Güvenlik Bilimleri Dergisi / Journal of Security Sciences

Jandarma ve Sahil Güvenlik Akademisi
Güvenlik Bilimleri Enstitüsü
Güvenlik Bilimleri Dergisi, Mayıs 2022,Cilt:11, Sayı:1, 263-286
doi:10.28956/gbd.1109776

Gendarmerie and Coast Guard Academy
Institute of Security Sciences
Journal of Security Sciences, May 2022,Volume:11, Issue:1, 263-286
doi:10.28956/gbd.1109776

Makale Türü ve Başlığı / Article Type and Title
Araştırma / Research Article
G7 Ülkelerinin Siber Güvenlik Performanslarının Analizi: ENTROPİ Tabanlı MABAC Yöntemi ile Bir Uygulama
Analysis of Cyber Security Performances of G7 Countries: An Application With ENTROPY-Based MABAC Method

Yazar(lar) / Writer(s)
Furkan Fahri ALTINTAŞ, Jandarma Genel Komutanlığı, furkanfahrialtintas@yahoo.com,

Bilgilendirme / Acknowledgement:
Yazarlar aşağıdaki bilgilendirmeleri yapmaktadırlar:
Makalemizde etik kurulu izni ve/veya yasal/özel izin alınmasını gerektiren bir durum yoktur.
Bu makalede araştırma ve yayın etiğine uyulmuştur.

Bu makale Turnitin tarafından kontrol edilmiştir.
This article was checked by Turnitin.

Makale Geliş Tarihi / First Received : 27.07.2021
Makale Kabul Tarihi / Accepted : 11.03.2022

Atıf Bilgisi / Citation:
Altıntaş, F. F. (2022). G7 ülkelerinin siber güvenlik performanslarının analizi: ENTROPİ tabanlı MABAC yöntemi ile bir uygulama. *Güvenlik Bilimleri Dergisi, 11(1), ss 263-286, doi:10.28956/gbd.1109776*

G7 ÜLKELERİNİN SİBER GÜVENLİK PERFORMANSLARININ ANALİZİ: ENTROPİ TABANLI MABAC YÖNTEMİ İLE BİR UYGULAMA

Öz

Çalışmanın amacı, G7 ülkelerinin 2020 Küresel Siber Güvenlik Endeksi (GCSI) bileşen değerleri üzerinden siber güvenlik performanslarını ENTROPİ tabanlı MABAC yöntemi ile ölçmek ve GCSI'nın ENTROPİ tabanlı MABAC yöntemi ile açıklanabileceğini göstermektir. Bulgulara göre, ülkelerin siber güvenlik performans değerleri ABD, İngiltere, Almanya, Fransa, Kanada, Japonya ve İtalya olarak sıralanmıştır. Araştırmada, ABD ve İngiltere'nin siber güvenlik performanslarının fazla olması açısından diğer ülkeler ile belirgin farklılıklar olduğu tespit edilmiştir. Dolayısıyla ülkelerin siber güvenlik konusunda uyum içinde olmaları için Almanya, Fransa, Kanada, Japonya ve İtalya'nın siber güvenlik performanslarını artırmaları gerektiği sonucuna ulaşılmıştır. Ülkelerin GCSI ile bazı ENTROPİ tabanlı çok kriterli karar verme yöntemleri (ÇKKV) (ARAS, BTA, COPRAS, EDAS, ROV, WASPAS, TOPSIS, Gri İlişkisel Analiz) ile tespit edilen siber güvenlik performans değerleri arasındaki ilişkiler ölçülmüştür. Sonuçlara göre, ülkelerin GCSI değerleri, en fazla ENTROPİ tabanlı MABAC yöntemi ile ölçülen değerler ile ilişki içinde olduğu belirlenmiştir. Buna göre, GCSI'nın söz konusu ÇKKV yöntemleri içinde en fazla ENTROPİ tabanlı MABAC yöntemi ile açıklanabileceği bulgusuna ulaşılmıştır.

Anahtar Kelimeler: *Siber Güvenlik, Siber Güvenlik Performansı, ENTROPİ, MABAC.*

ANALYSIS OF CYBER SECURITY PERFORMANCES OF G7 COUNTRIES: AN APPLICATION WITH ENTROPY-BASED MABAC METHOD

Abstract

The aim of the study is to measure the cyber security performances of G7 countries over the 2020 Global Cyber Security Index (GCSI) component values with the ENTROPY-based MABAC method and to show that GCSI can be explained with the ENTROPY-based MABAC method. According to the findings, the cyber security performance values of the countries are listed as USA, England, Germany, France, Canada, Japan and Italy. In the research, it has been determined that there are significant differences with other countries in terms of the high cyber security performance of the USA and the UK. Therefore, it has been concluded that Germany, France, Canada, Japan and Italy should increase their cyber security performances in order for countries to be in harmony on cyber security. The relationships between the countries' GCSI and some ENTROPI-based multi-criteria decision-making methods (ÇKKV) (ARAS, BTA, COPRAS, EDAS, ROV, WASPAS, TOPSIS, Gray Relational Analysis) were measured. According to the results, it was determined that the GCSI values of the countries were most correlated with the values measured by the ENTROPY-based MABAC method. Accordingly, it has been found that GCSI can be explained the most by the ENTROPI-based MABAC method among the mentioned MCDM methods.

Keywords: *Cybersecurity, Cybersecurity Performance, ENTROPY, MABAC.*

GİRİŞ

Bilişim teknolojileri, hayatı kolaylaştırmanın yanında güvenlik kaygılarının oluşmasına neden olmuştur. Artık günümüz dünyasında mağdur ile aynı fiziksel ortam paylaşılmaksızın siber kapsamında suç filleri meydana gelmektedir. Bu çerçevede bilişim teknolojisi suç örgütlerinin iletişim kabiliyetini artırmış ve propaganda olanaklarını genişletmiştir. Dolayısıyla ülkeler, siber güvenliğin sağlanması açısından savunma sistemlerini oluşturma gereksinimi duymuştur (Hekim ve Başıbüyük, 2013, s. 136).

Siber güvenlik, genel anlamda bir bilgisayar ya da bilgisayar grubunun bir sisteme veya ağa yetkisiz girme, bilgilerini alma, değiştirme veya kaldırma faaliyetlerinden korunması olarak tanımlanmaktadır. Diğer bir tanıma göre siber güvenlik, genel anlamda siber ortamdan faydalanan kurumların ve kullanıcıların varlıklarını güvence altına almak maksadıyla kullanılan araçlar, uygulamalar, güvenlik teminatları, eğitimler ve en iyi uygulamalar bütünü olarak tanımlanmaktadır (von Solms ve van Neikerk, 2013, s. 97; Karacı ve Bilgici, 2017, s. 2080). Ülkelerin karşılaştıkları siber güvenlik algısı ve bu konudaki farklı faaliyetleri siber güvenlik tanımlamasının ülkelere göre farklılaşmasına neden olmuştur (Luiijf vd. 2013). Bu kapsamda bazı ülkelere göre siber güvenlik tanımlamaları Tablo 1'de gösterilmiştir.

Tablo 1. Ülkelere Göre Siber Güvenlik Kavramının Tanımları

Ülkeler	Tanımlar
Avustralya	Elektronik veya benzer yollarla işlenen, saklanan veya iletilen bilgilerin gizliliği, kullanılabilirliği ve bütünlüğü ile ilgili önlemlerdir.
Kanada	Elektronik bilgilere erişmek ve iletişim sağlamak için kasıtlı ve yetkisiz erişimin önlenmesine yönelik manipülasyon, kesinti ve imha faaliyetleridir.
Almanya	Küresel siber alan riskinin IT güvenlik modu kapsamında birimlere yapılan izinsiz girişlere engellemeye yönelik stratejilerdir.
Fransa	Depolanan, işlenen veya iletilen verilerin bilgi ve iletişim sistemlerinin sunduğu ilgili hizmetlerin kullanılabilirliğini, bütünlüğünü veya gizliliğini tehlikeye atabilecek siber uzaydan kaynaklanan olası saldırılara direnme faaliyetlerdir.
Hindistan	Bilgi ve bilgi sistemlerinin (ağlar, bilgisayarlar, veri tabanları, veri merkezleri) ve uygun prosedüre ve teknoloji güvenlik önlemleri kapsamında korunmasına yönelik faaliyetleridir.
ABD	Siber uzay bölümlerini güvence altına almak için sağlanan önlemlerdir.
İngiltere	Bilgi ve bilgi sistemlerinin yetkisiz erişim, kullanım, ifşa, kesinti, değişiklik veya imhadan korunmasına yönelik önlemlerdir.

Kaynak: Luiffjf vd. 2013, s. 6-7'den uyarlanmıştır.

Siber güvenliğin ana unsurunu siber saldırılara karşı sağlanan önlemler oluşturmaktadır. Dolayısıyla siber saldırılara karşı siber güvenliğin sağlanması adına savunma yöntemleri oluşturulmuştur. Söz konusu bu siber saldırılara karşı ülkeler münferit ve müşterek faaliyetler gerçekleştirmektedir. Siber saldırıların en önemli özelliklerinden bir tanesi; gelişen bilgisayar teknolojisi ve teknikleriyle beraber saldırıların niteliğinin de değişmesidir. Dolayısıyla gelişen ve değişen siber tehditlere karşı siber güvenlik savunma yöntemlerinin de değişim ve gelişim göstermesi büyük önem arz etmektedir (Kumar, 2015). Buna göre günümüzde siber saldırı türleri ile siber saldırılara karşı savunma yöntemleri Tablo 2'de açıklanmıştır.

Tablo 2. Siber Saldırılar ve Siber Savunma Yöntemleri

Siber Saldırılar	Siber Savunma Yöntemleri
Kabloya Saplama Yapma	Güvenlik Duvarı
Hizmet Dışı Bırakma (Dos, Ddos)	Anti Virüs
Kriptografik Saldırılar	Sayısal İmza
Yemleme (Phishing)	İçerik Filtreleme
Yerine Geçme (Masquerading)	Adli Bilişim
Köle Bilgisayarlar	Bal Küpü
Yazılımlar (Truva atı, solucan, virüs, arka kapılar, mantık bombası, kök kullanıcı takımı, klavye dinleme)	Siber Tehditleri Algılama Sistemi, Şifreleme Sistemleri, Kimlik Doğrulama Sistemleri

Kaynak: Ercan, 2015, s. 16-26; Goutam, 2015, s. 15

Ülkelerin gizli bilgilerinin diğer devletler tarafından ele geçirilmesi, diğer ülkelerin zayıf yanlarının ortaya çıkmasına ve söz konusu devletlerin uluslararası alanda itibarının zedelenmesine yol açmaktadır (Ada ve Çakır, 2017, s. 633). Siber güvensizliğin oluşturacağı maliyet, siber güvenliği sağlamak için yapılacak maliyetlerden daha fazla olacağı için ülkeler siber güvenliğe yönelik stratejiler geliştirmektedir (Ögün ve Kaya, 2013; Goutam, 2015, s. 14; Aslay, 2017, s. 27). Dolayısıyla siber güvensizlik dünya çapında büyüyen bir sorun teşkil ettiğinden devletler siber güvenlik konusunda istikrarı artırmaya çalışmaktadır (Ruhl vd. 2020, s. 1). Buna göre ülkeler sürekli olarak kendilerinin siber güvenlik performanslarını takip etmektedir. Böylece ülkeler, siber güvenlik performansları hakkında kendilerinde farkındalık sağlayarak siber güvenlik konusundaki eksikliklerini, yeterliliklerini ve üstünlüklerini tespit edebilmektedir. Böylelikle ülkeler, siber güvenlik potansiyelinin farkındalığıyla siber güvenlik konusunda eksikliklerini gidermek, yeterliliklerini geliştirmek ve üstünlüklerinin sürdürebilirliğini sağlamak için stratejiler, yöntemler, yönetimler, politikalar ve

faaliyetler gerçekleştirebilmektedir. Ayrıca ülkeler birbirlerinin siber güvenlik performanslarını takip ederek siber güvenlik konusunda iyi olan ülkeler ile iş birlikleri ve ortaklıklar sağlayabilmektedir. Buna göre, ülkelerin siber güvenlik performanslarının ölçümü önem kazanmakta, ülkeler siber güvenlik performanslarını ölçen metriklere gereksinim duymaktadır.

Uluslararası alanda tanınan ve ülkelerin siber güvenlik performanslarını ölçen ölçeklerden bir tanesi Uluslararası Telekominikasyon Birliği (International Telecominication Union - ITU) tarafından geliştirilen Küresel Siber Güvenlik Endeksi (Global Cyber Security Index – GCSI)'dir (ITU, 2020, s. 6). Endeks sayesinde ülkeler, siber güvenlik politikalarını ve stratejilerini daha gerçekçi, etkin, etkili ve verimli olarak sağlayabilmektedir (ITU, 2020). Endeksin temel amacı, ülkelerin siber güvenlik alanlarını belirlemelerine rehberlik etmek ve ülkelerin siber güvenlik performanslarını artırmak için yardımcı olmaktır (ITU, 2017, s. 4; Yerina, 2021,s 7).

Tablo 3. GCSI Bileşen ve Alt Bileşenleri

GCI Bileşenleri	GCI Alt Bileşenleri
Yasal Ölçümler	Siber suçlar mevzuatı
	Siber güvenlik değerlendirmeleri
Teknik Ölçümler	Ulusal bazda siber olaylara müdahale ekibi
	Sektörel bazda siber olaylara müdahale ekibi
	Siber güvenlik standartların uygulanması
	Çocuk çevrim içi koruma politikaları
Organizasyonel Ölçümler	Ulusal siber güvenlik stratejisi
	Sorunlu ajanslar
	Siber güvenlik ölçekleri
Kapasite Gelişimi Ölçümleri	Siber güvenlik bilinçlendirme çalışmaları
	Siber güvenlik uzmanlığı eğitimi
	Siber güvenlik alanında eğitim programları
	Siber güvenlik AR-GE programları
	Ulusal siber güvenlik endüstrisi
	Siber güvenliğe yönelik devlet teşvik sistemi
İş birliği Ölçümleri	Diğer ülkeler ile siber güvenlik konusunda ikili anlaşmalar
	Siber güvenlik faaliyetleriyle ilgili olarak ilgili uluslararası mekanizmalara hükümet katılımı
	Siber güvenlik ile ilgili çok taraflı anlaşmalar
	Özel sektör ortaklıkları
	Kurumlar arası ortaklıklar

Kaynak: ITU, 2020, s. 137-155

GCSI ile ilk olarak 2015 yılında ülkelerin siber güvenlik performansları ölçülmüştür. En son ve güncel olan 2020 yılı için 194 ülkenin siber güvenlik performansları hesaplanmıştır. GCSI 5 bileşen ve 5 bileşene bağlı 20 alt bileşen ile 20 alt bileşene bağlı 82 anket sorusundan oluşmaktadır. Anket sorularının ve alt bileşenlerin ağırlıkları 84 uzman tarafından belirlenmiştir. Bileşenlerin ağırlıkları eşit seviyede olup 1 ile 20 değer arasında puanlandırılmıştır. Bileşenlerin toplam skorlarıyla ülkelerin GCSI değerleri tespit edilebilmektedir (ITU, 2020). Bu kapsamda GCSI bileşen ve alt bileşenleri Tablo 3'de açıklanmıştır.

Siber güvenlik özellikle finans sistemlerini siber tehditlerden korumak G7 ülkeleri açısından büyük önem arz etmektedir. Çünkü G7 ülkelerinde özellikle siber suç tehdidi bakımından kişisel bilgilerin çalınması ve kişisel gizliliğin tehlikeye girmesi son yıllarda çok arttığından G7 ülkeleri siber güvenlik konusuna oldukça yoğunlaşmaktadır[1]. G7 ülkeleri, dünya ekonomisinin yaklaşık olarak %40'ını temsil etmektedir[2]. Bu nedenle sermayenin ve ekonomik faaliyetlerin yoğunlaştığı G7 ülkelerinde siber saldırıların olması muhtemeldir. Dünya genelinde siber saldırılara en fazla maruz kalan ülkeler G7 grubunda olan ABD, Almanya, Fransa ve İngiltere olmuştur (Güntay, 2016, s. 103). 2016 yılı için siber saldırı kapsamında kimlik hırsızlığı olayında ABD, Fransa, Kanada ve Japonya ilk 10 ülke içindedir (Öztürk, 2018, s. 215). Dolayısıyla G7 ülkelerinin siber güvenlik faaliyetlerinin küresel ekonomi ve finansın korunmasında büyük payı olduğu düşünülmektedir. G7 ülkelerinin siber güvenlik–faaliyetleri diğer ülkelerin siber güvenlik faaliyetlerini de etkileyebilmektedir. Sayılan nedenlerden ötürü G7 ülkelerinin siber güvenlik performanslarının analizi büyük önem taşımaktadır.

ENTROPİ yöntemi, farklı karar verme süreçlerindeki farklı değerlendirme olaylarında çok iyi sonuçlar çıkarmaktadır. Çünkü bu yöntemle kriterler arasındaki düzensizlikler hesaplanarak karar vericiler karmaşık olmayan sonuçlar çıkarabilmektedirler (Ecer, 2020, s. 5). Böylelikle kriterlerin önemlilik derecelerinin ve ağırlık katsayılarının ölçülmesinde ENTROPİ yönteminden akademik araştırmalarda sıklıkla faydalanılmıştır (Ulutaş ve Topal, 2020). MABAC yöntemi ise rasyonel karar vermede pratik, faydalı ve güvenilir bir matematiksel araç olmasının yanında tutarlı çözüm üreten bir Çok Kriterli Karar Verme (ÇKKV) yöntemidir (Ecer, 2020: 283). Bu çerçevede 2020 yılı için G7 ülkelerinin siber güvenlik performansları ENTROPİ tabanlı MABAC yöntemi ile

[1] www.g7.utoronto.ca/evaluations/muharına-cybersecurity-2021.html. Erişim Tarihi: 05/08/2021
[2] www.aa.com.tr/2270274. Erişim Tarihi: 05/08/2021

ölçülmüş ve sıralanmıştır. Araştırmanın literatür kısmında ENTROPİ ve MABAC yöntemleri ile ilgili çalışmalar açıklanmıştır. Araştırmanın yönteminde ise veri seti ve ENTROPİ ile MABAC yöntemleri belirtilmiştir. Sonuç kısmında çıkarımlar tartışılmış ve öneriler sunulmuştur.

1. LİTERATÜR TARAMASI

Araştırmanın literatürü iki kısımdan oluşmaktadır. Bunlardan birincisinde siber güvenlik ile ilgili araştırmalar açıklanmıştır. İkincisinde ENTROPİ ve MABAC yöntemleri ile ilgili çalışmalar belirtilmiştir.

GCSI literatürünün ana kaynağı, ITU tarafından oluşturulan GCSI raporlarına dayanmakta olup ülkelerin siber güvenlik performansları 2015, 2017, 2018 ve 2020 yılı için ölçülmüştür. Bu çerçevede literatürde tüm GCSI raporları 2015, 2017, 2018 ve 2020 yıllarına göre en fazla siber güvenlik performansı gösteren ilk 10 ülke Tablo 4'de açıklanmıştır.

Tablo 4. GCSI'ya Göre Ülkelerin Siber Güvenlik Performans Sıralamaları

Sıralama	2015	2017	2018	2020
1	ABD	Singapur	İngiltere	ABD
2	Kanada	ABD	ABD	İngiltere
3	Avustralya	Malezya	Fransa	Suudi Arabistan
4	Malezya	Ürdün	Litvanya	Avusturya
5	Ürdün	Estonya	Estonya	Estonya
6	Yeni Zelanda	Mauritius	Singapur	Güney Kore
7	Norveç	Avustralya	İspanya	Singapur
8	Brezilya	Gürcistan	Malezya	Rusya
9	Estonya	Fransa	Norveç	Bir. Arap Emirliği
10	Almanya	Kanada	Kanada	Malezya

Kaynaklar: ITU (2015), ITU (2017), ITU (2018), ITU (2020)

Tablo 4 incelendiğinde, tüm raporlara göre ABD'nin siber güvenlik performansı açısından ilk iki sıra içinde olduğu gözlenmiştir. Dolayısıyla ABD diğer ülkelere kıyasla siber güvenliğe daha çok önem vermektedir. Ayrıca İngiltere'nin siber güvenlik performans sıralamasında 2015 ve 2017 yıllarında ilk 10 ülke içinde bulunmazken 2018 ve 2020 yılları için ilk iki sırada olduğu tespit edilmiştir. Tablo 4 değerlendirildiğinde, 2015 ve 2017 yılları için 3, 2018 yılı için 4 ve 2020 yılı için 2 G7 ülkesi siber güvenlik performans sıralamasında ilk 10 ülke içinde yer almıştır. Ayrıca Japonya haricinde tüm G7 ülkelerinin ITU raporlarında ilk 10 ülke içinde olduğu belirlenmiştir. Bu durum genel anlamda siber güvenlik performansı sağlamanın G7 ülkeleri için önemli olduğunu göstermektedir.

Onumo vd. (2017), 89 ülkenin 2015 yılı için GCSI ve Hostede kültürel boyut endeksi bileşenlerine ait değerler üzerinden siber güvenlik boyutunun kültürel boyuta olan etkisini hiyerarşik regresyon analizi ile belirlemişlerdir. Araştırmada, siber güvenlik boyutunun kültürel boyutu anlamlı, pozitif yönde ve orta düzeyde etkilediği tespit edilmiştir.

Ruvin (2020), 2018 yılı için Ukrayna İç İşleri Bakanlığı, Ukrayna Siber Polis Departmanlığı, Ukrayna İstatistik Kurumu, Avrupa İstatistik Kurumu (EUROSTAT), Ukrayna'da bulunan Uluslararası şirketler ve akademik araştırmalara ilişkin veriler ile siber saldırıya uğrayan Ukrayna'nın bölgelerini kümeleme analizi ile gruplandırmıştır. Analize göre Luhansk ve Chernikiv'in en fazla siber saldırıya maruz kalan bölgeler olduğu gözlenmiştir.

Bruggemann vd. (2019), 2019 yılı için 10 ülkenin GCSI bileşenlerine ait değerler üzerinden söz konusu ülkelerin siber güvenlik performanslarını Hasse diyagramı ile tasniflemişlerdir. Bulgulara göre, siber güvenlik performansı en fazla olan ülkelerin birinci küme kapsamında İngiltere ve ABD olduğu tespit edilmiştir. Bunu ikinci küme olarak Avustralya, Estonya ve Norveç, üçüncü küme kapsamında Kanada ve İspanya ve son olarak dördüncü küme kapsamında ise Kanada ve İspanya takip etmiştir. Araştırmada Hasse diyagramına göre Singapur ve Malezya tasnif dışı kaldığı gözlenmiştir.

Göçoğlu ve Aydın (2019); ABD, Rusya ve Çin'in siber güvenlik politikalarını karşılaştırmışlardır. Araştırmada, ABD'de devlet kurumlarına yönelik oluşabilecek siber saldırılara karşı savunma mekanizmaların gelişmesine yönelik faaliyetler yapıldığı belirtilmiştir. Rusya'ya da ise siber güvenlik stratejilerinin savunma odaklı olduğu işaret edilmiştir. Araştırmada Rusya'nın siber güvenlik konusunda savunma sistemlerinin sağlanmasında müttefikleriyle yapılan iş birliklerine önem verdiği vurgulanmıştır. Son olarak Çin'de ABD ve Rusya'dan farklı olarak millî siber ağlarını kullanılarak ve uluslararası yaygın siber ağlarının kullanımını yasaklanarak siber savunma konusunda güçlü bir savunma sistemi oluşturulduğu tespit edilmiştir.

Kravetz (2019), GCSI ve Ulusal Siber Güvenlik Endeksi (National Cybersecurity Index-NCSI) metriklerini karşılaştırmışlardır. Araştırmada her iki endeksin alt bileşen değerlerinin uzman görüşlerine göre belirlendiği tespit edilmiştir. Ayrıca her iki endekse ait bileşenlerin birbirleri ile ilişkili fakat birbirinden farklı olduğu ifade edilmiştir. Bununla beraber araştırmada, GCSI'nın NCSI'ya göre daha kapsamlı, NCSI'nın ise GCSI'ya göre daha güncel bilgiler ile hazırlandığı vurgulanmıştır.

Ruiz vd. (2020) İngiltere'deki üniversitelerin siber güvenlik kurslarının niteliğini 1 ile 5 puan arasında derecelendirmişlerdir. Sonuçlara göre, İngiltere'deki üniversitelerin siber güvenlik kurslarının %54'ünün 1 puan, %26'sının 2 puan, %11'inin 3 puan, %6'sının 4 puan ve %4'ünün 5 puan aldığını ve İngiltere'deki üniversitelerin siber güvenlik kurslarının yaklaşık olarak %21'inin nitelikli olduğu sonucuna ulaşılmıştır.

Topcu (2020), Çin'in siber güvenlik sistemini analiz etmiştir. Buna göre Çin'de siber güvenlik sorunlarının ulusal güvenlik ile eş değer sayıldığı ifade edilmiştir. Bu kapsamda araştırmada Çin'de siber güvenlik algılarının üç bölümden oluştuğu belirtilmiştir. Bu bölümlerden birincisi, siber güvenlik saldırısında veya tehdidinde ulusal güvenlik konusunda risk oluşturmasıdır. İkincisi siber güvenlik tehdit algısının Çin'deki rejimin istikrarını engellemeye yönelik potansiyel tehdit olduğudur. Üçüncüsü, gelişecek siber saldırıların su, enerji, kamu hizmeti, sağlık, eğitim gibi önemli altyapıları hedef alacak olmasıdır.

Tvaronavičienė vd. (2020); 2018 yılı için İngiltere, ABD, Fransa, Estonya ve Litvanya ülkelerinin GCSI alt bileşenlerine ait değerler üzerinden söz konusu ülkelerin siber güvenlik altyapı koruma performanslarını ölçen bir metrik geliştirmişlerdir. Metriğin bileşenleri yasal süreç, sağlam devlet, risk yönetimi, güvenlik kültürü, teknoloji ve vaka yönetimi olarak belirlenmiştir. Metriğe göre siber güvenlik altyapı koruma performansı en iyi olan ülkenin ABD olduğu tespit edilmiştir. ABD'yi sırasıyla İngiltere, Estonya, Fransa ve Litvanya takip etmiştir.

Güleç ve Kişman (2021), NATO'nun siber güvenlik stratejilerini analiz etmişlerdir. Bu kapsamda araştırmada, NATO'nun çeşitli siber saldırılar sonrasında güçlü stratejiler geliştirmeye başladığı ifade edilmiştir. Araştırmada, NATO üyelerinin herhangi bir siber saldırıya uğraması durumunun NATO üyesi diğer ülkelerde bir güvenlik meselesi olarak görüldüğü belirtilmiştir. Bunların dışında araştırmada, siber saldırılara karşı NATO üyelerinin müşterek olarak hareket ettiği ve NATO üyesi ülkelerin NATO'nun geliştirdiği siber güvenlik sistemlerine odaklandığı gözlenmiştir.

Kharlamov ve Pogrebna (2021), 74 ülkenin 2018 yılı için GCSI ile Scwartz teorisindeki insani bileşen (uyum, eşitlikçilik, hiyerarşi, ustalık, duygusallık ve entelektüel) değerleri arasındaki ilişkiyi Pearson korelasyon katsayısı ile belirlemişlerdir. Araştırma sonucuna göre, GCSI'nın uyum, ustalık, hiyerarşi ve eşitlikçilik bileşenleri ile anlamsız; duygusallık ve entelektüel bileşenleri ile pozitif yönlü ve anlamlı ilişki içinde olduğu tespit edilmiştir.

ÇKKV literatürü incelendiğinde, ENTROPİ ve MABAC yöntemlerini konu alan pek çok araştırmaya rastlamak mümkündür. Buna göre literatürde tespit edilen bazı ENTROPİ ve MABAC yöntemleri ile ilgili olan araştırmalar Tablo 5'te açıklanmıştır.

Tablo 5. ENTROPİ ve MABAC ile İlgili Çalışmalar

Araştırmacılar	Yöntem	Araştırma Konusu
Pamucar ve Cirovic (2015)	DEMATEL tabanlı MABAC	Lojistik merkezlerinde nakliye araçlarının seçim problemi
Biswas ve Das (2018)	ENTROPİ tabanlı MABAC	Çevre dostu hibrid araçların seçim problemi
Milosavijavic (2018)	Delphi ve ENTROPİ tabanlı TOPSIS, ELECTRE ve MABAC	Sırbistan'da demir yolu konteyner seçim problemi
Ayçin ve Çakır (2019)	ENTROPİ tabanlı MABAC	Ülkelerin inovasyon performanslarının ölçümü
Bakır (2019)	SWARA tabanlı MABAC	Hava yolu şirketlerinin müşteri memnuniyet performanslarının ölçümü
Biswas vd. (2019)	ENTROPİ tabanlı MABAC	En iyi portföy seçim problemi
Ulutaş (2019)	ENTROPİ tabanlı MABAC	Mobilya atölyesi için en uygun pazarlama yöneticisinin seçim problemi
Çınaroğlu (2020)	ENTROPİ tabanlı MABAC	Yenilikçi girişimlere ve sektörlere ait faaliyetlerin performans ölçümü
Fan vd. (2020)	ENTROPİ tabanlı MABAC	Bulanık çevrede üçüncü taraf lojistik tedarikçi seçimi
Çalık (2021)	BWM, ENTROPİ, CRITIC tabanlı COPRAS, WASPAS ve MABAC	Gıda endüstrisi için yeşil tedarikçi seçim problemi
Chackraborty vd. (2021)	DEMATEL tabanlı MABAC	Hindistan'daki akıllı şehirlerin performansların ölçülmesi

Literatür değerlendirildiğinde, ülkelerin siber güvenliği hakkında pek çok araştırmaya rastlanılmıştır. Bu durum ülkeler için siber güvenlik meselesinin önemini göstermektedir. Ayrıca ÇKKV literatüründe karar alternatiflerinin performans ölçümünde ENTROPİ ve MABAC yöntemi ile ilgili fazla çalışma olması, söz konusu yöntemler ile araştırmaya konu olan ülkelerin siber güvenlik performanslarının ölçümünün sağlanabileceğini göstermektedir.

2. YÖNTEM

2.1. Araştırmanın veri seti ve analizi

Araştırmanın veri setini, 2020 yılı için G7 ülkelerinin GCSI bileşenlerine ait değerler oluşturmaktadır. Araştırmada kolaylık sağlaması açısından GCSI bileşenlerinin kısaltmaları Tablo 6'da gösterilmiştir.

Tablo 6. GCSI Bileşenleri ve Bileşenlerin Kısaltmaları

Bileşenler	Kısaltmalar
Yasal Ölçümler: Siber suçlar ve siber güvenlikle ilgili yasa ve yönetmeliklerin ölçülmesi.	**CSI1**
Teknik Ölçümler: Ulusal ve sektöre özel ajanslar aracılığıyla teknik yeteneklerin uygulanmasının ölçülmesi.	**CSI2**
Organizasyonel Ölçümler: Siber güvenliği uygulayan ulusal stratejilerin ve kuruluşların ölçülmesi.	**CSI3**
Kapasite Gelişimi Ölçümleri: Siber güvenlik kapasitesinin geliştirilmesi için farkındalık kampanyaları, eğitim, öğretim ve teşviklerin ölçülmesi.	**CSI4**
İş birliği Ölçümleri: Ajanslar, firmalar ve ülkeler arasındaki ortaklıkların verimliliğinin ölçülmesi.	**CSI5**

2.2. ENTROPİ Yöntemi

ENTROPİ yöntemi, ÇKKV literatüründe yer alan ağırlık hesaplama tekniklerinden objektif olanlar kategorisinde yer almaktadır. Bu yöntemde, karar vericilerin değerlendirmelerine gerek olmadan karar alternatiflerine ilişkin veriler kullanılarak nesnel sonuçlar sağlanmaktadır. Ayrıca ENTROPİ yönteminde değerleri yüksek olan veri grubundaki belirsizlik daha fazla olmaktadır (Ayçin, 2019, s. 122). ENTROPİ yöntemi özellikle veri kümeleri arasındaki farklılıkların belirlenmesinde üstün bir performans sağlamaktadır. ENTROPİ yöntemi ile veri kümelerindeki belirsizlik ölçülür ve ölçülen belirsizlik değeri ile veri kümelerinin farklılaşma değerleri elde edilir. Her bir kriter için farklılaşmanın toplam farklılaşma içindeki payı o kriterin ağırlık değerine karşılık gelmektedir (Dinçer, 2019, s. 36).

Buna göre ENTROPİ yönteminin uygulama aşamaları aşağıda açıklanmıştır (Ayçin, 2019, s. 122-124):

A_i: i. Karar Alternatifi (i=1,2,…..m).

D: Karar Matrisi

In (x)= Doğal Logaritma Fonksiyonu

C_j: j. Değerlendirme Kriteri (j=1,2, …..n).

x_{ij}: j. Değerlendirme Kriterine göre i. Alternatifin Aldığı Yer.

p_{ij}: j. Değerlendirme Kriterine göre i. Alternatifin Aldığı Normalize Değer.

k: Entropi Katsayısı

e_j: Entropi Değeri

d_j: Farklılaşma Derecesi

w_j: j. Değerlendirme Kriterinin Ağırlığı (j=1,2,…..n).

1. Aşama: Karar Matrisinin Oluşturulması

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

2. Adım: Karar Matrisinin Normalizasyonu

$$p_{ij}=\frac{x_{ij}}{\sum_{i=1}^{m} x_{ij}} \quad \forall\, i, j \quad (2)$$

3. Adım: Kriterlerin ENTROPİ Değerlerinin Bulunması

$$k=(In(m))^{-1} \quad 0\leq e_j\leq 1 \quad (3)$$

$$e_{ij}=-k.\sum_{j=1}^{n} p_{ij}\ .\ In(p_{ij})\ i=1,2…..m;\ j=1,2,…..n \quad (4)$$

4. Adım: Farklılaşma Derecelerin Hesaplanması

$$d_j=1-e_j \quad j=1,2,…..n \quad (5)$$

5. Adım: ENTROPİ Kriter Ağırlıklarının Tespiti

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

2.3. MABAC Yöntemi

MABAC (Multi Attributive Border Approximation Arae Comparison – Çok Ölçümlü Sınır Yaklaşım Alanı Kıyaslaması) yöntemi, her bir karar alternatifine ait kriter fonksiyonunun sınır yaklaşım alanına olan uzaklığının tespit edilmesi durumuna dayanmaktadır. Ayrıca nihai sonucun geniş kapsamlılığının sağlanabilmesi için MABAC yönteminde potansiyel kazanç ve kayıp değerleri dikkate alınmaktadır. Diğer bir ifade ile MABAC yönteminde potansiyel getiri ve kayıp değerler ölçülerek sonuçların mümkün olduğunca kesin duruma getirilmesi esastır (Ecer, 2020, s. 282). MABAC yönteminin uygulama aşamaları aşağıda açıklanmıştır (Ecer, 2020, s. 283-286):

1. Aşama: Karar Matrisinin Sağlanması Oluşturulması

$$X=\begin{array}{c} \\ A_1 \\ A_2 \\ \cdots \\ A_m \end{array}\begin{array}{c} \begin{array}{cccc} C_1 & C_2 & \ldots & C_n \end{array} \\ \begin{bmatrix} x_{11} & x_{12} & \cdots & x_{1n} \\ x_{21} & x_{22} & \cdots & x_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ x_{m1} & x_{m2} & \cdots & x_{mn} \end{bmatrix} \end{array} \quad (7)$$

2. Aşama: Karar Matrisinin Standartlaştırılması

Fayda Temelli Kriterlerin Standartlaştırılması:

$$n_{ij}=\frac{x_{ij}-x_i^-}{x_i^+-x_i^-} \quad (8)$$

Maliyet Temelli Kriterlerin Standartlaştırılması:

$$n_{ij}=\frac{x_{ij}-x_i^+}{x_i^--x_i^+} \quad (9)$$

x_i^+ Karar Matrisindeki maksimum, x_i^- ise minimum değeri göstermektedir.

Bu kapsamda N standartlaştırılmış matris elde edilir.

$$N=\begin{array}{c} \\ A_1 \\ A_2 \\ \cdots \\ A_m \end{array}\begin{array}{c} \begin{array}{cccc} C_1 & C_2 & \ldots & C_n \end{array} \\ \begin{bmatrix} n_{11} & n_{12} & \cdots & n_{1n} \\ n_{21} & n_{22} & \cdots & n_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ n_{m1} & n_{m2} & \cdots & n_{mn} \end{bmatrix} \end{array} \quad (10)$$

3. Aşama: Standartlaştırılmış Matrisin Ağırlıklandırılması:

$$v_{ij}=w_i.n_{ij}+w_{ij} \quad (11)$$

v_{ij}Standartlaştırılmış değerleri ağırlıklandırılmasını, w_i i. kriterlerin ağırlığını ifade etmektedir. Böylece ağırlıklı matris (V) Eşitlik 12 ile elde edilir.

$$V=\begin{array}{c} \\ A_1 \\ A_2 \\ \cdots \\ A_m \end{array}\begin{array}{c} \begin{array}{cccc} \end{array} \\ \begin{bmatrix} v_{11} & v_{12} & \cdots & v_{1n} \\ v_{21} & v_{22} & \cdots & v_{2n} \\ \cdots & \cdots & \cdots & \cdots \\ v_{m1} & v_{m2} & \cdots & v_{mn} \end{bmatrix} \end{array} \quad (12)$$

4. Aşama: Sınır Yaklaşım Alanı Matrisinin Oluşturulması:

Bu matrisin elemanları, ağırlıklı matrisin sütun elemanlarının geometrik ortalamasıdır.

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

Eşitlik 13'de gösterilen sınır yaklaşım alanı matrisi (G Matrisi) sağlanır. G matrisinin her bir elemanı, ilgili kriterlere göre bir sınır yaklaşım alanını ifade eder.

$$\begin{matrix} & C_1 & C_2 & \dots & C_n \\ G= & [g_1 & g_2 & \cdots & g_n] \end{matrix} \tag{14}$$

5. Aşama: Karar Alternatiflerinin Sınır Yaklaşım Alanı Matrisine Uzaklıkları

Karar alternatiflerinin sınır yaklaşım alanı matrisi (Q matrisi), ağırlıklı matris değerlerinden, sınır yaklaşım alanı matris değerlerinin farkıyla hesaplanır. Buna istinaden bu durum eşitlik 15'de gösterilmiştir:

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

A_i karar alternatifini belirtmek üzere, $A_i \in \{G\ VG^{+}VG^{-}\}$ koşulunda üst sınır yaklaşım alanı en iyi alternatif olan A^{+}'yı, alt sınır yaklaşım alanı ise en kötü alternatif olan A^{-}'yi bünyesinde barındırmaktadır. Buna göre eşitlik 16'dan faydalanılarak A_i alternatifi için ait olduğu alan tespit edilir.

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

A_i karar alternatifinin mevcut karar alternatifler arasında en iyi alternatif olması, bu alternatifin birçok kritere göre üst yaklaşım alanında yer almasına bağlı olmaktadır. Dolayısıyla $q_{ij} > 0$ olması karar alternatifin en iyi olmaya, $q_{ij} < 0$ olması durumunda ise karar alternatifinin en kötü alternatif olmaya sevk etmektedir.

6. Aşama: Karar Alternatiflerinin Performanslarının Belirlenmesi

Her bir karar alternatifi için sınır yaklaşım oranlarına olan uzaklıkların toplamları ölçülür. Ölçülen değerler büyükten küçüğe doğru sıralanır.

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

3. BULGULAR

Elde edilen karar matrisi, karar matrisinin normalizasyon ve bileşenlerin entropi değerleri ile bileşenlerin farklılaşma dereceleri ve önemlilik dereceleri Tablo 7'de gösterilmiştir.

Tablo 7. ENTROPİ Yöntemiyle Tespit Edilen Değerler

Karar Matrisi						
Ülkeler	**GSCI**	**CSI1**	**CSI2**	**CSI3**	**CSI4**	**CSI5**
Almanya	97,41	20	19,54	18,98	19,48	19,41
ABD	100	20	20	20	20	20
Fransa	97,60	20	19,21	18,98	20	19,41
İngiltere	99,54	20	19,54	20	20	20
İtalya	96,13	19,68	17,56	20	19,48	19,41
Japonya	97,82	20	19,08	18,74	20	20
Kanada	97,68	20	18,27	20	20	19,41
Normalize Değerler						
Ülkeler		**CSI1**	**CSI2**	**CSI3**	**CSI4**	**CSI5**
Almanya		0,143	0,147	0,139	0,140	0,141
ABD		0,143	0,150	0,146	0,144	0,145
Fransa		0,143	0,144	0,139	0,144	0,141
İngiltere		0,143	0,147	0,146	0,144	0,145
İtalya		0,140	0,132	0,146	0,140	0,141
Japonya		0,143	0,143	0,137	0,144	0,145
Kanada		0,143	0,137	0,146	0,144	0,141
Entropi Değerleri						
Ülkeler		**CSI1**	**CSI2**	**CSI3**	**CSI4**	**CSI5**
Almanya		-0,278	-0,282	-0,274	-0,275	-0,276
ABD		-0,278	-0,285	-0,281	-0,279	-0,28
Fransa		-0,278	-0,279	-0,274	-0,279	-0,276
İngiltere		-0,278	-0,282	-0,281	-0,279	-0,28
İtalya		-0,276	-0,267	-0,281	-0,275	-0,276
Japonya		-0,278	-0,278	-0,272	-0,279	-0,28
Kanada		-0,278	-0,272	-0,281	-0,279	-0,276
In(m)		**0,513898342**				
e_j		**1**	**0,9996**	**0,9998**	**1**	**1**
Farklılaşma Dereceleri						
d_j		**8E-06**	**0,0004**	**0,0002**	**4E-05**	**6E-05**
Bileşenlerin Önemlilik Dereceleri						
w_j		**0,011**	**0,587**	**0,276**	**0,049**	**0,077**
Sıralama		**5**	**1**	**2**	**4**	**3**

Tablo 7 incelendiğinde bileşenlerin önemlilik dereceleri CSI2 (w_{CSI2}=0,587), CSI3 (w_{CSI3}=0,276), CSI5 (w_{CSI5}=0,077), CSI4 (w_{CSI4}=0,049) ve CSI1 (w_{CSI2}=0,011) olarak sıralanmıştır. Tablo 7'ye göre, CSI2 bileşenin önemlilik derecesi ile diğer bileşenlerin önemlilik derecesi arasında belirgin farklılıklar tespit edilmiştir. Buna karşın, bileşenlerin önemlilik derecelerinin az olması açısından CSI1, CSI4 ve CSI5 bileşenlerinin diğer bileşenleri arasındaki farkın fazla olduğu gözlenmiştir.

MABAC yönteminin birinci aşamasında eşitlik (7) ile karar matrisi oluşturulur. Söz konusu karar matrisi ENTROPİ yöntemi kapsamında daha önceden Tablo 7'de sağlanmıştır. Yöntemin ikinci aşamasında karar matrisi eşitlik (8) ve eşitlik (10) ile standartlaştırılmıştır. Standartlaştırılmış karar matrisi Tablo 8'de açıklanmıştır.

Tablo 8. Standartlaştırılmış Karar Matrisi

Ülkeler	CSI1	CSI2	CSI3	CSI4	CSI5
Almanya	1	0,811	0,190	0	0
ABD	1	1	1	1	1
Fransa	1	0,676	0,190	1	0
İngiltere	1	0,811	1	1	1
İtalya	0	0	1	0	0
Japonya	1	0,623	0	1	1
Kanada	1	0,291	1	1	0

Üçüncü aşamada, standartlaştırılan karar matrisi eşitlik (11) ve eşitlik (12) ile ağırlıklandırılmıştır. Buna ilişkin olarak standartlaştırılmış karar matrisinin ağırlık değerleri Tablo 9'dadır.

Tablo 9. Standartlaştırılmış Karar Matrisinin Ağırlıklandırılması

Ülkeler	CSI1	CSI2	CSI3	CSI4	CSI5
	w_{CSI1}=0,011	**w_{CSI2}=0,587**	**w_{CSI3}=0,276**	**w_{CSI4}=0,049**	**w_{CSI5}=0,077**
Almanya	0,02199	1,0639	0,32882	0,0489	0,07659
ABD	0,02199	1,17462	0,55243	0,0978	0,15318
Fransa	0,02199	0,98447	0,32882	0,0978	0,07659
İngiltere	0,02199	1,0639	0,55243	0,0978	0,15318
İtalya	0,011	0,58731	0,55243	0,0489	0,07659
Japonya	0,02199	0,95318	0,27621	0,0978	0,15318
Kanada	0,02199	0,75821	0,55243	0,0978	0,07659

Yöntemin dördüncü aşamasında eşitlik (13) ve eşitlik (14) ile sınır yaklaşım alan matrisi sağlanmıştır. Buna göre sınır yaklaşım alan matris değerleri Tablo 10'dadır.

Tablo 10. Sınır Yaklaşım Alan Matrisi (G Matrisi)

Bileşenler	CSI1	CSI2	CSI3	CSI4	CSI5
g_i	0,020	0,919	0,431	0,080	0,103

5'inci aşamada, eşitlik (15) ve eşitlik (16) ile karar alternatiflerinin (ülkelerin) sınır yaklaşım alanı matrisine olan uzaklıkları (Q Matrisi) hesaplanmıştır. Yöntemin son aşamasında ise eşitlik (17) ile ülkelerin siber güvenlik performansları (S_i) ölçülmüştür. Bu kapsamda ülkelerin sınır yaklaşım alanı matrisine olan uzaklık ile siber güvenlik performans değerleri Tablo 11'de gösterilmiştir.

Tablo 11. Q Matrisi ve S_i Değerleri

Q Matrisi						S_i	Sıralama
Ülkeler	**CSI1**	**CSI2**	**CSI3**	**CSI4**	**CSI5**		
Almanya	0,002	0,144	-0,103	-0,031	-0,026	-0,014	3
ABD	0,002	0,255	0,121	0,018	0,05	0,446	1
Fransa	0,002	0,065	-0,103	0,018	-0,026	-0,044	4
İngiltere	0,002	0,144	0,121	0,018	0,05	0,335	2
İtalya	-0,009	-0,33	0,121	-0,031	-0,026	-0,278	7
Japonya	0,002	0,034	-0,155	0,018	0,05	-0,052	6
Kanada	0,002	-0,16	0,121	0,018	-0,026	-0,047	5
					Ortalama	0,049	------

Tablo 11 değerlendirildiğinde, ülkelerin siber güvenlik performansları ABD (0,446), İngiltere (0,335), Almanya (-0,014), Fransa (-0,044), Kanada (-0,047), Japonya (-0,052) ve İtalya (-0,278) olarak sıralanmıştır. Tablo 11'e göre, özellikle ABD ve İngiltere'nin siber güvenlik performans değerleri ile diğer ülkelerin performans değerleri arasında farklılıkların fazla olduğu tespit edilmiştir. Bu durum, ülkelerin ortalama siber güvenlik performans değerinin yükselmesine neden olmuştur. Ayrıca Tablo 11'e göre, sadece ABD ve İngiltere'nin siber güvenlik performans değerlerinin ortalama değerden fazla olduğu tespit edilmiştir. Dolayısıyla bu sonuç, ABD ve İngiltere'nin siber güvenlik kapsamında özellikle önemlilik dereceleri yüksek olan CSI2 ve CSI3 bileşenleri açısından diğer ülkelere kıyasla daha verimli faaliyet yürüttüğünü göstermektedir.

Araştırmada MABAC yönteminin duyarlılık seviyesi ölçülmüştür. ÇKKV literatüründe duyarlılık analizi, bileşen ağırlıklarının veya önemlilik derecelerinin farklı değerler ile senaryolar oluşturulması ve oluşan sıralamalar arasındaki

farklılıklara göre sağlanabilmektedir (Gigovic, 2016: 24). Oluşturulan senaryolara göre bileşenlerin ağırlıkları Tablo 12'de belirtilmiştir.

Tablo 12. Kriter Ağırlıkları Değiştirilerek Oluşturulan Senaryolar

Senaryolar	CSI1	CSI2	CSI3	CSI4	CSI5
Senaryo 1	0,276	0,011	0,587	0,077	0,049
Senaryo 2	0,077	0,587	0,049	0,276	0,011
Senaryo 3	0,049	0,276	0,077	0,011	0,587
Senaryo 4	0,077	0,587	0,011	0,049	0,276
Senaryo 5	0,049	0,011	0,276	0,587	0,077
Senaryo 6	0,011	0,276	0,587	0,049	0,077
Senaryo 7	0,077	0,049	0,276	0,587	0,011

Tablo 12'de belirtilen senaryolara istinaden bileşenlerin farklı bileşen ağırlığa sahip olması çerçevesinde oluşan ülkelerin siber güvenlik performans değerleri ve performans değerlerinin sıralamaları Tablo 13'te açıklanmıştır.

Tablo 13. ENTROPİ Tabanlı MABAC Yönteminin Duyarlılık Analizi

ENTROPİ		Birinci Senaryo		İkinci Senaryo		Üçüncü Senaryo	
Değer	**Sıralama**	**Değer**	**Sıralama**	**Değer**	**Sıralama**	**Değer**	**Sıralama**
-0,014	3	-0,229	7	-0,04	6	-0,161	4
0,4459	1	0,3737	1	0,397	1	0,551	1
-0,044	4	-0,154	5	0,157	3	-0,188	5
0,3352	2	0,3716	2	0,287	2	0,499	2
-0,278	7	-0,039	4	-0,55	7	-0,373	7
-0,052	6	-0,218	6	0,127	4	0,37	3
-0,047	5	0,317	3	-0,03	5	-0,232	6
Dördüncü Senaryo		**Beşinci Senaryo**		**Altıncı Senaryo**		**Yedinci Senaryo**	
Değer	**Sıralama**	**Değer**	**Sıralama**	**Değer**	**Sıralama**	**Değer**	**Sıralama**
0,0279	4	-0,493	7	-0,21	6	-0,456	7
0,4727	1	0,3961	1	0,447	1	0,375	1
-0,003	5	0,0924	5	-0,19	5	0,124	4
0,3619	2	0,3941	2	0,395	2	0,366	2
-0,516	7	-0,328	6	0,034	4	-0,349	6
0,2402	3	0,1158	4	-0,24	7	0,08	5
-0,22	6	0,3118	3	0,175	3	0,329	3

Tablo 13 değerlendirildiğinde, duyarlılık analizine göre ülkelerin siber güvenlik performans değerlerinin sırasında önemli değişiklikler olduğu gözlenmiştir. Dolayısıyla bu durum, ENTROPİ tabanlı MABAC yönteminin ülkelerin siber güvenlik performanslarının ölçülmesinde kullanılabilir olduğunu göstermektedir.

Ülkelerin siber güvenlik performansları ayrıca ENTROPİ tabanlı ARAS, BTA, COPRAS, EDAS, ROV, WASPAS, TOPSIS ve Gri İlişkisel Analiz (GİA) yöntemleriyle de ölçülmüştür. Yöntemlere göre ölçüm değerleri arasındaki korelasyon Tablo 14'tedir.

Tablo 14. Yöntemlere Göre Ülkelerin Siber Güvenlik Performans Değerleri Arasındaki Korelasyon

Yöntemler	1	2	3	4	5	6	7	8	9	10
(1) GCSI	1									
(2) MABAC	,988**	1								
(3) ARAS	,935**	,957**	1							
(4) BTA	,937**	,959**	,999**	1						
(5) COPRAS	,935**	,957**	,999**	,999**	1					
(6) EDAS	,937**	,964**	,999**	,999**	,999**	1				
(7) ROV	,986**	,999**	,957**	,959**	,957**	,964**	1			
(8) WASPAS	,936**	,958**	,999**	,999**	,999**	,998**	,958**	1		
(9) TOPSIS	,854*	,882**	,978**	,976**	,978**	,972**	,882**	,977**	1	
(10) GİA	,932**	,960**	0,865*	,869*	,865*	,886**	,960**	,866*	,771*	1

****p<.01, *p<.05**

Tablo 14'e göre GCSI değerleri, TOPSIS yöntemi haricinde diğer ÇKKV yöntemleri ülkelerin siber güvenlik performans değerleri arasında pozitif yönlü, anlamlı ve çok yüksek, TOPSIS yöntemi ile ülkelerin siber güvenlik performans değerleri ile pozitif yönlü, anlamlı ve yüksek değerde ilişki olduğu tespit edilmiştir. Tablo 14 incelendiğinde, GCSI'nın tüm ÇKKV yöntemleri içinde en fazla MABAC yöntemi ile ilişki içinde olduğu belirlenmiştir. Bu durum, GCSI'nın en iyi MABAC yöntemi ile açıklanabileceğini göstermektedir. Ayrıca araştırmanın yöntemini konu alan MABAC tekniği ile ölçülen ülkelerin siber güvenlik performans değerleri ile ROV yöntemi ile ölçülen değerler arasındaki ilişkinin 0,999 olması, MABAC yönteminin ROV yöntemiyle benzer nitelikte ÇKKV teknikleri olduğunu göstermektedir.

SONUÇ VE TARTIŞMA

Ülkelerin siber güvenlik performansları konusunda farkındalık kazanmasıyla siber güvenlik performanslarının artırımına yönelik uygun stratejiler ve politikalar geliştirebilecektir. Dolayısıyla ülkelerin siber güvenlik performanslarının ölçümü büyük önem arz etmektedir. Bu kapsamda araştırmada dünyanın en gelişmiş ekonomilerine sahip G7 grubu ülkelerinin siber güvenlik performansları ENTROPİ tabanlı MABAC yöntemi ile ölçülmüştür.

Bulgulara göre, ENTROPİ yöntemi ile ülkelere göre siber güvenlik performansını belirleyen bileşenlerin önemlilik dereceleri tespit edilmiştir. Buna göre bileşenlerin önemlilik dereceleri teknik ölçümler (GCSI2), organizasyonel ölçümler (GCSI3), iş birliği ölçümleri (GCSI5), kapasite ölçümleri (GCSI4) ve yasal ölçümler (GCSI1) olarak belirlenmiştir. GCSI bileşenlerinin önemlilik dereceleri değerlendirildiğinde, özellikle teknik ölçümler ve organizasyonel ölçümler bileşenlerinin önemlilik derecelerinin fazla olduğu ortaya konulmuştur. Bu durum, teknik ölçümler (GCSI12) ve organizasyonel ölçümler (GCSI23) bileşenlerinin (ülkeler arasındaki) performans farklılıklarının diğer bileşenlerin (ülkeler arasındaki) performans farklılıklarından fazla olduğunu göstermektedir.

Başka bir bulguya göre, ENTROPİ tabanlı MABAC yöntemine göre ülkelerin siber güvenlik performanslarının sıralamaları ABD, İngiltere, Almanya, Fransa, Kanada, Japonya ve İtalya olarak tespit edilmiştir. Özellikle ABD ve İngiltere'nin siber güvenlik performans değerlerinin fazla olması bakımından diğer ülkelerin siber güvenlik performans değerleri arasında farklılıkların fazla olduğu belirlenmiştir. Ayrıca ülkelerin siber güvenlik performans değerleri ortalamasının üstünde olan ülkelerin sadece ABD ve İngiltere olduğu gözlenmiştir. Dolayısıyla bu durum, ABD ve İngiltere'nin siber güvenlik konusunu diğer G7 ülkelerine kıyasla daha fazla önemsediğini göstermektedir.

Araştırmada ayrıca ENTROPİ tabanlı MABAC yönteminin kullanılabilirliğini göstermek amacıyla duyarlılık analizi yapılmıştır. Duyarlılık analizine göre ülkelerin siber güvenlik performans değerlerinin sırasında önemli değişiklikler olduğu ve buna göre ENTROPİ tabanlı MABAC yönteminin ülkelerin siber güvenlik performanslarının ölçümünde kullanılabilir olduğu sonucuna ulaşılmıştır.

ENTROPİ tabanlı bazı ÇKKV yöntemleriyle ülkelerin siber güvenlik performans değerleri ölçülmüş ve söz konusu ülkelerin siber güvenlik performans değerleri arasındaki korelasyon hesaplanmıştır. Tüm yöntemlere göre performans değerleri arasında anlamlı, pozitif yönlü, yüksek ve çok yüksek korelasyonlar

olduğu sonucuna ulaşılmış, MABAC yöntemi ile belirlenen ülkelerin siber güvenlik performans değerleri en fazla ENTROPİ tabanlı ROV yöntemi ile ölçülen değerler arasında ilişki içinde olduğu gözlenmiştir. Bu sonuca göre, ENTROPİ tabanlı MABAC ve ENTROPİ tabanlı ROV yöntemlerinin benzer oldukları değerlendirilmiştir.

Literatür değerlendirildiğinde, ülkelerin GCSI veya herhangi bir ölçekle siber güvenlik performanslarını herhangi bir ÇKKV yöntemi ile ölçen bir araştırmaya rastlanmamıştır. Bu açıdan bu çalışmanın literatüre katkı sağladığı düşünülmüştür. Literatürde Bruggemann vd. (2021)'nin araştırmasında Hasse diyagramı ile ülkeler 2019 yılı için GCSI bileşen değerleri üzerinden siber güvenlik performanslarına göre tasniflenmiş, ABD ve İngiltere'nin en fazla siber güvenlik performansı gösteren ülkeler olduğu gözlenmiştir. Bu araştırmada 2020 GCSI bileşen değerleri üzerinden ABD ve İngiltere'nin siber güvenlik performanslarının diğer ülkelerden belirgin farklılıkların olması açısından Bruggemann vd. (2021) araştırmasıyla tutarlılık göstermiştir. Bu durumda, ABD ve İngiltere'nin siber güvenlik performanslarının belirtilen yıllara göre istikrarlı olduğu düşünülmüştür.

Ortalama siber güvenlik performans değerinin altında olan Almanya, Fransa, Kanada, Japonya ve İtalya özellikle teknik ve organizasyonel ölçüm bileşenlerine önem vererek kendi siber güvenlik performanslarını artırabilirler. Ülkeler özellikle teknik ve organizasyonel ölçümler bileşenlerinin birbirlerini ve diğer bileşenleri sağlayacak faaliyetler gerçekleştirecek stratejiler ve politikalar üreterek kendi siber güvenlik performanslarını iyileştirebilir. Böylelikle Almanya, Fransa, Kanada, Japonya ve İtalya G7 grubu ülkelerin siber güvenlik konusunda ABD ve İngiltere ile uyum içinde olup siber güvenliğinin küresel anlamda sağlanmasına katkılarını artırabilir. Gelecek çalışmalar için söz konusu ülkelerin siber güvenlik performansları farklı ÇKKV ve yöntemleri ile ölçülerek sonuçlar arasında karşılaştırma yapılıp tartışılabilir. Bunun yanında, ülkelerin siber güvenlik performanslarının daha ayrıntılı olarak analizinin sağlanması için GSCI bileşen sayısı artırılabilir ya da her ülkeye özgü bileşenler oluşturulabilir.

KAYNAKÇA

Ada, M., ve Çakır, H. (2017). Kuzey atlantik antlaşma örgütü'nün (NATO) Siber güvenlik stratejisinin incelenmesi. *Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 5*, 632-656.

Aslay, F. (2017). Siber saldırı yöntemleri ve Türkiye'nin siber güvenlik mevcut durum analizi. *International Journal of Multidisciplinary Studies and Innovative Technologies, 1*(1), 24–28.

Ayçin, E. (2019). *Çok kriterli karar verme* . Ankara: Nobel Yayın.

Biswas, T. K. (2018). Selection of hybrid vehicle for green environment using multi-attributive border approximation area comparison method. *Management Science Letters, 8*, 121–130.

Bruggemann, R., Koppatz, P., Scholl, M., ve Schuktomow, R. (2021). Global cybersecurity index (GCI) and the role of its 5 pillars. *Social Indicators Research*, 1-19.

Chakraborty, S., Ghosh, S., Agarwal, S., ve Chakraborty, S. (2021). An integrated performance evaluation approach for the indian smart cities. *Operational Research Society of India* , 1-36.

Cyber security. (2021). Erişim Tarihi: 09.07.2021, http://www.g7.utoronto.ca/evaluations/muharına-cybersecurity-2021.html.

Çalık, A. (2021). Grup karar verme yöntemlerini kullanarak yeşil tedarikçi seçimi: gıda endüstrisinden bir örnek olay çalışması. *Ekonomik ve Sosyal Araştırmalar Dergisi, 17*(1), 1-16.

Çınaroğlu, E. (2020). Yenilikçi girişimlere ait faaliyetlerin entropi destekli mabac yöntemi ile değerlendirilmesi. *Girişimcilik ve İnovasyon Yönetimi Dergisi, 9*(1), 111-135.

Dinçer, S. E. (2019). *Çok kriterli karar alma.* Ankara: Gece Akademi.

Ecer, F. (2020). *Çok kriterli karar verme.* Ankara: Seçkin Yayıncılık.

Ercan, M. (2015). *Kritik alyapıların korunmasına ilişkin belirlenen siber güvenlik stratejileri.* Gebze Teknik Üniversitesi Sosyal Bilimler Enstitüsü, Yayımlanmamış Yüksek Lisans Tezi, Bursa.

Fan, J., Guan, R., ve Wu, M. (2020). Z-MABAC method for the selection of third-party logistics suppliers in fuzzy environment. *IEEEAccess, 8*, 199111-199119.

Gigovic, L., Pamucar, D., Bajic, Z., ve Milicevic, M. (2016). The combination of expert judgment and GIS-MAIRCA analysis for the selection of sites for ammunition depots. *Sustainability, 8*, 1-30.

Goutam, R. K. (2015). Importance of cyber security. *International Journal of Computer Applications, 111*(7), 14-17.

Göçoğlu, V., ve Aydın, M. D. (2019). Siber güvenlik politikası: ABD, Rusya ve Çin üzerine karşılaştırmalı bir analiz. *Güvenlik Bilimleri Dergisi,, 8*(2), 229-252.

Güleç, Ö., ve Kişman, Z. A. (2021). Akademik Açı. *1*(1), 127-154.

Güntay, C. (2016). Cyberpolitik Journal. *1*(1), 95-113.

G7 ülkeleri (2021), Erişim Tarihi: 10.07.2021, http://www.aa.com.tr/2270274.

Hekim, H., ve Başıbüyük, O. (2013). Siber suçlar ve Türkiye'nin siber güvenlik politikaları. *Uluslararası Güvenlik ve Terörizm Dergisi, 4*(2), 135-158.

ITU. (2015). *Global cyber security index.* Geneva: ITU Publication.

ITU. (2017). *Global cyber security index.* Geneva: ITU Publication.

ITU. (2018). *Global cyber security index.* Geneva: ITU Publication.

ITU. (2020). *Global cyber security index.* Geneva: ITU Publication.

Karacı, A., Akyüz, H. İ., ve Bilgici, G. (2017). Üniversite öğrencilerinin siber güvenlik davranışlarının incelenmesi. *Kastamonu Eğitim Dergisi, 25*(6), 2079-2094.

Kharlamov, A. (2021)). Using human values-based approach to understand cross-cultural commitment toward regulation and governance of cybersecurity. *Regulation ve Governance, 15*, 709–724.

Kravets, V. M. (2019). Comparative analysis of the cybersecurity ındices and their applications. *Igor Sikorsky Kyiv Polytechnic Institute, 1*(1), 97-102.

Kumar, V., Srivastava, J., ve Lazaravic, A. (2006). *Maneging cyber thereats ıssues, aprroaches, and challanges.* heilderberg: springer science ve business media.

Luiijf, E., Besseling, K., ve de Graaf, P. (2013). Nineteen national cyber security strategies. *Int. J. Critical Infrastructures, 9*(1/2), 3-31.

Onumo, A., Cullen, A., ve Ullah-Awan, I. (2017). An empirical study of cultural dimensions and cybersecurity development. *2017 IEEE 5th International*

Conference on Future Internet of Things and Cloud, Prague, 70-76, doi: 10.1109/FiCloud.2017.45,

Öğün, M. N., ve Kaya, A. (2013). Siber güvenliğin milli güvenlik açısından önemi ve alınabilecek tedbirler. *Güvenlik Stratejileri, 9*(18), 145-181.

Öztürk, S. (2018). Siber saldırılar, siber güvenlik denetimleri ve bütüncül bir denetim modeli önerisi. *Muhasebe ve Vergi Uygulamaları Dergisi*(Special Issue of the 10th Year), 208-232.

Pamucar, D., ve Cirovic, G. (2015). The selection of transport and handling resources in logistics centers using multi-attributive border approximation area comparison. *Expert Systems with Applications, 42*, 3016–3028.

Ruhl, C., Hollis, D., Hoffman, W., ve Maurer, T. (2020). *cyberspace and geopolitics: assessing global cybersecurity norm pro cesses at a crossroads.* washington: carnegie endowment for ınternational peace.

Ruiz, N., Shukla, P., ve Kazemian, H. (2020). Cyber security index for undergraduate computer science courses in the UK. *Taylor ve Francis in Journal of Applied Security Research, doi: 10.1080/19361610.2020.1798173*, 1-7.

Ruvin, O., Isaieva, N., Sukhomlyn, L., Kalachenkova, K., ve Bilianska, N. (2020). Cybersecurity as an element of financial security. *Journal of Security and Sustainability Issues, 10*(1), 175-188.

Topcu, N. (2020). Bir siber güç olarak Çin'in siber güvenlik stratejileri. *Cyberpolitik Journal, 5*(10), 219-239.

Tvaronavičienė, M., Plėta, T., Casa, S. D., ve Latvys, J. (2020). Cyber security management of critical energy ınfrastructure in national cybersecurity strategies: cases OF USA, UK, France, Estonia and Lithuania. *Insights into Regional Development, 2*(4), 802-813.

Ulutaş, A. (2019). Entropi ve MABAC yöntemleri ile personel seçimi. *OPUS Uluslararası Toplum Araştırmaları Dergisi, 13*(19), 1552-1573.

von Solms, R., ve van Niekerk, J. (2013). From information security to cyber security. *Computer ve Security, 38*, 97-102.

Yerina, A. M., Honchar, I. A., ve Zaiets, S. V. (2021). statistical ındicators of cybersecurity development in the context of digital transformation of economy and society. *Sci. innov., 17*(3), 3-13.