Yönetim Bilimleri Dergisi/Journal of Administrative Sciences
Cilt/Volume: 23, Sayı/No: 56, ss./pp.: 993-1012
DOI: https://doi.org/10.35408/comuybd.1584175

-ARAŞTIRMA MAKALESİ-

TÜRKİYE'NİN YAPAY ZEKA TABANLI SİBER GÜVENLİK STRATEJİSİ: ULUSAL GÜVENLİĞİ GÜÇLENDİRMEK VE KÜRESEL SİBER YÖNETİŞİME YÖN VERMEK

Aylin Ece ÇİÇEK[1]

Öz

Bu çalışma, Türkiye'nin siber güvenlik yaklaşımını yapay zekâ (YZ) stratejileri üzerinden, ulusal güvenlik ve uluslararası iş birliği bağlamında analiz etmektedir. 20.Yüzyılın sonunda, Türkiye de dahil olmak üzere, siber güvenlik suçları dünyada bireyleri ilgilendiren suçlar olarak kabul görmüştür. Siber saldırıların ulusal güvenliği ilgilendiren ve hızla artan tehditleri sonucunda siber suçlar, ulusal güvenliğe karşı suçlar olarak sınıflandırılmış ve bu tehditleri önleyebilecek mekanizmalar kurulması amaçlanmıştır. Benzer dönemlerde dijital dönüşüm, çeşitli kritik sektörleri yeniden şekillendirirken, siber güvenlikte YZ'nin rolü de vazgeçilmez hale gelmiştir. Büyük miktarda veri işleyebilme, örüntü tanıma, bağımsız karar verme ve yanıtları otomatikleştirme yeteneğiyle YZ, savunma mekanizmalarının etkinliğini artırarak siber tehditlerle mücadelede güçlü bir araç haline gelmiştir. Avrupa ile Orta Doğu arasındaki stratejik konumunun getirdiği artan dijital risklerle karşı karşıya kalan Türkiye, öncelikle enerji, sağlık, finans ve iletişim gibi kritik alanlardaki altyapısını korumak ve dışa bağımlılığı azaltmak amacıyla ulusal siber güvenlik stratejilerine YZ'yi entegre etmiştir. Türkiye'nin siber güvenlik hedefleri yalnızca ulusal güvenliği sağlamakla sınırlı kalmayıp çeşitli tatbikatlar ve platformlara katılım yoluyla NATO ve AB gibi bölgesel ve küresel güvenlik yapılarıyla iş birliğine de katkıda bulunmayı amaçlamaktadır. Bu makale, Türkiye'nin YZ tabanlı siber güvenlik çabalarıyla bölgesel istikrar sağlayıcı bir güç olarak nasıl konumlandığını incelerken, bu teknolojilerin getirdiği mahremiyet, gözetim ve insan denetimi gibi etik soruları da ele almaktadır. Realizm ve orta büyüklükte güç yaklaşımını uygulayarak, Türkiye'nin YZ destekli siber güvenlik stratejilerinin sadece ulusal altyapıyı korumakla kalmayıp, aynı zamanda uluslararası siber güvenlik normlarına katkı sağladığını ortaya koymaktadır. Türkiye'nin YZ tabanlı siber güvenlik stratejisinin sürdürülebilir başarısının, etik standartlar, şeffaflık ve insan haklarına bağlılıkla mümkün olacağı vurgulanmaktadır.

Anahtar Kelimeler: *Yapay Zeka, Siber Güvenlik, Ulusal Güvenlik, Türkiye, Güvenlik stratejisi*
JEL Kodları: *F52, F53, O33.*

Başvuru: *13.11.2024* **Kabul:** *05.03.2025*

[1] Dr. Öğr. Üyesi, İstanbul Üniversitesi, Siyasal Bilgiler Fakültesi, Siyaset Bilimi ve Uluslararası İlişkiler Bölümü, email: aylin.cicek@istanbul.edu.tr, ORCID: 0000-0002-9606-509X

TURKİYE'S AI-DRIVEN CYBERSECURITY STRATEGY: ENHANCING NATIONAL SECURITY AND SHAPING GLOBAL CYBER GOVERNANCE

Abstract

This study analyzes Türkiye's approach to cybersecurity through artificial intelligence (AI) strategies within the context of national security and international collaboration. By the late 20th century, including in Türkiye, cybercrimes were considered as individual offenses. However, with growing cyber-attack threats to national security, they were reclassified as national security crimes, prompting efforts to develop preventive mechanisms. As digital transformation reshapes various critical sectors, AI's role in enhancing cybersecurity has become indispensable in the same periods. With the ability to process vast data, recognize patterns, make autonomous decisions, and automate responses, AI enhances the efficiency and responsiveness of defense mechanisms, making it a powerful tool in combating cyber threats. Facing increasing digital risks due to its strategic location between Europe and the Middle East, Türkiye has integrated AI into its national cybersecurity strategies to safeguard critical infrastructure in energy, health, finance, and communication and reduce reliance on external digital defenses. Türkiye's cybersecurity objectives extend beyond domestic security, aiming to contribute to regional and global security frameworks, particularly within NATO and the EU through various exercises and platforms. This paper examines how Türkiye positions itself as a regional stabilizer through its AI-based cybersecurity efforts and investigates the ethical considerations raised by these technologies, such as privacy, surveillance, and human oversight. By applying realist and middle power theories, the study explores how Türkiye's AI-driven cybersecurity strategies not only protect national infrastructure but also elevate its role in international cybersecurity norms and collaborations. This balanced approach, while addressing national security needs, also positions Türkiye as an influential actor in global cybersecurity frameworks. The study concludes by assessing the implications of AI integration on Türkiye's long-term cybersecurity effectiveness, suggesting that sustainable success will depend on maintaining ethical standards, transparency, and adherence to human rights.

Keywords: *Artificial Intelligence, Cybersecurity, National Security, Middle-Power Theory, Realism.*

JEL Codes: *F52, F53, O33.*

"Bu çalışma Araştırma ve Yayın Etiğine uygun olarak hazırlanmıştır."

1. GİRİŞ

Dijitalleşmenin iletişimden sağlığa, sanayiden eğitime birçok kritik alanı dönüştürmesi, siber güvenliği ulusal güvenliğin vazgeçilmez bir parçası haline getirmiştir. Yapay zekânın büyük miktarda veriyi işleme, örüntü tanıma, karar alma ve eylemleri otomatikleştirme gibi yetenekleri, tehdit tespit süreçlerini hızlandırarak

savunma mekanizmalarını daha etkili hale getirmektedir. Bu önemli avantajlar, yapay zekâyı siber güvenlikte etkili bir araç konumuna taşımıştır (Rodriguez Vance, 2023: 77; UK Ministry of Defence, 2022: 9-11). Siber tehditlerin giderek sofistike ve yaygın hale gelmesiyle birlikte, devletlerin savunmalarını güçlendirmek ve kritik altyapılarını korumak amacıyla yapay zekâya yönelmesi daha anlamlı hale gelmektedir.

Türkiye'nin siber güvenlik çalışmaları, enerji şebekeleri, haberleşme sistemleri, ulaştırma altyapıları ve finansal sistemler gibi kritik altyapıları koruma ve siber alanda stratejik bağımlılığı azaltma hedefini taşımaktadır (T.C. Ulaştırma ve Altyapı Bakanlığı, 2024: 25). Avrupa ve Orta Doğu arasında stratejik bir konuma sahip olan Türkiye, jeopolitik önemi ve bölgesel bir güç olarak artan statüsü nedeniyle devlet destekli saldırılar ve organize siber suçlar gibi çeşitli tehditlere maruz kalmaktadır (Ongun, 2023). Bu tehditleri bertaraf etmek için Türkiye, yapay zekâ teknolojilerini ulusal siber güvenlik stratejisine proaktif olarak entegre etmiştir (T.C. Ulaştırma ve Altyapı Bakanlığı, 2024: 22).

Türkiye, siber güvenlik stratejileri ile sadece ulusal güvenliğini korumayı değil, bölgesel ve küresel güvenlik iş birliklerine katkıda bulunmayı da hedeflemektedir (T.C. Ulaştırma ve Altyapı Bakanlığı, 2024: 7; Halisdemir, 2021: 8). Bu iş birlikleri, Türkiye'nin uluslararası güvenlik çerçevesinde daha aktif bir aktör olarak konumlanmasına olanak tanırken (Akyeşilmen, 2022: 123), ülkenin geliştirdiği teknolojilerle uluslararası siber güvenlik çerçevelerine katkı sağlamasını da mümkün kılmaktadır (Eldem, 2019: 458). Aynı zamanda yapay zekâ teknolojileri, orta ölçekli bir güç olan Türkiye (Cooper ve Parlar Dal, 2016: 519; Müftüler ve Yüksel, 1997: 187) gibi ülkelere, NATO ve AB gibi uluslararası güvenlik çevrelerinde konumunu güçlendirme fırsatı sunmaktadır (Cristiano vd., 2023: 4; Kurç, 2023: 21-22; Sukumar, 2023: 109).

Çalışmada, Türkiye'nin yapay zekâ tabanlı siber güvenlik stratejisini küresel güvenlik ortamında nasıl konumlandırdığı incelenmekte. Siber tehditlerle mücadele, ulusal altyapıyı koruma ve uluslararası siber güvenlik süreçlerine katkı sağlama amacıyla yapay zekâyı nasıl kullandığını araştırılmaktadır. Temel araştırma sorusu: Türkiye, yapay zekâ tabanlı siber güvenlik stratejilerini, özellikle NATO ve AB gibi bölgesel ve küresel güvenlik yapılanmalarındaki rolünü güçlendirmek için nasıl kullanmaktadır?

Türkiye'nin ulusal siber güvenlik politikalarını ve yapay zekâ entegrasyonunu, uluslararası ilişkiler teorisi bağlamında, özellikle realizm ve orta güç teorisi perspektifinden analiz etmektedir. Mearshimer (2001:30-32), realizmin devlet davranışında güç ve güvenliği merkeze aldığını vurgularken, Müftüler ve Yüksel (1997) ile Holbraad (1984: 125) Türkiye gibi orta büyüklükte güçlerin NATO gibi güvenlik çerçevelerindeki rolüne değinmekte, Eldem (2019) ise diplomasinin önemine vurgu yaparak orta ölçekli güç teorisinin varsayımlarını desteklemektedir.

Bununla birlikte, yapay zekâ teknolojilerinin kullanımı bazı etik soruları da gündeme getirmektedir. Bireylerin mahremiyeti, devletin artan gözetimi, insan denetimi ve veri

güvenliği gibi konuların dikkatle ele alınması gerekmektedir. Taddeo ve diğerleri (2023), yapay zekâ tabanlı yönetişimin etik etkilerine dair içgörüler sunarak, bu zorlukların nasıl aşılabileceğini vurgular.

2. YÖNTEM

Çalışmada, Türkiye'nin yapay zekâ tabanlı siber güvenlik stratejisini analiz etmek amacıyla ikincil veri analizi yöntemi kullanılmıştır. Bu doğrultuda çevrimiçi veri tabanları ve kurum web sitelerinden erişilebilen akademik makaleler, kitaplar, resmi raporlar, strateji belgeleri, uluslararası kuruluşların raporları ve ilgili haberler incelenmiştir. Elde edilen veriler, realizm ve orta ölçekli güç teorisi çerçevelerine göre yorumlanmıştır.

2.1. Teorik Çerçeve

Türkiye'nin siber güvenlik yaklaşımı ve yapay zekâ kullanımı, realizm ve orta ölçekli güç teorisi çerçevesinde değerlendirilebilir. Bu teorik yaklaşımlar, devletlerin ulusal güvenlik politikalarını şekillendiren güç ve iş birliği dinamiklerini ele alarak, Türkiye'nin stratejik motivasyonlarını ve bölgesel ile uluslararası siber güvenlik normları üzerindeki etkisini anlamamıza olanak tanır.

Realizm teorisi, devletlerin güvenlik ve güç arayışını uluslararası ilişkilerde temel motivasyon olarak kabul eder. Güç, devletin kendi kendine yeterli bir biçimde, bağımsız olarak varlığını sürdürebilmesi için en temel motivasyondur. Türkiye'nin yapay zekâ tabanlı siber güvenlik stratejisi de realist bir perspektiften değerlendirildiğinde, ülkenin ulusal güvenliğini tehdit eden dijital saldırılara karşı güçlü bir savunma mekanizması oluşturma çabası olarak yorumlanabilir (Mearsheimer, 2001: 30-32). Siber saldırılara karşı güvenliği ön planda tutan bu yaklaşım, Türkiye'nin stratejik çıkarlarını korumak amacıyla yapay zekâ teknolojilerine yatırım yapmasının bir sonucudur. Ancak realizm, güç ve güvenliği öncelerken, modern siber güvenlik yönetiminde iş birliği ihtiyacını göz ardı edebilir. Bu nedenle, orta ölçekli güç teorisinden de faydalanılmaktadır.

Uluslararası ilişkilerde siber çatışma ve siber güvenlik çalışmalarının Arquilla ve Ronfeldt tarafından 1993 yılında yayınlanan çalışmalarında geliştirilen "siber savaş" ve "ağ savaşı" kavramlarıyla başladığı kabul edilir. Bu kavramlar hızla gelişmekte olan bilgi ve iletişim teknolojileri sebebiyle savaş gücünde geleneksel güçten çağdaş siber güce bir geçiş olacağını öngörmektedir (Craig & Valeriano, 2018). Belirtildiği üzere siber tehditler günümüzde en üst seviye ulusal güvenlik endişeleri arasında gelmekte ve hükümetlerin kritik altyapılara dair önlem almasını ve güçlü siber güvenlik ağları geliştirmesini zorunlu hale getirmektedir. 2016 yılında Amerika Birleşik Devletleri'nde gerçekleştirilen bir ankete göre vatandaşların %73'ü siber terörizmin kritik bir tehdit oluşturduğunu belirtmektedir (McCarthy, 2016)

Realist teori baskın bir otoritenin bulunmadığı uluslararası ortamda, devletler arasında güvensizliğin süregeldiği anarşik bir ortamın varlığını vurgular (Waltz, 1979). Siber savaşların gerçekleştiği "siber alan" dünyadaki bütün bilgisayar ağları ve bu ağların

her şeye bağlanıp kontrol ettiği alan olarak tanımlanır, bu alanı daha yaygın kullanımıyla internet olarak tanımlamak mümkündür. Neorealist teorisyenlerden James Adams, tanıma uygun olacak şekilde interneti anarşik bir sistem olarak tanımlar. Herhangi bir yönetimin veya polis kuvvetinin yokluğunda internet, yeni uluslararası savaş alanı haline gelmiştir. Böyle bir düzende her devlet tek başına ayakta kalmakta veya tam anlamıyla güvenebileceği ittifaklar geliştirmek durumundadır (Adams, 2001: 98; Petallides, 2012). Güncel teorik bulgulardan hareketle, klasik realizmin uluslararası düzeni tanımlarken kullandığı temel özelliklerden olan anarşi, aynı zamanda çağımızda siber savaşların gerçekleştiği internet ortamına da içkindir. Bu sebeple realizmin anarşi, güç ve güvenlik arayışı gibi varsayımları devletlerin siber güvenlik stratejilerini incelemekte etkin hale gelmektedir.

Orta ölçekli güç teorisi, Türkiye gibi orta büyüklükteki ülkelerin, büyük güçlerin baskın olduğu uluslararası sistemde diplomasi, çok taraflılık ve stratejik ittifaklardan yararlanarak iş birliği ve norm oluşturma yoluyla kendilerine stratejik bir alan açabileceğini savunur (Cooper vd., 1994: 17-25). Bu teori, Türkiye'nin NATO ve AB gibi uluslararası güvenlik yapılarıyla olan iş birliklerini anlamak açısından önem taşır. Orta bir güç olarak Türkiye, siber güvenlik alanında NATO'nun Siber Savunma Mükemmeliyet Merkezi (CCDCOE) gibi platformlara katılarak uluslararası güvenlik normlarına katkıda bulunmakta ve siber tehditlere karşı iş birliğini geliştirmektedir (Halisdemir, 2021: 2).

3. BULGULAR

Stratejik konumu ve giderek dijitalleşen altyapısı nedeniyle Türkiye, geniş kapsamlı siber tehditlerle karşı karşıya kalmaktadır. Devlet destekli aktörlerden organize suç örgütlerine kadar farklı kaynaklardan gelen bu tehditler, ülkenin kritik altyapısı için ciddi riskler oluşturmaktadır (Ongun, 2023). Türkiye, siber güvenlik stratejisinde yapay zekâya yer vererek dijital güvenliğini sağlama ve ulusal güvenlik kapasitesini artırma yolunda adımlar atmıştır. Yapay zekâ destekli bu strateji, yalnızca tehdit tespiti ve olay müdahalesinde değil, aynı zamanda uluslararası iş birliği yoluyla Türkiye'yi küresel güvenlik yapıları içinde etkili bir aktör olarak konumlandırma çabalarında da önemli bir rol oynamaktadır (T.C. Ulaştırma ve Altyapı Bakanlığı, 2024: 22-25).

3.1. Türkiye'de Siber Güvenliğin Gelişimi

Türkiye'nin siber güvenlik yolculuğu, 1991 yılında Türk Ceza Kanunu'na bilişim suçlarının eklenmesiyle başlamış ve siber saldırılar o dönemde, dünyanın geri kalanında olduğu gibi, ulusal güvenlik problemi yerine suç olarak değerlendirilmiştir (Karakehya, 2009: 190). Ancak, siber saldırıların yalnızca bireylere yönelik bir tehdit oluşturmadığının anlaşılmasıyla siber güvenlik, ulusal ve uluslararası güvenliğin bir parçası olarak ele alınmaya başlanmıştır (Akyeşilmen, 2022: 118). Avrupa, Asya ve Orta Doğu'nun kesişim noktasında bulunan Türkiye, devlet destekli saldırılar da dahil

olmak üzere çeşitli aktörlerden gelen tehditlere karşı sürekli tetikte kalmak zorundadır.

27 Ekim 2010 tarihli Milli Güvenlik Kurulu toplantısında, "siber tehdidin global ölçekte ulaştığı boyutlar ve ulusal güvenliğe etkileri" değerlendirilmiş ve siber güvenliğin ulusal güvenliğin ayrılmaz bir parçası olduğu vurgulanmıştır (Milli Güvenlik Kurulu, 2010). Türk Silahlı Kuvvetleri, siber alanı da bir operasyon sahası olarak kabul ederek bu alanda yapılanmaya başlamıştır. 2013 yılında kurulan Siber Savunma Komutanlığı ile Türkiye'nin siber savunma ve caydırıcılık kapasitesi artırılmıştır. Siber Savunma Komutanlığı, ulusal tatbikatların yanı sıra uluslararası siber savunma tatbikatlarına katılarak müttefik ülkelerle iş birliği yapmaktadır. Bu bağlamda, Türkiye'nin siber güvenliği ulusal güvenlikte merkezi bir unsur haline gelmiş ve savunma stratejilerinin öncelikli bir parçası olarak konumlandırılmıştır (Halisdemir, 2021: 16)

Dinamik tehdit ortamına uyum sağlamak amacıyla Türkiye, 2013 yılında ilk Ulusal Siber Güvenlik Stratejisi'ni (USGS) açıklamıştır. Bu strateji, enerji şebekeleri, finansal sistemler ve telekomünikasyon ağları gibi kritik altyapıların korunmasına öncelik tanımaktadır. Aynı yıl kurulan Ulusal Siber Olaylara Müdahale Merkezi (USOM) ve Siber Olaylara Müdahale Ekipleri (SOME) ile Türkiye, siber güvenlik alanında kurumsal bir yapı kazanmıştır. Bu ekipler, kritik sektörlerde faaliyet göstererek siber güvenlik çalışmalarını koordine etmekte ve Türkiye'nin siber savunma stratejisini güçlendirmektedir. Ayrıca kamu kurumları arasında sağlanan koordinasyon sayesinde Türkiye'nin siber güvenlik ekosisteminin dayanıklılığı artırılmıştır (Siber Güvenlik Kurulu, 2013; T.C. Ulaştırma ve Altyapı Bakanlığı, 2020; T.C. Ulaştırma ve Altyapı Bakanlığı, 2024).

Bu gelişmelerle paralel olarak, Türkiye veri sızıntıları konusunda ciddi siber güvenlik ihlalleriyle karşı karşıya kalmıştır. 2010 yılında bazı kamu görevlilerinin vatandaşlık verilerini sattığı iddiasıyla yapılan gözaltılar (Atilla, 2010) ve 2016'da 49 milyon vatandaşın bilgilerinin internete sızdırılması, devletin dijitalleşme süreçlerinde siber güvenlik önlemlerini artırmasını zorunlu hale getirmiştir. Ancak alınan tedbirlere rağmen, 2023 yılında vatandaşların aile bağları, adresleri ve telefon numaraları gibi hassas bilgilerine erişim sağlayan sorgu panellerinin internette yaygınlaşması, veri güvenliği konusundaki endişeleri artırmıştır. 2024 yılında ise 108 milyon kişiye ait verilerin sızdırıldığı iddiaları gündeme gelmiştir. Yetkililer bu iddiaları reddederken, pandemi döneminde sağlık sisteminden veri sızıntısı yaşandığını kabul etmişlerdir (BBC News Türkçe, 2024). Bu olaylar, Türkiye'nin dijitalleşme sürecinde siber güvenliğe yönelik daha kapsamlı ve etkili stratejiler geliştirmesi gerektiğini bir kez daha ortaya koymuştur.

İlk USGS yayınlandığından bu yana, siber tehditlerin hem sayısı artmış hem de daha sofistike hale gelmiştir. Örneğin, 2019 yılında Türkiye'de yaklaşık 136.000 siber saldırı gerçekleşmiştir (Halisdemir, 2021: 8). Ulaştırma ve Altyapı Bakanlığı'nın 2020 yılında verdiği bilgilere göre, son üç yılda toplam 325 bin siber saldırı engellenmiştir (DHA, 2020). Ayrıca Türkiye, enerji ve madencilik gibi kritik

sektörlerde denetleme ve veri toplama gibi önemli operasyonel işlevleri yürüten endüstriyel kontrol sistemlerine (ICS bilgisayarları) yönelik en fazla saldırının tespit edildiği bölgelerden biridir (Ongun, 2023). Bu tehdit seviyesindeki artış, Türkiye'nin siber güvenlik yaklaşımını giderek karmaşıklaşan siber tehditler ve dijital altyapının ulusal güvenlikte artan önemi doğrultusunda son on yılda önemli ölçüde evrim geçirmeye yönlendirmiştir. Siber güvenlik, fiziksel güvenlik kadar önemli hale gelmiş ve hem kamu hem de özel sektörü bu alanda yatırım yapmaya teşvik etmiştir.

Bu çerçevede, kamu, özel ve askeri alanlarda önemli savunma kuruluşları tarafından ciddi yatırımlar yapılmış, akademik alanda siber güvenlik enstitüleri kurulmuş ve nitelikli personel yetiştirmek üzere siber güvenlik bölümleri açılmıştır. Yerli imkânlarla yeni ürün ve teknolojiler geliştirilmiştir (Halisdemir, 2021: 8-9).

2024-2028 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı, önceki stratejilerin ve faaliyetlerin üzerine inşa edilmekle birlikte bazı önemli farklılıklar içermiştir. Yeni strateji, siber dayanıklılık, proaktif siber savunma ve caydırıcılık, insan odaklı siber güvenlik, teknolojinin güvenli kullanımı, yerli ve milli teknolojilerin geliştirilmesi ve uluslararası alanda Türkiye markasının güçlendirilmesi gibi altı ana stratejik amaca odaklanmıştır (T.C. Ulaştırma ve Altyapı Bakanlığı, 2024: 20).

2024-2028 stratejisi, insan odaklı yaklaşımı daha belirgin hale getirerek toplumsal düzeyde bir siber güvenlik kültürünün yerleşmesini ve yetkin bir siber güvenlik iş gücünün oluşturulmasını hedeflemektedir. Yeni strateji, Türkiye'nin küresel alanda güçlenmesi için siber diplomasi yoluyla uluslararası iş birliklerini genişletmeyi ve ülkenin siber güvenlik alanında lider konumda olmasını amaçlamaktadır. 2024 yılında yayımlanan strateji ayrıca yapay zekânın siber güvenlikteki rolüne daha fazla vurgu yaparak tehdit tespiti, önleme ve müdahale kapasitesini artırmak için yapay zekâya daha fazla dayanmaktadır. Bu güncellemeler, Türkiye'nin teknolojik gelişmelere uyumlu, esnek ve dayanıklı siber güvenlik önlemlerini güçlendirme kararlılığını yansıtmaktadır.

Bu çabaların bir sonucu olarak, Türkiye son dönemde siber güvenlik alanında en başarılı ülkeler arasında yer almaya başlamıştır. 2022-2023 Siber Savunma Endeksi'nde Türkiye 20 üzerinden 19 puan almıştır. Aynı endeksin üç farklı başlığında Türkiye'nin aldığı puanlar şu şekildedir: Kritik altyapılar, 18; Siber güvenlik kaynakları,17; Organizasyonel kapasite, 19 (Connor, 2023). Türkiye'yi politika oluşturma, siber suçla mücadele, iş birliği ve farkındalık yaratma konularında elde ettiği başarılarla, Uluslararası Telekomünikasyon Birliği (ITU) Siber Güvenlik Endeksi'nde rol model olarak gösterilen ülkeler arasında göstermiştir (Uluslararası Telekomünikasyon Birliği, 2024: 126).

Yukarıda belirtilen olumlu gelişmelere zıt olarak Türkiye'nin eksiklerini vurgulayan uluslararası değerlendirmeler de bulunmaktadır. Düzenli tehdit analizi yapılmaması, temel hizmetlerin korunmasına yönelik çalışmaların eksikliği ya da bu konularda kamuya yeterli bilgilendirme yapılmaması nedeniyle Türkiye, Ulusal Siber Güvenlik Endeksi'nde 55. sıraya gerilemiştir (E-Governance Academy, 2023).

3.2. Türkiye'nin Yapay Zekâ Destekli Siber Savunma Stratejisi

Türkiye'nin yapay zekâ destekli savunma stratejisi, teknolojik yenilikleri savunma kapasitesini artırmak amacıyla etkin bir şekilde kullanmayı hedefleyen kapsamlı bir yaklaşımdır. Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı tarafından yayımlanan 2020-2023 ve 2024-2028 Ulusal Siber Güvenlik Stratejisi belgeleri, siber güvenliğin sağlanmasında yapay zekânın rolünü detaylandırarak ülkenin savunma kapasitesini artırmayı ve siber tehditlere karşı dayanıklılığını güçlendirmeyi amaçlayan somut hedefler ortaya koymaktadır (T.C. Ulaştırma ve Altyapı Bakanlığı, 2020; T.C. Ulaştırma ve Altyapı Bakanlığı, 2024).

Buna karşılık, 2021-2025 Ulusal Yapay Zekâ Stratejisi (2021) siber güvenliğe yalnızca genel bir bakış sunmakta, bu alana dair ayrıntılı hedef ve stratejiler içermemektedir. 28 Mayıs 2024 tarihli Milli Güvenlik Kurulu toplantısında ise yapay zekânın sunduğu fırsatlar ve siber alanda yarattığı yeni tehditler ele alınarak Türkiye'nin bu alanda ileri kabiliyetler geliştirmesinin önemi vurgulanmıştır (Milli Güvenlik Kurulu, 2024). Ayrıca, ulusal siber güvenlik faaliyetlerini merkezi bir şekilde yürütmek üzere hükümetin çalışmalar yürüttüğü bilgisi (Ekiz, 2024) göz önünde bulundurulduğunda, Türkiye'nin yapay zekâyı geniş kapsamlı bir araç olarak konumlandırmasına karşın, siber güvenliği daha odaklanmış ve merkezi koordinasyon gerektiren stratejik bir alan olarak değerlendirdiği anlaşılmaktadır.

Yayımlanan strateji belgelerinde, ülkenin güvenlik kapasitesini artırmaya ve kritik altyapıları korumaya odaklanmaktadır. Yapay zekâ, siber güvenlikte sağladığı büyük veri işleme, desen tanıma, öngörü ve hızlı karar verme yetenekleri sayesinde tehditlerin erken tespiti, saldırılara hızlı yanıt verilmesi ve siber olaylara müdahale kapasitesini artırarak Türkiye gibi orta ölçekli güçler için önemli bir savunma aracı işlevi görmektedir (Rodriguez Vance, 2023: 77). Bu teknolojiler hem reaktif hem de proaktif savunma mekanizmaları sunarak Türkiye'nin siber güvenlik yapısını daha dayanıklı hale getirmektedir. Yapay zekânın en önemli kullanım alanlarından biri, tehdit tespiti ve anormalliklerin belirlenmesidir. Türkiye, savunma yeteneklerini güçlendirmek amacıyla yapay zekâ tabanlı araçlar geliştirmektedir. Hem uluslararası arenadaki çalkantılardan etkilenmemek hem de tasarım aşamasından itibaren güvenlik ilkesiyle yerli ve milli siber güvenlik araçları oluşturulmasına önem verilmektedir (T.C. Ulaştırma ve Altyapı Bakanlığı, 2024: 25; T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ve T.C. Sanayi ve Teknoloji Bakanlığı, 2021: 13).

3.3. Yapay Zekâ ve Ulusal Altyapıların Korunması

Günümüzde ekonomik hayatın sürdürülebilirliği, devletin kamu hizmetlerini devam ettirmesi, sosyal ve bireysel güvenliğin korunması, çevrimiçi hizmetlerin kesintisiz olarak sürmesine büyük ölçüde bağımlıdır (Çifci, 2024a: 205). Türkiye, dijital dönüşüm sürecinde yaşanan hızlı gelişmeler ve artan siber tehditlerle başa çıkmak için ulusal siber güvenlik stratejisini yeniden yapılandırmaya odaklanmıştır. Coğrafi konumu ve bölgesel liderlik rolü, Türkiye'yi siber tehditlere karşı güçlü bir savunma geliştirmeye teşvik etmektedir.

Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı'nın yayımladığı 2020-2023 ve 2024-2028 Ulusal Siber Güvenlik Stratejisi belgelerinde, yapay zekânın savunma kapasitesini geliştirme ve siber tehditlere karşı direnci artırma konularındaki rolü açıkça belirtilmiştir. Bu belgelerde, siber tehditlerin erken tespit edilmesi ve hızlı müdahale sağlanması için yapay zekâ tabanlı sistemlerin uygulanması amaçlanmaktadır (T.C. Ulaştırma ve Altyapı Bakanlığı, 2024: 22). Kritik altyapıların korunması, ülke ekonomisi ve güvenliği açısından stratejik bir öneme sahip olduğundan, yapay zekâ çözümleri devlet politikalarıyla da desteklenmektedir.

Enerji, finans, sağlık ve iletişim gibi kritik altyapılar, Türkiye'nin siber güvenlik stratejisinde öncelikli alanlar olarak tanımlanmıştır. Devlet destekli aktörler veya organize suç grupları tarafından hedef alınabilecek bu hayati sektörlerin güvenliğini sağlamak, Türkiye'nin siber güvenlik önlemlerinin merkezinde yer almaktadır (Özker, 2022: 4). Yapay zekâ tabanlı siber güvenlik çözümleri, altyapıların korunması için veri analizi, anomali tespiti ve tehditlere hızlı müdahale gibi kabiliyetler sunarak ülkenin savunma kapasitesini önemli ölçüde artırmaktadır. Bu sistemler, enerji sektöründe şebeke güvenliğini sağlamak, finans sektöründe dolandırıcılığı tespit etmek, hassas verilere yetkisiz erişimleri engellemek ve saldırılara hızlı müdahale sağlamak gibi işlevler üstlenmektedir (Özker, 2022: 9).

Türkiye'nin yapay zekâ destekli savunma stratejisinin temel odak noktalarından biri, ulusal güvenlik ve ekonomik istikrar açısından büyük önem taşıyan kritik altyapıların korunmasıdır. 2010 yılında İran'ın nükleer zenginleştirme tesislerine yönelik Stuxnet saldırısı gibi olaylar, güvenlik açıklarının proaktif olarak tespit edilip kapatılmasının önemini açıkça göstermiştir (Lindsay, 2013: 365). Devlet destekli olduğu düşünülen bir hacker saldırısı sonucunda 2015 yılında Türkiye'de birçok şehirde 12 saat süren elektrik kesintileri yaşamıştır (Daşkın, 2019: 28). Bu bağlamda, Türkiye'nin yapay zekâ tabanlı siber savunmaya yönelerek altyapılarının güvenliğini artırması ve olası siber tehditlere karşı dayanıklılığını sağlaması kritik bir gereklilik haline gelmiştir.

Türkiye'nin geliştirdiği yapay zekâ ve makine öğrenimi tabanlı çeşitli araçlar, olağandışı aktiviteleri tespit ederek olası tehditlere karşı erken uyarı sağlamaktadır. AVCI, AZAD, KASIRGA, ATMACA ve KULE gibi yazılımlar, siber güvenlik alanında etkin bir şekilde kullanılmaktadır. Bu yazılımlar, büyük veri içerisinde özel analiz yöntemleri kullanarak zararlı yazılımların tespiti, tehdit istihbaratı ve zararlı alan adları ile sahte sitelerin belirlenmesi gibi işlemleri gerçekleştirmektedir. Örneğin, KASIRGA sistemi, aralıksız olarak 16 milyon IP adresini tarayarak zafiyet içeren sistemleri saldırganlardan önce tespit etmektedir (Bilgi Teknolojileri ve İletişim Kurumu, 2018; Bilgi Teknolojileri ve İletişim Kurumu, 2022).

Yapay zekâ sistemleri, tehdidin türüne göre uygun yanıt stratejileri önererek veya otomatik müdahaleler gerçekleştirerek zaman kazandırmaktadır. Ulusal Siber Olaylara Müdahale Merkezi (USOM), 2024 yılında 97 binden fazla zararlı bağlantıyı tespit ederek altyapı seviyesinde erişimlerini engellemiştir. Kasırga projesi ile haftalık olarak 838 binden fazla kritik web sitesinin zafiyet taraması yapılmakta, Atmaca sistemi ise olası güvenlik açıklarını proaktif olarak engellemektedir. Ayrıca,

USOM'un yapay zekâ tabanlı sistemleri sayesinde kimlik avı amacıyla oluşturulan 61 binden fazla zararlı alan adı tespit edilerek erişime kapatılmıştır. Bu çalışmalar, Türkiye'nin ulusal altyapı güvenliğini koruma konusunda güçlü bir dirence sahip olduğunu göstermektedir (Melek ve Öztürk, 2024).

Türkiye'nin siber güvenlik stratejisinde yapay zekâ, gerçek zamanlı izleme ve siber tehditlerin erken tespitini sağlama kabiliyetiyle önemli bir yer edinmiştir. Bu yetenek, kritik altyapılarda meydana gelebilecek aksaklık riskini en aza indirirken, siber tehditlere karşı uzun vadeli direnç oluşturmayı hedefleyen proaktif bir savunma sağlamaktadır. Yapay zekânın büyük veri işleme ve anormallikleri tespit etme yeteneği, Sıfır-Gün açıkları, ağlarda uzun süre tespit edilmeden kalabilen Gelişmiş Kalıcı Tehditler (APT'ler) ve sistemleri erişilmez hale getirebilen Dağıtılmış Hizmet Reddi (DDoS) saldırılarının önceden tespit edilmesinde büyük değer taşımaktadır (Sodipe vd., 2024: 196-198). Ancak, Türkiye'nin kritik altyapılarını korumak amacıyla hangi yapay zekâ sistemlerini kullandığına dair ayrıntılı bilgiler kamuya açık kaynaklarda yer almamaktadır.

3.4. Uluslararası İş Birliğinin Rolü

Türkiye, siber güvenlik alanında çeşitli etkinlikler, tatbikatlar ve üyelik girişimleriyle yoğun bir uluslararası iş birliği içerisindedir. Bu yoğun iş birliği nedeniyle Siber Güvenlik Endeksi'nde de üst sıralarda yer almıştır (Uluslararası Telekomünikasyon Birliği, 2024: 126). Siber güvenliğe yönelik çalışmalara adanmış olan ITU (Uluslararası Telekomünikasyon Birliği), IMPACT (Siber Tehditlere Karşı Uluslararası Çok Taraflı Ortaklık), CAMP (Karşılıklı İlerleme için Siber Güvenlik İttifakı), GFCE (Küresel Siber Uzmanlık Forumu) ve FIRST (Olay Müdahale ve Güvenlik Ekipleri Forumu) gibi birçok uluslararası organizasyona üyedir. Türkiye, Budapeşte Siber Suç Sözleşmesi'ni imzalayan ülkeler arasında yer almaktadır. Türkiye ayrıca NATO'nun Locked Shields, Cyber Coalition ve Trident Javelin gibi uluslararası tatbikatlarda aktif rol almakta; bunun yanı sıra hükümet desteğiyle düzenlenen Uluslararası Siber Savaş ve Güvenlik Konferansı gibi önemli etkinliklere ev sahipliği yapmaktadır. (Çifci, 2024b: 200; FIRST, 2024).

Türkiye'nin siber güvenlik stratejisi, Avrupa Birliği (AB) uyum süreci ve NATO gibi uluslararası kuruluşlarla olan iş birlikleri ile güç kazanmıştır. Örneğin, 1991'de AB'nin üye ülkelere yönelik "bilgisayar programlarının yasal korunması" direktifi, Türkiye'nin siber güvenlik alanındaki ilk adımlarında etkili olmuştur (Karakehya, 2009). Bu uyum süreci, Türkiye'nin siber güvenlik politikasının AB normlarıyla uyumlu bir şekilde gelişmesine katkı sağlamıştır. Türkiye, özel sektördeki girişimlerini uluslararası ortaklıklar kurmaya teşvik ederken, siber güvenlik alanında iş birliğini de artırmaktadır. Ancak savunma yapay zekâ yeteneklerini geliştirme konusunda kendi kendine yeterlilik ilkesine yönelmiştir. Bununla birlikte, NATO girişimlerine katılmaya da istekli davranmakta; örneğin, TÜBİTAK BİLGEM ve SAGE, NATO'nun Kuzey Atlantik Savunma İnovasyon Hızlandırıcısı (DIANA) girişimi kapsamında test merkezi olarak seçilmiştir. Bu adımlar, Türkiye'nin savunma yapay zekâ yeteneklerini geliştirirken NATO standartlarını gözettiğini ve bu

sistemlerin müttefiklerle birlikte çalışabilirliğine önem verdiğini göstermektedir (Kurç, 2023: 21-22).

Türkiye'nin siber güvenlik alanındaki en önemli uluslararası iş birliklerinden biri, NATO iş birliği çerçevesinde olmuştur. NATO'nun Siber Savunma Mükemmeliyet Merkezi (CCDCOE) gibi platformlarda Türkiye'nin aktif katılımı, ülkenin siber güvenlik kapasitesini güçlendirmeye ve küresel siber güvenlik normlarının oluşturulmasına katkı sağlamasına olanak tanımaktadır. Ayrıca, Türkiye'nin NATO bünyesinde düzenlenen "Locked Shields" gibi siber savunma tatbikatlarına katılması, askeri alandaki siber güvenlik yeteneklerinin geliştirilmesine önemli katkılar sunmaktadır (Halisdemir, 2021: 14; Eldem, 2019: 458).

Türkiye, Avrupa Birliği'ne aday ülke olarak, 2010 yılında Avrupa Konseyi'nin Siber Suçlar Sözleşmesi'ni imzalamış ve 2014 yılında da bu sözleşmeye ilişkin 6533 sayılı Sanal Ortamda İşlenen Suçlar Sözleşmesine İlişkin Kanunu çıkarmıştır (Kurnaz ve Önen, 2019: 94). Ulusal Yapay Zekâ Stratejisi'nde de Avrupa Birliği projelerine katılımın teşvik edileceğinin altı çizilmiştir. Ancak, AB ve üye ülkelerle siber güvenlik alanında yürütülen ortak çalışmaların kamuya açık olanlarının oldukça sınırlı olduğu görülmektedir (T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2021: 9).

Türkiye'nin uluslararası iş birliği yoluyla siber güvenlik alanındaki stratejisini geliştirme çabası, yalnızca ülkenin dijital altyapısını korumakla kalmamış; aynı zamanda bölgesel ve küresel güvenlik yapıları içerisinde etkin bir aktör olmasına katkı sağlamıştır. Bu süreçte yürütülen iş birlikleri, Türkiye'nin siber güvenlik kapasitesini güçlendirmesine yardımcı olurken, ülkenin küresel siber güvenlik çerçevesinde daha fazla tanınan bir aktör haline gelmesini sağlamıştır.

3.5. Etik Sorunlar ve Yönetişim

Siber güvenlikte yapay zekâ kullanımı, pek çok etik sorun ve yönetişim zorluğunu beraberinde getirmektedir. Yapay zekânın otonom karar alma ve hızlı veri işleme potansiyeli verimliliği artırsa da şeffaflık, hesap verebilirlik ve etik sınırların korunması açısından riskler doğurur. Yapay zekâ sistemlerinde şeffaflık, kullanıcıların bu sistemlerin karar alma süreçlerini anlamalarını sağlayarak güveni artırmaktadır. (Kim vd., 2020: 3) Ancak yapay zekânın karmaşıklığı nedeniyle 'kapalı kutu' olarak sunulması, hatalı sonuçlar doğuran veya kararlar veren sistemlerden hesap sorulabilmesini zorlaştırır (Cheong, 2024: 2). Bazı eleştirmenler tam şeffaflığın her durumda gerekli veya yararlı olmadığını, kullanıcıların bilgiyle aşırı yüklenmemesi için şeffaflığın ihtiyaçlara göre uyarlanması gerektiğini öne sürmektedir. Siber güvenlikte yapay zekâ sistemlerinde şeffaflık ve hesap verebilirliğin güveni güçlendirdiği vurgulanırken, kamu eğitimi ve katılımın da kritik olduğu savunulmaktadır. Bu çerçevede, kapsamlı bir strateji, kamuoyunun yapay zekâ sistemlerini hem anlamasını hem de güven duymasını sağlamada etkili olabilir (Cheong, 2024:7).

Yapay zekâ algoritmalarındaki önyargılar, dikkatli yönetilmezse mevcut eşitsizlikleri pekiştirebilir veya yeni önyargıların oluşmasına neden olabilir (Taddeo vd., 2023: 167). Bu önyargılar ayrıca çeşitli hak ihlallerinin gerçekleşmesine neden olabilir. Örneğin, siber güvenlik sistemlerinde ayrımcı algoritmalar belirli bir toplumsal grubun görüşlerini yansıtan içerikleri riskli olarak değerlendirerek ağ üzerinde engellemeye başladığında, ifade özgürlüğü ihlallerine yol açabilir. Bu nedenle, yapay zekâ yönetişimi, yalnızca teknik uzmanların değil, politika yapıcıların, sivil toplum kuruluşlarının ve kamuoyunun da dahil olduğu çok paydaşlı bir iş birliğini gerektirir; böylece, yapay zekânın daha kapsayıcı bir şekilde geliştirilmesi sağlanabilir.

Türkiye'nin Ulusal Yapay Zekâ Stratejisi ve Ulusal Siber Güvenlik Stratejisi (USGS), insan odaklı bir yaklaşımı vurgulamaktadır. 2013-2015 ve 2016-2019 dönemlerine ait USGS belgelerinde siber güvenliğin sağlanmasında hukukun üstünlüğü ile temel insan hak ve hürriyetlerinin korunmasına, şeffaflık, hesap verebilirlik ve etik değerlerin göz önünde bulundurulmasına ilkeler bölümünde yer verilmiştir. Ancak, 2020-2023 USGS belgesinde özgürlükler ile hak ve hürriyetlere dair ilkeler çıkarılmış, 2024-2028 USGS belgesinde ise tüm bu ilkeler belgede yer almamıştır.

4. TARTIŞMA

Türkiye'nin yapay zekâ tabanlı siber güvenlik stratejileri, realizm ve orta ölçekli güç teorisi çerçevesinde değerlendirildiğinde, ülkenin ulusal güvenlik hedeflerini ve uluslararası iş birliklerindeki dinamiklerini daha iyi anlamamızı sağlar. Realizme göre devletler, güç ve güvenliği temel motivasyon olarak görür. Bu bağlamda Türkiye, yapay zekâ tabanlı siber güvenlik yatırımlarıyla kritik altyapılarını korumayı ve ulusal güvenliğini sağlamayı amaçlar. Mearsheimer'ın ifade ettiği gibi realizm, devletlerin ulusal güvenliği merkeze almasını ve kendine yeterlilik stratejilerini benimsemesini savunur (Mearsheimer, 2001). Türkiye'nin yapay zekâ destekli siber güvenlik stratejisi de bu yaklaşıma uygun olarak, devlet destekli tehditler ve organize suç gruplarına karşı güçlü bir savunma mekanizması oluşturmayı hedefler.

Türkiye'nin NATO ve AB gibi uluslararası kuruluşlarla yaptığı iş birlikleri, savunma kapasitesini artırma konusunda katkı sağlasa da Türkiye'nin bağımsız sistemler geliştirmeye odaklanması, uluslararası iş birliğine dayalı fakat bağımsız bir savunma anlayışını öne çıkarır (Holbraad, 1984). Realist perspektifte bu, ulusal çıkarlarını koruyan bir devlet olarak Türkiye'nin kendine yeterliliğe verdiği önemi gösterir.

Orta ölçekli güç teorisi bağlamında Türkiye, NATO gibi büyük güvenlik yapılanmalarında diplomasi ve iş birliği yoluyla etkisini artırma stratejisini benimser. Orta ölçekli güçler, çok taraflı iş birlikleri ve diplomatik yetenekleriyle küresel ve bölgesel istikrara katkı sağlamayı hedefler (Holbraad, 1984). Türkiye'nin NATO Siber Savunma Mükemmeliyet Merkezi (CCDCOE) gibi platformlarda aktif rol alması, büyük güçlerle stratejik uyum sağlarken aynı zamanda kendi siber güvenlik kapasitesini de güçlendirmesine olanak tanır. Bu iş birlikleri, Türkiye'nin NATO içinde daha fazla söz sahibi olmasına katkı sağlarken, stratejik bağımsızlığını korumasına ve bölgesel istikrar sağlayıcı bir güç olarak konumlanmasına da yardımcı

olur (Kurç, 2023). Bu tür bir denge politikası, orta ölçekli güç diplomasisinin karakteristik bir özelliğidir.

Ancak, orta ölçekli güç teorisi, Türkiye'nin bu ittifaklar içindeki etkisinin sınırlı kalabileceğini de öngörür. NATO ve AB gibi büyük güçlerin baskın olduğu yapılarda Türkiye'nin karar alma süreçlerinde tam bağımsızlık sağlaması zordur. Özellikle AB uyum sürecinde yaşanan zorluklar, Türkiye'nin bu yapılar içindeki etkisini sınırlayan bir unsur olarak öne çıkar.

Türkiye'nin siber güvenlik stratejisinde şeffaflık, hesap verebilirlik ve insan hakları gibi ilkeler son dönemlerde geri planda kalmış ve güvenlik odaklı bir yaklaşım ön plana çıkmıştır. Savaş ve Karataş (2022) siber yönetişimin başarılı olabilmesi için açıklık, şeffaflık, katılım ve hesap verebilirlik gibi ilkelerin yanı sıra insan haklarının korunmasının da kritik bir öneme sahip olduğunu vurgular. Türkiye'nin 2013-2015 ve 2016-2019 dönemlerine ait Ulusal Siber Güvenlik Strateji belgelerinde insan haklarına vurgu yapılırken, bu ilkeler 2020-2023 ve 2024-2028 stratejilerinde yer almamıştır. Bu durum, Türkiye'nin güvenliğe öncelik veren bir yaklaşımı benimsediğini göstermektedir. Ancak, NATO ve AB iş birliklerinde güvenilir bir aktör olabilmesi için Türkiye'nin insan hakları yükümlülüklerini ihmal etmemesi ve şeffaflık ile hesap verebilirlik gibi değerlere önem vermesi gerekmektedir. Aksi halde, Türkiye'nin bu güvenlik politikaları uluslararası kamuoyunda olumsuz bir algı yaratabilir.

Türkiye'nin siber güvenlik stratejilerinde şeffaflık eksikliği, konunun daha derinlemesine analiz edilmesini zorlaştırmaktadır. Birleşik Krallık'taki Ulusal Siber Güvenlik Merkezi (National Cyber Security Centre - NCSC) ve ABD'deki Siber Güvenlik ve Altyapı Güvenliği Ajansı (Cybersecurity and Infrastructure Security Agency - CISA) gibi kurumlar, siber güvenlik alanında karşılaşılan saldırılar, alınan önlemler ve yürütülen politikalar hakkında kamuoyuna düzenli olarak bilgi sunmaktadır. Bu tür şeffaflık uygulamaları, akademik araştırmaların somut veriler üzerinden ilerlemesini sağlarken, kamuoyunun bilinçlenmesine ve siber tehditlere karşı daha iyi hazırlıklı olunmasına da katkı sunmaktadır. Oysa Türkiye'de bu tür bilgilerin kamuya açık bir şekilde paylaşılmaması, akademik analiz kapasitesini sınırlamakta ve siber güvenlik politikalarının etkinliğinin bağımsız olarak değerlendirilmesini güçleştirmektedir. Bu durum, aynı zamanda hesap verebilirlik ve kamu denetimi mekanizmalarının zayıflamasına neden olmaktadır.

Bununla birlikte, Türkiye'nin siber güvenlik stratejilerinde yapay zekâ tabanlı sistemlerin nasıl işlediğine dair detaylı teknik bilgilerin kamuya açık olmaması, bu alandaki analizleri büyük ölçüde teorik çerçevelerle sınırlı bırakmaktadır. Örneğin, ATMACA, AVCI ve KASIRGA gibi yapay zekâ destekli siber güvenlik sistemlerinin hangi algoritmaları kullandığı, etkinliği ve karşılaşılan teknik zorluklar konusunda kamuya açık doğrulanabilir veri bulunmamaktadır. Türkiye'de siber güvenlik alanında daha şeffaf bir yönetişim anlayışı benimsenmesi, bu alandaki akademik çalışmaların derinleşmesini sağlayacağı gibi, kamuoyunun da güvenlik politikalarına dair bilinçlenmesine katkı sunacaktır.

Yapay zekâ tabanlı siber güvenlik sistemlerinde yaşanan yanlış pozitif ve negatif tespitler en önemli zayıflıklardan biridir. Yanlış pozitif tespitler, gereksiz müdahalelere yol açarak önemli altyapılarda kesintilere neden olabilirken; yanlış negatif tespitler ise gerçek tehditlerin gözden kaçmasına neden olabilir. Bu tür zafiyetlerin önlenebilmesi için Türkiye'nin yapay zekâ algoritmalarını sürekli olarak güncellemesi ve veri analiz süreçlerinde hassasiyeti artırması gereklidir (Rodriguez Vance, 2023).

Siber Savunma Endeksi (2022-2023) Türkiye'nin yapay zekâ tabanlı siber güvenlik stratejisini 17 farklı sektöre ve teknolojiye ne derece entegre edebildiğini göstermektedir. Endeks, 166 ülkeyi sıralamakta ve Brezilya, Güney Afrika, Meksika, Endonezya ve BAE gibi orta büyüklükteki güçlerle Türkiye'yi sektörel ve teknolojik hazırlıkları bakımından karşılaştırmaktadır. Sıralamaya göre Türkiye, araştırma ve geliştirme ve bilgi ve iletişim teknolojileri alanlarında Hindistan, Suudi Arabistan, Brezilya ve BAE gibi ülkelerin arkasında kalmıştır. (Cyber Defence Index, 2023; Connor, 2024)

Türkiye'nin insan merkezli ilkelerden uzaklaşan yaklaşımı, etik sorunları da beraberinde getirmektedir. Özellikle yapay zekâ destekli sistemlerde denetim, önyargı ve şeffaflık eksiklikleri öne çıkmaktadır. Türkiye'nin siber güvenlik stratejilerinde bu etik sorunların göz ardı edilmesi, kamuoyunda güven kaybına neden olabilir. Orta ölçekli bir güç olarak Türkiye, yapay zekâ tabanlı siber güvenlik sistemlerinde etik standartları koruyarak uluslararası iş birliklerinde güvenilirliğini artırabilir ve bu bağlamda NATO ve AB'nin demokratik değerleri ile uyum sağlayabilir

Sonuç olarak, Türkiye'nin siber güvenlik stratejisi, realizm çerçevesinde ulusal güvenliği koruma amacı taşırken, orta ölçekli güç teorisi perspektifinde uluslararası iş birlikleri ile etkisini artırmaya çalışmaktadır. Ancak, insan merkezli ilkelerden uzaklaşması, Türkiye'nin uluslararası güvenlik normları ile uyumunu zayıflatabilir ve iş birliği kapasitesini sınırlayabilir. Bu nedenle, Türkiye'nin siber güvenlik stratejilerinde güvenlik ve hak koruma dengesini sağlaması, ulusal güvenlik hedefleri ile uluslararası iş birlikleri arasındaki dengeyi koruyabilmesi açısından önem taşımaktadır.

SONUÇ

Bu çalışma, Türkiye'nin siber güvenlik stratejisinde yapay zekâ teknolojilerini kullanma biçimini, ulusal güvenlik hedefleri ve uluslararası iş birlikleri bağlamında ele almıştır. Yapay zekâ teknolojilerinin veri işleme, tehdit tespiti ve hızlı müdahale kapasitesini artırması, Türkiye gibi orta ölçekli güçlerin siber güvenlik alanında daha dirençli bir savunma mekanizması kurmalarına yardımcı olmuştur. Türkiye, özellikle NATO ve AB gibi güvenlik yapılanmaları içindeki rolünü güçlendirme hedefi doğrultusunda, yapay zekâ destekli siber güvenlik stratejileriyle hem ulusal hem de uluslararası güvenlik çerçevesine katkı sunmaktadır.

Realist perspektiften değerlendirildiğinde, Türkiye'nin siber güvenlik stratejisi, dijital tehditlere karşı kendine yeterlilik esasına dayalı güçlü bir savunma mekanizması oluşturma hedefiyle uyum göstermektedir. Türkiye'nin devlet destekli siber saldırılar gibi güvenlik tehditlerine karşı yapay zekâ yatırımlarını artırması, ulusal güvenliği merkeze alan bir yaklaşımı yansıtmaktadır. Orta ölçekli güç teorisi bağlamında ise Türkiye, NATO ve diğer uluslararası kuruluşlarla olan iş birlikleri sayesinde siber güvenlik alanında etkili bir aktör olarak öne çıkmaktadır. Türkiye'nin NATO'nun Siber Savunma Mükemmeliyet Merkezi gibi uluslararası platformlarda aktif olarak yer alması, yalnızca kendi güvenlik kapasitesini artırmakla kalmamakta, aynı zamanda bölgesel istikrar sağlamada rol üstlenmesine olanak tanımaktadır.

Ancak, yapay zekâ tabanlı siber güvenlik stratejilerinin artan kullanımı, bazı etik ve yönetişim sorunlarını da beraberinde getirmektedir. Bireylerin mahremiyeti, devletin gözetim kapasitesindeki artış, insan denetimi ve veri güvenliği gibi konular, Türkiye'nin bu alandaki stratejilerini yürütürken göz önünde bulundurması gereken önemli faktörlerdir. Türkiye'nin siber güvenlik stratejisinde insan hakları ve etik standartlara daha fazla yer vermesi, yalnızca iç güvenliğini değil, uluslararası iş birliklerinde güvenilirliğini artırması açısından da önem taşımaktadır.

Öte yandan, Türkiye'nin siber güvenlik çalışmalarına dair şeffaflık düzeyi oldukça düşüktür, bu da bu alanda veri ve bilgiye erişimi sınırlamaktadır. Strateji belgeleri dışında, siber güvenliğe dair çalışmaların detayları çoğunlukla kamuya açık olmadığından, siber güvenlik stratejilerinin etkinliğine dair bilgi toplamak oldukça zordur. Türkiye'nin siber güvenlik politikalarına dair daha şeffaf bir yaklaşım benimsemesi, kamuoyunun güvenini artırırken, uluslararası iş birliklerinde güvenilir bir aktör olarak konumlanmasını da pekiştirebilir.

Sonuç olarak, Türkiye'nin yapay zekâ tabanlı siber güvenlik stratejileri, mevcut ve gelecekteki dijital tehditlerle başa çıkmada önemli bir rol oynamaktadır. Türkiye'nin bu stratejideki başarısı, siber güvenlik kapasitesini artırmakla birlikte, ülkeyi küresel siber güvenlik alanında daha etkili bir aktör haline getirme potansiyeline sahiptir. Bununla birlikte, bu stratejilerin sürdürülebilirliği ve uluslararası güvenlik normlarıyla uyumlu hale getirilmesi, etik kaygılar, insan hakları ve şeffaflık açısından dengeli bir yaklaşım geliştirilmesine bağlı olacaktır. Bu bağlamda, Türkiye'nin yapay zekâ destekli siber güvenlik stratejisinin uzun vadeli başarısı hem ulusal güvenlik hem de etik sorumlulukları eşit derecede gözeten, şeffaf bir politika izlenmesine bağlıdır.

TÜRKİYE'S AI-DRIVEN CYBERSECURITY STRATEGY: ENHANCING NATIONAL SECURITY AND SHAPING GLOBAL CYBER GOVERNANCE

1. INTRODUCTION

The transformation driven by digitalization across critical sectors like telecommunications, healthcare, industry, and education has made cybersecurity a

core component of national security. Within this context, the application of artificial intelligence (AI) in cybersecurity has fortified states' resilience against digital threats. AI's capabilities in processing large volumes of data, recognizing patterns, decision-making, and automating responses have enhanced the speed and efficiency of threat detection and response mechanisms, positioning AI as a valuable tool in combating cyber threats. Türkiye, given its strategic location and growing status as a regional power, faces a range of threats, including state-sponsored attacks and organized cybercrime. To counter these threats, Türkiye has proactively integrated AI-based technologies into its national cybersecurity strategy.

Türkiye's cybersecurity initiatives prioritize the protection of critical infrastructure, such as energy grids, communication systems, transportation networks, and financial systems, while aiming to reduce its strategic dependency in cyberspace. Through its AI-powered cybersecurity strategies, Türkiye not only seeks to ensure national security but also plays an active role in regional and global security frameworks, including NATO and the EU. This study examines Türkiye's AI-driven cybersecurity strategies in terms of securing national interests, fostering international cooperation, and addressing ethical challenges associated with AI in cybersecurity.

2. METHODS

The study applies a secondary data analysis approach to analyze Türkiye's AI-driven cybersecurity strategies. Data were collected from academic articles, books, official reports, and strategic documents from various databases and reviewed within the frameworks of realism and middle power theories.

Türkiye's approach to cybersecurity and AI integration is examined through the lenses of realism and middle power theory. Realism, which considers security and power pursuits as the primary motivation for state behavior, helps to analyze Türkiye's AI-driven cybersecurity strategy. This perspective highlights Türkiye's efforts to build a defense mechanism against digital threats and to protect its national interests. Middle power theory, meanwhile, provides insight into Türkiye's strategic initiatives within major security structures like NATO and the EU, which offer a framework for contributing to regional stability and advancing Türkiye's global positioning.

3. RESULTS

Türkiye's strategic position and increasingly digitalized infrastructure expose it to a broad spectrum of cyber threats, ranging from state-sponsored actors to organized criminal networks. Türkiye's AI-based cybersecurity strategy is critical not only for threat detection and response but also for positioning Türkiye as a proactive actor in international security frameworks.

Türkiye's journey in cybersecurity began with the inclusion of cybercrimes in the Turkish Penal Code in 1991. Since then, Türkiye has progressively expanded its cybersecurity strategy, prioritizing the protection of critical sectors such as energy,

finance, and telecommunications. The 2013 National Cybersecurity Strategy formalized a structural approach to cybersecurity.

Türkiye's AI-driven cybersecurity strategy aims to leverage technological innovation to strengthen defense capacities. The focus on large-scale data processing and threat detection allows these systems to respond quickly to cyber incidents, enhancing Türkiye's resilience. With AI-driven tools, Türkiye seeks to establish a proactive defense against potential threats.

4. DISCUSSION

Türkiye's AI-driven cybersecurity strategies, examined within the frameworks of realism and middle power theories, provide insight into its national security goals and dynamics in international cooperation. According to realism, Türkiye aims to safeguard national security and establish an independent security mechanism through AI-driven cybersecurity investments. By enhancing its cybersecurity through NATO and EU cooperation, Türkiye also seeks to bolster its strategic autonomy, though achieving full independence within these alliances is anticipated to be challenging.

From a middle power perspective, Türkiye's active involvement in platforms such as NATO's Cooperative Cyber Defence Centre of Excellence (CCDCOE) enables it to contribute to the establishment of international security norms, positioning itself as a stabilizing force in the region. Türkiye's emphasis on human rights and ethical standards in its cybersecurity strategy could further enhance its role as a credible actor in international collaborations.

CONCLUSION

Türkiye's AI-driven cybersecurity strategies demonstrate potential to ensure national security and establish Türkiye as an effective actor within international security structures. With AI-driven defense systems, Türkiye builds a resilient defense mechanism against digital threats, gaining a more active stance within entities like NATO. However, the sustainability of these strategies and their alignment with international security norms require a balanced approach to ethical concerns, human rights, and transparency. Türkiye's long-term success with AI-driven cybersecurity strategies will depend on a policy that equally emphasizes both national security and ethical responsibility.

KAYNAKÇA

Adams, J. (2001). Virtual defense. *Foreign Affairs*, *80*(3), 98–112.

Akyeşilmen, N. (2022). Türkiye in the Global Cybersecurity Arena: Strategies in Theory and Practice. *Insight Türkiye*, 24(3), 109-134.

Arquilla, J. ve Ronfeldt, D. (1993). Cyberwar is coming! *Comparative Strategy*, 12(2), 141–165.

Atilla, T. (2010). Tüm bilgileriniz şu anda satılıyor olabilir. Hürriyet. Erişim: 1 Mart 2025, https://www.hurriyet.com.tr/gundem/tum-bilgileriniz-su-anda-satiliyor-olabilir-15430731

BBC News Türkçe. (2024). '108 milyon kişinin verileri çalındı' iddiası: Bakanlık ne açıkladı, tepkiler ne oldu?. BBC News Türkçe. Erişim: 1 Mart 2025, https://www.bbc.com/turkce/articles/cn8789ez2q7o

Bilgi Teknolojileri ve İletişim Kurumu. (2018). Siber Dünyada En Zayıf Halka Kadar Güçlüyüz. Erişim: 30 Ekim 2024, https://eng.btk.gov.tr/haberler/siber-dunyada-en-zayif-halka-kadar-gucluyuz

Bilgi Teknolojileri ve İletişim Kurumu. (2022). Siber Güvenlik Ekosisteminin Geliştirilmesi Zirvesi BTK'da Başladı. Erişim: 30 Ekim 2024, https://eng.btk.gov.tr/haberler/siber-guvenlik-ekosisteminin-gelistirilmesi-zirvesi-btk-da-basladi

Cheong, B. C. (2024). Transparency and Accountability in AI Systems: Safeguarding Wellbeing in the Age of Algorithmic Decision-making. *Frontiers in Human Dynamics,* 6.

Connor, S. (2023). Middle Powers: Digital Ambitions Meet Rising Cyber Risks. Erişim: 4 Mart 2025, https://www.controlrisks.com/our-thinking/insights/middle-powers-digital-ambitions-meet-rising-cyber-risks

Cooper, A. F. ve Parlar Dal, E. (2016). Positioning the third wave of middle power diplomacy: Institutional elevation, practice limitations. *International Journal: Canada's Journal of Global Policy Analysis,* 71(4), 516–528.

Cooper, A. F., Higgott, R. A. ve Nossal, K. R. (1994). *Relocating middle powers*. Vancouver, BC, Canada: UBC Press.

Craig, A. Ve Valeriano, B. (2018). Realism and Cyber Conflict: Security in the Digital Age. Erişim: 4 Mart 2025, https://www.e-ir.info/2018/02/03/realism-and-cyber-conflict-security-in-the-digital-age/

Cristiano, F., Broeders, D., Delerue, F., Douzet, F. ve Géry, A. (Ed.). (2023). Artificial Intelligence and International Conflict in Cyberspace. Londra: Routledge.

Çifci, H. (2024a). Analysis of Türkiye's Cybersecurity Strategies: Historical Developments, Scope, Content And Objectives. *Sakarya University Journal of Science*, 28(1), 204–219.

Çifci, H. (2024b). Cybersecurity Maturity of Türkiye: An Assessment with ENISA's National Capabilities Assessment Framework (NCAF). *Savunma Bilimleri Dergisi*, 20(2), 191–210.

Daşkın, E. (2019). The Turkish Cyber Security Strategy: Structure, Legislation, and Challenges. *Journal of Intelligence and Cyber Security*,2(1), 1-39.

DHA. (2020). 3 Yılda Türkiye'yi Hedef Alan 325 Bin Siber Saldırı Engellendi. *Hürriyet.* Erişim: 30 Ekim 2024, https://www.hurriyet.com.tr/teknoloji/3-yilda-turkiyeyi-hedef-alan-325-bin-siber-saldiri-engellendi-41701144

E-Governance Academy (2023). National Cyber Security Index: Türkiye. Erişim: 3 Kasım 2024.

Ekiz, A. (2024). Siber Güvenlik Alanının Çatısını Oluşturacak Yasal Düzenleme Geliyor. *Anadolu Ajansı*. Erişim: 30 Ekim 2024, https://www.aa.com.tr/tr/gundem/siber-guvenlik-alaninin-catisini-olusturacak-yasal-duzenleme-geliyor/3286012

Eldem, T. (2019). The Governance of Türkiye's Cyberspace: Between Cyber Security and Information Security. *International Journal of Public Administration,* 43(5), 452–465.

FIRST (2024). Forum of Incident Response and Security Teams. Erişim: 30 Ekim 2024, https://www.first.org/members/teams/tr-cert

Halisdemir, E. (2021). National Cybersecurity Organisation: Türkiye. *NATO Cooperative Cyber Defence Centre of Excellence*. Erişim: 3 Kasım 2024.

Holbraad, C. (1984). *Middle Powers in International Politics*. London: Macmillan Press.

Karakehya H. (2009). Türk Ceza Kanunu'nda Bilişim Sistemine Girme Suçu. *Türkiye Barolar Birliği Dergisi*, 22(81), 187-210.

Kim, B., Park, J. ve Suh, J. (2020). Transparency and Accountability in AI Decision Support: Explaining and Visualizing Convolutional Neural Networks for Text Information. *Decision Support Systems*, 134(113302).

Kurç, C. (2023). Enabling Technology of Future Warfare: Defense AI in Türkiye (DAIO Study No. 23/08). *Defense AI Observatory, Helmut Schmidt University*. Erişim: 30 Ekim 2024.

Kurnaz, S. ve Önen, S. M. (2019). Avrupa Birliğine Uyum Sürecinde Türkiye'nin Siber Güvenlik Stratejileri. *International Journal of Politics and Security,* 1(2), 82-103.

Lindsay, J. R. (2013). Stuxnet and the Limits of Cyber Warfare. *Security Studies,* 22(3), 365–404.

McCarthy, J. (2016). Americans Cite Cyberterrorism Among Top Three Threats to U.S. Erişim: 4 Mart 2025, https://news.gallup.com/poll/189161/americans-cite-cyberterrorism-among-top-three-threats.aspx

Mearshimer, J. J. (2001). *The Tragedy of Great Power Politics*. New York: WW Norton.

Melek, A. ve Öztürk C. (2024). Bakan Uraloğlu: 97 Binin Üzerinde Zararlı Bağlantı Tespit Ederek Erişimlerini Engelledik. *Demirören Haber Ajansı.* Erişim: 30 Ekim 2024, https://www.dha.com.tr/politika/bakan-uraloglu-97-binin-uzerinde-zararli-baglanti-tespit-ederek-erisimlerini-engelledik-2519631

MIT Technology Review, *Cyber Security Index (2023).* Erişim: 4 Mart 2025, https://www.technologyreview.com/2022/11/15/1063189/the-cyber-defense-index-2022-23/

Milli Güvenlik Kurulu (2010). 27 Ekim 2010 Tarihli Toplantı. Erişim: 30 Ekim 2024, https://www.mgk.gov.tr/index.php/27-ekim-2010-tarihli-toplanti

Milli Güvenlik Kurulu (2024). 28 Mayıs 2024 Tarihli Toplantı. Erişim: 30 Ekim 2024, https://www.mgk.gov.tr/index.php/28-mayis-2024-tarihli-toplanti

Müftüler, M. ve Yüksel, M. (1997). Türkiye: A Middle Power in the New Order. A. F. Cooper (Ed.), *Niche Diplomacy: Middle Powers after the Cold War* içinde, (s. 184–196). London: Palgrave Macmillan UK.

Ongun, T. (2023). Türkiye Among World's Top Cybercrime Targets in 2023. *Anadolu Ajansı*. Erişim: 30 Ekim 2024, https://www.aa.com.tr/en/turkiye/turkiye-among-worlds-top-cybercrime-targets-in-2023/3076238

Özker, U. (2022). Türkiye'de Kritik Altyapı ve Siber Güvenlik. *Konrad-Adenauer-Stiftung Türkiye*. Erişim: 30 Ekim 2024.

Petallides, C. J. (2012). Cracking the digital vault: A study of cyber espionage. *Inquiries Journal, 4*(4), 1–3.

Rodriguez Vance, T. (2023). Examination of Applications of Artificial Intelligence in Cybersecurity: Strengthening National Defense with AI. *International Journal of Computer Science and Information Technology Research*, 11(3), 77-90.

Savaş, S. ve Karataş, S. (2022). Cyber Governance Studies in Ensuring Cybersecurity: An Overview of Cybersecurity Governance. *International Cybersecurity Law Review*, 3(1), 7–34.

Siber Güvenlik Kurulu (2013). Ulusal Siber Güvenlik Stratejisi ve 2013-2014 Eylem Planı. Erişim: 30 Ekim 2024, https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf

Sodipe, A. O., Abel, N. O., Ntichika, H. C., Daniel, E. E. ve Agboare, E. I. (2024). The Role of AI in Enhancing Network Security. *Iconic Research And Engineering Journals* 8(3),196-205. Erişim: 30 Ekim 2024.

Sukumar, A. M. (2023). The Middleware Dilemma of Middle Powers. F. Cristiano, D. Broeders, F. Delerue, F. Douzet ve A. Géry (Ed.), *Artificial Intelligence and International Conflict in Cyberspace* içinde (s. 109–134). Londra: Routledge.

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi ve Sanayi ve Teknoloji Bakanlığı. (2021). Ulusal Yapay Zekâ Stratejisi 2021-2025. Erişim: 30 Ekim 2024, https://www.cbddo.gov.tr/UYZS

T.C. Ulaştırma ve Altyapı Bakanlığı. (2020). Ulusal Siber Güvenlik Stratejisi 2020-2023. Erişim: 30 Ekim 2024, https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/ulusal-siber-guvenlik-stratejisi-ve-eylem-plani-2020-2023.pdf

T.C. Ulaştırma ve Altyapı Bakanlığı. (2024). Ulusal Siber Güvenlik Stratejisi 2024-2028. Erişim: 30 Ekim 2024, https://www.uab.gov.tr/uploads/pages/siber-guvenligin-yol-haritasi-yerli-ve-milli-tekno/ulusal-siber-guvenlik-stratejisi-2024-2028.pdf

T.C. Ulaştırma, Denizcilik ve Haberleşme Bakanlığı. (2016). 2016-2019 Ulusal Siber Güvenlik Stratejisi. Erişim: 30 Ekim 2024, https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf

Taddeo, M., McNeish, D., Blanchard, A. ve Edgar, E. (2023). Ethical Principles for Artificial Intelligence in the Defence Domain. F. Cristiano, D. Broeders, F. Delerue, F. Douzet ve A. Géry (Ed.), *Artificial Intelligence and International Conflict in Cyberspace* içinde (s. 159-185). Londra: Routledge.

UK Ministry of Defence (2022). Defence Artificial Intelligence Strategy. Erişim: 30 Ekim 2024, https://www.gov.uk/government/publications/defence-artificial-intelligence-strategy

Uluslararası Telekomünikasyon Birliği (ITU) (2024). Global Cybersecurity Index (GCI). Erişim Tarihi: 30 Ekim 2024, https://www.itu.int/en/ITU-D/Cybersecurity/Documents/GCIv5/2401416_1b_Global-Cybersecurity-Index-E.pdf

Waltz, K. N. (1979). *Theory of international politics*. Addison-Wesley.