır.

3.1.1. Entropi Yöntemi

Entropi kavramı ilk olarak 1865 yılında Rudolph Clausius tarafından sistem içindeki belirsizlik ve kargaşa düzeyini tanımlamak amacıyla tanıtılmıştır (Zhang vd., 2011). Bu yöntem günümüzde var olan veri setinin sahip olduğu yararlı bilgiyi ölçerek karar kriterlerine ilişkin ağırlıkların belirlenmesinde de kullanılmaktadır. (Wu vd., 2011). Alternatifler arasındaki farklılıkları ve bu farklılıkların karar verme sürecine etkisini değerlendirerek karar sürecindeki karmaşıklığı azaltmaya yönelik basit ve pratik bir çözüm sunmaktadır. Ayrıca değerlendirme işleminde karar vericilerin sübjektif düşüncelerini dikkate almadan sadece matematiksel çözümleri kullandığı için objektif bir yaklaşım olarak kabul edilmektedir (Lotfi ve Fallahnejad, 2010). Bu üstünlükleri nedeniyle çalışma kapsamında indikatör ağırlıklarının belirlenmesinde Entropi yöntemi tercih edilmiştir. Yöntemin işlem adımları şu şekildedir (Li vd., 2011; Wu vd., 2011);

1.Adım: Probleme ilişkin karar matrisi oluşturulur. Bu matris, m sayıdaki alternatifin n sayıdaki kriterlere ilişkin skorlarını gösterir. Oluşturulan matris, 1 numaralı eşitlik formuna sahiptir.

$$D = \begin{matrix} A_1 \\ A_2 \\ \vdots \\ A_m \end{matrix} \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \vdots & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{bmatrix} \quad (1)$$

2. Adım: Karar matrisi normalize edilir. Bu işlem esnasında 2 numaralı eşitlik kullanılır.

$$r_{ij} = \frac{x_{ij}}{\sum_{i=1}^{m} x_{ij}} \quad (2)$$

3. Adım: Entropi katsayısı ve Entropi değeri hesaplanır. Bu işlemler esnasında Entropi katsayısı için 3 numaralı eşitlik, Entropi katsayısı için ise 4 numaralı eşitlik kullanılır.

$$k = (\ln(m))^{-1} \quad (3)$$

$$ej = -k \sum_{j=1}^{n} r_{ij} \ln(r_{ij}) \quad (4)$$

4. Adım: Farklılaşma dereceleri hesaplanır. Bu işlem esnasında 5 numaralı eşitlikten yararlanılır.

$$d_j = 1 - ej \quad (5)$$

5. Adım: Entropi kriter ağırlıkları hesaplanır. Bu işlem esnasında 6 numaralı eşitlikten yararlanılır.

$$w_j = \frac{d_j}{\sum_{1=1}^{n} d_j} \quad (6)$$

3.1.2. MABAC Yöntemi

Pamučar ve Ćirović tarafından 2015 yılında geliştirilen MABAC yöntemi, en iyi alternatifi sınır yakınlık karşılaştırması yaparak belirlemeye çalışmaktadır. Yöntemin temel varsayımı, alternatiflerin sınır yaklaşım alanına olan uzaklığının tanımlanmasıdır. Hem nitel hem de nicel kriterleri kullanabilen bu yöntem karmaşık problemlere güvenilir ve istikrarlı çözümler sunabilmektedir. Bu özellikleri nedeniyle bu çalışmada ülkeleri sıralamak için tercih edilmiştir. Yöntemin çözüm adımları aşağıdaki gibidir (Pamučar ve Ćirović, 2015);

1.Adım: Alternatiflerin kriterlere ilişkin performanslarını gösteren X başlangıç karar matrisi oluşturulur. Bu matris, 7 numaralı eşitlik formundadır.

$$X = \begin{matrix} & C_1 & C_2 & \cdots & C_n \\ A_1 \\ A_2 \\ \vdots \\ A_3 \end{matrix} \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{bmatrix} \quad (7)$$

Bu matriste i=1,2,…,m ve j=1,2,…,n olmak üzere her x_{ij} i. alternatifin j. kritere ilişkin performansını göstermektedir.

2. Adım: Alternatiflerin farklı birimlerle ifade edilen kriterler bakımından karşılaştırılabilmesi için başlangıç karar matrisi normalize edilir. Bu işlem esnasında fayda yönlü kriterler için 8 numaralı eşitlik, maliyet yönlü kriterler için ise 9 numaralı eşitlik kullanılır.

$$n_{ij} = \frac{x_{ij} - x_j^-}{x_j^+ - x_j^-} \tag{8}$$

$$n_{ij} = \frac{x_{ij} - x_j^+}{x_j^- - x_j^+} \tag{9}$$

Normalizasyon işlemi sonrasında alternatiflerin her bir kritere ilişkin 0-1 aralığında değişen değerlerini gösteren normalize karar matrisi (N) elde edilir. Bu yeni matris 10 numaralı eşitlik formuna sahiptir.

$$N = \begin{matrix} \\ A_1 \\ A_2 \\ \vdots \\ A_3 \end{matrix} \begin{matrix} \begin{matrix} C_1 & C_2 & \cdots & C_n \end{matrix} \\ \begin{bmatrix} n_{11} & n_{12} & \cdots & n_{1n} \\ n_{21} & n_{22} & \cdots & n_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ n_{m1} & n_{m2} & \cdots & n_{mn} \end{bmatrix} \end{matrix} \tag{10}$$

3. Adım: Kriterlere ilişkin ağırlıklar (w_j) doğrultusunda ağırlıklandırılmış karar matrisi (V) oluşturulur. Bu işlem esnasında matrisin her bir elemanı (v_{ij}) 11 numaralı eşitlik yardımıyla hesaplanır.

$$v_{ij} = \omega_j(n_{ij} + 1) \tag{11}$$

Ağırlıklandırma işlemi sonrasında elde edilen matris 12 numaralı eşitlik formundadır.

$$V = \begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{bmatrix} = \begin{bmatrix} \omega_1(n_{11}+1) & \omega_2(n_{12}+1) & \cdots & \omega_n(n_{1n}+1) \\ \omega_1(n_{21}+1) & \omega_2(n_{22}+1) & \cdots & \omega_n(n_{2n}+1) \\ \vdots & \vdots & \ddots & \vdots \\ \omega_1(n_{m1}+1) & \omega_2(n_{m2}+1) & \cdots & \omega_n(n_{mn}+1) \end{bmatrix} \tag{12}$$

4. Adım: 13 numaralı eşitlik yardımıyla her bir kritere ilişkin sınır yakınlık alan değeri (g_j) hesaplanarak sınır yakınlık alan matrisi (G) oluşturulur. Oluşturulan matris 14 numaralı eşitlik formundadır.

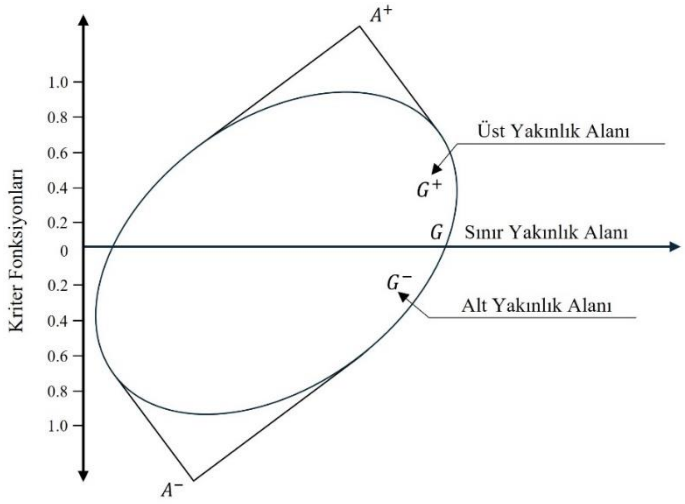
$$g_j = \left(\prod_{i=1}^{m} v_{ij} \right)^{1/m} \tag{13}$$

$$G = \begin{matrix} \begin{matrix} C_1 & C_2 & \cdots & C_n \end{matrix} \\ \begin{bmatrix} g_1 & g_1 & \cdots & g_n \end{bmatrix} \end{matrix} \tag{14}$$

5. Adım: Ağırlıklandırılmış karar matrisinden (V) sınır yakınlık alan matrisi (G)çıkartılarak alternatiflerin sınır yakınlık alanından uzaklıklarına ilişkin Q matrisi elde edilir. Bu işlem 15 numaralı eşitlikte gösterilmiştir.

$$Q = V - G = \begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{bmatrix} - \begin{bmatrix} g_1 & vg_2 & \cdots & g_1 \\ g_1 & g_2 & \cdots & g_2 \\ \vdots & \vdots & \ddots & \vdots \\ g_1 & g_2 & \cdots & g_2 \end{bmatrix} = \begin{bmatrix} q_{11} & q_{12} & \cdots & q_{1n} \\ q_{21} & q_{22} & \cdots & q_{2n} \\ \vdots & \vdots & \ddots & \vdots \\ q_{m1} & q_{m2} & \cdots & q_{mn} \end{bmatrix} \tag{15}$$

Bu matriste q_{ij} i. alternatifin j. kriter bakımından sınır yakınlık alanından uzaklığını gösterir. İşlem sonucunda alternatifler üst yakınlık alanı (G^+) veya alt yakınlık alanı (G^-) sınırları içerisinde konumlanabilmektedir. Sınır yakınlık alanları Şekil 1'de gösterildiği gibidir.



Şekil 1. Sınır Yakınlık Alanları

Sınır yakınlığında G^+ alanında yer alacak alternatifler ideal alternatifler olurken; G^- alanında yer alacak olan alternatifler ideal olmayan alternatif durumundadır. Alternatiflerin hangi yakınlık alanında yer alacağı 16 numaralı eşitlik yardımıyla belirlenmektedir.

$$A_i \in \begin{cases} G^+ \; ise \; q_{ij} > 0 \\ G \;\; ise \; q_{ij} = 0 \\ G^- \; ise \; q_{ij} < 0 \end{cases} \tag{16}$$

Herhangi bir alternatifin (A_i) en iyisi olarak seçilebilmesi için mümkün olduğu kadar çok kriterinin üst yakınlık alanında (G^+) yer alması gerekmektedir.

6. Adım: 17 numaralı eşitlik yardımıyla her bir alternatif için kriter fonksiyon değeri (S_i) hesaplanarak alternatifler S_i değerleri bakımından büyükten küçüğe sıralanır.

$$S_i = \sum_{i=1}^{n} q_{ij} \quad j = 1,2,\dots n, \quad i = 1,2,\dots,m \tag{17}$$

Hesaplamalar sonucunda en büyük S_i değerine sahip olan alternatif, en iyi alternatif olarak belirlenmiş olur.

4. Analiz ve Bulgular

Değerlendirme sürecinin ilk aşamasında Entropi yöntemi ile KSGİ indikatörlerinin ağırlıkları belirlenmiştir. Bu bağlamda ilk olarak yeni sanayileşmiş ülkelerin Tablo 2'de yer alan KSGİ indikatörlerine ilişkin skorları 2 numaralı eşitlik yardımıyla normalize edilmiş ve Tablo 3'te sunulan normalize karar matrisi oluşturulmuştur.

Tablo 3. Entropi yöntemine ilişkin normalize karar matrisi

Ülkeler	C_1	C_2	C_3	C_4	C_5
Brezilya	0,1053	0,1066	0,1147	0,1088	0,1020
Çin	0,1053	0,1021	0,1005	0,1063	0,0993
Endonezya	0,0973	0,1086	0,1078	0,1088	0,1051
Filipinler	0,1053	0,0740	0,0716	0,0711	0,1020
Güney Afrika	0,0885	0,0902	0,0755	0,0858	0,0942
Hindistan	0,1053	0,1086	0,1112	0,1117	0,1051
Malezya	0,1053	0,1086	0,1147	0,1117	0,1051
Meksika	0,0821	0,1018	0,0888	0,0901	0,0911
Tayland	0,1006	0,0886	0,1066	0,0940	0,0911
Türkiye	0,1053	0,1112	0,1085	0,1117	0,1051

Normalizasyon işleminin ardından 3 numaralı eşitlik yardımıyla Entropi değeri (k) hesaplanmış ve 0,4343 olduğu görülmüştür. Ardından 5 numaralı eşitlik yardımıyla farklılaşma dereceleri, 6 numaralı eşitlik yardımıyla da her bir indikatörün ağırlığı hesaplanmıştır. Bu işlemler sırasında elde edilen değerler **Hata! Başvuru kaynağı bulunamadı.**'te yer almaktadır.

Tablo 4. Yeni sanayileşen ülkelerin KSGİ indikatörlerine İlişkin ej, dj ve wj değerleri

Hesaplanan Değerler	İndikatörler				
	C_1	C_2	C_3	C_4	C_5
ej	0,9986	0,9970	0,9948	0,9960	0,9993
d_j	0,0014	0,0030	0,0052	0,0040	0,0007
w_j	0,0986	0,2079	0,3635	0,2832	0,0468

Hata! Başvuru kaynağı bulunamadı. incelendiğinde siber güvenlik düzeyine ilişkin en belirleyici i ndikatörün 0,3635 ağırlık değeri ile C_3 kodlu Organizasyonel önlemler olduğu görülmektedir. Ayrıca bu indikatörü 0,2832 ağırlık değeri ile C_4 kodlu kapasite geliştirme ve 0,2079 ağırlık değeri ile C_2 kodlu teknik yetenekler indikatörlerinin izlediği, diğer indikatörlerin nispeten düşük ağırlık değerlerine sahip oldukları anlaşılmaktadır.

Değerlendirme işleminin bir sonraki aşamasında yeni sanayileşmiş ülkelerin siber güvenlik düzeyleri MABAC yöntemiyle hesaplanmıştır. Bu bağlamda öncelikle indikatörlere ilişkin skorlar MABAC yöntemine uygun bir şekilde normalize edilmiştir. Bu işlem sırasında tüm indikatörler fayda yönlü olduğu için 8 numaralı eşitlik kullanılmıştır. Oluşturulan normalizasyon matrisi Tablo 5'te sunulmuştur.

Tablo 5. MABAC yöntemine ilişkin normalize karar matrisi

Ülkeler	C_1	C_2	C_3	C_4	C_5
Brezilya	1,0000	0,8761	1,0000	0,9284	0,7782
Çin	1,0000	0,7554	0,6704	0,8678	0,5902
Endonezya	0,6538	0,9297	0,8401	0,9284	1,0000
Filipinler	1,0000	0,0000	0,0000	0,0000	0,7782
Güney Afrika	0,2756	0,4358	0,0912	0,3623	0,2218
Hindistan	1,0000	0,9297	0,9201	1,0000	1,0000
Malezya	1,0000	0,9297	1,0000	1,0000	1,0000
Meksika	0,0000	0,7492	0,3997	0,4669	0,0000
Tayland	0,7973	0,3930	0,8121	0,5647	0,0000
Türkiye	1,0000	1,0000	0,8569	1,0000	1,0000

Normalizasyon işleminin ardından 11 numaralı eşitlik yardımıyla her bir ülkenin indikatörlere ilişkin skorları doğrultusunda ağırlıklandırılmış karar matrisi (V) oluşturulmuştur. Oluşturulan bu matris Tablo 6'da sunulmuştur.

Tablo 6. Ağırlıklandırılmış karar matrisi

Ülkeler	C_1	C_2	C_3	C_4	C_5
Brezilya	0,1972	0,3900	0,7270	0,5462	0,0832
Çin	0,1972	0,3649	0,6072	0,5290	0,0744
Endonezya	0,1631	0,4012	0,6689	0,5462	0,0936
Filipinler	0,1972	0,2079	0,3635	0,2832	0,0832
Güney Afrika	0,1258	0,2985	0,3966	0,3858	0,0572
Hindistan	0,1972	0,4012	0,6979	0,5665	0,0936
Malezya	0,1972	0,4012	0,7270	0,5665	0,0936
Meksika	0,0986	0,3637	0,5088	0,4155	0,0468
Tayland	0,1772	0,2896	0,6587	0,4432	0,0468
Türkiye	0,1972	0,4158	0,6750	0,5665	0,0936

Ağırlıklandırma işleminin ardından 13 numaralı eşitlik yardımıyla her bir kritere ilişkin sınır yakınlık alan değeri (g_j) hesaplanarak Tablo 7'de yer alan sınır yakınlık alan matrisi (G) oluşturulmuştur.

Tablo 7. Sınır yakınlık alan değerleri

	C_1	C_2	C_3	C_4	C_5
g_j	0,1707	0,3465	0,5873	0,4744	0,0740

Sınır yakınlık alan değerleri belirlendikten sonra MABAC yönteminin işlem adımları doğrultusunda ağırlıklandırılmış karar matrisinden (V) sınır yakınlık alan matrisi (G) çıkartılarak ülkelerin sınır yakınlık alanından uzaklıklarına ilişkin Q matrisi elde edilmiştir. Elde edilen bu matris, Tablo 8'de sunulmuştur.

Tablo 8. Ülkelerin Sınır Yakınlık Alanından Uzaklıkları

Ülkeler	C_1	C_2	C_3	C_4	C_5
Brezilya	0,0264	0,0435	0,1396	0,0718	0,0092
Çin	0,0264	0,0184	0,0198	0,0546	0,0004
Endonezya	-0,0077	0,0546	0,0815	0,0718	0,0195
Filipinler	0,0264	-0,1386	-0,2238	-0,1912	0,0092
Güney Afrika	-0,0450	-0,0480	-0,1907	-0,0886	-0,0169
Hindistan	0,0264	0,0546	0,1106	0,0921	0,0195
Malezya	0,0264	0,0546	0,1396	0,0921	0,0195
Meksika	-0,0722	0,0171	-0,0786	-0,0589	-0,0272
Tayland	0,0065	-0,0569	0,0713	-0,0312	-0,0272
Türkiye	0,0264	0,0693	0,0876	0,0921	0,0195

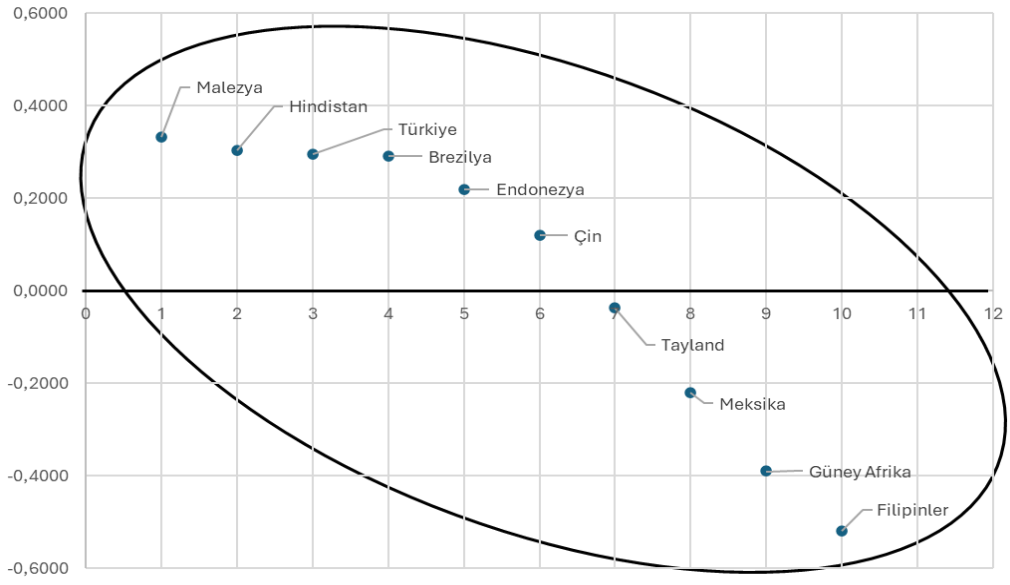
Son olarak 17 numaralı eşitlik yardımıyla yeni sanayileşen ülkelerin kriter fonksiyon değeri (S_i) hesaplanarak ülkeler görece sıralanmıştır. Yapılan sıralamaya ilişkin sonuçlar Tablo 9 yer almaktadır.

Tablo 9. Ülke sıralamaları

Ülkeler	S_i	Sıra
Brezilya	0,2906	4
Çin	0,1197	6
Endonezya	0,2198	5
Filipinler	-0,5180	10
Güney Afrika	-0,3891	9
Hindistan	0,3033	2
Malezya	0,3323	1
Meksika	-0,2197	8
Tayland	-0,0376	7
Türkiye	0,2950	3

Tablo 9'dan anlaşılacağı üzere yeni sanayileşen ülkeler arasında en iyi siber güvenlik düzeyine sahip ülke, Malezya iken en düşük siber güvenlik düzeyine sahip ülke Filipinler olmuştur. Malezya'nın tüm siber güvenlik indikatörlerinde yüksek skorlara sahip olması ve indikatörler bağlamında sınır yakınlık alanından uzaklıklarının tamamının pozitif olması bu bulgunun sebebi olarak görülmektedir. Tablo 9'da dikkat çeken bir diğer husus ise Malezya'yı takip eden Hindistan, Türkiye ve Brezilya'nın çok küçük farklarla sıralanmış olmasıdır. Bu durum ülkeler arasındaki sıralamanın her an değişebileceğine işaret etmektedir.

Son olarak araştırmaya konu olan ülkelerin hesaplanan kriter fonksiyon değerleri ve sıraları doğrultusunda sınır yakınlık alanındaki konumları belirlenmiştir. Bu işlem sonucunda oluşturulan grafik, Şekil 2'de sunulmuştur.



Şekil 2. Ülkelerin sınır yakınlık alanlarına ilişkin konumları

Şekil 2, ülkelerin S_i değerlerine göre belirlenen göreceli konumlarını görsel olarak ifade etmektedir. Üst sınır yakınlık alanında bulunan ülkeler ile alt sınır yakınlık alanında bulunan ülkeler arasındaki mesafeler dikkate alındığında, üst sınır yakınlık alanındaki ülkelerin siber güvenlik düzeyleri açısından daha rekabetçi bir pozisyona sahip oldukları açıkça görülmektedir.

5. Sonuç

Endüstri 5.0 yaklaşımı, şirketlerin daha esnek ve otonom sistemler aracılığıyla bireysel müşterilere kişiselleştirilmiş deneyimler sunma kapasitesini artırmaktadır. Bununla birlikte, iş modellerinde, tasarımdan satış sonrası hizmete kadar üretim sürecinin her aşamasını etkileyen dönüştürücü değişiklikleri de beraberinde getirmektedir. Otomasyon sistemleri ve robotlar iş yerlerine entegre edilmekte, makinelerin ve insanların iş birliği yaptığı bir üretim yaklaşımı teşvik edilmektedir. Bu bağlamda birbirine bağlı seriler, siber-fiziksel sistemler, yapay zekâ, nesnelerin interneti ve endüstriyel internet gibi teknolojiler her geçen gün daha fazla işletme tarafından kabul görmektedir. Bu teknolojik araçların eş zamanlı kullanımı üretim süreçlerini optimize ederek endüstrilere önemli avantajlar sağlasa da çeşitli sistem ve süreçlerin siber ağlar üzerindeki karşılıklı bağımlılığı, istismar edilebilecek potansiyel güvenlik açıkları yaratarak geniş çaplı sorunlara neden olabilmektedir. Zira Endüstri 5.0 teknolojilerinin birbirine bağlı yapısı ve kısmi bağımsızlıkları, kötü niyetli kişilerin değerli verilere erişmesi veya sistemin verimliliğini bozması için potansiyel kanallar oluşturmaktadır. Ayrıca, her birinin kendine ait zayıf noktaları ve riskleri olan birden fazla ortağın yer aldığı günümüz tedarik zincirlerindeki bir güvenlik açığı veya arıza, diğer ortaklar üzerinde oluşturacağı kademeli etkilerle, üretimi kesintiye uğratarak önemli mali kayıplara neden olabilmektedir. Bu nedenle verilerin, cihazların, sistemlerin ve ağların korunması, Endüstri 5.0'a geçiş sürecinde üzerinde durulması gereken en kritik konuların başında gelmektedir.

İşbirliğine dayalı robotik sistemler gibi siber-fiziksel sistemlerin endüstriyel ortamlara entegrasyonu, güvenli çalışmayı sağlamak için sağlam güvenlik önlemlerinin oluşturulmasını gerektirmektedir. Endüstriler, Endüstri 5.0'a doğru ilerlemeye devam ettikçe özellikle de endüstriyel süreçler daha entegre ve birbirine bağlı hale geldikçe siber güvenliğin önemi giderek artmaktadır. Dolayısıyla endüstriyel tesislerin siber tehditlere karşı güvende kalmasını sağlayacak strateji ve çözümlere olan ihtiyaç, her geçen gün kendini daha da hissettirmektedir. Bu bağlamda işletmeler, kullanıcı farkındalığı programları, gelişmiş teknolojik çözümler, özel siber güvenlik kontrolleri ve proaktif tehdit istihbaratı yönetimi gibi girişimlerle siber tehditlere karşı dayanıklılıklarını güçlendirmeye ve kritik endüstriyel operasyonlarını korumaya çalışmaktadırlar. Ancak siber güvenliğin tam manasıyla sağlanabilmesi, kamu kurumlarının aktif katılımını içeren çok yönlü bir yaklaşım gerektirmektedir. Dolayısıyla Endüstri 5.0'a geçiş sürecinde devletlerin tutum ve yaklaşımları, siber güvenlik için hayati bir rol oynamaktadır. Bu nedenle ülkelerin siber güvenliğe ilişkin tutum ve yaklaşımları yakından izlenmeli, yeteneklerini artırmaya ve üstünlüklerini sürdürmeye yönelik önerilere yeteri kadar önem verilmelidir.

Uluslararası Telekomünikasyon Birliği, KSGİ ile ülkelerin siber güvenlik düzeylerini değerlendirmeye yönelik etkili bir çerçeve sunmaktadır. Ancak bu çerçeve ülkelerin siber güvenlik düzeylerini değerlendirirken indikatörlerin ortalamalarını esas almakta ve indikatörlerin önem düzeylerini göz ardı etmektedir. Bu çalışmada KSGİ'nin sunduğu bilgilerin daha etkin bir şekilde değerlendirilmesi amacıyla Entropi ve MABAC yöntemleri birleştirilerek hibrit bir şekilde kullanılmıştır. Entropi yöntemiyle KSGİ indikatörlerinin ağırlıkları belirlenerek her bir indikatörün siber güvenlik düzeyine olan etkisi daha doğru bir şekilde anlaşılmaya çalışılmıştır. MABAC yöntemiyle de Endüstri 5.0'ın hem ekonomik büyüme hem de teknolojik dönüşüm açısından büyük potansiyel oluşturduğu yeni sanayileşmiş ülkelerin siber güvenlik düzeyleri göreceli olarak değerlendirilmiştir.

Değerlendirme işlemlerinde yeni sanayileşmiş ülkelerin siber güvenlik düzeyleri için en önemli indikatörün 0,3635 ağırlık değeri ile organizasyonel önlemler olduğu görülmüştür. Bu sonuç, Altıntaş'ın (2022) G7 ülkeleri üzerine gerçekleştirmiş olduğu çalışmada bulunan 0,276 değerinden bir miktar farklılık göstermektedir. Bu durum, araştırmaya konu olan ülkelerin farklılığından kaynaklanmaktadır. Entropi yönteminin doğası gereği farklı ülke gruplarının incelenmesi halinde ağırlık değerlerinin farklılık göstermesi, olağan bir sonuç olarak görülmektedir. Ülkelerin siber güvenlik düzeyleri bakımından MABAC yöntemiyle gerçekleştirilen sıralama işleminde ise Malezya'nın ilk sırada yer aldığı, bu ülkeyi Hindistan, Türkiye ve Brezilya'nın takip ettiği tespit edilmiştir. Bu sıralamanın çok küçük farklarla

oluşması, bu ülkelerin benzer tutumlar sergilediğini ve yapacakları küçük iyileştirmelerin dahi sıralamayı değiştirebileceğini göstermektedir. Bununla birlikte bu dört ülkenin siber güvenlik ile ilgili tutumları nedeniyle yeni sanayileşen ülkelerde yenilikçi teknolojiler kullanarak üretim yapmak isteyen işletmeler için son derece çekici olacakları düşünülmektedir. Zira bu ülkeler siber güvenlik düzeyleriyle Endüstri 5.0 teknolojilerinin birbirine bağlı yapısı ve kısmi bağımsızlıkları nedeniyle oluşan siber tehditlere karşı yeni sanayileşen ülkeler içerisinde en hazırlıklı ülkelerdir. Sıralamada dikkat çeken bir diğer nokta ise Meksika, Tayland ve Çin'in alt sıralarda yer almalarıdır. Özellikle Çin'in son yıllarda siber güvenlikte önemli ilerlemeler kaydetmesine rağmen sıralamanın üst basamaklarında yer alamaması, güçlü siber güvenlik stratejileri oluşturmanın zorluklarını gözler önüne sermektedir. Nitekim Çin, Siber Güvenlik Yasası'nı uygulamaya almış ve çeşitli ulusal siber güvenlik girişimlerini hayata geçirmiş olsa da KSGİ organizasyonel önlemler indikatöründe henüz yüksek skorlar elde edememiştir. Bu durum, yasal çerçevenin uygulanmasında yaşanan karmaşadan kaynaklanabileceği gibi toplumsal bilincin henüz yeterince gelişmemesinden de kaynaklanıyor olabilir. Çin'in dünya ekonomisindeki payı göz önünde bulundurulduğunda bu tür sorunlar, Endüstri 5.0'a geçiş sürecinde ciddi yatırım kayıplarına neden olabilir.

Siber tehditlere karşı sağlam stratejiler geliştirme ihtiyacı, tüm dünyada Endüstri 5.0 geçiş süreciyle birlikte oldukça belirgin hale gelmiştir. Bu nedenle hem ekonomik büyüme hem de teknolojik dönüşüm açısından büyük potansiyele sahip yeni sanayileşmiş ülkelerde endüstriyel tesislerin siber tehditlerden korunmasına yönelik strateji ve çözümlerin geliştirilmesine öncelik verilmelidir. Bu bağlamda yeni sanayileşen ülkelerde sürekli olarak güvenlik açıkları belirlenerek siber tehditlerin potansiyel etkisini değerlendiren kapsamlı risk analizleri gerçekleştirilmelidir. Siber güvenliğin hem teknolojik hem de insani yönlerini ele alan güvenlik önlemleri alınmalı, kritik sistemleri ve verileri yetkisiz erişime veya manipülasyona karşı korumaya önem verilmelidir. Bununla birlikte müdahale ve kurtarma planları hazırlayarak gelecekte benzer olayların önlenmesi için etkilenen sistemlerin izole edilmesine, operasyonların geri yüklenmesine ve olay sonrası kapsamlı analizlerin yapılmasına yönelik protokoller gözden geçirilmeli; eksiklikleri varsa giderilmelidir. Ayrıca endüstriyel tesislerde çalışanların farkındalığını artıracak proaktif müdahale önlemlerini birleştiren bütünsel bir yaklaşım desteklenmelidir. Böylece siber tehditlerin oluşturduğu riskler etkili bir şekilde azaltılabilir ve operasyonların güvenliği ve sürekliliği sağlanarak daha fazla yatırım çekme fırsatı yakalanabilir.

Bu çalışma Endüstri 5.0'a geçiş sürecinde yeni sanayileşen ülkelerin siber güvenlik düzeylerine odaklanmıştır. Değerlendirme işlemini Uluslararası Telekomünikasyon Birliği tarafından kamuoyu ile paylaşılan KSGİ verileri doğrultusunda gerçekleştirmiştir. Değerlendirme işleminde ise Entropi ve MABAC yöntemleri kullanılmıştır. Bu nedenle çalışmada elde edilen çıkarımlar bu kıstasların sınırlılıklarını taşımaktadır. Farklı veri kaynaklarının kullanılması, farklı ülke kümelerinin incelenmesi ya da farklı yöntemlerin tercih edilmesi halinde sonuçların bu çalışmada elde edilenlerden farklı olması muhtemeldir. Gelecekte yapılacak çalışmalarda ülkelerin siber güvenlik düzeylerini ölçmeye yönelik metrikler geliştirilebileceği gibi ülkelerin performansları farklı yöntemlerle ve farklı yaklaşımlarla yeniden değerlendirilebilir. Ayrıca farklı ülke grupları incelenerek ülkelerin benzerlikleri ve farklılıkları ortaya koyulabilir, ülkelere eksikliklerini gidermek ve güçlü yönlerini geliştirmeleri için öneriler geliştirilebilir.

Yazarların Makaleye Olan Katkıları

Yazar 1'in makaleye katkısı %100'dür.

Yazarların Makaleye Olan Katkıları

Bu makalede çıkar çatışması bulunmamaktadır.

Kaynaklar

Ahmed, I., Hossain, N. U. I., Fazio, S. A., Lezzi, M., ve Islam, M. S. (2024). A decision support model for assessing and prioritization of industry 5.0 cybersecurity challenges. *Sustainable Manufacturing and Service Economics,* (3), 100018. https://doi.org/10.1016/j.smse.2024.100018

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

Bustamante, F., Fuertes, W., Tulkeredis, T., ve Ron, M. (2018). Situational status of global cybersecurity and cyber defense according to global indicators. Adaptation of a Model for Ecuador. Rocha, Á., Guarda, T. (Eds), *Developments and Advances in Defense and Security (MICRADS 2018)* (s. 1-4) içinde. Cham, Springer. https://doi.org/10.1007/978-3-319-78605-6_2

Corallo, A., Lazoi, M., Lezzi, M., ve Luperto, A. (2022). Cybersecurity awareness in the context of the industrial internet of things: A systematic literature review. *Computers in Industry*, (137), 103614. https://doi.org/10.1016/j.compind.2022.103614

Cotta, W. A. A., Lopes, S. I., ve Vassallo, R. F. (2023). Towards the cognitive factory in industry 5.0: From concept to implementation. *Smart Cities,* 6(4), 1901-1921. https://doi.org/10.3390/smartcities6040088

Czeczot, G., Rojek, I., Mikołajewski, D., ve Sangho, B. (2023). AI in IoT management of cybersecurity for industry 4.0 and industry 5.0 purposes. *Electronics,* 12(18), 3800. https://doi.org/10.3390/electronics12183800

Gervasi, R., Barravecchia, F., Mastrogiacomo, L., ve Franceschini, F. (2022). Applications of affective computing in human-robot interaction: state-of-art and challenges for manufacturing. *Proceedings of the Institution of Mechanical Engineers Part B Journal of Engineering Manufacture*, 237(6-7), 815-832. https://doi.org/10.1177/09544054221121888

Güdek, B. (2023). Endüstriyel dönüşüm ve endüstri 5.0. *Ömer Halisdemir Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 16(4), 1129-1142. https://doi.org/10.25287/ohuiibf.1331731

International Telecommunication Union. (2020). Global cybersecurity index. https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2021-PDF-E.pdf

Kumar, S., ve Mallipeddi, R. R. (2022). Impact of cybersecurity on operations and supply chain management: Emerging trends and future research directions. *Production and Operations Management,* 31(12), 4488-4500. https://doi.org/10.1111/poms.13859

Leng, J., Sha, W., Wang, B., Zheng, P., Zhuang, C., Liu, Q., … Wang, L. (2022). Industry 5.0: Prospect and retrospect. *Journal of Manufacturing Systems*, 65, 279-295. https://doi.org/10.1016/j.jmsy.2022.09.017

Li, X., Wang, K., Liu, L., Xin, J., Yang, H., ve Gao, C. (2011). Application of the entropy weight and TOPSIS method in safety evaluation of coal mines. *Procedia Engineering*, 26, 2085-2091. https://doi.org/10.1016/j.proeng.2011.11.2410

Longo F, Padovano A, Umbrello S. (2020). Value-oriented and ethical technology engineering in industry 5.0: A human-centric perspective for the design of the factory of the future. *Applied Sciences,* 10(12), 4182. https://doi.org/10.3390/app10124182

Lotfi, F. H., ve Fallahnejad, R. (2010). Imprecise shannon's entropy and multi attribute decision making. *Entropy,* 12(1), 53-62. https://doi.org/10.3390/e12010053

Maddikunta, P. K. R., Pham, Q. V., Prabadevi, B., Deepa, N., Dev, K., Gadekallu, T. R., ... Liyanage, M. (2022). Industry 5.0: A survey on enabling technologies and potential applications. *Journal of Industrial Information Integration*, 26, 100257. https://doi.org/10.1016/j.jii.2021.100257

Odebade, A. T., ve Benkhelifa, E. (2023). A comparative study of national cyber security strategies of ten nations. *Computers and Society,* 13938. https://doi.org/10.48550/arXiv.2303.13938

Pamučar, D., ve Ćirović, G. (2015). The selection of transport and handling resources in logistics centers using multi-attributive border approximation area comparison (MABAC*). Expert Systems with Applications*, 42(6), 3016-3028. https://doi.org/10.1016/j.eswa.2014.11.057

Peter, A. S. (2017). Cyber resilience preparedness of Africa's top-12 emerging economies. *International Journal of Critical Infrastructure Protection*, 17, 49-59. https://doi.org/10.1016/j.ijcip.2017.03.002

Raja Santhi, A., ve Muthuswamy, P. (2023). Industry 5.0 or industry 4.0S? Introduction to industry 4.0 and a peek into the prospective industry 5.0 technologies. *International Journal on Interactive Design and Manufacturing*, 17(2), 947-979. https://doi.org/10.1007/s12008-023-01217-8

Rajabion, L. (2023). Industry 5.0 and cyber crime security threats. Bakkar, M.N. ve McKay E. (Ed.), *In Advanced Research and Real-World Applications of Industry 5.0* İçinde (s.66-76) IGI Global.

Maisikeli, S. (2023). *UAE Cybersecurity perception and risk assessments compared to other developed nations.* 3rd International Conference on Information and Computer Technologies (ICICT) (s.432-439) içinde. San Jose, CA, USA: İEE. https://doi.org/10.1109/ICICT50521.2020.00075

Sverko, M., Grbac, T., ve Mikuc, M. (2022). Scada systems with focus on continuous manufacturing and steel industry: A survey on architectures, standards, challenges and industry 5.0. *Ieee Access,* 10, 109395-109430. https://doi.org/10.1109/access.2022.3211288

Vevera, A. V., Cîrnu, C. E., ve Rădulescu, C. Z. (2022). O abordare multi-criterială pentru calculul unui indicator complex de Securitate Cibernetică și Dezvoltare Digitală. *Romanian Journal of Information Technology & Automatic Control/Revista Română de Informatică și Automatică*, 32(4). https://doi.org/10.33436/v32i4y202202

Wu, J., Sun, J., Liang, L., ve Zha, Y. (2011). Determination of weights for ultimate cross efficiency using shannon entropy. *Expert Systems with Applications*, 38(5), 5162-5165. https://doi.org/10.1016/j.eswa.2010.10.046

Yarovenko, H., Kuzmenko, O., ve Stumpo, M. (2020). Strategy for determining country ranking by level of cybersecurity. *Financial Markets, Institutions and Risks,* 4(3), 124-137. http://doi.org/10.21272/fmir.4(3).124-137.2020

Zhang, H., Gu, C.l., Gu, L.W., ve Zhang, Y. (2011). The evaluation of tourism destination competitiveness by TOPSIS & information entropy – A Case in the yangtze river delta of China. *Tourism Management*, 32(2), 443-451. https://doi.org/10.1016/j.tourman.2010.02.007