BİLGİSAYAR MÜHENDİSLİĞİ

Alanında Uluslararası Çalışmalar

Mart 2025

EDİTÖR

PROF. DR. SELAHATTİN BARDAK

SERÜVEN YAYINEVİ

Genel Yayın Yönetmeni / Editor in Chief • Eda Altunel

Kapak & İç Tasarım / Cover & Interior Design • Serüven Yayınevi

Birinci Basım / First Edition • © Mart 2025

ISBN • 978-625-5552-97-6

Serüven Yayınevi / Serüven Publishing
Türkiye Adres / Turkey Address: Kızılay Mah. Fevzi Çakmak 1. Sokak
Ümit Apt No: 22/A Çankaya/ANKARA
Telefon / Phone: 05437675765
web: www.seruvenyayinevi.com
e-mail: seruvenyayinevi@gmail.com

Baskı & Cilt / Printing & Volume
Sertifika / Certificate No: 42488

BİLGİSAYAR MÜHENDİSLİĞİ

ALANINDA ULUSLARARASI ÇALIŞMALAR

EDİTÖR

PROF. DR. SELAHATTİN BARDAK

SERÜVEN YAYINEVİ

İÇİNDEKİLER

SAĞLIK SEKTÖRÜNDE KANBAN İLE ÇEVİK YAZILIM GELİŞTİRME SÜREÇLERİ

Fadile ÖZTÜRK[1], Nursena BAYGIN[2], Işıl KARABEY AKSAKALLI[3]

1 Erzurum Teknik Üniversitesi, Mühendislik ve Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, Bilgisayar Mühendisliği Anabilim dalı, Yakutiye/Erzurum, fadile.ozturk97@erzurum.edu.tr, https://orcid.org/0009-0000-7724-9830
2 Erzurum Teknik Üniversitesi, Mühendislik ve Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, Bilgisayar Mühendisliği Anabilim dalı, Yakutiye/Erzurum, nursenabaygin@erzurum.edu.tr, https://orcid.org/0000-0003-4457-5503
3 Erzurum Teknik Üniversitesi, Mühendislik ve Mimarlık Fakültesi, Bilgisayar Mühendisliği Bölümü, Bilgisayar Mühendisliği Anabilim dalı, Yakutiye/Erzurum, isil.karabey@erzurum.edu.tr, https://orcid.org/0000-0002-4156-9098

1. GİRİŞ

Çevik yazılım geliştirme (Agile Software Development), sürekli değişen ve belirsizliklerle dolu iş ortamlarında yenilikçi çözümler sunarak değişime hızlı bir şekilde adapte olmayı amaçlamaktadır. Günümüzde sağlık sektörü, hızla değişen ihtiyaçlar ve gelişen teknoloji ile karşı karşıyadır. Hasta bakım kalitesini artırmak ve operasyonel verimliliği sağlamak, sağlık kuruluşları ve çalışanları için her zamankinden daha önemli hale gelmiştir. Bu noktada, yazılım geliştirme süreçleri büyük bir rol oynamaktadır. Sağlık sektöründe kullanılan yazılımların esnek ve verimli olması hem sağlık çalışanlarına hem de hastalara önemli avantajlar sunmaktadır (Highsmith & Cockburn, 2001).

Sağlık sektöründe yazılım geliştirme süreçlerinin başarısı; hasta ihtiyaçlarına hızlı yanıt verebilme, hata toleransının düşük olması nedeniyle yüksek doğrulama gereksinimi ve kullanıcı dostu yazılımsal çözümler sunma gibi birçok faktöre bağlıdır. Bu faktörlerin asıl amacı, insan hayatıyla doğrudan ilişkili olduğu için yazılımların güncel ve güvenilir tutulmasını sağlamaktır (Kokol, 2022). Sağlık sistemlerinin düzgün çalışması, hastaların daha iyi bir bakım ve takip süreçleri ile sağlık sorunlarının giderilmesine katkıda bulunmaktadır (Papalexi et al., 2016). Bu doğrultuda, çevik metodolojiler sağlık sektöründeki zorlukları aşmada güçlü bir araç olarak öne çıkmaktadır. Çevik metodolojilerin önemli bir parçası olan kanban, yazılım geliştirme süreçlerinde iş akışlarını görselleştirme, süreç optimizasyonu ve sürekli iyileştirme (Kaizen) gibi özellikleriyle sağlık yazılımlarının verimli bir şekilde geliştirilmesine katkı sağlamaktadır (Dorca et al., 2016; Zayat & Senvar, 2020). Kanban, sağlık hizmetlerinde yürütülen süreçlerin hızlandırılmasını ve takibinin kolaylaştırılmasını amaçlamaktadır.

Kanban, sağlık sektörüne özel ihtiyaçlara yanıt veren etkili bir yöntem olup, yazılım geliştirme ekiplerinin daha verimli ve organize çalışmasına olanak tanımaktadır. Bu bağlamda, kanbanın sağladığı avantajlar, kullanım alanları ve sağlık sektöründeki uygulamaları incelenerek, çeşitli vaka örnekleriyle desteklenmiştir. Bu kitap bölümünde, kanban yöntemi ile çevik yazılım geliştirme süreçlerinin sağlık sektöründeki uygulamaları ele alınacaktır.

İkinci bölümünde, çevik yazılım geliştirme yöntemlerinin temelleri ve kanban ele alınmış, kanbanın avantajları ve dezavantajları detaylı olarak incelenmiştir. Üçüncü bölümde, sağlık sektöründeki yazılım geliştirme süreçleri ele alınarak kanban uygulamaları tartışılmıştır. Dördüncü bölümde, ele alınan genel durumlar değerlendirilmiş ve sonuçlar sunulmuştur. Son bölümde ise çalışmada kullanılan kaynaklar listelenmiştir.

2. ÇEVİK YAZILIM GELİŞTİRME YÖNTEMLERİNİN TEMELLERİ VE KANBAN

2.1. Çevik Yazılım Geliştirme

Birçok problemin çözümünün sağlanabilmesi için kullanılan yöntemler eskiden süregelen bir süreci kapsamaktadır. Bu sürecin takip edilmesi, uygulanması ve harekete geçirilmesi uzun bir zaman diliminde gerçekleşmiştir (Cohen et al., 2004). Zamanla değişen iş ihtiyaçları, müşteri talepleri gibi durumlar uzun süreli olan bu sistemi karşılamak için yetersiz kalmıştır. Maliyetin azaltılarak kalitenin artırılmasının hedeflenmesi ile; sürekli değişime uyum sağlayan ve müşteri odaklı anlayışa sahip olan çevik yöntemler önerilmiştir (Beck et al., 2001; Reifer, 2002).

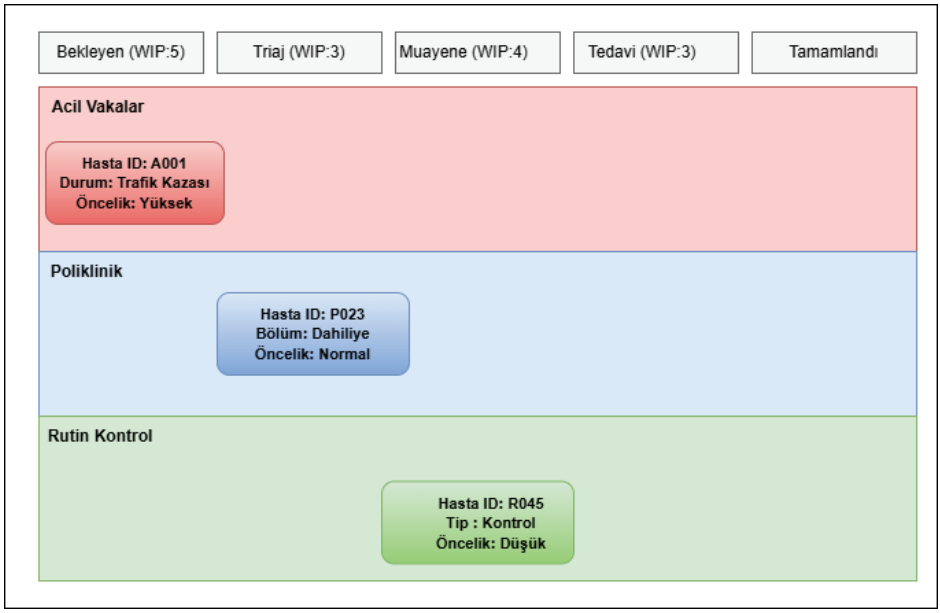
Çevik Manifesto'nun bazı prensipleri bulunmaktadır. Bu prensipler temelde müşteri ihtiyaçlarına hızla yanıt verme ve sürekli iyileştirme, ekip arası iletişim, çalışan; sonuç veren bir yazılım, müşteri iş birliği, değişime esnek bir yapı, kullanıcı dostu tasarım gibi değerler üzerine odaklanmaktadır (Campanelli & Parreiras, 2015; Fowler et al., 2001; Manifesto, 2001). Çevik yazılımın kısa zamanda, az maliyetle, yüksek kalitede gereksinimleri karşılaması diğer yöntemlere kıyasla temel özellikler arasında yer almaktadır (Campanelli & Parreiras, 2015; Stainier & De Jaegere, n.d.).

Çevik yazılım geliştirme süreçleri, gereksinimlerin belirlenmesi ile başlamaktadır. Bu gereksinimler ilk başta tam anlamıyla anlamlandırılamaz zamanla müşterinin isteklerine göre şekillenmektedir. Müşterinin bu gereksinimleri "kullanıcı hikayeleri" şeklinde tanımlanmaktadır (Lei et al., 2017). Daha sonra yapılacak işler zaman dilimlerine göre parçalanmakta ve planlama yapılmaktadır. Yapılan planlama sürecinden sonra ekip iş birliği içerisinde geliştirme sürecine başlanmaktadır. Her bir tamamlanan yazılım parçası müşteriye sunulmakta ve müşterinin ürünü kullanması sağlanmaktadır. Çevik yazılım geliştirme süreci burada başlamaktadır. Müşteriden sürekli geri bildirim alınarak düzeltilmesi gereken bir yer var ise güncellemeye tabi tutulmaktadır (Cockburn & Highsmith, 2001). Bu süreçte zamanla değişen isteklere ve güncellemelere bağlı olarak yazılımın kalite standardı arttırılıp müşteriye teslimatı yapılmaktadır. Bu aşama da yürütülen bu süreç, Şekil 1'de gösterilmiştir.

Şekil 1.*Çevik Yazılım Geliştirme*

2.2. Kanbanın Tanımı ve İlkeleri

Çevik yöntemlerin bir alt kümesi olan kanban, yazılım süreçlerini daha düzenli, verimli ve görselleştirilebilir hale getiren bir yaklaşım sunmaktadır. Japoncadan türetilip görsel kart anlamı taşımaktadır. Çalışma yapısı: To do: yapılacak, in progress: devam ediyor ve done: tamamlandı olacak şekildedir. Bu şekilde sütunlara ayrılma sebebi yapılan işin her aşamasını takip etmektir. Böylelikle sistemde iş sürecini yavaşlatan, sistemi tıkayan noktaların tespit edilmesiyle ortadan kaldırılmasını hedeflemektedir. Yapılan bu değişiklikler süreci iyileştirmeyi hedefleyip daha verimli hale gelmesini sağlamaktadır (Dorca et al., 2016; Fowler et al., 2001; Muris, 2010). Kanban aynı anda çok fazla iş üzerinde çalışmayı önlemek amacıyla çalışmaya sınır getirmekte bu da sonuç itibariyle ekibin tek iş üzerine odaklanmasını ve performansını arttırmayı hedeflemektedir (Ikonen et al., 2011; Moran, 2014). Bu süreç Şekil 2'de gösterilmiştir.



Şekil 2. *Sağlık Sektörü İçin Örnek Kanban Board*

2.3. Kanban Avantajları

Kanban iş takibi, hızlı adapte olma, iyileştirme yapma, erken hata tespiti gibi birçok imkan sağlamaktadır.

- ***İş Akışının Görselleştirilmesi:*** Kanban iş sürecinin takibinin kolaylaştırılması için görselleştirme tablosu (kanban board) sunmaktadır.

- ***Güncel ve Hızlı Adaptasyon:*** Kanban, iş süreci boyunca müşteri isteklerinin sürekli değiştiği durumlarda hızlı bir şekilde adapte olmayı sağlayarak projeyi sürekli güncel tutmaktadır.

- ***Sürekli Takip ve İyileştirme (Kaizen):*** Kanban iş sürecini, takip ederek gerektiği durumlarda iyileştirme yapmakta ve sürekli güncel kalmasını sağlamaktadır.

- ***Verimlilik:*** Kanban görselleştirme tablosunda mevcut iş bölümü devam ederken yeni bir iş gelmesi engellenerek, aynı anda birçok iş üzerinde çalışma engellenmektedir.

- ***Hızlı Geri Bildirim ve Hataların Erken Tespiti:*** Kanban, müşteri ile sürekli geri bildirimde bulunarak hataların erken tespit edilmesini sağlanmaktadır.

- ***Farklı Sektörlere Uygulanabilirlik****:* Kanban yazılım geliştirme dışında sağlık, üretim, finans gibi birçok farklı sektörde kullanılabilmektedir (Bouchereau, 2016; Brkljač et al., 2013; Gencer & Kayacan, 2017; Junior & Godinho Filho, 2010; Muris, 2010)**.**

2.4. Kanban Dezavantajları

Kanbanın birçok avantajının yanı sıra dezavantajları da bulunmaktadır.

- ***Yetersiz Gereksinim Anlatımı:*** Kanbanda, ilk aşamada gereksinimler yeterince net bir şekilde tanımlanmadığı için ilerleyen süreçlerde işlerin önceliklendirilmesi ve doğru bir şekilde yönlendirilmesi zordur.

- ***Sınırlı Planlama:*** Kanbanda, projeye başlarken veya süreç boyunca ayrıntılı bir planlama yapılması, daha çok anlık iş akışına odaklanıldığından zordur.

- ***Ekipte İletişim Eksikliği:*** Kanbanda, ekip çalışanları farklı iş bölümlerinde bulunduğundan dolayı iletişim eksikliği yaşanabilmektedir (Alaidaros et al., 2021; Junior & Godinho Filho, 2010).

3. SAĞLIK SEKTÖRÜNDE KANBAN UYGULAMALARI

Yazılım geliştirme süreçleri Şekil 3'te gösterildiği gibi finans, eğitim, oyun, e-ticaret, üretim, lojistik, sağlık gibi birçok farklı sektörde kullanılmaktadır (Khalfan et al., 2008)**.**

Bu kitap bölümünde, yazılım geliştirme süreçlerinin sağlık sektörü üzerindeki etkileri ve uygulamaları detaylı bir şekilde incelenmiştir. Sağlık sektörü, yazılım geliştirme açısından diğer sektörlerden daha karmaşıktır. Bunun sebebi insan hayatının göz önünde bulundurularak sağlık verilerinin daha hassas ve doğru işlenmesinin gerekliliğidir. Verilerin korunması, doğru tahminlenip sonuçlandırılması oldukça titiz bir yaklaşım gerektirmektedir (Sunden & Hammarberg, 2014). Bunun uygulanmasında da yazılım geliştirme süreçleri aktif rol almaktadır.

Şekil 3. *Yazılım Geliştirme Süreçleri Kullanılan Sektörler*

Kanban, bir süreç boyunca ilerleyen işleri görselleştirerek, sürece hız ve akış kazandırmaktadır (Junior & Godinho Filho, 2010). Sağlık hizmetlerinde malzeme yönetimi, stok yöntemi, lojistik süreç, hasta verilerini analiz etme gibi birçok alanda kullanılmaktadır. Bunun yanı sıra, kanban sistemi, hastanelerde ilaç ve tıbbi malzeme stoklarının optimize edilmesi, gereksiz bilgi birikiminin önlenmesi ve zamanında tedarik süreçlerinin sağlanmasında etkin bir rol oynamaktadır. Bu sistem, çalışanların iş yükünü azaltmayı hedeflerken, sağlık kaynaklarının daha verimli ve doğru kullanılmasını sağlamaktadır (Heikkilä et al., 2016). Örneğin, hasta kayıtlarının dijital ortamda düzenlenmesi, ilaçlar ve sağlık malzemelerinin takibi, ameliyat, anestezi gibi operasyon malzemelerinin zamanında hazırlanması ve eczane stoklarının daha düzenli takip edilebilmesi gibi birçok alanda kullanılmaktadır. Bu durumla beraber oluşan bu sistematik yapıyla hastalar daha kısa sürede tedavi edilebilecek, tıbbi hatalar minimum seviyeye indirgenerek sağlıkta hizmet kalitesi attırılmış olacaktır (Lanza-León et al., 2021).

Kanban kullanılarak ekiplerin mevcut durumları, ilerlemeleri, yapacakları işler daha düzenli takip edilebileceğinden, oluşabilecek hatalar önceden tespit edilip oluşabilecek krizler engellenebilecektir. Bununla da sağlık sistemi daha pratik ve düzgün bir şekilde kullanılabilecektir (Eleftheria, 2017).

3.1. Kanban Uygulamalarının Sağlık Sektörüne Katkıları

Kanban, sağlık sektöründe iş akışlarını düzenleyerek ekiplerin daha verimli çalışmasını sağlamaktadır. Sağlık ekiplerinin bir kanban şeması üzerine yapacakları ilerleme süreciyle iş bölümü daha kısa zamanda ve daha partik hale gelebilecektir (Eleftheria, 2017). Böylelikle hastalara erişim, hastalıklarına yönelik tedavi önerileri daha kolay şekilde sunulabilecektir.

- ***Malzeme Yönetimi:*** Malzeme yönetiminde, stok düzeyleri daha kolay takip edilebileceğinden depolama da kolaylık ve kolay erişim sağlanır.

- ***Hasta Hizmetlerinin Takibi:*** Kanban hasta hizmetlerinde takibi kolaylaştırır. Hastaya dair bilgilerin tutulduğu bir sistemde karmaşıklığı önleyerek kolay izleme yöntemi sunar.

- ***Hızlı Geri Bildirim ve Zaman Tasarrufu:*** Hastaların ve sağlık ekiplerinin kısa sürede bilgiye erişimi, erişimin kolaylığı gibi faktörlerle zaman tasarrufu sağlanmaktadır.

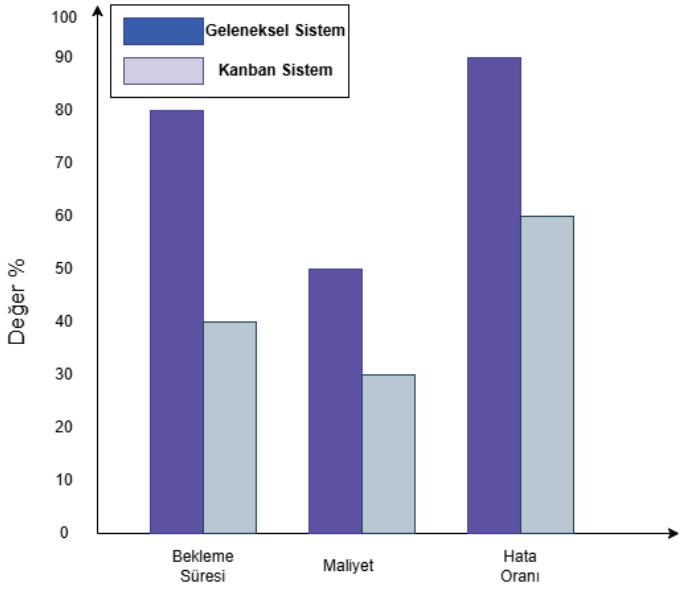
- ***Hasta Memnuniyeti:*** Ekiplerin hastalara kısa sürede dönüş sağlamaları, doğru takip süreci yürütmeleri, hastalarla yakından iletişim içinde olmaları hastaları memnun etmektedir.

- ***Sektöre Uyum ve Esneklik:*** Sağlık sektörü sürekli değişen ve güncel tutulması gereken bir alandır. Kanbanın değişken ve uyumlu olması bu sürece etki etmekte ve yeni güncellemelere adapte olmayı hızlandırmaktadır**.** (Bhosekar et al., 2021; Khanna et al., 2016; Lanza-León et al., 2021; Oliveira et al., 2021; Rahman et al., 2021)

Kanbanın sağlık sektöründe olumlu etkisinin yanı sıra olumsuz etkileri; dezavantajları da bulunmaktadır (Al-Baik & Miller, 2015). Bunlar arasında sağlık ekiplerinin yeterince bilgiye erişememesi ve sürece hâkim olamaması, yeni sisteme karşı korku durumu, farkındalık eksikliği gibi birçok sorun ortaya çıkmaktadır (Heikkilä et al., 2016)**.** Bu sorunlarla beraber ekipler arasında anlaşmazlık, sürecin yavaş ilerlemesi, hata oranının artması gibi faktörler sektörde görülebilmektedir (de Oliveira Tavares, 2022)**.**

Kanban sistemi kullanılmadan önce geleneksel yöntemler yaygın bir şekilde kullanılmaktaydı ve günümüzde de birçok alanda kullanılmaya devam etmektedir (Aguilar-Escobar et al., 2015)**.** Şekil 4'te, kanban sistemi ile geleneksel yöntemlerin temel düzeyde bir karşılaştırması su-

nulmuştur. Grafik, kanban sistemiyle sağlanabilecek olası yenilikleri ve iyileştirmeleri temsili olarak görselleştirmektedir. Kullanılan değerler, yöntemin daha iyi tasvir edilebilmesi için oluşturulmuştur.



Şekil 4. *Kanban Sistemi ile Sağlanan İyileştirmeler*

3.2. Sağlık Sektöründe Kanban Örnek Senaryoları

Kanbanın sağlık sektöründe kullanılmasının daha açıklayıcı şekilde ifade edilebilmesi için aşağıda, bir hastane eczanesinde kanban sisteminin uygulanmasıyla ilgili basit bir senaryo yer almaktadır. Bu senaryo, kanbanın sağlık sektöründe nasıl etkili bir çözüm sunduğunu ve süreç iyileştirmelerine nasıl katkı sağladığını göstermek amacıyla hazırlanmıştır.

3.2.1. Hastane Acil Servis Senaryosu

Bu senaryo da kanban, hastanenin acil servisinde kullanılmaktadır. Kanban tahtası üzerindeki sütunlara:

- Yeni Gelen Hastalar
- Tıbbi İnceleme Bekliyor
- Tedavi Ediliyor
- Taburcu Edildi

gibi bilgiler eklenmiştir. Bu sistem sayesinde hastanede bulunan sağlık çalışanları hangi hastaya hangi tedavi uygulanmalı, hangisi uygulanmakta, hangisi tamamlandı gibi tüm süreci anlık olarak kontrol altında tutabilmektedir (Aguilar-Escobar et al., 2015; Ferrão & Canedo, 2015; Heikkilä et al., 2016; Mouaky et al., 2019).

3.2.2. Eczane Stok Senaryosu

Bu senaryoda kanban, eczanede kullanılmaktadır. Eczanede ilaçların düzenlenmesi gerekmektedir. İlaçların sipariş miktarı, rafta bekleme süresi, son kullanma süresi geçenlerin tespiti, imha edilmesi, Fazla satılan ilaçların belirlenmesi gibi durumlar söz konusudur. Eczanede ilaçların depolanması ve düzeninin takip edilebilmesi için görsel takip şeması (kanban) tasarlandı. Kanban tahtası üzerindeki sütunlara:

- En Çok Tüketilenler
- Orta Düzeyde Tüketilenler
- Az Tüketilenler

gibi bilgiler eklenmiştir. Bu sistem sayesinde eczane de bulunan çalışanlar tarafından; örneğin ağrı kesiciler en çok tüketilenler arasında sınır olarak 50 tane belirlendi. Kanban kartı üzerinde takibi yapılan ilaçlar arasında en çok tüketilenler grubu 50'nin altına düştüğü zaman eczacı tarafından yeni ilaç teminatı sağlanır. Böylelikle acil durumlarda oluşabilecek ilaç eksikliğinin önüne geçilmiş oldu. Diğer bir durumda az tüketilen ilaçlar sürekli sipariş verilmek yerine gerektiği zamanda tedarik edilebildi. Bu süreçle beraber eczane sisteminde ilaç takibi daha hızlı ve doğru bir şekilde yapılabildi. Bununla beraber maliyet düşürülürken, zamandan kar edildi ve hastalar için hizmet kalitesi oranı arttırılmış oldu (Borges, 2019; Lanza-León et al., 2021; Prado-Prado et al., 2020).

3.2.3. Ameliyathanede Malzeme Yönetimi Senaryosu

Bu senaryo da kanban, hastanede gerçekleştirilen ameliyathane sürecinde kullanılmaktadır. Ameliyat sürecinden önce malzeme yönetiminin nasıl yapılması gerektiğini göstermektedir.

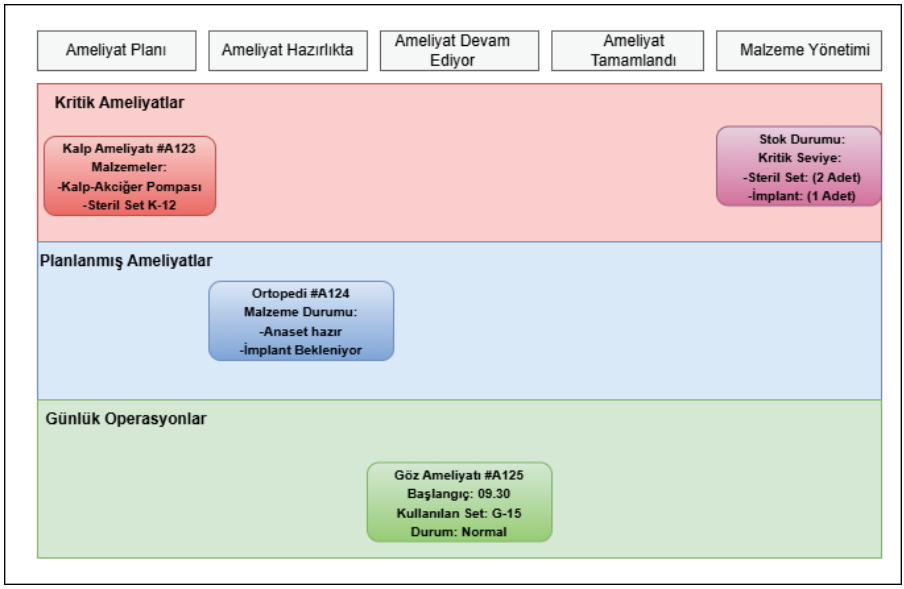
Kanban tahtası üzerindeki sütunlara:

- Ameliyat Planı
- Ameliyat Hazırlıkta
- Ameliyat Devam Ediyor

- Ameliyat Tamamlandı
- Malzeme Yönetimi

Bu sistem sayesinde, kanban tahtasında süreç şu şekilde ilerlemektedir: İlk olarak hastane çalışanları tarafından ameliyat planı hazırlanır ve gerekli malzemeler listelenmektedir. Daha sonra ameliyat işlemi gerçekleştirilmekte ve devam ediyor olarak işaretlenmektedir. Ameliyat işlemi gerçekleştirildikten sonra, kullanılan malzemeler ve kullanılmayanlar ayıklanmaktadır. Böylece kullanılan malzemelerin hijyeni sağlanırken, kullanılmayan malzemeler ayrı tutulduğu için boşa atılması engellenmiş olmakta ve tasarruf sağlanmaktadır.

Kanban tahtası sayesinde, süreç daha izlenebilir ve kolaylaştırılmıştır. Hastane çalışanları, ameliyat planlarını, hazırlıklarını, devam eden ameliyatları ve tamamlanan ameliyatları anlık olarak takip edebilmektedirler. Ayrıca, malzeme yönetimi sütunu sayesinde, stok durumu ve malzeme kullanımı hakkında gerçek zamanlı bilgi alabilmektedir. Bu sayede, malzeme yetersizliği veya fazlalığı gibi sorunlar önceden tespit edilebilmekte ve gerekli önlemler zamanında alınabilmektedir (Castro et al., 2020; Permanajati & Puspita, 2024; Persona et al., 2008). Şekil 5'te, kanban sistemi ile kurulan ameliyathane malzeme yönetim senaryosu tablo şeklinde verilmiştir.



Şekil 5. *Kanban Sistemi Örnek Senaryo Gösterimi*

4. SONUÇ VE ÇIKTILAR

Sonuç olarak, bu çalışmada sağlık sektöründe çevik yazılım geliştirme süreçlerinin kanban metodolojisi üzerinden uygulanabilirliği ele alınmıştır. Sağlık sektörünün hızla değişen yeniliklere uyum sağlaması için kullanılan kanban teknolojisi ilkeleriyle, avantaj ve dezavantajlarıyla ele alınmıştır. Kanbanla birlikte görselleştirme, süreç iyileştirme ve hızlı geri bildirim mekanizmalarının, sağlık çalışanlarının iş yükünü azaltmada ve hasta memnuniyetini artırmada önemli katkılarından bahsedilmiştir.

Kanbanın başarılı bir şekilde uygulandığı örnek senaryoları, sistematik bir yaklaşımla sağlık sektöründe süreçlerin nasıl daha verimli hale getirilebileceğini göstermiştir. Bununla birlikte, yeni sistemlere adaptasyon sürecinde bilgi eksikliği, ekipler arasında iletişim problemleri gibi dezavantajlar da ele alınmıştır.

Sonuç olarak, bu çalışma, sağlık sektöründe yazılım geliştirme süreçlerine kanban metodolojisiyle yenilikçi bir bakış açısı kazandırmayı hedeflemektedir. Gelecekteki çalışmalar, kanban uygulamalarının diğer sağlık alanlarına genişletilmesi ve bu süreçlerin daha kapsamlı analizlerle değerlendirilmesi için bir temel oluşturması hedeflenmektedir. Sağlık sektöründe daha etkin ve esnek yazılım çözümleri geliştirmek isteyen proje yöneticileri ve yazılım ekipleri için bu çalışma, rehber niteliğinde bir kaynak sunmaktadır.

KAYNAKLAR

Aguilar-Escobar, V. G., Bourque, S., & Godino-Gallego, N. (2015). Hospital kanban system implementation: Evaluating satisfaction of nursing personnel. *Investigaciones Europeas de Dirección y Economía de la Empresa*, 21(3), 101-110, https://doi.org/10.1016/j.iedee.2014.12.001.

Alaidaros, H., Omar, M., & Romli, R. (2021). The state of the art of agile kanban method: challenges and opportunities. *Independent Journal of Management & Production*, *12*(8), 2535–2550,https://doi.org/10.14807/ijmp.v12i8.1482.

Al-Baik, O., & Miller, J. (2015). The kanban approach, between agility and leanness: a systematic review. *Empirical Software Engineering*, *20*, 1861–1897, https://doi.org/10.1007/s10664-014-9340-x.

Beck, K., Beedle, M., Van Bennekum, A., Cockburn, A., Cunningham, W., Fowler, M., Grenning, J., Highsmith, J., Hunt, A., Jeffries, R., & others. (2001). *The agile manifesto.*

Bhosekar, A., Işk, T., Ekşioğlu, S., Gilstrap, K., & Allen, R. (2021). Simulation-optimization of automated material handling systems in a healthcare facility. *IISE Transactions on Healthcare Systems Engineering*, *11*(4), 316–337,https://doi.org/10.1080/24725579.2021.1882622.

Borges, G. A. and T. G. and R. M. and P.-S. A. (2019). Lean implementation in healthcare supply chain: a scoping review. *Journal of Health Organization and Management*, *33*, 304–322, https://doi.org/10.1108/JHOM-06-2018-0176.

Bouchereau, F. (2016). *Kaizen Kanban: A Visual Facilitation Approach to Create Prioritized Project Pipelines*. Quality Press.

Brkljač, M., Stanković, J. M., & Gajić, S. B. (2013). Gaining a competitive advantage by integration of marketing and logistics. *Ist Logistics International Conference*, 28–30.

Campanelli, A. S., & Parreiras, F. S. (2015). Agile methods tailoring–A systematic literature review. *Journal of Systems and Software*, *110*, 85–100,https://doi.org/10.1016/j.jss.2015.08.035.

Castro, C., Pereira, T., Sá, J. C., & Santos, G. (2020). Logistics reorganization and management of the ambulatory pharmacy of a local health unit in Portugal. *Evaluation and Program Planning*, *80*, 101801,https://doi.org/10.1016/j.evalprogplan.2020.101801.

Cockburn, A., & Highsmith, J. (2001). Agile software development, the people factor. *Computer*, *34*(11), 131–133,https://doi.org/10.1109/2.963450 .

Cohen, D., Lindvall, M., & Costa, P. (2004). An introduction to agile methods. *Adv. Comput.*, *62*(03), 1–66.

De Oliveira Tavares, M. I. H. (2022). *Lean Healthcare: Implementation of a Lean System in a Community Pharmacy-Case Study*. ISCTE-Instituto Universitario de Lisboa (Portugal).

Dorca, V., Munteanu, R., Popescu, S., Chioreanu, A., & Peleskei, C. (2016). Agile approach with Kanban in information security risk management. *2016 IEEE International Conference on Automation, Quality and Testing, Robotics (AQTR)*, 1–6, https://doi.org/10.1109/AQTR.2016.7501278.

Eleftheria, M. (2017). Kanban System Design for Hospital Pharmacy–Case study. *Journal of Statistical Science and Application*, *5*(1–2), 30–38, https://doi.org/10.17265/2328-224X/2017.0102.003.

Ferrão, S. É. R., & Canedo, E. D. (2015). A study of the applicability of an agile methodology scrum allied to the Kanban method. *2015 10th Iberian Conference on Information Systems and Technologies (CISTI)*, 1–6, https://doi.org/10.1109/CISTI.2015.7170382.

Fowler, M., Highsmith, J., & others. (2001). The agile manifesto. *Software Development*, *9*(8), 28–35.

Gencer, C., & Kayacan, A. (2017). Yazlm proje yönetimi: Şelale modeli ve çevik yöntemlerin karşlaştrlmas. *Bilişim Teknolojileri Dergisi*, *10*(3), 335–352,https://doi.org/10.17671/gazibtd.331054.

Heikkilä, V. T., Paasivaara, M., & Lassenius, C. (2016). Teaching university students Kanban with a collaborative board game. *Proceedings of the 38th International Conference on Software Engineering Companion*, 471–480,https://doi.org/10.1145/2889160.2889201.

Highsmith, J., & Cockburn, A. (2001). Agile software development: The business of innovation. *Computer*, *34*(9), 120–127.

Ikonen, M., Pirinen, E., Fagerholm, F., Kettunen, P., & Abrahamsson, P. (2011). On the impact of Kanban on software project work: An empirical case study investigation. *2011 16th IEEE International Conference on Engineering of Complex Computer Systems*, 305–314, https://doi.org/10.1109/ICECCS.2011.37.

Junior, M. L., & Godinho Filho, M. (2010). Variations of the kanban system: Literature review and classification. *International Journal of Production Economics*, *125*(1), 13–21,https://doi.org/10.1016/j.ijpe.2010.01.009.

Khalfan, M., McDermott, P., Oyegoke, A. S., Dickinson, M. T., Li, X., & Neilson, D. (2008). Application of kanban in the UK construction industry by public sector clients. *Proceedings of the 16th Annual Conference of the International Group for Lean Construction*, 347–359.

Khanna, S., Sier, D., Boyle, J., & Zeitz, K. (2016). Discharge timeliness and its impact on hospital crowding and emergency department flow performance. *Emergency Medicine Australasia*, *28*(2), 164–170, https://doi.org/10.1111/1742-6723.12543.

Kokol, P. (2022). Agile software development in healthcare: a synthetic scoping review. *Applied Sciences*, *12*(19), 9462,https://doi.org/10.3390/app12199462.

Lanza-León, P., Sanchez-Ruiz, L., & Cantarero-Prieto, D. (2021). Kanban system applications in healthcare services: A literature review. *The International*

Journal of Health Planning and Management, *36*(6), 2062–2078, https://doi.org/10.1002/hpm.3276.

Lei, H., Ganjeizadeh, F., Jayachandran, P. K., & Ozcan, P. (2017). A statistical analysis of the effects of Scrum and Kanban on software development projects. *Robotics and Computer-Integrated Manufacturing*, *43*, 59–67,https://doi.org/10.1016/j.rcim.2015.12.001.

Manifesto, A. (2001). *Manifesto for agile software development*.

Moran, A. (2014). Agile software development. In *Agile Risk Management* (pp. 1–16). Springer.

Mouaky, M., Berrado, A., & Benabbou, L. (2019). Using a kanban system for multi-echelon inventory management: the case of pharmaceutical supply chains. *International Journal of Logistics Systems and Management*, *32*(3–4), 496–519,https://doi.org/10.1504/IJLSM.2019.098333.

Muris, L. J. (2010). Variations of the kanban system: Literature review and classification. *International Journal of Production Economics*, *125*(1), 13–21,https://doi.org/10.1016/j.ijpe.2010.01.009.

Oliveira, I. S. de, Lima, E. de F. A., Silva, R. I. C. da Figueiredo, K. C., Dias, I. C. B., & Primo, C. C. (2021). Software development for emergency bed management. *Revista Brasileira de Enfermagem*, *74*(Suppl 5), e20200055.

Papalexi, M., Bamford, D., & Dehe, B. (2016). A case study of kanban implementation within the pharmaceutical supply chain. *International Journal of Logistics Research and Applications*, *19*(4), 239–255, https://doi.org/10.1080/13675567.2015.1075478.

Permanajati, A., & Puspita, P. M. (2024). Using Kanban to Improve Indonesian Health Coverage Patient Task Id at Astrini Hospital Wonogiri. *International Journal of Medical Science and Clinical Research Studies*, *4*(01), 103–106.

Persona, A., Battini, D., & Rafele, C. (2008). Hospital efficiency management: the just-in-time and Kanban technique. *International Journal of Healthcare Technology and Management*, *9*(4), 373–391,https://doi.org/10.1504/IJHTM.2008.019674.

Prado-Prado, J. C., Garc\'\ia-Arca, J., Fernández-González, A. J., & Mosteiro-Añón, M. (2020). Increasing competitiveness through the implementation of lean management in healthcare. *International Journal of Environmental Research and Public Health*, *17*(14), 4981, https://doi.org/10.3390/ijerph17144981.

Rahman, M., Das, S., Tazim, M. Z., Rana, M., Tuhin, R. A., & Das, A. K. (2021). State of the Art of ICT based Telemedicine and E-health Services in Bangladesh. *2021 6th International Conference on Inventive Computation Technologies (ICICT)*, 1266–1272, https://doi.org/10.1109/ICICT50816.2021.9358778.

Reifer, D. J. (2002). How good are agile methods? *IEEE Software*, *19*(4), 16–18, https://doi.org/10.1109/MS.2002.1020280.

Stainier, L., & De Jaegere, T. (n.d.). *Study of the Agile methods efficiency to mitigate the risk of project failure: the case of consulting firms.*

Sunden, J., & Hammarberg, M. (2014). *Kanban in Action*. Simon and Schuster.

Zayat, W., & Senvar, O. (2020). Framework study for agile software development via scrum and Kanban. *International Journal of Innovation and Technology Management*, *17*(04), 2030002,https://doi.org/10.1142/S0219877020300025.

YENİLENEBİLİR ENERJİ SİSTEMLERİNDE YAPAY SİNİR AĞLARI UYGULAMALARI

Mete ÖZBALTAN[1]

1 Doç. Dr.; İzmir Bakırçay Üniversitesi Mühendislik ve Mimarlık Fakültesi Elektrik-Elektronik Mühendisliği Bölümü. mete.ozbaltan@bakircay.edu.tr ORCID No: 0000-0002-3215-6363

GİRİŞ

Nüfus artışı, şehirlere göçlerin artması ve büyüyen sanayiler gibi sebeplerle sürekli olarak enerji ihtiyacı artmaktadır. Enerji ihtiyacının hızlı bir şekilde artmasının yanı sıra enerji kaynaklarının kullanımı yetersiz kalarak enerji açığına sebebiyet vermektedir. Günümüzde enerji üretimi sınırlı ve dünya üzerinde homojen olarak dağılmamış geleneksel kaynaklara dayandığı için çevre üzerinde olumsuz etkilere sahiptir. Başta petrol, kömür ve doğal gaz olmak üzere fosil yakıtların kullanımı karbon salınımını arttırmakta ve küresel ısınmayla birlikte global sorunlara neden olmaktadır. Bu sebeplerle yenilenebilir enerji kaynaklarının kullanımı oldukça önem taşımaktadır.

Yenilenebilir enerji sistemleri, rüzgar, güneş, hidro, biyogaz ve yakıt hücreleri gibi kaynakları çoğu zaman hibrit bir şekilde kullanır. Yenilenebilir enerji sistemleri, hem daha güvenilir hem de çevre dostu oldukları için sürdürülebilir bir şekilde enerji ihtiyacını karşılayabilir. Her ne kadar yenilenebilir enerji sistemleri rüzgar hızı ve güneş ışınımı gibi çevresel koşullara bağlı olsa da, literatürde sunulan yaklaşımlar ile çevre dostu ve sürdürülebilir enerji arzını sağlama potansiyeline sahiptir.

Günümüzde enerji ihtiyacını karşılayan kaynaklar, çoğunlukla sera etkisi, küresel ısınma ve asit yağmurları gibi olumsuz çevresel etkilere sahip kaynaklardan sağlanmaktadır. Başta çevre üzerindeki olumsuz etkilerin kaldırılması ve ülkelerin enerji üretim kapasitelerinin arttırılmasında yenilenebilir enerji kaynaklarının kullanılması veya mevcut enerji sistemlerine entegrasyonu dikkate alınması gereken bir durumdur. Literatürde yapılan çalışmalar, yenilenebilir enerji kaynaklarının entegrasyonunda verimliliği artırmak ve geleneksel enerji kaynakları yerine sürdürülebilir ve güvenilir kaynaklar olması açısından ele alır ve bu alanda yapılan çalışmalar ivmelenerek devam etmektedir.

Yenilenebilir enerji kaynakları ile ilgili yapılan çalışmalar ele alınırken, sadece teknik açıdan değerlendirilmekle kalmaz; çünkü doğrudan sosyo-politik bir konu olduğu için sosyo-ekonomik ve teknik meseleler bir arada değerlendirilir. Yani yenilenebilir enerji sistemlerinin entegrasyonu sadece teknik bir çalışma değil, ayrıca çevresel ve toplumsal bir sorumluluk olarak ele alınır.

Yenilenebilir enerji kaynaklarının entegrasyonu ile ilgili yapılan çalışmalar genellikle enerji akış tahmini ve verimlilik değerlendirmelerini konu alır ve bu süreç genellikle karmaşık algoritmaları içeren diferansiyel denklemler ve programlama kodlarını kullanır. Hesaplama karmaşıklığı büyük zaman ve emek gerektirmektedir. Ancak bu geleneksel karmaşık

hesaplamalar ve yöntemler yerine yapay sinir ağları bu süreci çok daha büyük bir hassasiyetle, güvenilir bir şekilde yapabilmektedir.

Yapay zeka, basit olarak bir makinenin insan gibi düşünmesi ve aynı şekilde karar verebilme mekanizmasını temsil eden bir hesaplama yöntemidir (Kalogirou, 2001). Yapay zeka, her ne kadar insan düşüncesini taklit etmeye çalışsa da bu, gerçek bir düşünceyi tam olarak karşılamaz. Bilgisayarlar, insanlardan daha iyi performans gösterebilir; ancak bilgisayarlar ne kadar işlem kapasitesi ile donatılırsa donatılsın, yalnızca işlemleri algoritmalar vasıtasıyla seri bir şekilde yapabilme yeteneğine sahiptir. Bunun yanında, insan beyni paralel işleme yeteneğine sahip olup oldukça karmaşık süreçleri içermektedir. Yapay zeka genel olarak yapay sinir ağları ve uzman sistemler olarak ikiye ayrılabilir. Uzman sistemler, mevcut verileri yorumlayarak alternatifler arasında seçim yaparak karar verme sürecini sağlar. Uzman sistemler, daha önceden belirlenmiş kural tabanlı çıkarımlarla geleneksel programların algoritma tabanından çıkarak daha hızlı bir şekilde karar alma süreçlerinde bulunmalarını sağlar; ancak yine de insan düşüncesine yaklaşamazlar. Yapay sinir ağları ise birbirine bağlı küçük işlem hücrelerinden oluşarak bilgileri bu hücreler arasında ileterek çalışır. Her bir bağlantının iki değeri vardır: biri giriş, diğeri ağırlıktır; çıktı ise toplam değerin bir fonksiyonu olarak ifade edilir. Yapay sinir ağları, bir program olarak çalışmazlar; mevcut veri setleri ile eğitilerek kendilerine sunulan örüntüyü öğrenirler ve eğitim süreci tamamlandıktan sonra yeni örüntüler veya veriler için tahmin veya sınıflandırmalar sağlayabilirler.

Bu çalışma, yenilenebilir enerji sistemleri ve yapay sinir ağları hakkında temel bilgi edinmek isteyen araştırmacılar için önemli bir referans kaynağı olarak kullanılabilir. Çalışmada, yenilenebilir enerji sistemlerinde yapay sinir ağlarının kullanımına yönelik yapılan çalışmalar ele alınarak analiz edilmiş ve yeni sonuçlar çıkarılmıştır. Yapay sinir ağları kapsamında, yenilenebilir enerji kaynaklarının kullanımına yönelik en önemli teknik sistemler tanımlanmakta ve bunlar için önemli hesaplama ve simülasyon yöntemleri tanıtılmaktadır. Bu çalışmanın amacı, yenilenebilir enerji problemlerinde sinir ağlarının çeşitli uygulamalarını sunmaktır. Bu, yapay sinir ağlarının yenilenebilir enerji sistemleri tahmini ve modellemesi için araçlar olarak kapasitesini gösterecektir.

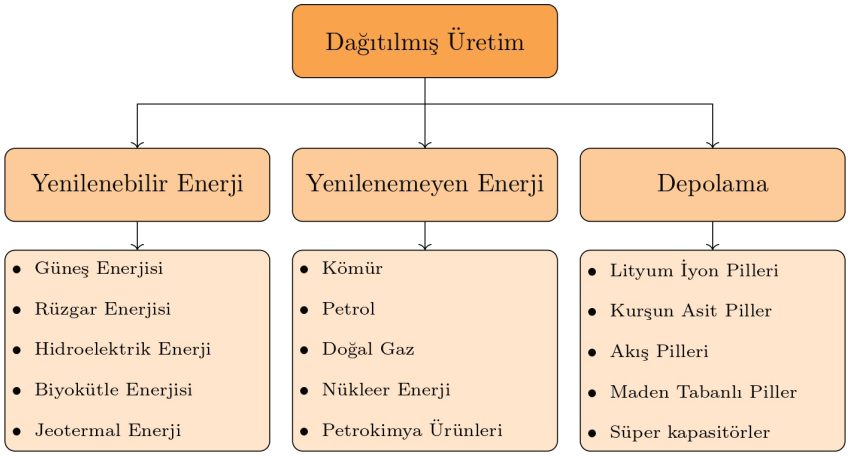
Çalışmanın geri kalan kısmı şu şekilde ilerlemektedir: Bölüm 2'de, yenilenebilir enerji kaynakları ile önemli temel bilgiler sunulmaktadır. Bölüm 3'de yenilenebilir enerji sistemlerinde yapay sinir ağları uygulamaları verilmektedir. Bölüm 4'de ise bu çalışmada işlenen bütün çalışmaların kapsamlı bir analizini araştırmacılar için sunulmaktadır. Son olarak Bölüm 5'de bu çalışmanın sonuç kısmı ele alınmıştır.

YENİLENEBİLİR ENERJİ KAYNAKLARI

Enerji kavramı çeşitli bağlamlarda kullanılabilmektedir; bu çalışmada yenilenebilir enerji sistemleri alanında değerlendirilmektedir (Quaschning, 2014). Enerji, bir sistemin dış etkiler yaratma yeteneği olarak tanımlanırken, iş ise bu enerjinin değişimi olarak gösterilir ve güçte birim zamanda yapılan iş olarak tanımlanabilir. Enerji, mekanik, potansiyel, kinetik, termal, manyetik, elektriksel, radyasyon, nükleer ve kimyasal gibi çeşitli biçimlerde var olabilir. Enerjinin korunumu ilkesi gereği enerji yok edilemez, var da edilemez; enerji sabit olarak kalmakta, ancak bir enerji türü diğerine dönüşebilir. Örneğin, içten yanmalı bir motorda benzin kimyasal enerjiyi kinetik enerjiye çevirerek motorların hareketine dönüştürmektedir. Durma durumunda ise enerji ısı olarak çevreye verilmekte, ancak bu durum genellikle enerji kaybı olarak adlandırılmaktadır. Yani yüksek kaliteli enerji, düşük kaliteli enerjiye dönüştürülmekte veya başka bir deyişle, verimli bir şekilde enerji kullanılamamaktadır.

Sanayi Devrimi ile birlikte odun, rüzgar ve hidro güç gibi enerji kaynakları yerine, o güne kadar henüz kullanımı artmamış olan kömür ve petrol gibi enerji kaynaklarına yönelmeye başlandı. Buhar motoru teknolojisiyle ilk olarak kömür ana enerji kaynağı haline dönüştü, ardından hala günümüzde de kullanılan içten yanmalı motorların keşfiyle petrol en önemli enerji kaynağı haline geldi. Son yüzyıl içerisinde de doğal gaz ve nükleer enerji kaynaklarıyla birlikte, günümüzde enerji üretiminin büyük bir bölümü fosil yakıtlardan karşılanmaktadır. Ancak dünya ülkelerinde sanayinin büyümesi enerji ihtiyacını hızla artırmaktadır ve şu anda dahi enerji arzı, sınırlı fosil kaynaklardan veya nükleer santraller için kullanılan uranyum rezervlerinden karşılanamamaktadır. Mevcut rezervler, bir müddet daha fosil yakıtları ve nükleer enerjiyi desteklese de, yakın gelecekte yetersiz kalacağı açık bir şekilde görülmektedir.

Çevresel etkiler üzerinde baktığımızda, fosil yakıtların ve nükleer enerjinin kullanımı büyük sorunlara sebep olmaktadır. Fosil kaynakların kullanımından kaynaklı karbondioksit, su buharı ve metan, güneş ışınlarını tutarak sera etkisi yaratır. Fosil yakıt kullanımı, sera gazı emisyonlarının ana kaynağıdır; bu kaynakların yanı sıra kimya endüstrisi, ormanların yok edilmesi ve tarım da önemli etkilere sahiptir. Bugün küresel sıcaklık artışlarının ana sebebi olarak insan kaynaklı emisyonlar kabul edilmektedir ve bu artış başka sonuçlar da doğurmaktadır. İklim değişikliğinin belirgin göstergeleri arasında sıcaklık artışları, buzul erimeleri ve deniz seviyesinin yükselmesi bulunmaktadır.



Şekil 1: *Dağıtılmış Üretim Sistemleri*

Fosil yakıtların kullanımı önemli ölçüde azaltılabilse bile, nükleer enerjinin uzun vadede alternatif olmadığı görülmektedir ve gelecekteki enerji ihtiyacının güvence altına alınması gerekmektedir. Burada üzerinde durulması gereken bir nokta, enerji verimliliğini artırarak karbondioksit emisyonlarının azaltılmasıdır. Yukarıda bahsedilen sebepler doğrultusunda enerji ihtiyacının fosil yakıtlar ve nükleer enerji harici kaynaklardan, yani yenilenebilir enerji kaynaklarından elde edilmesi zorunluluğu ortaya çıkmaktadır. Bu geçiş sürecinin, mevcut konvansiyonel enerji rezervlerinin tükenmeden gerçekleştirilmesi gerekmektedir. Şekil 1' dağıtılmış üretim sistemleri; yenilenebilir enerji kaynakları, yenilenemeyen enerji kaynakları ve enerji depolama çözümleri ile birlikte genel yapısını göstermektedir.

Günümüzde sürdürülebilirlik ve çevre dostu enerji sistemleri arasındaki artan talebi karşılamak için yenilenebilir enerji kaynakları en iyi seçenek olarak görünmektedir. Yenilenebilir enerji kaynaklarını, insanlık için tükenmez, sonsuz enerji kaynakları olarak düşünebiliriz. Yenilenebilir enerji türleri üç ana alana ayrılabilir: güneş enerjisi, rüzgar enerjisi ve jeotermal enerji; sırasıyla yıl başına enerji miktarı 4 milyon, 100 bin ve 1 milyon PJ'dir.

Rüzgar ve yağmurda depolanan enerjiler gibi diğer yenilenebilir enerji kaynakları da enerji arzını karşılamak için kullanılabilir. Teorik olarak, yenilenebilir enerji kaynakları tüm küresel enerji arzını karşılayabilme potansiyeline sahiptir; ancak bu geçiş sürecinde karşılaşılacak çeşitli problemler mevcuttur. Şu anda mevcut enerji ihtiyacı büyük ölçüde fosil enerji kaynaklarına dayanmaktadır ve merkezi enerji santrallerinin eko-

nomik bir şekilde yenilenebilir enerji sistemlerine dönüştürülmesi gerekmektedir. Ayrıca, yenilenebilir enerji kaynakları ile ilgili sorunlardan biri de stabil olmamalarıdır. Sadece yenilenebilir enerji kaynaklarından enerji üretimi yapmakla kalmayıp, aynı zamanda büyük enerji depolama sistemleri, küresel enerji taşımacılığı veya talebin mevcut enerjiye uyum sağlamasıyla bu süreçler gerçekleştirilebilir.

Bu çalışma kapsamında, başlıca yenilenebilir enerji kaynaklarında yapay sinir ağları uygulamalarıyla mevcut problemlerin nasıl ele alındığı vurgulanmakta ve kapsamlı bir analiz ile sonuçlar sunulmaktadır.

YENİLENEBİLİR ENERJİ SİSTEMLERİNDE ANN UYGULAMALARI

Yapay sinir ağları, insan beynindeki nöronlardan ilham alarak karmaşık veriler arasındaki ilişkileri öğrenen, katmanlı yapılarla çalışan bir makine öğrenmesi alt dalıdır. Girdi, gizli ve çıkış katmanlarından oluşan bu yapılar, matematik, mühendislik, tıp ve finans gibi çeşitli alanlarda kullanılır. Sinapslarda olduğu gibi, nöronlar arasındaki bilgi akışı ağırlıklar aracılığıyla modellenir ve bu ağırlıklar öğrenme sürecinde güncellenir. Üç ana türü olan ileri beslemeli (FFNN), tekrarlı (RNN) ve evrişimli sinir ağları (CNN) farklı uygulama alanlarında öne çıkar. Yapay sinir ağları, özellikle belirsiz ve eksik veri setleri ile başa çıkmada etkilidir ve karmaşık sistemlerde anlamlı sonuçlar üretme yeteneğine sahiptir. Bu bölümde de yenilebilir enerji sistemlerinde yapay sinir ağları uygulamaları tanıtılmaktadır.

SOLAR ENERJİ SİSTEMLERİNDE ANN UYGULMALARI

Solar Enerji Sistemlerinde FFNN Uygulamaları

(Mellit vd., 2010) meteorolojik zaman serilerinin (güneş ışınımı, hava sıcaklığı, nem ve rüzgar hızı) tahmini için Evrimsel Polinom Sinir Ağı (EPNN) kullanılmıştır. Tahmin, geçmiş verilerin kullanılarak gelecekteki değerleri tahmin edilmesi üzerine kurulmuştur. Cezayir'de beş yıl boyunca toplanan veriler kullanılarak yapılan tahminler, ölçülen ve tahmin edilen değerler arasında 0,9821 ile 0,9923 arasında bir korelasyon katsayısı sağlamış ve ortalama göreceli hata %15,4'ü geçmemiştir. EPNN, diğer yöntemler olan wavenet ve ANFIS ile karşılaştırıldığında daha doğru sonuçlar vermiştir. Tahmin edilen veriler, fotovoltaik sistemlerin boyutlandırılması ve enerji çıkışının tahmini için de kullanılmıştır. (Fentis vd., 2017) enerji şebekesi yönetimi için fotovoltaik tahminler sağlayan çevrimdışı bir model sunulmuş ve intra-saat güneş enerjisi tahmini için iki modelin performansı değerlendirilmiştir. LS-SVR ve Levenberg-Marquardt algoritması ile eğitilmiş FFNN kullanılarak oluş-

turulan modeller, çeşitli performans göstergeleri ile karşılaştırılmıştır. En iyi model, %15,23 RRMSE değeri ile iyi sonuçlar elde etmiştir. (Alblawi vd., 2022) PV hücre sıcaklığı ve çıkış gücünü tahmin etmek için bir ALO optimizatörü ve ANN içeren bir karışık optimizasyon tekniği geliştirilmiştir. Optimizasyon, ANN'nin gizli katman nöron sayısı, ağırlıklar ve biasların belirlenmesine yönelik yapılmıştır. Suudi Arabistan'daki bir PV istasyonundan elde edilen verilerle, MFFNN modellerinin doğruluğu değerlendirilmiştir. NRMSE değerleri, DC güç tahmini için MFFNN-GA, MFFNN-MVO ve MFFNN-ALO modelleri için sırasıyla 2.781E-3, 7.11E-4 ve 6.08E-4 olarak belirlenmiştir. (Rodriguez vd., 2022) fosil yakıt eksikliği ve iklim değişikliği bağlamında güneş fotovoltaik üretiminin önemine dikkat çekmiştir. Güneş ışınımı ve dış sıcaklık, fotovoltaik jeneratörlerin enerji üretiminde kritik rol oynamaktadır. Ancak, meteorolojik parametrelerin belirsizliği, çıkış gücünde dalgalanmalara yol açmaktadır. Bu bağlamda, dalgacık tabanlı zaman-frekans analizi ile derin öğrenme sinir ağları kullanılarak, gelecek 10 dakikada güneş ışınımının tahmin edilmesi hedeflenmiştir. Sonuçlar, önerilen modelin %4'ten daha düşük bir sapma ile yüksek doğruluk sağladığını göstermiştir. (Khatib vd., 2012) saatlik güneş ışınımı tahmini için yapay sinir ağı tabanlı yaklaşımları değerlendirmiştir. Dört ANN topolojisi incelenmiştir ve sonuçlar, GRNN yönteminin diğerlerine kıyasla en yüksek doğruluk sağladığını göstermektedir. FFNN ve CFNN kabul edilebilir sonuçlar verse de, kötü ışınım koşullarında performansları düşmektedir. ELMNN ise en kötü sonuçları vermiştir. GRNN'nin tüm iklim koşullarında kullanılması, yüksek doğruluk ve etkinlik sunmaktadır.

Solar Enerji Sistemlerinde RNN Uygulamaları

(Jebli vd., 2021) RNN, LSTM ve GRU gibi derin öğrenme teknikleri kullanarak 2016-2018 yılları arasında Errachidia bölgesine ait gerçek meteorolojik verilerle güneş enerjisi tahminleri yapmıştır. Modellerin etkinliği, hata metrikleriyle değerlendirilmiştir. Sonuçlar, RNN ve LSTM'nin, uzun vadeli bağımlılıkları koruma yetenekleri sayesinde GRU'dan daha iyi performans gösterdiğini ortaya koymuştur. Bu durum, güvenilir şebeke yönetimi ve fotovoltaik sistemin maliyet etkinliğini artırmayı amaçlamaktadır. (Beigi vd., 2022) ANN yönteminin fotovoltaik enerji sistemlerinin (PVPS) güneş enerjisi çıktısını tahmin etme yeteneğini değerlendirmeyi amaçlamaktadır. Önemli meteorolojik faktörler giriş olarak kullanılarak bir tekrarlayan sinir ağı (RNN) oluşturulmuştur. Eğitilen RNN, eğitim dışındaki günlerde enerji çıktısını tahmin etmiştir. Performans sonuçları, test verileri için 0.97774 regresyon değeri, 0.0248 MJ RMSE ve ortalama 0.538 MJ çıkış gücü ile yeterli tahmin doğruluğu sağlamıştır. (Massaoudi vd., 2019) güneş enerjisi üretimindeki hava parametrelerinin değişkenliğinin, enerji yönetiminde doğru PV güç tah-

mininin önemini artırdığını vurgulamaktadır. Nonlinear Autoregressive Exogenous (NARX) modeli, uzun vadeli tahminler için umut verici bir yöntemdir ancak kaybolan gradyan problemi nedeniyle performansı sınırlıdır. Bu sorunu aşmak için, NARX ve Long Short-Term Memory (LSTM) ağlarını birleştiren bir hibrit teknik önerilmektedir. Bu yeni yaklaşım, Avustralya'da bir yıl boyunca PV güç tahmini için uygulanmış ve doğruluğu artırarak diğer karşılaştırmalı modellere göre daha iyi sonuçlar elde edilmiştir. (Raju vd., 2020) gelecek nesillerin enerjiye erişimi için yenilenebilir kaynakların önemini vurgulamakta ve güneş enerjisinin uzun vadeli bir çözüm sunduğunu belirtmektedir. Güneş enerjisi sistemlerinin meteorolojik koşullara bağlı olarak yüksek değişkenlik gösterdiği için, güvenilir tahmin bilgilerinin geliştirilmesi gerekmektedir. Makalede, bir çatı güneş enerjisi santralinden elde edilen canlı ölçüm verilerine dayanan zaman serisi modelleri incelenmiştir. Dört yıl boyunca toplanan verilerle, LSTM modeli kullanılarak eğitim yapılmış ve sonuçlar Keras ve TensorFlow ile elde edilmiştir. Elde edilen ortalama kare hata (MSE) değeri 0.015 olarak bulunmuştur. (Park vd., 2021) enerji verimliliğini artırmak amacıyla derin öğrenme ve büyük veri teknolojilerinin bina enerji yönetim sistemlerinde kullanımını incelemektedir. Fotovoltaik (PV) enerji üretimini tahmin etmek için tekrarlayan sinir ağı (RNN) kullanılmıştır. Önceki hava durumu ve PV enerji üretim verileri ile gelecekteki üretim tahmin edilmiştir. Model oluşturma sürecinde normalizasyon, veri sınıflandırması ve katman ayarları gibi optimizasyon işlemleri gerçekleştirilmiştir. Tek katmanlı ve üç katmanlı modeller karşılaştırılmış ve kök ortalama kare hata katsayısı (Cv(RMSE)) tek katman için %13.8, çok katmanlı model için %13.2 olarak bulunmuştur. Çok katmanlı modelin hata oranı hafifçe daha düşük çıkmıştır. Bu çalışmalar, yenilenebilir enerji kaynaklarından enerji üretimini ve talebini tahmin ederek stabil bir enerji tedarik sistemi kurulmasına katkı sağlayabilir.

Solar Enerji Sistemlerinde CNN Uygulamaları

(Ishaq vd., 2022) güneş enerjisinin rastgele doğasının mevcut enerji sistemlerini zorlaştırabileceğini belirtmektedir. Kısa vadeli güneş enerjisi tahmini için, CNN DeepESN ağı ve PCA yöntemi önerilmiştir. Avustralya'nın Alice Springs şehrinden elde edilen verilerle yapılan deneyler, önerilen sistemin MAE, MAPE ve RMSE değerlerini sırasıyla 0.0381, 3.3313 ve 0.3101 olarak bulmuştur. Bu sonuçlar, modelin enerji tahminindeki etkinliğini göstermektedir. (Al-Ali vd., 2023) yüksek enerji tüketimine sahip yeni şehirlerin gelişiminde yeşil enerjinin önemini vurgulayarak güneş enerjisinin şebekeye entegrasyonu için doğru tahminlerin gerekliliğini ele almaktadır. Güneş enerjisi üretimini tahmin etmek amacıyla Konvolüsyonel Sinir Ağı (CNN) ve Uzun Kısa Vadeli Bellek (LSTM) ağı kombinasyonu kullanılmıştır. Girdi verilerinin analizi için kümeleme

tekniği ve kendiliğinden oluşturulan haritalar ile önemli özellikler seçilmiştir. Fingrid açık veri setiyle eğitilen hibrit model, diğer modellere göre en yüksek doğruluk oranını elde etmiş ve bu modelin güneş enerjisinin şebekelere entegrasyonunu kolaylaştıran güvenilir bir tahmin aracı olabileceği sonucuna varılmıştır. (Anu Shalini ve Sri Revathi, 2023) güneş ve rüzgar enerjisi sistemlerinden beslenen modifiye edilmiş Z kaynak dönüştürücü, iki yönlü dönüştürücü ve batarya depolama sistemi içeren bir şebeke bağlı hibrit sistemin tasarımını sunmaktadır. Sürekli DC güç sağlamak için yüksek kazançlı bir switched Z kaynak dönüştürücü ve hibrit derin öğrenme (HDL) algoritması olarak CNN-BiLSTM modeli önerilmiştir. 1.5 kW'lık hibrit sistem MATLAB/SIMULINK yazılımında tasarlanmış ve laboratuvar prototipi geliştirilmiştir. Deneysel sonuçlar, SVPWM ile ANN kontrolörünün %2.2'lik THD değeri sunduğunu ve bu değerin IEEE 519 standardı içinde olduğunu göstermektedir. Bu, ANN-SVPWM yönteminin diğer kontrolörlerden daha az harmonik akım enjekte ettiğini ortaya koymaktadır. (Alharkan vd., 2023) güneş enerjisinin enerji sistemine entegrasyonunun ekonomik ve çevresel faydalarını incelemektedir. Güneş enerjisi üretimindeki kesintili ve rastgelelik, mevcut enerji sisteminde zorluklar yaratmaktadır. Doğru enerji üretim tahminleri yapmak için, derin öğrenmeye dayalı bir çift akışlı konvolüsyonel sinir ağı (CNN) ve uzun kısa vadeli bellek (LSTM) ağı ile birlikte DSCLANet ağı önerilmiştir. CNN mekansal kalıpları, LSTM ise zamansal özellikleri öğrenir. Özellik vektörleri birleştirildikten sonra optimal özellikler seçilmektedir. Sonuç olarak, DSCLANet, DKASC Alice Spring veri setinde hata oranlarını 0.0136 MSE, 0.0304 MAE ve 0.0458 RMSE değerine kadar düşürmüştür. (Lim vd., 2022) fotovoltaik (PV) teknolojisinin önemini ve çevresel faktörlerin enerji üretimine etkisini ele almaktadır. PV sistemlerinin enerji üretimi, güneş radyasyonu, sıcaklık ve diğer değişkenlere bağlı olarak değişkenlik göstermektedir. Bu nedenle, PV enerji üretiminin doğru tahmin edilmesi büyük bir ihtiyaçtır. Önerilen model, konvolüsyonel sinir ağı (CNN) ve uzun kısa vadeli bellek (LSTM) kombinasyonunu kullanarak hava koşullarını sınıflandırmakta ve enerji üretim kalıplarını öğrenmektedir. Model, Kore'nin Busan şehrindeki bir güç santralinin verileri ile eğitilmiş ve test edilmiştir. Güneşli günlerde %4.58, bulutlu günlerde %7.06'lık ortalama mutlak yüzdelik hata elde edilmiştir. Sonuçlar, önerilen modelin enerji üretim kalıplarındaki anlık değişikliklere hassas tahminler yapabileceğini ve PV santrali operasyonlarını optimize etmeye yardımcı olabileceğini göstermektedir.

RÜZGAR GÜCÜ TABANLI ENERJİ SİSTEMLERİNDE ANN UYGULMALARI

Rüzgar Gücü Tabanlı Enerji Sistemlerinde FFNN Uygulmaları

(Zafar vd., 2021) yenilenebilir enerji kaynaklarının kesintili doğasının güç tahminini zorlaştırdığını belirtmektedir. Hibrit PV/Rüzgar enerji sistemlerinin kısa vadeli güç tahmini için AOS optimizasyon algoritmalarıyla eğitilen bir ileri beslemeli sinir ağı (FNN) önermektedir. AOS-FNN, gri kurt optimizasyonu, barnakle eşleşme optimizasyonu ve balina optimizasyon algoritmalarıyla karşılaştırıldığında daha düşük test ve eğitim hataları ile daha az işlem süresi sunmaktadır. Sonuçlar, AOS-FNN'nin değişken çevresel koşullar altında hibrit sistemin güç tahmininde etkili olduğunu göstermektedir. (Lawan vd., 2017) Malezya'nın Sarawak bölgesindeki rüzgar enerjisi potansiyelini yer istasyonu verileri ve tahmin modelleri ile incelemektedir. Ölçüm yapılmayan alanlarda rüzgar hızını tahmin etmek için bir topografik ileri beslemeli sinir ağı (T-FFNN) önerilmiştir. Model, dokuz meteorolojik ve coğrafi parametre kullanarak %3.4 MAPE ve 0.91 korelasyon ile etkili sonuçlar elde etmiştir. Rüzgar hızı dağılımında Gamma ve Weibull modelleri diğerlerine göre daha iyi performans sergilemiştir. Rüzgar gücü yoğunluğu sınıf 1 seviyesinde bulunmuş, yıllık enerji çıktısı (AEO) değerleri ise 5800–13,622 kWh/yıl arasında değişiklik göstermiştir. Sonuçlar, küçük ölçekli rüzgar enerjisi kullanımının mümkün olduğunu göstermektedir. (Mansoor vd., 2022) rüzgar enerjisi dönüşüm sistemlerinin (WECS) güç şebekesine entegrasyonunun rüzgar gücü üretimindeki belirsizliklere yol açtığını vurgulamaktadır. Rüzgarın doğası, hava koşulları ve rüzgar hızının üretilen güce etkisi, şebeke voltajı ve harmonikler üzerinde etkili olmaktadır. Stabil bir şebeke için, mevcut elektrik gücünün gerçek zamanlı tahmin edilmesi gerekmektedir. Bu amaçla, stokastik optimizasyon temelli Yapay Sinir Ağı (ANN) eğitimi önerilmektedir. Önerilen yöntem, mevsimsel vaka çalışmaları ile tanınmış tekniklerle karşılaştırıldığında daha iyi tahmin performansı göstermiştir. SChoANN, kış ve yaz mevsimlerinde sırasıyla %94.87 ve %97.18 daha düşük eğitim hatası ile %96.42 ve %83.64 daha düşük test hatası elde etmiştir. (Dhibi vd., 2022) rüzgar enerjisinin yenilenebilir enerji üretimindeki önemini ve rüzgar enerjisi dönüşüm (WEC) sistemlerinin araştırmalardaki merkez konumunu vurgulamaktadır. Arıza tespiti ve tanısı (FDD), WEC güvenliği için kritik bir rol oynamaktadır. Son yıllarda, sinir ağları arıza tanısında etkili sonuçlar sunarken, topluluk öğrenme (EL) teknikleri de dikkat çekmektedir. Bu çalışmada, bagging, boosting ve rastgele alt alan kombinasyon tekniklerini kullanan bir sinir ağları temelli topluluk sınıflayıcı geliştirilmekte ve doğrulanmaktadır. Ayrıca, bu yöntemin geliştirilmiş bir uzantısı sunulmakta ve önerilen tekniklerin diğer yöntemlerle karşılaştırılmasıyla avantajları

gösterilmektedir. (Bhaskar ve Singh, 2012) artan rüzgar enerjisi penetrasyonu ile enerji sistemlerinde doğru rüzgar gücü tahmininin önemini vurgulamaktadır. Sayısal hava tahmini (NWP) girdileri kullanmadan, iki aşamalı bir istatistik temelli rüzgar gücü tahmin yöntemi önerilmektedir. Birinci aşamada, rüzgar serisinin dalgacık ayrıştırması yapılmakta ve uyarlamalı dalgacık sinir ağı (AWNN) kullanılarak rüzgar hızı 30 saat ileriye tahmin edilmektedir. İkinci aşamada ise, ileri beslemeli sinir ağı (FFNN) ile rüzgar hızı rüzgar gücü tahminine dönüştürülmektedir. Önerilen yöntemin etkinliği, PER ve NR benchmark modelleri ile karşılaştırılmış ve sonuçlar önerilen modelin daha başarılı olduğunu göstermiştir.

Rüzgar Gücü Tabanlı Enerji Sistemlerinde RNN Uygulmaları

(Paramasivan, 2021) rüzgar enerjisi tahmininde derin öğrenmenin önemini ve Tekrarlayan Sinir Ağları (RNN) modellerinin kritik analizini sunmaktadır. RNN ve varyantları (LSTM, GRU, İki Yönlü RNN) mevsimsel değişim ve belirsizlikleri etkili bir şekilde yönetirken, zaman bağımlılıklarını yakalamakta başarılıdır. Derleme, rüzgar enerjisi tahmininde kullanılan RNN modellerini, veri kaynaklarını ve performanslarını hata ölçütleriyle incelemekte, derin öğrenmeye dayalı RNN'lerin geleneksel tekniklere göre daha iyi performans gösterdiğini ortaya koymaktadır. (Srivastava vd., 2020) 21. yüzyılda enerji sektörünün ekonomi üzerindeki etkisini ve yenilenebilir enerjinin (özellikle rüzgar enerjisinin) artan önemini vurgulamaktadır. Artan nüfus ve teknolojik gelişmeler, elektrik talebini yükseltmektedir. Özel enerji şirketleri, rekabetçi pazarda hayatta kalmak için gelecekteki talebi doğru bir şekilde tahmin etmek istemektedir. Mevcut tahmin yöntemleri, hem lineer (ARIMA gibi) hem de non-lineer (sinir ağları gibi) modelleri içermektedir. Bu çalışma, rüzgar hızı verilerini kullanarak rüzgar enerjisi üretimini tahmin etmek için RNN, GBM ve LSTM tabanlı üç sinir ağı modelini değerlendirip, en iyi performansı gösteren modeli belirlemeye odaklanmaktadır. (Mansouri vd., 2022) rüzgar enerji dönüşüm (WEC) sistemlerinde arıza tespiti ve tanısı (FDD) için geliştirilmiş Tekrarlayan Sinir Ağı (RNN) tekniklerini sunmaktadır. Mevcut RNN uygulamalarının sınırlamalarını aşmak amacıyla, eğitim süresini ve karmaşıklığı azaltan bir azaltılmış RNN modeli geliştirilmiştir. Bu model, Hiyerarşik K-ortalama kümeleme kullanarak eğitim verilerinden daha az gözlem çıkarır. Ayrıca, farklı WEC sistem çalışma modlarını ayırt etmek için iki aralık değerli veri tekniği önerilmektedir. Bu teknikler, uzun süreli işlemlerde arıza tanısı dayanıklılığını artırırken, %98'den fazla doğrulukla etkili bir performans sergilemektedir. (Shabbir vd., 2019) rüzgar enerjisi tahmininin zorlukları ele almakta ve Tekrarlayan Sinir Ağı (RNN) tabanlı bir algoritma kullanılarak Estonya'da rüzgar kaynaklarından enerji üretiminin üç gün öncesine yönelik tahminleri yapmaktadır. Önerilen RNN algoritması, Estonya enerji

düzenleme otoritesinin algoritması ile karşılaştırıldığında daha düşük RMSE değeri elde etmiş ve daha iyi tahmin sonuçları sağlamıştır. (Kisvari vd., 2021) rüzgar enerjisi tahmininin önemini vurgulamakta ve rüzgarın yüksek değişkenliğini ele almak için yenilikçi bir veri odaklı yaklaşım sunmaktadır. Gated Recurrent Unit (GRU) adlı derin öğrenme modeli, Long Short-term Memory (LSTM) ile karşılaştırılmıştır. Modelde, rüzgar hızı, jeneratör ve dişli kutusu sıcaklığı gibi on iki özellik kullanılmıştır. Sonuçlar, önerilen yaklaşımın yüksek doğruluk sağlarken daha düşük hesaplama maliyetleri sunduğunu ve GRU'nun tüm testlerde LSTM'yi geride bıraktığını göstermektedir.

Rüzgar Gücü Tabanlı Enerji Sistemlerinde CNN Uygulmaları

(Wu vd., 2021) büyük ölçekli rüzgar enerjisi entegrasyonunun dalgalanma ve kesintilerinin enerji sisteminin istikrarını tehdit ettiğini vurgulamakta ve rüzgar gücü tahmininin önemini ele almaktadır. Önerilen mekansal-zamansal korelasyon modeli (STCM), konvolüsyonel sinir ağları ve uzun kısa süreli hafıza (CNN-LSTM) kullanarak ultra-kısa süreli rüzgar gücü tahmini yapmaktadır. Model, farklı yerlerdeki meteorolojik verileri yeniden yapılandırarak girdi olarak kullanmakta ve CNN, mekansal özellikleri çıkarırken, LSTM zamansal ilişkileri analiz etmektedir. Sonuçlar, STCM'nin geleneksel modellere göre daha doğru tahminler sunduğunu göstermektedir. (Zhang vd., 2021) rüzgar gücü tahmininin enerji üretim planları ve sistem güvenliği için önemli olduğunu vurgulamaktadır. Rüzgar gücü, rüzgar hızı, yönü, sıcaklık ve nem gibi birçok faktörden etkilenmektedir. Yalnızca tarihsel verilerle uzun vadeli tahmin yapmak zor olduğundan, bu makalede konvolüsyonel sinir ağı (CNN) ve uzun kısa süreli bellek (LSTM) kombinasyonu ile bir tahmin yöntemi önerilmektedir. CNN, rüzgar gücü ve etkileyen faktörlerden özellikler çıkarırken, LSTM bu verileri kullanarak tahmin yapmaktadır. Önerilen yöntem, belirli bir rüzgar çiftliğinde test edilmiş ve sonuçlar diğer yöntemlerle karşılaştırıldığında etkili ve uygulanabilir olduğu kanıtlanmıştır. (Wang vd., 2022) rüzgar gücü tahmininin enerji arz ve talebini dengelemek için belirsizliği azalttığını vurgulamaktadır. Tahmin doğruluğunu artırmak amacıyla, konvolüsyonel sinir ağı ve Informer modelini kullanarak bir ortalama rüzgar gücü tahmin yöntemi önerilmektedir. 2-B konvolüsyonel sinir ağı, ek zaman özellikleri ve trend bilgisi çıkarmak için kullanılırken, Informer modeli uzun dizilimli girdi tahmininin doğruluğunu artırmak için uygulanmıştır. Model, Çin'deki bir rüzgar çiftliği verileri ile test edilmiş ve sonuçlar, önerilen yöntemlerin tahmin doğruluğunu etkili bir şekilde artırdığını göstermiştir. (Malakouti vd., 2022) rüzgar enerjisinin emisyon hedefleri ve iklim değişikliği ile uyumu açısından önemine vurgu yaparak, rüzgar gücü tahmini için güvenilir bir yaklaşımın kritik olduğunu belirtmektedir. Rüzgar gücü

serilerinin durağan olmayan doğası, klasik tahmin yöntemlerinin doğruluğunu zorlaştırmakta ve sistemde riskler yaratmaktadır. Çalışmada, rüzgar türbini gücünü tahmin etmek için makine öğrenimi teknikleri, özellikle CNN-LSTM yöntemi önerilmektedir. Sonuçlar, en düşük ortalama kare hata değerinin CNN-LSTM yöntemine ait olduğunu ve bu yöntemin daha yüksek doğruluk sağladığını göstermektedir. Topluluk yöntemi ise yüksek hızıyla birlikte kabul edilebilir sonuçlar sunmaktadır. (Huang vd., 2022) kısa dönem rüzgar gücü tahmini için BiLSTM-CNN-WGAN-GP (LCWGAN-GP) tabanlı bir model önermektedir. Model, variational mode decomposition (VMD) algoritmasıyla orijinal rüzgar enerjisi verilerini doğal mod fonksiyonlarına ayırarak başlar. Bu ayrım, verilerin dinamik davranışlarını ortaya çıkarır. BiLSTM, rüzgar gücünün çıktı dağılımını elde etmek için kullanılırken, CNN ayrımcı model olarak görev yapar. İki model arasında minimum-maksimum değerleri oluşturularak tahmin doğruluğu artırılır. Gansu Eyaleti'ndeki Jiuquan şehrine ait gerçek verilerle yapılan testler, önerilen yönteminin diğer tahmin algoritmalarına göre daha iyi performans sergilediğini göstermektedir.

DİĞER YENİLENEBİLİR ENERJİ SİSTEMLERİNDE ANN UYGULAMALARI

Diğer Yenilenebilir Enerji Sistemlerinde FFNN Uygulamaları

(Rahman vd., 2021) zaman serisi tahmininde makine öğrenimi ve yapay sinir ağları kullanımını incelemektedir. Fosil yakıtların tükenmesi ve kırsal bölgelerin alternatif enerjiye ihtiyaç duyması, hibrit yenilenebilir enerji sistemlerini önemli kılmaktadır. Yenilenebilir enerji kaynaklarının belirsizliği, ANN yöntemlerinin bu alanda kullanılmasını desteklemektedir. Çalışma, güneş, rüzgar ve hidroelektrik enerji tahminlerinde MLP, RNN, CNN ve LSTM gibi ANN mimarilerini ele almakta ve bu modellerin kısa vadeli tahminler yapma yeteneklerini vurgulamaktadır. (Kumar vd., 2022) hidroelektrik enerjinin yenilenebilir ve öngörülebilir bir kaynak olduğunu belirtmekte ve enerji tarifelerinin sabit ile değişken ücretlerden oluştuğunu açıklamaktadır. Yapay sinir ağları kullanarak, UJVN Ltd.'ye ait 12 hidroelektrik santralinin 2011-20 yılları arasındaki enerji üretim hedeflerini tahmin etmek için bir yaklaşım sunulmuştur. Elde edilen tahminlerin doğruluk katsayısı %99'un üzerindedir. (Chinas-Palacios vd., 2021) tarım ve orman atıklarının sentez gazı üretiminde kullanılmasını ve bu gazın kırsal topluluklarda enerji üretiminde entegrasyonunu ele almaktadır. Değişken enerji talebi, gazlaştırma tesisi verimliliğini etkilerken, bir Biyokütle Gazlaştırma Tesisi için Parçacık Sürü Optimizasyonu (PSO) ile hibritleştirilmiş bir Yapay Sinir Ağı modeli geliştirilmiştir. Model, diğer geleneksel yöntemlerden %23.2 daha iyi performans göstererek gerekli biyokütle miktarını doğru bir şekilde

tahmin etmektedir. (Tesha ve Kichonge, 2015) yapay sinir ağı çok katmanlı algılayıcı (ANN-MLP) kullanarak biyokütle enerji tüketimini analiz etmek ve Tanzanya'da biyokütle tüketimini etkileyen demografik ve ekonomik göstergeleri belirlemektir. Üç model (Tanzanya kırsal, kentsel ve nüfus) oluşturulmuş ve ANN-MLP, 0.9972 istatistiksel korelasyon katsayısı ile umut verici sonuçlar vermiştir. Ayrıca, nüfus modelinin biyokütle tüketiminin analizi ve tahmininde diğer modellere göre daha iyi sonuçlar verdiği bulunmuştur. (Abrasaldo vd., 2024) güvenilir sensörler ve hesaplama gelişmeleri sayesinde jeotermal enerji endüstrisinde veri yoğun algoritmaların gerçek zamanlı karar verme için uygulanabilir hale geldiğini vurgulamaktadır. Sistematik inceleme, üst düzey jeotermal operasyonlarda veri analitiği uygulamalarını, kullanılan veri setlerini ve makine öğrenimi algoritmalarını incelemektedir. Dört veritabanından 830 yayın taranmış ve 63 makale seçilmiştir. Sonuçlar, makine öğreniminin tasarım optimizasyonu, performans izleme ve arıza tespiti gibi alanlarda kullanıldığını göstermektedir. Eğitim alan modellerin %95'i yapay sinir ağlarından oluşmakta olup, inceleme, özellik seçimi ve model değerlendirme gibi alanlarda daha fazla araştırma potansiyeli olduğunu ortaya koymaktadır. (Dikeh vd., 2022) yer altı sayısal modellerin uzun inşa ve çalışma süreleri nedeniyle enerji endüstrisinin proxy modellere yönelmesini ele almaktadır. Jeotermal bir rezervuar kullanarak, ileri beslemeli sinir ağı ve konvolüsyonel sinir ağı (CNN) gibi iki derin öğrenme algoritmasının proxy modelleme için uygunluğu değerlendirilmiştir. Sonuçlar, CNN'nin daha az hata ve hiperparametre ile daha iyi performans gösterdiğini, ancak ileri beslemeli ağın daha hızlı olduğunu ortaya koymuştur. Çalışma, benzer yaklaşımların petrol ve gaz rezervuar modellemesine uygulanabileceğini ve sinir ağlarının yer altı rezervuar modellemesi için uygun olduğunu göstermektedir.

Diğer Yenilenebilir Enerji Sistemlerinde RNN Uygulamaları

(Galvao Filho vd., 2020) hidroelektrik enerji üretimi için su akışını tahmin eden bir Long Short-Term Memory (LSTM) modeli önermektedir. Jirau Hidroelektrik Santrali'nden elde edilen verilerle geliştirilen model, günlük zaman adımlarıyla düşük tahmin hataları göstermiştir. Uzmanlar, sonuçların gerçek operasyonlarda kullanılabileceğini onaylamıştır. LSTM modeli, su akışını tahmin etmede etkili bir yöntem olarak değerlendirilmektedir. (Liao vd., 2019) hidroelektrik santralleri için arıza teşhisi amacıyla bir boyutlu evrişimsel sinir ağları (1-D CNN) ve GRU'dan oluşan bir sistem önermektedir. Ham titreşim verileri, veri segmentasyonu ile yeniden yapılandırılarak eğitim verimliliği artırılmakta ve model, farklı çalışma koşullarını dikkate alarak arıza kategorilerini belirlemektedir. Dört makine öğrenimi yöntemiyle doğrulanan bu sistem, pratik uygulamalarda başarılı bir şekilde kullanılmıştır. (Sharma vd., 2021) bi-

yolojik çeşitliliği etkilemeden biyokütle kaynaklarından enerji üretimini tahmin etmek amacıyla makine ve derin öğrenme algoritmalarını kullanmaktadır. Ayrıca, biyokütle enerji üretimini hesaplamak için çeşitli makine ve derin öğrenme yaklaşımları ile performans analizi için araçlar sunulmaktadır. (Sharma vd., 2022) biyokütle gazlaştırmasının ikincil gaz fazı reaksiyonları için 800-1000 °C sıcaklık aralığında bir tekrar eden sinir ağı (RNN) modeli geliştirmektedir. GRU kullanılarak, inert bir ortamda doğru tahminler sağlamak amacıyla detaylı bir kinetik şemadan indirgenmiş kompakt bir model referans olarak alınmıştır. Çeşitli biyokütle bileşimleri ve reaktör koşullarıyla geniş bir eğitim verisi seti oluşturulmuştur. Geliştirilen model, akışkan yatak reaktöründeki önemli reaktan ve ürünlerin zaman içindeki evrimini tahmin edebilmekte ve hesaplama maliyetini dört sıfır azaltmaktadır. (Li vd., 2024) jeotermal enerjinin karbon nötr geçişteki önemini vurgulayarak, üretim sıcaklıklarını tahmin etmek için ANN ve BiGRU kullanan hibrit bir model geliştirmektedir. 22 faktörü inceleyerek, ANN'in doğrusal olmayan etkileşimleri ve BiGRU'nun zaman içindeki değişimleri etkili bir şekilde yönetme kapasitesini ortaya koymuştur. BiGRU, üretim sıcaklığı tahmininde diğer geleneksel modellere göre daha başarılı olurken, tahmin belirsizliği RMSE ve MAE ile 0.15 içinde kalmaktadır. Bu çalışma, yenilenebilir enerji geçişine katkıda bulunacak yüksek hassasiyetli bir tahmin çerçevesi sunmaktadır. (Jiang vd., 2022) jeotermal rezervuarların enerji üretim tepkilerini tahmin etmek için bir CNN-RNN mimarisi geliştirmekte ve veri boşluklarını yönetmek için etiketleme şemasını içermektedir. Ayrıca, modelin uygulanmasına yönelik kapsamlı bir iş akışı sunmakta ve performansı çeşitli veri setleri ile değerlendirilmektedir.

Diğer Yenilenebilir Enerji Sistemlerinde CNN Uygulamaları

(Dao vd., 2024) hidro-türbin arıza teşhisi için Bayes optimizasyonu (BO), evrişimsel sinir ağları (CNN) ve uzun-kısa süreli bellek (LSTM) yöntemlerini birleştiren bir model önermektedir (BO–CNN-LSTM). CNN, arıza özelliklerini çıkartarak LSTM'ye iletirken, BO algoritması modelin hiperparametrelerini optimize etmektedir. Deney sonuçları, BO-CNN-LSTM modelinin sırasıyla %92.7, %98.4 ve %90.4 doğruluk oranları ile geleneksel modellere göre belirgin bir üstünlük sağladığını göstermektedir. Bu model, optimize edilmemiş CNN-LSTM modeline göre doğruluğu %5.5 ila %9.0 artırarak hidro-türbin arıza teşhisinde önemli bir katkı sunmaktadır. (Li vd., 2024) hidroelektrik ünitelerin verimliliğini ve arıza tespit doğruluğunu artırmak için Gramian angular summation field (GASF) ile geliştirilmiş Koati Optimizasyon Algoritması-Paralel Evrişimsel Sinir Ağı (ICOA-PCNN) entegrasyonunu içeren bir model önermektedir. Model, arıza tanımlama doğruluğunu artırmak için MSA ve SVM ile optimize edilmiştir. GASF, bir boyutlu zaman seri-

si sinyallerini iki boyutlu görüntülere dönüştürerek özellik çıkarımında kullanılmaktadır. Deneyler, modelin %100 doğruluk oranı elde ettiğini ve optimize edilmemiş modellere göre önemli bir üstünlük sağladığını göstermektedir. Bu araştırma, modern hidroelektrik üniteleri için arıza teşhisinde önemli bir katkı sunmaktadır. (Buratto vd., 2024) zaman serisi tahmin teknikleriyle biyokütle mevcudiyeti ve elektrik üretimini doğru tahmin etmek için dalgacık dönüşümü, evrişimsel sinir ağları (CNN) ve uzun-kısa süreli bellek (LSTM) yöntemlerini kullanmıştır. %0.0148 hata oranı ile umut verici sonuçlar elde edilmiştir. Ayrıca, model değerlendirme ve doğrulama stratejileri vurgulanmakta, hibrit bir yöntemle tahminlerin iyileştirilmesi ana katkı olarak belirtilmektedir. Gelecekteki araştırmalar, sürdürülebilir enerji üretiminde yenilikleri teşvik etmeyi amaçlamaktadır. (Shi vd., 2023) 2012-2022 yılları arasında yayımlanan 96 makaleyi inceleyerek yapay zekanın biyoyakıt sistemlerindeki uygulamalarını değerlendiriyor. Biyoyakıt sistemlerini üç ana alana biyoyakıt sistemleri, biyokütle materyalleri ve YZ teknikleri ayırarak, bu sistemlerin biyokütle hammaddesi tespiti, üretim ve enerji kullanımı aşamalarındaki sorunları çözmeyi amaçlıyor. Sonuçta, 44 YZ algoritması ve 11 veri seti belirlenmiş; Yapay Sinir Ağı ve SVM gibi yöntemler en sık kullanılanlar olarak öne çıkmıştır. (Zhu vd.., 2023) sıcak kuru kaya jeotermal enerjisini tahmin etmek için CNN, LSTM ve CNN-LSTM hibrid modeller kullanmaktadır. Elde edilen veriler, EGS çıkarımının dinamik ekonomik performansına ilişkin simülasyonlardan elde edilmiştir. CNN-LSTM modelinin, jeotermal enerji üretimini doğru ve stabil bir şekilde tahmin edebildiği ve diğer modellerden daha iyi performans gösterdiği bulunmuştur. (King vd., 2024) BHE'nin çıkış sıvı sıcaklığını tahmin etmek amacıyla Konvolüsyonel Sinir Ağı (CNN) ve Tekrarlayan Sinir Ağı (RNN) mimarilerini birleştiren bir hibrit model önermektedir. Model, girdi özelliklerini (giriş sıvısı, çevresel hava, yer altı sıcaklıkları) kullanarak etkili bir girdi-çıktı eşlemesi oluşturur. Sonuçlar, önerilen modelin geleneksel yöntemlere göre daha düşük hata oranlarıyla (RMSE: 0.818, MAE: 0.642, R^2: 98.75%) daha doğru tahminler sağladığını göstermektedir. Bu bulgular, modelin BHE sistemlerinin verimli çalışmasına ve sürdürülebilirliğine katkıda bulunabileceğini vurgulamaktadır.

TARTIŞMA VE DEĞERLENDİRME

Bu çalışma, yenilenebilir enerji sistemlerinin önemini ve yapay sinir ağlarının bu sistemlerdeki rolünü kapsamlı bir şekilde incelemiştir. Yenilenebilir enerji kaynaklarının entegrasyonu ve yapay sinir ağlarının kullanımı, enerji sektöründe önemli bir dönüşüm sağlamaktadır. Aşağıdaki tablolar, bu bağlamda elde edilen bulguların analizi ve değerlendirilmesine yardımcı olacaktır.

Tablo 1: *Yenilenebilir Enerji Kaynaklarının Çevresel Etkileri*

Enerji Kaynağı	Karbon Salınımı (ton CO2/kWh)	Sera Gazı Etkisi	Su Tüketimi (litre/kWh)	Diğer Çevresel Etkiler
Güneş	0.05	Düşük	100	Arazi kullanımı
Rüzgar	0.01	Çok düşük	0	Gürültü
Biyokütle	0.02	Düşük	200	Hava kirliliği
Fosil Yakıtlar	0.9	Yüksek	500	Su kirliliği

Tablo 1, çeşitli enerji kaynaklarının çevresel etkilerini göstermektedir. Yenilenebilir kaynaklar, fosil yakıtlar ile karşılaştırıldığında daha düşük karbon salınımı ve sera gazı etkisi sunmaktadır.

Tablo 2: *Yapay Sinir Ağları ve Geleneksel Yöntemlerin Karşılaştırılması*

Yöntem	Hassasiyet (%)	Hesaplama Süresi (dakika)	Veri Seti Büyüklüğü	Uygulama Alanları
Yapay Sinir Ağları	95-98	10-20	Büyük	Enerji tahmini, optimizasyon
Geleneksel Yöntemler	80-85	30-60	Küçük	Basit hesaplamalar

Tablo 2, yapay sinir ağlarının geleneksel yöntemlere göre sağladığı avantajları özetlemektedir. Yapay sinir ağları, yüksek hassasiyet ve daha kısa hesaplama süreleri ile dikkat çekmektedir.

Yenilenebilir enerji sistemleri, çevresel etkileri azaltma ve enerji arzını güvence altına alma potansiyeline sahiptir. Bu çalışma, yapay sinir ağlarının bu sistemlerin verimliliğini artırmadaki rolünü vurgulamaktadır. Yapay sinir ağları, karmaşık veri setlerini analiz edebilme yetenekleri sayesinde, enerji akış tahmini ve sistem optimizasyonu gibi konularda önemli katkılar sağlamaktadır.

Sonuç olarak, yenilenebilir enerji sistemlerinin entegrasyonu ve yapay sinir ağlarının kullanımı, çevresel sürdürülebilirliği artırmak ve enerji verimliliğini sağlamak için kritik bir önem taşımaktadır. Gelecekteki araştırmalar, bu alanın daha da derinlemesine incelenmesi ve yeni yöntemlerin geliştirilmesi için zemin oluşturacaktır. Bu, yenilenebilir enerji sistemlerinin daha verimli ve ekonomik hale gelmesine yardımcı olacaktır.

SONUÇ

Bu çalışma, günümüzde artan enerji ihtiyacını karşılamak üzere yenilenebilir enerji sistemlerinin önemini ve yapay sinir ağlarının bu sistemler içindeki rolünü kapsamlı bir şekilde ele almıştır. Nüfus artışı, sanayileşme ve şehirleşme gibi faktörler, enerji talebinin sürekli artmasına yol açmakta ve bu durum, fosil yakıtların çevresel etkileri ile birleştiğinde, sürdürülebilir enerji çözümlerinin gerekliliğini daha da vurgulamaktadır.

Yenilenebilir enerji kaynakları, çevre dostu alternatifler sunmakta ve fosil yakıtların olumsuz etkilerini azaltma potansiyeline sahiptir. Güneş, rüzgar, hidroelektrik, biyokütle ve jeotermal enerji gibi kaynaklar, gelecekte enerji arzını güvence altına alacak sürdürülebilir çözümler olarak öne çıkmaktadır. Bununla birlikte, bu kaynakların verimli bir şekilde entegrasyonu, enerji akış tahmini ve sistem optimizasyonu gibi karmaşık sorunlar içermektedir.

Yapay sinir ağları, bu bağlamda, enerji sistemleri için güçlü bir araç olarak değerlendirilmektedir. Geleneksel yöntemlerin zorluklarını aşmak için sağladıkları yüksek hassasiyet ve güvenilirlik, yenilenebilir enerji sistemlerinin performansını artırmak adına önemli bir katkı sunmaktadır. Bu çalışma, yapay sinir ağlarının enerji üretiminde, tahmininde ve optimizasyonunda nasıl kullanılabileceğini göstermekte ve bu alanda yapılacak gelecekteki çalışmalar için bir temel oluşturmaktadır.

Sonuç olarak, yenilenebilir enerji sistemlerinin entegrasyonu ve bu süreçte yapay sinir ağlarının kullanımı, enerji sektöründeki dönüşüm için kritik öneme sahiptir. Bu çalışma, araştırmacılar ve uygulayıcılar için yenilenebilir enerji sistemleri ve yapay zeka uygulamaları arasındaki ilişkiyi daha iyi anlamalarına yardımcı olmayı hedeflemektedir. Gelecekte, bu alandaki çalışmaların daha da derinlemesine incelenmesi, yenilenebilir enerji sistemlerinin daha verimli, sürdürülebilir ve ekonomik hale gelmesine katkıda bulunacaktır. Bu bağlamda, enerji verimliliğinin artırılması ve karbondioksit emisyonlarının azaltılması, çevresel sürdürülebilirliği sağlamak için hayati öneme sahiptir.

REFERANSLAR

Abrasaldo, P. M. B., Zarrouk, S. J., and Kempa-Liehr, A. W. (2024). A systematic review of data analytics applications in above-ground geothermal energy operations. Renewable and Sustainable Energy Reviews, 189:113998.

Al-Ali, E. M., Hajji, Y., Said, Y., Hleili, M., Alanzi, A. M., Laatar, A. H., and Atri, M. (2023). Solar energy production forecasting based on a hybrid cnn-lstm-transformer model. Mathematics, 11(3):676.

Alblawi, A., Said, T., Talaat, M., and Elkholy, M. (2022). Pv solar power forecasting based on hybrid mffnn-alo. In 2022 13th international conference on electrical engineering (ICEENG), pages 52–56. IEEE.

Alharkan, H., Habib, S., and Islam, M. (2023). Solar power prediction using dual stream cnn-lstm architecture. Sensors, 23(2):945.

Anu Shalini, T. and Sri Revathi, B. (2023). Hybrid power generation forecasting using cnn based bilstm method for renewable energy systems. Automatika: ˇcasopis za automatiku, mjerenje, elektroniku, raˇcunarstvo i komunikacije, 64(1):127–144.

Beigi, M., Beigi Harchegani, H., Torki, M., Kaveh, M., Szymanek, M., Khalife, E., and Dziwulski, J. (2022). Forecasting of power output of a pvps based on meteorological data using rnn approaches. Sustainability, 14(5):3104.

Bhaskar, K. and Singh, S. N. (2012). Awnn-assisted wind power forecasting using feed-forward neural network. IEEE transactions on sustainable energy, 3(2):306–315.

Buratto, W. G., Muniz, R. N., Nied, A., Barros, C. F. d. O., Cardoso, R., and Gonzalez, G. V. (2024). Wavelet cnn-lstm time series forecasting of electricity power generation considering biomass thermal systems. IET Generation, Transmission & Distribution.

Chiˇnas-Palacios, C., Vargas-Salgado, C., Aguila-Leon, J., and Hurtado-P´erez, E. (2021). A cascade hybrid pso feed-forward neural network model of a biomass gasification plant for covering the energy demand in an ac microgrid. Energy Conversion and Management, 232:113896.

Dao, F., Zeng, Y., and Qian, J. (2024). Fault diagnosis of hydro- turbine via the incorporation of bayesian algorithm optimized cnn-lstm neural network. Energy, 290:130326.

Dhibi, K., Mansouri, M., Bouzrara, K., Nounou, H., and Nounou, M. (2022). Reduced neural network based ensemble approach for fault detection and diagnosis of wind energy converter systems. Renewable Energy, 194:778–787.

Dikeh, C., Ikeokwu, C., Egbe, T. I., Ochuba, M. N., Adekanye, M., Anifowose, E., and Okoroafor, E. R. (2022). Artificial neural networks for geothermal reservoirs: Implications for oil and gas reservoirs. In SPE Nigeria Annual International Conference and Exhibition, page D021S006R001. SPE.

Fentis, A., Bahatti, L., Mestari, M., and Chouri, B. (2017). Short-term solar power forecasting using support vector regression and feed-forward nn. In 2017 15th IEEE international new circuits and systems conference (NEWCAS), pages 405–408. IEEE.

Galvao Filho, A. R., Silva, D. F. C., De Carvalho, R. V., Ribeiro, F. d. S. L., and Coelho, C. J. (2020). Forecasting of water flow in a hydroelectric power plant using lstm recurrent neural network. In 2020 International Conference on Electrical, Communication, and Computer Engineering (ICECCE), pages 1–5. IEEE.

Huang, L., Li, L., Wei, X., and Zhang, D. (2022). Short-term prediction of wind power based on bilstm–cnn–wgan-gp. Soft Computing, 26(20):10607–10621.

Ishaq, M., Kwon, S., et al. (2022). A cnn-assisted deep echo state network using multiple time-scale dynamic learning reservoirs for generating short-term solar energy forecasting. Sustainable Energy Technologies and Assessments, 52:102275.

Jebli, I., Belouadha, F.-Z., Kabbaj, M. I., and Tilioua, A. (2021). Deep learning based models for solar energy prediction. Advances in Science, Technology and Engineering Systems Journal, 6(1):349–355.

Jiang, A., Qin, Z., Faulder, D., Cladouhos, T. T., and Jafarpour, B. (2022). Recurrent neural networks for short-term and long-term prediction of geothermal reservoirs. Geothermics, 104:102439.

Kalogirou, S. A. (2001). Artificial neural networks in renewable energy systems applications: a review. Renewable and sustainable energy reviews, 5(4):373–401.

Khatib, T., Mohamed, A., Sopian, K., and Mahmoud, M. (2012). Assessment of artificial neural networks for hourly solar radiation prediction. International journal of Photoenergy, 2012(1):946890.

King, M., Woo, S. I., and Yune, C.-Y. (2024). Utilizing a cnn-rnn machine learning approach for forecasting time-series outlet fluid temperature monitoring by long-term operation of bhes system. Geothermics, 122:103082.

Kisvari, A., Lin, Z., and Liu, X. (2021). Wind power forecasting–a data-driven method along with gated recurrent neural network. Renewable Energy, 163:1895–1909.

Kumar, K., Saini, G., Kumar, N., Kaiser, M. S., Kannan, R., and Shah, R. (2022). Prediction of energy generation target of hydropower plants using artificial neural networks. In Sustainable Developments by Artificial Intelligence and Machine Learning for Renewable Energies, pages 309–320. Elsevier.

Lawan, S., Abidin, W., Masri, T., Chai, W., and Baharun, A. (2017). Wind power generation via ground wind station and topographical feedforward neural network (t-ffnn) model for small-scale applications. Journal of cleaner production, 143:1246–1259.

Li, X., Zhang, J., Xiao, B., Zeng, Y., Lv, S., Qian, J., and Du, Z. (2024a). Fault diagnosis of hydropower units based on gramian angular summation field and parallel cnn. Energies, 17(13):3084.

Li, Y., Peng, G., Du, T., Jiang, L., and Kong, X.-Z. (2024b). Advancing fractured geothermal system modeling with artificial neural network and bidirectional gated recurrent unit. Applied Energy, 372:123826.

Liao, G.-P., Gao, W., Yang, G.-J., and Guo, M.-F. (2019). Hydroelectric generating unit fault diagnosis using 1-d convolutional neural network and gated recurrent unit in small hydro. IEEE Sensors Journal, 19(20):9352–9363.

Lim, S.-C., Huh, J.-H., Hong, S.-H., Park, C.-Y., and Kim, J.-C. (2022). Solar power forecasting using cnn-lstm hybrid model. Energies, 15(21):8233.

Malakouti, S. M., Ghiasi, A. R., Ghavifekr, A. A., and Emami, P. (2022). Predicting wind power generation using machine learning and cnn-lstm approaches. Wind Engineering, 46(6):1853–1869.

Mansoor, M., Ling, Q., and Zafar, M. H. (2022). Short term wind power prediction using feedforward neural network (fnn) trained by a novel sine-cosine fused chimp optimization algorithm (schoa). In 2022 5th International Conference on Energy Conservation and Efficiency (ICECE), pages 1–6. IEEE.

Mansouri, M., Dhibi, K., Hajji, M., Bouzara, K., Nounou, H., and Nounou, M. (2022). Interval-valued reduced rnn for fault detection and diagnosis for wind energy conversion systems. IEEE Sensors Journal, 22(13):13581–13588.

Massaoudi, M., Chihi, I., Sidhom, L., Trabelsi, M., Refaat, S. S., and Oueslati, F. S. (2019). A novel approach based deep rnn using hybrid narx-lstm model for solar power forecasting. arXiv preprint arXiv:1910.10064.

Mellit, A., Drif, M., and Malek, A. (2010). Epnn-based prediction of meteorological data for renewable energy systems. Journal of Renewable Energies, 13(1):25–47.

Paramasivan, S. K. (2021). Deep learning based recurrent neural networks to enhance the performance of wind energy forecasting: A review. Revue d'Intelligence Artificielle, 35(1).

Park, M. K., Lee, J. M., Kang, W. H., Choi, J. M., and Lee, K. H. (2021). Predictive model for pv power generation using rnn (lstm). Journal of Mechanical Science and Technology, 35(2):795–803.

Quaschning, V. (2014). Understanding renewable energy systems. Routledge.

Rahman, M. M., Shakeri, M., Tiong, S. K., Khatun, F., Amin, N., Pasupuleti, J., and Hasan, M. K. (2021). Prospective methodologies in hybrid renewable energy systems for energy prediction using artificial neural networks. Sustainability, 13(4):2393.

Raju, V. V. R., Raju, N. G., Shailaja, V., and Padullaparti, S. (2020). Iot based solar energy prophecy using rnn architecture. In E3S Web of Conferences, volume 184, page 01007. EDP Sciences.

Rodr´ıguez, F., Azc´arate, I., Vadillo, J., and Galarza, A. (2022). Forecasting intra-hour solar photovoltaic energy by assembling wavelet based time-frequency analysis with deep learning neural networks. International Journal of Electrical Power & Energy Systems, 137:107777.

Shabbir, N., K¨utt, L., Jawad, M., Amadiahanger, R., Iqbal, M. N., and Rosin, A. (2019). Wind energy forecasting using recurrent neural networks. In 2019 Big Data, Knowledge and Control Systems Engineering (BdKCSE), pages 1–5. IEEE.

Sharma, K. G., Kaisare, N. S., and Goyal, H. (2022). A recurrent neural network model for biomass gasification chemistry. Reaction Chemistry & Engineering, 7(3):570–579.

Sharma, S., Khanra, P., and Ramkumar, K. (2021). Performance analysis of biomass energy using machine and deep learning approaches. In Journal of Physics: Conference Series, volume 2089, page 012003. IOP Publishing.

Shi, Z., Ferrari, G., Ai, P., Marinello, F., and Pezzuolo, A. (2023). Artificial intelligence for biomass detection, production and energy usage in rural areas: A review of technologies and applications. Sustainable Energy Technologies and Assessments, 60:103548.

Srivastava, T., Vedanshu, and Tripathi, M. (2020). Predictive analysis of rnn, gbm and lstm network for short-term wind power forecasting. Journal of Statistics and Management Systems, 23(1):33–47.

Tesha, T. and Kichonge, B. (2015). Analysis of tanzanian biomass consumption using artificial neural network. Journal of Fundamentals of Renewable Energy and Applications, 5:1–7.

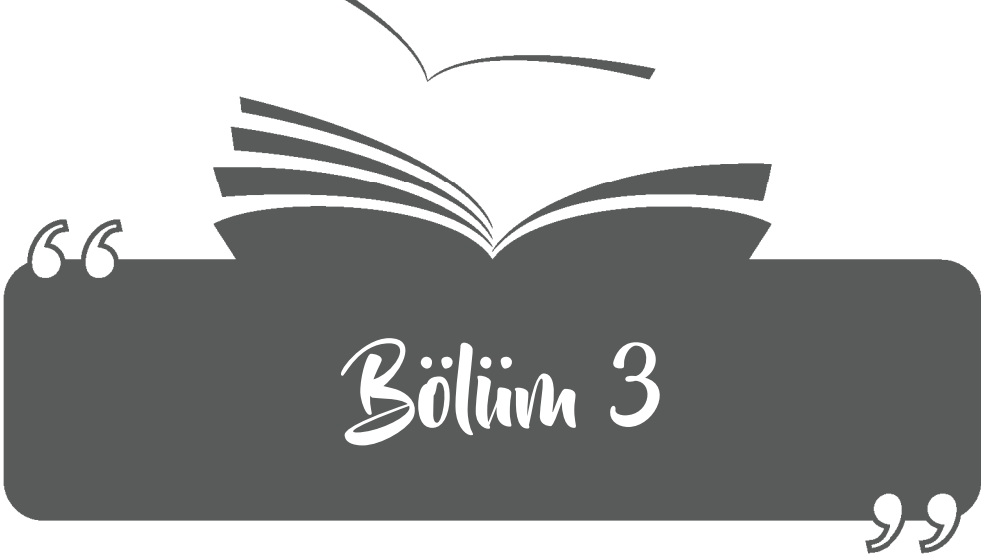
Wang, H.-K., Song, K., and Cheng, Y. (2022). A hybrid forecasting model based on cnn and informer for short-term wind power. Frontiers in Energy Research, 9:788320.

Wu, Q., Guan, F., Lv, C., and Huang, Y. (2021). Ultra-short-term multi-step wind power forecasting based on cnn-lstm. IET Renewable Power Generation, 15(5):1019–1029.

Zafar, M. H., Khan, N. M., and Khan, U. A. (2021). Short term hybrid pv/wind power forecasting for smart grid application using feedforward neural network (fnn) trained by a novel atomic orbital search (aos) optimization algorithm. In 2021 International conference on frontiers of information technology (FIT), pages 72–77. IEEE.

Zhang, H., Zhao, L., and Du, Z. (2021). Wind power prediction based on cnn-lstm. In 2021 IEEE 5th Conference on Energy Internet and Energy System Integration (EI2), pages 3097–3102. IEEE.

Zhu, C.-Y., Huang, D., Yu, B., Gong, L., and Xu, M.-H. (2023). Enhanced geothermal system performance prediction based on deep learning neural networks. In International Conference on Computational & Experimental Engineering and Sciences, pages 1007–1022. Springer.



KUANTUM HATA DÜZELTME ENTEGRASYONU İLE GROVER SALDIRILARINA DİRENEN HİBRİT SİMETRİK ŞİFRELEME YAKLAŞIMI

Özge TAŞ[1]

1 Öğr.Gör., Kapadokya Üniversitesi, Bilgisayar Programcılığı, ORCID: https://orcid.org/0000-0001-7220-5054

Hibrit şifreleme yaklaşımı kuantum hata düzeltme entegrasyonu ve grover saldırılarına karşı direnç göstermektedir. Gelişen kuantum hesaplama yöntemleriyle kriptografik sistemlerin güvenliğini arttırmak için yenilikçi hesaplama yöntemleri geliştirilmiştir.Kuantum algoritması olan grover algoritması geleneksel simetrik şifreleme yöntemlerini tehdit ettikçe kuantum hata düzeltmeyi içeren hibrit şifreleme yöntemleri geliştirilmesi giderek önemli hale gelmiştir. Bu yaklaşımla hassas verilerin korunması kuantum tehtidlerinin oluşturduğu diğer güvenlik açıklarını ele almak için simetrik ve asimetrik şifreleme yöntemlerinin birleşim yöntemleri kullanılmaktadır. Hibrit simetrik şifreleme çalışma prensibi simetrik bir anahtarın verilerin büyük bir kısmını şifrelediği ve asimetrik sistemin bu simetrik anahtarı ilettiği çift katmanlı bir mekanizma kullanır. Kuantum hata düzeltme tekniklerine entegre ederek bu yöntem şifrelenmiş verilerin iletim sırasında hatalara ve saldırılara karşı bütünlüğünü korumayı amaçlar ve bu durum modern iletişim altyapılarının güvenliğini sağlamada kritik önem taşır.Bu tür gelişmeler yalnızca gizliliği ve verimliliği sağlamakla kalmaz aynı zamanda kriptografik sistemlerin kuantum teknolojilerine hakim olduğu bir sistem sağlar.Bu hibrit yaklaşım önemli düzeydeki etkileri gelişmiş güvenlik önemlerinin alınmasına olanak sağlayarak , siber güvenlik alanında kuantum hesaplama zorluklarına uyum sağlama konusunda artan ihtiyaçlara yanıt sunar. Dünya çapındaki kurumlar Grover algoritmasının etkilerini ve yerleşik şifreleme standartlarına yönelik potansiyel risklerini araştırırken kuantum hata düzeltmenin hibrit şifreleme çözümlerine entegrasyonu veri güvenliğini korumak için proaktif bir önlem olarak görülmektedir. Bu değişimler özellikle geleneksel ve kuantum dirençli metodojiler arasındaki kriptografik uygulamaların geleceği hakkında önemli tartışmalara yol açmaktadır. Alanda yapılan önemli çalışmalar bu hibrit sistemlerin uygulanmasına, anahtar boyutlarında gerekli ayarlamalara ve kuantum sonrası kriptografik çözümlere geçişe odaklanmaktadır. Kuruluşların bu teknolojileri entegre etmesi için klasik ve kuantum teknolojilerinin getirdiği tehditlere dayanabilen güvenli ve ölçeklenebilir kriptografik çerçevelerin geliştirilmesinin araştırmalar için kritik öneme sahiptir.

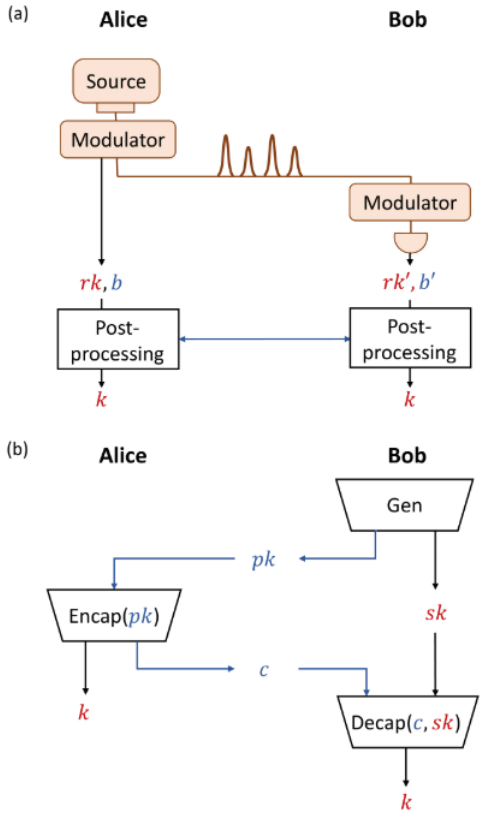
Kuantum Bilgisayarları ve Grover Algoritması

Kuantum hesaplama klasik bilgisayarların yapamayacağı hesaplamaları gerçekleştirmek için kuantum mekaniğinin prensiplerinden yararlanan bir paradigmadır. Bu alandaki önemli bir gelişme klasik bilgisayarlara kıyasla yapılandırılmamış arama problemleri için hızlı işlem gücü ile avantaj sağlayan Grover algoritmasıdır. Özellikle $Q\sqrt{N}$ değerlendirme gerektiren yüksek olasılıkla bir kara kutu fonksiyonuna benzersiz bir girdinin tanımlanmasına olanak tanır; burada N fonksiyonun etki alanının

boyutudur. Bu Q(N) değerlendirmeleri gerektirecek olan klasik algoritmalara kıyasla büyük gelişmeyi temsil eder.

Kuantum Kriptografisinde Anahtar Kapsülleme Mekanizması (KEM)

Kuantum kriptografisi, bir anahtar kapsülleme mekanizması (KEM) simetrik anahtarları güvenli bir şekilde dağıtmada kritik bir rol oynar. KEM, genellikle Alive ve Bop olarak adlandırılan taraflar arasında paylaşılan gizli bilgiyi oluşturmak için açık anahtar şifrelemesini kullanır. İşlem üç ana adımı içerir; anahtar oluşturma, kapsülleme ve kapsülden çıkarma. Başlangıçta, Bob bir anahtar çifti oluşturur ve açık anahtarı Alice ile paylaşır.Daha sonra, Alice Bob'un açık anahtarını kullanarak rasgele bir mesajı şifreler ve ardından Bob'a gönderdiği bir şifreli metin oluşturur. Son olarak, Bob şifreli metni özel anahtarını kullanarak kapsülden çıkarır ve böylece güvenli iletişim için paylaşılan simetrik anahtarı elde eder.



Şekil 1 . iki simetrik anahtar dağıtım protokolünün gösterimi. (a) Hazırla ve ölç kuantum anahtar dağıtım (QKD) protokolleri. (b) Kuantum sonrası kriptografi (PQC) sistemine dayalı anahtar kapsülleme mekanizması (Zenh, e.i 2024).

Kuantum teknolojileri gelişmeye devam ettikçe klasik şifreleme yöntemlerinin güvenliği önemli tehditlerle karşı karşıyadır. Geleneksel simetrik şifreleme algoritmaları genellikle anahtar alanını etkili bir şekilde yarıya indirebilen ve daha kısa anahtarları saldırılara karşı daha duyarlı hale getiren Grover algoritmasına karşı savunmasızdır. Sonuç olarak kuantum hata düzeltme (QEC) tekniklerinin entegrasyonu bu tür saldırılara karşı hibrit simetrik şifreleme yaklaşımlarının dayanıklılığını arttırmak için zorunludur. QEC kuantum bilgilerinin bütünlüğünü korumayı ve hesaplama veya iletim sırasında ortaya çıkan hataların şifrelenmiş verilerin güvenliğini tehlikeye atmamayı amaçlar.

Hibrit Simetrik Şifreleme Yaklaşımı

Hibrit simetrik şifreleme, veri güvenliğini ve iletim verimliliğini artırmak için hem simetrik hem de asimetrik şifreleme tekniklerinin avantajlarını birleştiren bir kriptografik yöntemdir. Bu yaklaşım, özellikle modern siber tehditler ve kuantum bilişim zorlukları bağlamında, izole olarak kullanıldığında her şifreleme yöntemiyle ilişkili güvenlik açıklarını etkili bir şekilde azaltır. Hibrit simetrik şifreleme, verilerin büyük kısmını şifrelemek için simetrik bir anahtar kullanılmasını içerirken, asimetrik şifreleme simetrik anahtarın kendisini güvenli bir şekilde iletmek için kullanılır. İşlem, gerçek mesajın hızlı bir şekilde şifrelenmesi için kullanılan rastgele simetrik bir anahtarın, yani oturum anahtarının oluşturulmasıyla başlar. Mesaj şifrelendikten sonra, bu simetrik anahtar alıcının genel anahtarı kullanılarak şifrelenir. Bu çift katmanlı şifreleme, yalnızca verilerin gizli kalmasını sağlamakla kalmaz, aynı zamanda potansiyel olarak güvenli olmayan kanallar üzerinden şifreleme anahtarlarının güvenli bir şekilde değiştirilmesine de olanak tanır. Hibrit simetrik şifrelemenin birincil avantajı, asimetrik şifrelemenin güvenlik avantajlarını simetrik şifrelemenin hızıyla birleştirme becerisinde yatmaktadır. Simetrik şifreleme büyük miktarda veriyi işlemek için daha hızlı ve daha verimli olsa da genellikle anahtar dağıtımı ve yönetimiyle ilgili zorluklar yaşar. Buna karşılık, asimetrik şifreleme anahtar değişimi için sağlam bir mekanizma sağlar ancak genellikle daha yavaştır ve bu da onu toplu veri şifrelemesi için daha az uygun hale getirir. Hibrit şifrelemeyi kullanarak, kuruluşlar yüksek performansı koruyan güvenli bir iletişim kanalı elde edebilirler. Hibrit simetrik şifreleme, veri iletim hızını optimize etmek için tasarlanmıştır. Simetrik şifreleme algoritmaları, verileri asimetrik muadillerinden daha hızlı işleyebildiğinden, hibrit yaklaşım, güvenlikten ödün vermeden büyük veri kümelerinin hızlı bir şekilde iletilmesine olanak tanır. Bu verimlilik, finansal işlemler veya gerçek zamanlı iletişimler gibi zamana duyarlı verilerin güvenli ve hızlı bir şekilde iletilmesi gereken ortamlarda özellikle önemlidir.

Kuantum bilişiminin ortaya çıkmasıyla birlikte, geleneksel şifreleme yöntemleri, özellikle simetrik şifrelemenin etkili anahtar gücünü önemli ölçüde azaltabilen Grover algoritması gibi algoritmalardan kaynaklanan potansiyel tehditlerle karşı karşıyadır. Hibrit simetrik şifreleme yaklaşımları, bu tür kuantum saldırılarına karşı güvenliği artırmak için kuantum hata düzeltme tekniklerini birleştirebilir ve bu da onları geleceğe yönelik kriptografik sistemlerin geliştirilmesinde hayati bir bileşen haline getirir.

Hibrit simetrik şifrelemeyi etkili bir şekilde uygulamak, her iki şifreleme yönteminin de kapsamlı bir şekilde anlaşılmasını gerektirir. Anahtar oluşturma, asimetrik şifreleme için bir çift genel ve özel anahtar oluşturmayı ve ardından verileri şifrelemek için simetrik bir anahtar kullanmayı içerir. Alıcı daha sonra özel anahtarını kullanarak simetrik anahtarı şifresini çözer ve bu anahtar daha sonra mesajı şifresini çözmek için kullanılır. Bu süreç yalnızca veri gizliliğini sağlamakla kalmaz, aynı zamanda anahtar dağıtımını da basitleştirerek çeşitli uygulamalar için çok yönlü bir çözüm haline getirir(Garvin,Kondratyev e.i 2024).

Kuantum Hata Düzeltmesi

Kuantum Hata Düzeltmesi (QEC), gürültü ve uyumsuzluktan kaynaklanan hatalardan kuantum bilgisinin bütünlüğünü korumayı amaçlayan kuantum hesaplamanın temel bir bileşenidir.. QEC'nin temel hedefleri arasında hesaplamalar sırasında kuantum verilerinin korunması, kuantum sistemlerinin hatalara karşı hassasiyetinin azaltılması ve kuantum teknolojisi uygulamalarının ölçeklenebilirliğinin sağlanması yer alır. Kuantum sistemlerinde hatalar, kübit gürültüsü, kapı hataları ve ölçüm yanlışlıkları gibi çeşitli kaynaklardan kaynaklanabilir. Hata düzeltme kodlarının uygulanması, kuantum bilgisayarların bu hataları etkili bir şekilde azaltmasına olanak tanır ve güvenilir, hataya dayanıklı hesaplamayı kolaylaştırır. Yaygın olarak incelenen QEC kodları arasında, Surface Code ve Shor Code, birden fazla hatayı düzeltme ve bit-flip ve phase-flip hataları gibi yaygın gürültü türlerine karşı dayanıklılık sağlama yetenekleriyle özellikle dikkat çekicidir. Örneğin, Shor Kodu, tek kübit hatalarını düzeltmek ve iki kübit hatalarını tespit etmek için 9 kübitlik bir sabitleyici yapı kullanırken, 7 kübitlik Steane Kodu, tek kübitlik hata düzeltmesi için daha yüksek verimlilik sunar. Kritik önemine rağmen QEC, klasik hata düzeltme yöntemlerinden farklı benzersiz zorluklarla karşı karşıyadır. Kuantum üst üste binme ve dolanıklık, karmaşıklık katmanları ekleyerek kuantum sistemlerine uyarlanmış sofistike hata modellerini gerekli kılar. Araştırmacılar, bu hata modellerini anlamada önemli ilerlemeler kaydettiler ve kuantum hatalarının karmaşık doğasından kuantum bilgilerini etkili bir şekilde koruyabilen özel QEC kodlarının geliştirilmesine olanak sağladılar (Terhal B.M 2015).

Deneysel Uygulamalar

QEC'nin son deneysel gösterimleri, süperiletken kübitler ve hapsolmuş iyonlar dahil olmak üzere çeşitli fiziksel sistemlerde ümit verici sonuçlar göstermiştir. Örneğin, üç kübit ve beş kübit QEC kodlarının başarılı uygulamaları, kodlanmış kübitlerin bireysel fiziksel karşılıklarına kıyasla geliştirilmiş tutarlılık sürelerini vurgulamıştır. Ek olarak, Surface Code çeşitli gürültü türlerine karşı sağlam olduğunu kanıtlamış ve bu da onu büyük ölçekli kuantum hesaplama uygulamaları için güçlü bir aday yapmıştır(Terhal B.M 2015).

Gelecek Yönleri

Kuantum teknolojilerinin, özellikle kuantum hata düzeltmesi alanındaki evrimi, kriptografi için umut verici ancak karmaşık bir manzara sunmaktadır. Araştırmacılar yeni metodolojileri keşfetmeye devam ettikçe, kuantum hata düzeltmesinin hibrit simetrik şifrelemeyle bütünleştirilmesinin, özellikle klasik simetrik kriptografik sistemleri kırma sürecini önemli ölçüde hızlandırabilen Grover algoritması olmak üzere, kuantum saldırılarının oluşturduğu güvenlik açıklarını ele almada önemli bir rol oynaması beklenmektedir(Bernstein, e.i 2017),(Nadeem, e.i. 2024). Devam eden araştırmalar, kuantum bilgisayarlarının güvenilir çalışması için olmazsa olmaz olan kuantum hata düzeltme tekniklerini iyileştirmeye odaklanmıştır. Bu ilerlemeler, sınırlı hesaplama kaynaklarıyla bile pratik uygulamalara olanak tanıyan, son işlem prosedürlerinin ve ağ topolojilerinin verimliliğini optimize eden yenilikçi yaklaşımları içerebilir. Çığır açan gelişmeler meydana geldikçe, sağlam kriptografik önlemler gerektiren daha büyük ölçekli kuantum hesaplamalarına olanak sağlayabilirler.

Hibrit Kriptografik Çözümler

Potansiyel kuantum tehditleri ışığında, hibrit kriptografik çözümler güvenliği artırmak için geçici bir strateji olarak ortaya çıkıyor. Bu yaklaşım, klasik algoritmaların kanıtlanmış sağlamlığını, hala değerlendirme aşamasında olan yeni post-kuantum kriptografik (PQC) çözümlerle birleştiriyor. Almanya'nın BSI ve Fransa'nın ANSSI gibi kurumlar, tamamen kuantum dirençli sistemlere geçiş yaparken minimum düzeyde güvenlik sağlamak için çift kapsüllemeyi vurgulayarak bu yöntemi savunuyor. Bu geçiş, kuruluşların hem klasik hem de kuantum hesaplamalı saldırılara karşı dirençli kalmasını sağlaması açısından kritik önem taşıyor.

Grover Saldırılarına Karşı Direnç

Kuantum bilişiminin gelişi, özellikle Grover'ınki gibi simetrik anahtar alanlarında arama yapmanın karmaşıklığını etkili bir şekilde azaltabilen algoritmalar nedeniyle klasik kriptografiye önemli zorluklar getiriyor. Grover'ın algoritması, simetrik şifreleme sistemlerinin bit gücünü etkili bir şekilde yarıya indirerek, daha önce güvenli olan anahtar uzunluklarını (örneğin, 128 bit) uzun vadede yetersiz hale getiriyor. Sonuç olarak, kriptografi topluluğu, büyük ölçekli kuantum bilgisayarlar faaliyete geçmeden önce bu tür kuantum tehditlerine karşı direnci artırmak için çeşitli stratejiler araştırıyor (Saberi e.i 2024)(Bernstein & Lange 2017).

Temel Azaltma Stratejileri

Anahtar Boyutlarını Artır

Grover'ın algoritmasına karşı en basit savunmalardan biri, simetrik algoritmalar için anahtar boyutlarını artırmaktır. 128 bitlik anahtarlardan 256 bitlik anahtarlara geçmek, etkili anahtar arama alanının, Grover'ın sağladığı ikinci dereceden hızlanma ile bile saldırganlar için hesaplama açısından uygulanamaz kalması nedeniyle güvenliği önemli ölçüde artırır (Bernstein & Lange 2017). Modern yazılım kütüphaneleri daha büyük anahtarları yaygın olarak destekler ve bu da bunu birçok kuruluş için erişilebilir bir strateji haline getirir. Daha büyük anahtarlar hafif performans maliyetlerine yol açabilse de, gelişmiş güvenlik için bu ödün genellikle kabul edilebilirdir (Gitonga 2025).

Uzun Vadeli Siber Güvenlik Uyarlaması

Daha büyük anahtarlara doğru geçiş, siber güvenlik altyapılarında çeviklik gerektirir. Profesyoneller, sistemlerinin kuantum güvenli parametreleri barındırabildiğinden ve AES-256 gibi daha güçlü şifreleme standartlarına geçiş yapmaya başladığından emin olmalıdır. Bu proaktif yaklaşım, uzun süreler boyunca güvenli kalması amaçlanan verileri korumak için önemlidir (Bernstein & Lange 2017).

Araştırma ve Geliştirme

Devam eden araştırma, simetrik algoritmalardaki potansiyel güvenlik açıklarını belirlemeyi ve ele almayı amaçlamaktadır. Kriptograflar, Grover'ın algoritmasının ötesinde çağdaş kriptografik sistemlerdeki zayıflıkları istismar edebilecek yeni kuantum saldırılarının ortaya çıkmamasını sağlamaya özellikle odaklanmaktadır. Mevcut bulgular, Grover'ın birincil endişe olmaya devam ettiğini ve simetrik kriptoanalizde onu geride bırakacak önemli bir kuantum saldırısının bilinmediğini göstermektedir (Gorine, Suhaib 2024). Ayrıca araştırmacılar, kuantum anahtar da-

ğıtımını (QKD) kuantum sonrası kriptografiyle (PQC) birleştiren hibrit kriptografik şemaları araştırıyorlar; bu, ortak bir kuantum-klasik ağda gelişmiş güvenlik ve performans sunabilir (Zeng E.i, 2024).

Uygulamalar

Kuantum Dayanıklı Güvenlik Çözümleri

Kuantum dirençli teknolojilerin çeşitli uygulamalara entegrasyonu, sistemlerini kuantum tehditlerine karşı korumak isteyen kuruluşlar için odak noktası haline geldi. Örneğin ResQuant, tescilli Post-Quantum Kriptografi (PQC) Sistem-üzeri-Çip (SoC) teknolojisini içeren IP çekirdek lisansları ve FPGA hızlandırıcıları tasarlar. Bu teknoloji, otomotiv, Nesnelerin İnterneti (IoT), askeri ve Bilgi ve İletişim Teknolojisi (BİT) dahil olmak üzere çeşitli sektörlerde güvenli iletişim, veri bütünlüğü ve sistem şifrelemesi gibi belirli ihtiyaçları ele alırken güvenliği optimize etmek için tasarlanmıştır (Prasser 2025).

Ayrıca ResQuant, gelişmiş CHERI özellikli cihazlarda PQC algoritmalarının hızlandırılmasını daha da artırmak için SCI Semiconductor ile bir ortaklık kurdu ve bu, kuantum güvenlik önlemlerini güçlendirmek için farklı sektörler arasındaki artan iş birliğini gösteriyor (Prasser 2025).

Sağlık Hizmetlerinde Güvenli İletişim

Kuantum dirençli çözümlerin uygulanması, IoT cihazlarının hasta hayati belirtilerini izlemek ve ilaçları yönetmek için kullanıldığı sağlık hizmetleri gibi kritik sektörlere kadar uzanır. Bu cihazlar, HIPAA ve GDPR gibi düzenlemeler kapsamında hassas kişisel sağlık bilgilerini (PHI) korumalıdır. Güvenlik çözümleri, bu cihazların sınırlı kaynakları nedeniyle yalnızca verimli olmakla kalmamalı, aynı zamanda kuantum saldırılarına karşı geleceğe dönük olmalı ve sağlık hizmetleri ortamlarında güvenli iletişim protokollerinde sürekli inovasyona olan ihtiyacı vurgulamaktadır (Wang E.i 2024).

Kripto Sistemlerinin Gerçek Dünya Uygulaması

Gerçek dünya vaka çalışmaları, güvenliği artırmada çeşitli kripto sistemlerinin pratik uygulamasını göstermektedir. Örneğin, Matsumoto–Imai (MI) ve Hidden Field Equations (HFE) gibi şemalar, kuantum dirençli kimlik doğrulamada etkinlikleri açısından değerlendirilmiş ve geleneksel sistemlere kıyasla önemli avantajlar göstermiştir. Bu örnekler, verileri olası kuantum saldırılarından korumada bu kriptografik çözümlerin rolleri ve önemi hakkında değerli içgörüler sağlar (Wang E.i 2024).

Hibrit Kuantum-Klasik Ağlar

Hibrit Kuantum-Klasik Ağlar (HQCN'ler), mevcut kuantum donanım sınırlamalarını pratik kuantum avantajlarıyla köprülemek için umut vadeden bir çerçeve olarak ortaya çıkıyor. Kuantum ve klasik hesaplama kaynaklarını entegre ederek, HQCN'ler her iki paradigmadan da faydalanan karmaşık sorunları ele alabilir. Ancak, HQCN'lerin uygulanması, kuantum durumlarının içsel kırılganlığını yönetmek ve gerçek dünya senaryolarında güvenilir bir çalışma sağlamak için sağlam Kuantum Hata Düzeltme (QEC) yöntemlerini gerektirir (Tian. E.i, 2024).

Akademi, endüstri ve hükümetin ortak çabası, bu teknolojilerin dağıtımında kılavuz ilkeler ve en iyi uygulamalar oluşturmak ve kuruluşların giderek kuantum farkındalığı artan bir dünyada bilgilerini güvenle koruyabilmelerini sağlamak için kritik öneme sahiptir Aydeger E.i 2024).

Sonuç olarak, bu çalışma, kuantum hata düzeltme entegrasyonunun Grover saldırılarına karşı hibrit simetrik şifreleme yöntemleriyle nasıl birleştirilebileceğini ele alarak, kuantum bilgisayarların yükselişiyle birlikte ortaya çıkan güvenlik tehditlerine karşı yenilikçi çözümler sunmaktadır. Hibrit simetrik şifreleme hem klasik hem de kuantum sistemlerinin avantajlarını bir araya getirerek, veri güvenliğini artırmayı hedeflemektedir. Kuantum hata düzeltme tekniklerinin entegrasyonu, şifreleme algoritmalarının güvenliğini sağlamada kritik bir rol oynamaktadır. Bu çalışma, gelecekteki araştırmalara ve uygulamalara ışık tutarak, kuantum teknolojilerinin güvenli bir şekilde benimsenmesini amaçlamaktadır.

Referans

Aydeger, A., Zeydan, E., Yadav, A. K., Hemachandra, K. T., & Liyanage, M. (2024, October). Towards a quantum-resilient future: Strategies for transitioning to post-quantum cryptography. In *2024 15th International Conference on Network of the Future (NoF)* (pp. 195-203). IEEE.

Tian, C. 2024, A Survey of Quantum Error Correction in Hybrid Quantum-Classical Networks.

Wang, Y., Li, L., Zhou, Y., & Zhang, H. (2024). A Comprehensive Review of MI-HFE and IPHFE Cryptosystems: Advances in Internal Perturbations for Post-Quantum Security. *Axioms*, *13*(11), 741. https://doi.org/10.3390/axioms13110741

Gitonga, C. K. (2025). The Impact of Quantum Computing on Cryptographic Systems: Urgency of Quantum-Resistant Algorithms and Practical Applications in Cryptography. *European Journal of Information Technologies and Computer Science*, *5*(1), 1–10. https://doi.org/10.24018/compute.2025.5.1.146

Wang, Y., Li, L., Zhou, Y., & Zhang, H. (2024). A Comprehensive Review of MI-HFE and IPHFE Cryptosystems: Advances in Internal Perturbations for Post-Quantum Security. *Axioms*, *13*(11), 741. https://doi.org/10.3390/axioms13110741

SaberiKamarposhti, M., Ng, K. W., Chua, F. F., Abdullah, J., Yadollahi, M., Moradi, M., & Ahmadpour, S. (2024). Post-quantum healthcare: A roadmap for cybersecurity resilience in medical data. *Heliyon*, *10*(10).

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, *549*(7671), 188-194.

Gorine, A., & Suhaib, M. (2024). Exploring AES Encryption Implementation Through Quantum Computing Techniques.

Zeng, P., Bandyopadhyay, D., Méndez, J. A. M., Bitner, N., Kolar, A., Solomon, M. T., ... & Liu, J. (2024). Practical hybrid PQC-QKD protocols with enhanced security and performance. *arXiv preprint arXiv:2411.01086*.

David R. Prasser 2025 , 5 Top Post-Quantum Cryptography Companies and Startups to Watch in , February,2025.

Garvin, D., Kondratyev, O., Lipton, A., & Paini, M. (2024). Symmetric Encryption on a Quantum Computer. *Cryptology ePrint Archive*.

Bernstein, D. J., & Lange, T. (2017). Post-quantum cryptography. *Nature*, *549*(7671), 188-194.

Nadeem, M., Sarkar, A. K., & Ishrat, M. (2024). Securing information systems through quantum computing: Grover's algorithm approach. In *Computational Intelligence Applications in Cyber Security* (pp. 299-306). CRC Press.Kuantum Hata Düzeltmesindeki Gelişmeler

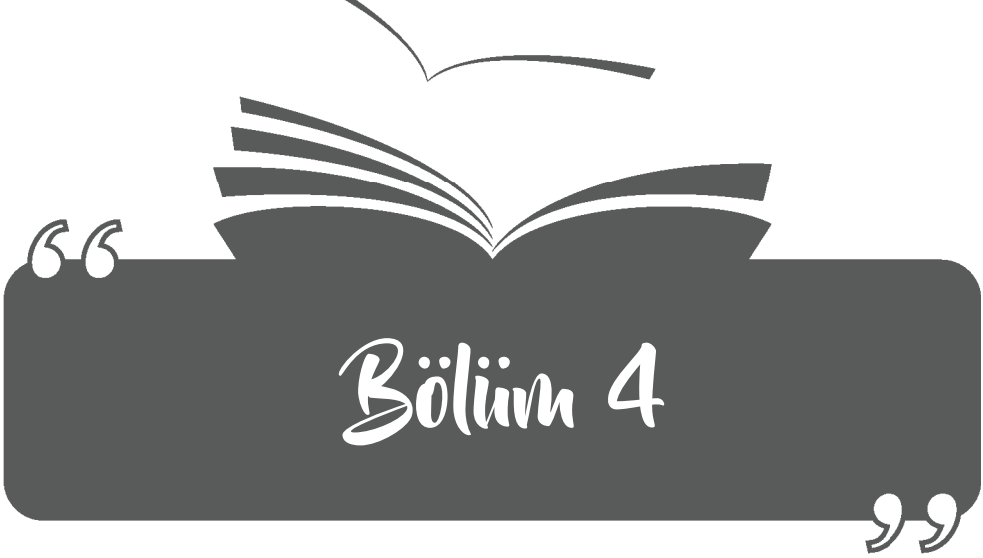
Zeng, P., Bandyopadhyay, D., Méndez, J. A. M., Bitner, N., Kolar, A., Solomon, M. T., ... & Liu, J. (2024). Practical hybrid PQC-QKD protocols with enhanced security and performance. *arXiv preprint arXiv:2411.01086*.

Terhal, B. M. (2015). Quantum error correction for quantum memories. *Reviews of Modern Physics*, *87*(2), 307-346.

Tian, C. A Survey of Quantum Error Correction in Hybrid Quantum-Classical Networks.

Fedorov, A. K. (2023). Deploying hybrid quantum-secured infrastructure for applications: When quantum and post-quantum can work together. *Frontiers in Quantum Science and Technology*, *2*, 1164428.

Gones V. 2025, Uncovering the advantages of hybridization and cryptoagility in quantum security March 7.



BULUT BİLİŞİM ORTAMINDA MAKİNE ÖĞRENİMİ DESTEKLİ SİBER SALDIRI TESPİT SİSTEMLERİ

Büşra GÜVEN[1], Soydan SERTTAŞ[2], Çiğdem BAKIR[3]

1 Kütahya Dumlupınar Üniversitesi, Bilgisayar Mühendisliği Anabilim Dalı, busrabasguven@gmail.com
2 Dr.Öğretim Üyesi, Kütahya Dumlupınar Üniversitesi,Bilgisayar Mühendisliği Bölümü, soydan.serttas@dpu.edu.tr,ORCID:0000-0001-8887-8675
3 Dr.Öğretim Üyesi, Kütahya Dumlupınar Üniversitesi,Yazılım Mühendisliği Bölümü, cigdem.bakir@dpu.edu.tr,ORCID: 0000-0001-8482-2412

1. GİRİŞ

Her geçen gün biraz daha değişen, gelişen teknoloji; bu duruma paralel olarak her geçen gün hayatımıza biraz daha fazla nüfuz etmeye başlamıştır. İnsanların ihtiyaç duydukları çoğu hizmet artık internet aracılığıyla karşılanabilmektedir. Yeme-içme, seyahat, alışveriş, eğitim vs. gibi ihtiyaçların giderilmesi internet teknolojilerini kullanarak daha hızlı ve kolay hale gelmiştir. TÜİK Hane Halkı Bilişim Teknolojileri Kullanım araştırmasının 2024 yılı sonuçlarına göre; internet kullanım oranı, 16-74 yaş grubundaki bireylerde 2023 yılında %87,1 iken, 2024 yılında %88,8 olmuştur. Cinsiyet ayrımında 2024 yılında internet kullanım oranı; erkeklerde %92,2 kadınlarda ise %85,4 olarak tespit edimiştir (TÜİK,2025). Gelişen internet teknolojileri, bünyesinde oldukça fazla avantajın yanında yine oldukça fazla dezavantajı da barındırmaktadır. Bu dezavatajların en üzerinde durulması gerekeni ise "bilgi güvenliği" konusudur. Endüstri 4.0'ın olmazsa olmazı haline bulut bilişim güvenliği de yukarıda bahsettiğimiz bilgi güvenliği kavramının en önemli alt dallarından biri haline gelmiştir. Günümüzde artık neredeyse kendisinden yararlanmadığımız alanın kalmadığı yapay zeka'dan bulut bilişim güvenliği konusunda da yararlanmaktayız. Bu çalışmamızda yapay zeka'nın en çok tercih edilen alt dallarından biri olan makine öğrenmesi yöntemleri ele alınarak, makine öğrenmesi yöntemlerinden bulut bilişim güvenliği konusunda nasıl yararlanıyoruz ve yararlanabiliriz konusu incelenmiştir.

1.1. Bulut Bilişim

Bilgisayarlar ve diğer bilişim cihazları tarafından, ihtiyaç halinde kullanılabilen, kullanıcılar arasında paylaşım yapılabilmesine imkan sağlayan, internet tabanlı bir hizmet sistemidir. Kullanıcılar ihtiyaç duydukları hizmetten herhangi bir altyapı, yazılım, dosya yükleme vs. gereksinimi duymadan, yararlanabilir. ABD Uluslararası Standartlar ve Teknoloji Enstitüsü (NIST) tarafından bulut bilişim şu şekilde tanımlanmıştır: "en az yönetim çabası ve hizmet sağlayıcı etkileşimiyle hızlıca tedarik edilebilen, yapılandırılabilir bilişim kaynaklarına isteğe bağlı erişimi sağlayan, her yerden erişilebilen bir hizmet sistemidir (NİST,2025).

1.1.2. Bulut Bilişim Mimarisi

NİST tarafından oluşturulan mimaride bulut bilişim 5 ana katmandan oluşmaktadır.

Bu katmanlar;

-Bulut tüketicisi

-Bulut denetçisi

-Servis sağlayıcı

-Bulut taşıyıcısı

-Bulut aracısı

1.1.2.1 Bulut Tüketicisi

Bulut tüketicisi, bulut sağlayıcısından kendi ihtiyacı doğrultusunda istediği hizmeti seçip, bulut sağlayıcısı ile hizmet sözleşmesi yaparak hizmetten yararlanan oluşumdur.

1.1.2.2 Bulut Denetçisi

Bulut Denetçisi, bulut hizmetinin performansın, güvenlik, tüketici ile yapılan sözleşmeye uygun hareket edilip edilmemesinin kontrolü, kalite gibi kriterler üzerinde objektif ve bağımsız denetimler gerçekleştirir.

1.1.2.3. Bulut Sağlayıcı

Talep edilen hizmeti, bulut tüketicisine vermekten sorumlu olan yapıdır. Verilecek hizmetin alt yapısını oluşturarak, hizmetin tüketiciye aradaki sözleşmeye uygun, kaliteli ve hızlı bir şekilde sunulmasını sağlar. Bulut sağlayıcı 3 ana modelden meydana gelir:

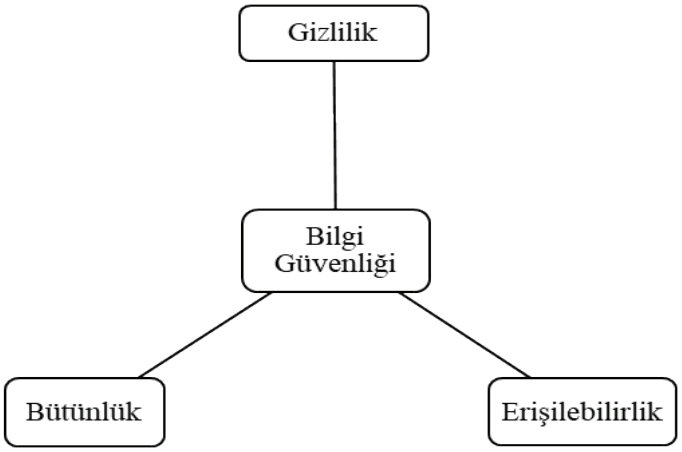
-Hizmet olarak yazılım (SaaS)

-Hizmet olarak platform (PaaS)

-Hizmet olarak Altyapı (IaaS)

1.2. Bilgi Güvenliği

Bilgi güvenliği bilgilerin izinsiz kullanımından, izinsiz ifşa edilmesinden, izinsiz yok edilmesinden, izinsiz değiştirilmesinden, bilgilere hasar verilmesinden koruma veya bilgilere yapılabilecek olan izinsiz erişimleri engelleme işlemidir (Wikipedia,2024). Bilgi güvenliğinin amacı veri bütünlüğünün korunması, erişim denetimi, gizliliğin korunması ve sistem devamlılığının sağlanması olarak sıralanmaktadır. Bilgi güvenliğinin değişmez üç yapıtaşı vardır. Bunlar; gizlilik, bütünlük ve erişilebilirliktir. Bu üç öğeden herhangi birinin eksik/yetersiz olması durumunda güvenlik zafiyeti durumu ortaya çıkmaktadır. Ancak bilgi güvenlik sistemlerinde bu üç unsurun dışında sağlanması gereken diğer bazı unsurlar da bulunmaktadır. Bunlar, bilginin güvenilir olması, bilginin inkâr edilememesi, kimliklendirme, kimlik sınaması, yetkilendirme, izlenebilirlik ve hesap verilebilirliktir (Karaman, 2020).



Şekil 1. Bilgi Güvenliği

1.3. Siber Güvenlik

Günümüzde, internet, ağlar, bilgisayar sistemleri ve bağlı cihazların hepsi bir siber ortam oluşturmaktadır. Bu ortamı oluşturan tüm sistemlerin saldırılardan korunması, bu siber ortamda bulunan bilgilerin güvenlik, bütünlük ve erişilebilirlik açısından güvenli durumda bulunması ve siber saldırıların tespit edilerek engellenmesi işlemlerinin tamamı siber güvenlik olarak tanımlanmaktadır (USOM,2024). Bu ifade, "bilgi teknolojisi güvenliği" veya "elektronik bilgi güvenliği" olarak da bilinmektedir. Siber güvenlik kavramı ağ güvenliği, uygulama güvenliği, bilgi güvenliği, operasyonel güvenlik gibi alt dallara ayrılabilmektedir. Hangi konu olursa olsun bir güvenlik zafiyetinden/probleminden bahsedilecekse burada mutlaka suç ve saldırı kavramları da devreye girmektedir.

1.3.1. Siber Suç

Bilgisayar, bilgisayar ağı veri ve sistemlerinin, dijital bilgi ve verilerinin gizliliğine ve doğruluğuna zarar verici eylemler ile bilgisayar sistemlerinin, bilgisayar ağlarının kötü amaçlı olarak kullanılması ile meydana gelen ve sürekli yukarı yönlü artış gösteren yeni bir suç tipi olup, çağımızın en önemli ve en tehlikeli suçlarından birisidir (Özocak ve Erdem,2014).

1.3.2. Siber Saldırı

Siber tehditlerin temel unsuru olan siber saldırı; belirli bir amaç doğrultusunda hedef alınan sistemlerin çökertilmesi, sistemlere zarar verilmesi, sistemlerden izinsiz bilgi sızdırılması ve kişilerin, şirketlerin, ulusların veya uluslararası kuruluşların takip edilmesi kapsamında, siber

ortamda iş ve işlemlerini yapamaz hale getirilmesi olarak tanımlanmaktadır (Gültekin,2022).

Çok çeşitli türleri olmakla birlikte bunlar; DOS (hizmet aksatma), DDOS (yoğun hizmet aksatma), IP aldatması, sniffing (koklama), sosyal mühendislik, SQL enjeksiyonu, arka kapılar, phishing (oltalama) , casus yazılım, virüs, truva atı, solucan, botnet, bukalemun, siteler ötesi istek sahteciliği, uzak kullanıcı saldırıları, tuş kaydedici, rootkit, ortadaki adam, portscan, bruteforce, doğru ayarlanmamış form elemanları, XSS(Cross-Site Scripting, sıfır gün saldırısı (zero-day) ve kaba kuvvet saldırısı, Probing(bilgi tarama), yönetici hesabı ile yerel oturum açma (Remote to Local-R2L), Kullanıcı Hesabının Yönetici Hesabına Yükseltilmesi olarak listelenmektedir.

1.3.3.Bulut Bilişime Yönelik Siber Saldırılar

Hizmet hırsızlığı, Hizmet aksatma, Müşteri veri manipülasyonu, Veri sızıntısı, Buluta kötü amaçlı yazılım enjeksiyonu, Çapraz VM-yan kanal, VM kaçışı, Kötücül VM oluşturma, Güvensiz VM göçü, Sanal ağların kandırılması, Kimlik avı, Botnetler, Sesli steganografi, VM geri alma bulut bilişime yönelik saldırıları oluşturmaktadır (Aksakallı, 2019).

1.3.4. Siber Saldırıların Sebep Olduğu Kayıp Türleri

Siber saldırılar birçok konuda hem kurum ve kuruluşları hem de kişileri tehdit etmektedir. Saldırı önleme ve tespit etme yapılamazsa, saldırılar çeşitli kayıplara sebep olmaktadır. Siber saldırıların günümüz koşullarında en fazla sebep olduğu kayıp türleri;

-Finansal kayıplar

-Güven/İtibar kayıpları

-Veri kayıpları

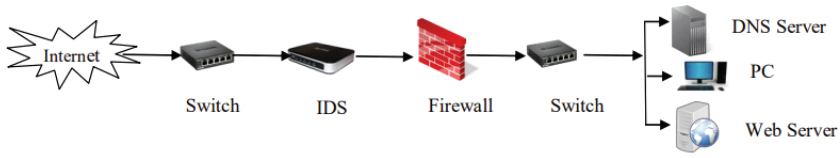
-Teknolojik/ Operasyonel kayıplar

-Psikolojik/Sosyal kayıplar'dır.

2. SİBER SALDIRI TESPİT SİSTEMLERİ

Saldırı tespit sistemleri (STS), bilgisayarların ve ağ sistemlerinin erişim verilerini inceleyerek, yapılmaya çalışılan yetkisiz erişimleri, kötüye kullanımları, sızma faaliyetlerini tespit ederek bilgi güvenliğinin korunmasını sağlayan sistemlerdir (Baykara, 2019). Saldırı tespit sistemleri belirlenirken göz önünde bulundurulan kriterler: saldırı tespit yöntemi,

mimari yapı, korunan sistemin türü, veri işleme zamanı ve kullanılan bilgi kaynağıdır (Baykara, 2019).



Şekil 2. Saldırı Tespit Sistemi Genel Mimarisi *(Jamal ve Aishwarya, 2017)*

Saldırı tespit sistemleri genellikle sistemin tespit mantığına göre iki yöntemle sınıflandırılırlar (Özgür ve Erdem, 2012);

İmza tabanlı STS ve Anomali tabanlı STS.

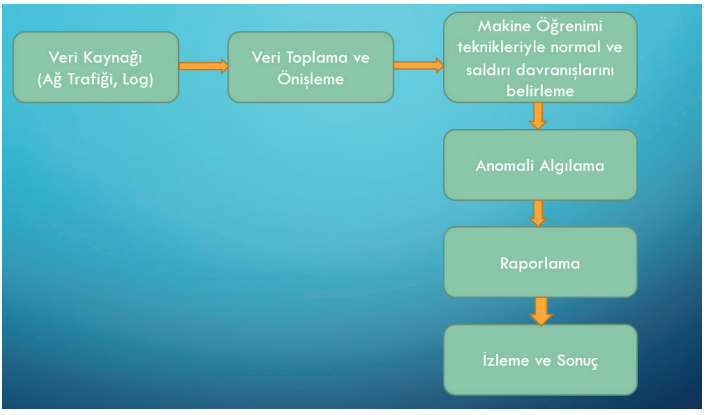
2.1. İmza Tabanlı Saldırı Tespit Sistemleri

İmza tabanlı STS, sisteme karşı yapılan her türlü saldırıyı kendi veri tabanına kaydeder. Her kaydettiği saldırı için bir imza (örüntü) oluşturur. Her imzayı veri tabanında saklar. Gelecekte bu kaydettiği imza ile karşılaşırsa mekanizmasını çalıştırır, bir saldırı geldiğini anlar ve uyarı verir. Güvenilir ve hızlıdır. Hata payı düşüktür. Hata payını en aza indirmek için veri tabanını düzenli olarak güncellemesi gerekir. Öte yandan, daha önce karşılaşmadıkları saldırılara karşı etkisizdirler (Taş, 2022).

Şekil 3. İmza Tabanlı saldırı tespit sistemi mimarisi

2.2. Anomali Tabanlı Saldırı Tespit Sistemleri

Anomali tabanlı STS, çeşitli yapay zeka yöntemleri vasıtasıyla normal ve anormal veriler kullanılarak sistem eğitilmektedir. İmza tabanlı STSler daha önce karşılaşılmış, tanınan saldırılar karşısında iyi çözüm üretirken Anomali tabanlı STSler daha önce karşılaşılmamış, tanınmayan ve tecrübe edilmemiş saldırılara karşı da çözüm üretmektedir. Fakat sistemin yanlış alarm verme ihtimali bulunmaktadır, bu da en büyük dezavantajlarıdır (Taş, 2022).



Şekil 4. Anomali tabanlı saldırı sistem mimarisi

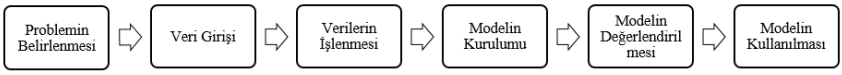
2.3. Saldırı Tespit Sistem Araçları

Saldırı Tespit Sistemleri, ağ trafiğini ve sistem etkinliklerini izleyerek şüpheli veya kötü niyetli faaliyetleri tespit ederek ya da siber saldırılara karşı erken uyarı sağlayarak raporlamaktadır. Böylece bu sistemler ağ güvenliğini artırarak mevcut ya da potansiyel tehditlerin hızlı bir şekilde belirlenmesine ve önlenmesine yardımcı olmaktadırlar. Günümüzde kullanılan STS araçlarını listeleyecek olursak; Hystack, WRS, Midas, İldes, Nadir, NSM, Hyperview, Ustat, Dids, Idiot, Ripper, Bro, Snort, Snortsam, Selks, Ossec, Firestorm, Kfsensor, Suricata, Snorby, Phpids, .Net Ids, Prelude, Aide, Samhain ve Acarm-ng örnek olarak verilebilir (Baykara, 2019).

Günümüzde başlayan ve gelecekte de devam edecek olan, yapay zekâ ve makine öğrenimi teknolojilerinin entegrasyonu sayesinde STS'lerin daha akıllı ve riskleri öngörür hale gelmesi beklenmektedir. Bu gelişmeler, yeni ortaya çıkan ve anlaşılması zor siber tehditleri daha etkin bir şekilde tespit etmeye olanak tanıyacaktır.

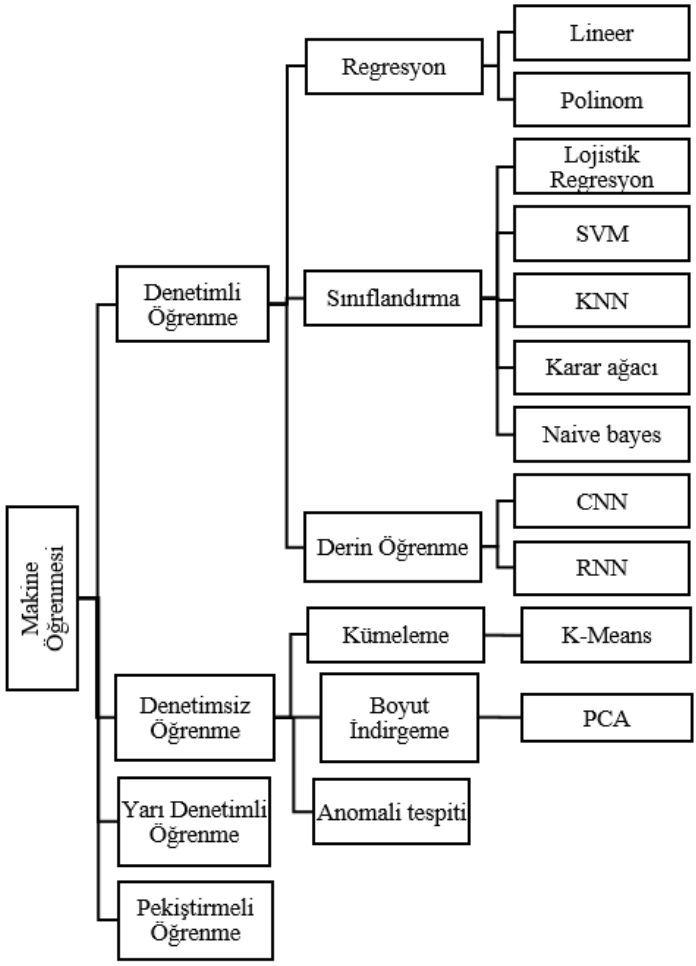
3. MAKİNE ÖĞRENMESİ

Makine öğrenmesi, bilgisayarların veri kümeleri üzerinden öğrenme yeteneği kazandığı ve kazandığı deneyimleri çalıştırıp geliştirebildiği bir yapay zeka alt kümesidir. Temel çalışma mantığı; bir görevi gerçekleştirebilmek için üzerinde çalıştığı veri setinden kurallar, algoritmalar, formüller çıkararak programlamaya ayrıca gerek kalmadan veri analizi yapabilmektir (Janiesch vd., 2021). Gündelik hayatımızda kullandığımız birçok uygulamanın alt yapısında da makine öğrenmesi algoritmaları görev yapmaktadır.



Şekil 3. Makine Öğrenmesi Çalışma Prensibi

Makine öğrenmesi algoritmaları denetimli öğrenme, denetimsiz öğrenme, yarı denetimli öğrenme ve pekiştirmeli öğrenme olarak dörde ayrılmaktadır.

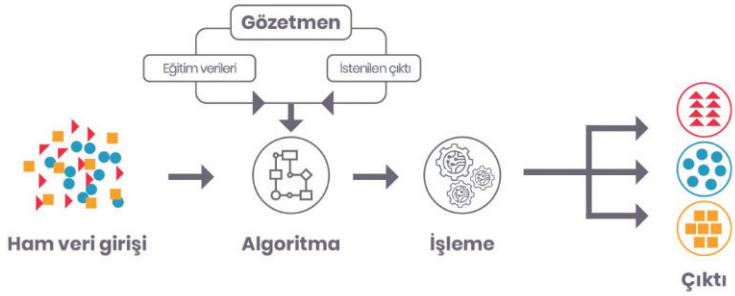


Şekil 4. Makine öğrenmesi çeşitleri

[https://www.dataexpertise.in/machine-learning-beginners-guide/] erişim:09.03.2025

3.1. Denetimli (Gözetimli) Öğrenme

Makine öğrenmesi yöntemlerinin en fazla tercih edilenidir. Modelin eğitimi için etiketli veriler kullanılır. Sistemde her girdi etiketine karşılık gelen bir çıktı etiketi bulunur. Eğitim verileriyle sistem eğitilir, sistemdeki girdi-çıktı ilişkilerini öğrenerek, daha önce karşılaşmadığı veriler için doğru tahminler yapabilmesi sağlanır. Denetimli öğrenme algoritmaları tahmin yaparken sınıflandırma veya regresyon yöntemlerini kullanır.



Şekil 5. Denetimli Öğrenme Mimarisi

[https://www.turhost.com/blog/makine-ogrenmesi-machine-learning-nedir/] erişim:10.03.2025

En fazla tercih edilen denetimli öğrenme algoritmaları; K-en yakın komşu(KNN) , karar ağaçları (decision tree), rasgele orman(random forest), lojistik regresyon, destek vektör makinesi(SVM), naive bayes olarak sıralanabilir (BTK,2025).

3.1.1.K-en yakın komşu (KNN)

KNN, sınıflandırma ve regresyon problemlerinin çözümünde kullanılan, fazlaca tercih edilen pratik bir algoritmadır. Bir veri noktasıyla ilgili tahmin yapabilmek için noktaya en yakın mesafedeki komşuların etrafındaki veri noktalarının değerlerinden faydalanır.

3.1.2.Karar ağaçları (decision tree)

Karar ağaçları hem regresyon hem de sınıflandırmada kullanılır. Ağaç yapısına benzer şekildeki algoritmaları ile veri tahmini yapmaya çalışır.

3.1.3.Rasgele orman

Birden fazla karar ağacının bir araya gelerek bir orman oluşturduğu denetimli öğrenme yöntemidir.

3.1.4.Lojistik regresyon

Bağımlı değişkenin kategorik türde olduğu durumlarda kullanılan, sınıflandırma işlemlerinde kullanılan bir algoritmadır.

3.1.5.Destek vektör makinesi (SVM)

Regresyon ve sınıflandırma problemlerinde fazlaca tercih edilen bir algoritmadır. Veri kümesini sınıflar arasında en doğru şekilde ayıracak

bir hiperdüzlem bulmaya çalışır. Doğrusal olmayan veri kümelerinde kullanılır.

3.1.6.Naive bayes

Bayes teoremi prensipleri üzerine kurulu bir algoritmadır. Olasılıklar üzerine çalışmalarda ve sınıflandırmalarda kullanılır.

3.2. Denetimsiz Öğrenme

Denetimsiz öğrenme, etiketsiz veriler üzerinde çalışır. Etiketsiz veriler arasındaki kuralları, işleyişleri, örüntüleri çözmeye çalışır. Denetimsiz öğrenme modellerinin kesin bir cevap anahtarı yoktur. Dolayısıyla birçok açıdan insan gözlemi içerir. Doğru tahmin başarı yüzdesi, ne kadar çok veri ile çalışırsa o kadar çok artar (Alloghani vd. 2020).

Denetimli öğrenme algoritmaları; K-Means kümeleme, Hiyerarşik kümeleme, DBSCAN (Gürültülü Uygulamalar için Yoğunluk Tabanlı Uzaysal Kümeleme) olmak üzere üç çeşittir.

3.2.1.K-Means kümeleme

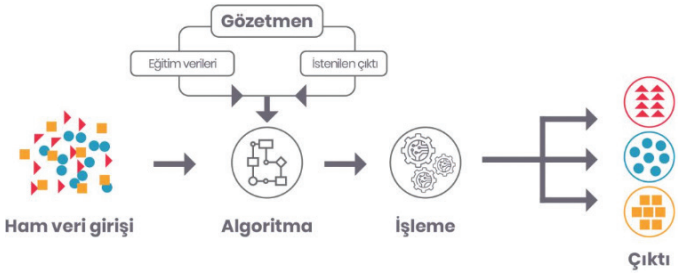
K-Means kümeleme, veri setindeki birbirine benzer örnekleri belirli sayıda kümelere ayırmak için kullanılır.

3.2.2.Hiyerarşik Kümeleme

Veri seti içerisindeki örnekleri hiyerarşik bir şekilde çeşitli kümelere ayıran algoritmadır.

3.2.3. DBSCAN

Düzensiz, belirli bir şekli olmayan veri setleri üzerinde çalışır. Veri noktalarının birbirlerine göre konumu ve yoğunluklarına göre kümeleme yapar.



Şekil 6. Denetimsiz Öğrenme Mimarisi
[https://www.turhost.com/blog/makine-ogrenmesi-machine-learning-nedir/]
erişim tarihi:06.02.2025

3.3. Yarı Denetimli Öğrenme

Yarı denetimli öğrenme, denetimli ve denetimsiz öğrenmenin bir araya gelerek işlediği bir algoritmadır. Modelde etiketli ve etiketsiz veriler birlikte bulunur. Bu sistemde amaç etiketlenmemiş verilerin, etiketsiz veriler ile aynı ortamda bulundurularak öğrenme performansını artırmaya çalışmaktır.

3.4. Pekiştirmeli Öğrenme

Pekiştirmeli öğrenme, bir ortamda ödülleri en üst düzeye çıkarmak için eylemleri seçmeye dayalı bir algoritmadır. Pekiştirmeli öğrenmede sistem ajan ve ödül üzerine kuruludur. Ajan deneme yanılma yöntemleriyle görevini öğrenip, bir dahaki sefere görevini başarıyla tamamlamaya çalışır (Bonaccorso,2018)

4. SALDIRI TESPİT SİSTEMİ TASARIMINDA EN YAYGIN KULLANILAN VERİ SETLERİ

Saldırı Tespit Sistemlerinin tasarımında araştırmacıların karşına çıkan en büyük zorluk veri seti elde etmektir. Çünkü gerçek bir ağ trafiğinin izlenmesi, gözlenmesi ve kaydedilmesi oldukça zahmetli, masraflı ve zaman gerektiren işlemlerdir. Bundan dolayı araştırmacılar çalışmalarında genellikle herkese açık veri setlerinden faydalanıp, çeşitli yöntemler kullanarak önceki çalışmalardaki doğruluk oranlarını daha üst bir seviyeye çekmeye çalışmaktadırlar. STS alanlarında en çok tercih edilen, laboratuvar ortamında oluşturulmuş bazı veri setleri bu çalışmada incelenmiştir.

Tablo 1. Veri Setleri Özellikleri

Veri Seti	İçerdiği Saldırı Sayısı	İçerdiği Öznitelik Sayısı
DARPA	57	≈80
KDDCUP99	24	41
NSL-KDD	24	42
UNSW-NB15	9	49
BOT-IOT	8	33
CICDDOS2019	11	83

4.1. DARPA (Defence Advanced Research Project Agency)

DARPA veri setleri DARPA 1998, 1999 ve 2000 olarak ayrı ayrı yıllarda güncellenmiş olan veri setleridir. Bu veri setleri DARPA' nın sponsor-

luğu ile MIT Lincoln Sponsorluğunda STS'lerin verimliliğini ölçmek için oluşturulmuştur. Farklı IP'ler arasındaki siber saldırı örnekleri barındırmaktadır (Aydın, 2005).

Veri setleri (1998, 1999, 2000) toplam 5 haftalık süreyi kapsamaktadır, ilk 3 haftası eğitim (training) verileri, son 2 haftası test verileridir. Yaklaşık 80 adet öznitelik bulundurmaktadır.

4.2. KDD Cup 99 (Knowledge Discovery and Data Mining Tools Cup)

KDD Cup 99 veri seti, Üçüncü Bilgi Keşfi ve Veri Madenciliği Araçları Yarışması'nda kullanılmak için sanal ortamdan transfer edilen veriler topluluğudur. Literatürde yapılan çalışmalarda ve deneylerde en çok kullanılan veri setlerinden biridir. Bu veri kümesi DARPA veri setinin güncellenmiş halidir. Dokuz haftalık ağ trafiğinden veriler alınmıştır. Verilerin yedi haftalık kısmı eğitim seti, iki haftalık kısmı da test seti olarak ayrılmıştır. Eğitim setinde yaklaşık beş milyon, test setinde iki milyon bağlantı bulunmaktadır. Neptune-DOS, pod-DOS, Smurf-DoS ve arabellek taşması gibi 22 adet farklı saldırı türü barındırmaktadır.41 adet feature(özellik) bulunmaktadır. Bu veri setinde normal durum ve saldırı durumu simüle edilerek veri kümesinde bu veriler birleştirilmiştir. Yani veri seti gerçek olmayıp gerçek bir ağın simüle edilmesi sonucunda elde edilmiştir (Karaman, 2020).

KDD Cup 99 veri setindeki saldırılar 4 ana kategoride sınıflandırılabilir. Bunlar Denial of Service (Hizmet Engelleme), Bilgi Tarama (Probing), Yönetici Hesabı ile Yerel Oturum Açma (Remote to Local-R2L), Kullanıcı Hesabının Yönetici Hesabına Yükseltilmesi'dir (KDD,2024).

4.3. NSL-KDD (Network Security Laboratory-Knowledge Discovery in Databases)

KDD Cup 99 veri seti, DARPA veri setlerinin zamanla iyileştirilmiş ve güncellenmiş halidir. NSL-KDD veri seti de KDD Cup 99 veri setindeki gereksiz görülen bazı kısımlarının çıkarılıp, iyileştirme yapılmış halidir. KDD Cup 99 veri seti içerisindeki fazla bağlantı kayıtları test verisinden kaldırılmıştır. Böylelikle makine öğrenmesi algoritmaları için daha uygun bir veri seti elde edilmiştir. İçerisinde 24 çeşit saldırı türü ve 42 öznitelik bulunmaktadır. NSL-KDD veri setinin kullanımın kolay, anlaşılır olması, sınıflandırma işlemleri açısından uygun olması, veri sayısının gayet makul olması, test ve eğitim verileri ayrılarak çalışıldığında sonuçların tatmin edici olması bu veri setinin tercih edilme sebeplerindendir (UNB,2024). Fakat gerçek zamanlı ağ trafiği verilerinden uzak olup, gü-

nümüz ağ trafikleri açısından güncel olmaması araştırmacıların yeni veri setleri elde etme konusunda arayışa yönlendirmiştir.

4.4. UNSW-NB15 (University of New South Wales - Network Based 15)

Literatürü genel olarak incelediğimizde STS konusunda en çok kullanılan veri setleri KDD Cup 99 ve NSL-KDD veri setleridir. Sıklıkla tercih edilmelerine rağmen bazı dezavantaj ve eksiklikleri de bünyelerinde barındırmaktadırlar. Örneğin bahsettiğimiz veri setlerinde atak tipi çeşitliliği azdır ve laboratuvar ortamlarında oluşturulmuş ağ trafiği senaryoları da günümüz ağ trafiklerine göre geri kalmış durumdadır. Bu sebeple eski veri setlerinin sınırlamalarını aşmak ve daha güncel saldırı türlerini kapsamak amacıyla IXIA PerfectStorm aracı kullanılarak Avusturya Siber Güvenlik Merkezi Laboratuvarlarında 100 GB büyüklüğünde UNSW-NB15 veri seti oluşturulmuştur (Moustafa ve Slay, 2016). UNSW-NB15, gerçekçi ağ trafiği senaryolarını temsil etmek üzere tasarlanmıştır ve 9 çeşit saldırı türü (örneğin, DDoS, exploitler, zararlı yazılımlar vb.) ve 49 adet feature içermektedir. Bu veri seti, makine öğrenimi ve derin öğrenme modellerinin ağ güvenliği alanında test edilmesi ve değerlendirilmesi için yaygın olarak kullanılmaktadır.

4.5. BoT-IoT (Botnet-Internet of Things)

Bot-Iot veri seti, Cyber Range laboratuvarında doğal bir ağ ortamı çalışılarak nesnelerin interneti (IoT) altyapısına uyum sağlanarak oluşturulmuştur. İçerinde 8 farklı saldırı türü ve 33 adet feature bulundurmaktadır. IoT cihazlarının (akıllı ev cihazları, sensörler, kameralar vb.) ağ trafiğini simüle eder. Bu, IoT cihazlarının güvenlik açıklarını ve botnet saldırılarına karşı savunmasızlığını analiz etmek için önemlidir (Korniotis vd., 2019).

4.6. CICDdos2019 (Canadian Institute for Cybersecurity Distributed Denial of Service 2019)

Kanada Siber Güvenlik Enstitüsü tarafından hazırlanmış olan CICDDoS2019 veri seti daha önce Enstitünün hazırlamış olduğu veri setlerindeki eksiklikler/problemler giderilerek tasarlanmış olup Dağıtılmış Hizmet Reddi (DDoS) saldırılarını tespit etmek amacıyla kullanılan bir veri setidir (UNB,2024). İçerisinde 11 çeşit DDOS saldırısı bulunmaktadır. Bu saldırılar, gerçek dünya senaryolarını temsil edecek şekilde simüle edilmiştir. Veri seti, ağ trafiğini analiz etmek için 83 adet özellik (feature) içerir. Bu özellikler, paket boyutu, protokol türü, zaman damgası, kaynak ve hedef IP adresleri gibi bilgileri kapsar (Elsayed vd., 2020).

5. VERİ İŞLEME

Günümüz teknolojisinde devletlerin, kurumların, şirketlerin hatta artık kişilerin de elinde çok fazla veri (data) bulunabilmektedir ve yukarı yönlü artış göstermektedir. Mevcut veriler ile çalışıp başarılı sonuçlar elde edilebilmesi için veri işleme denilen bir takım adımlar uygulanmalıdır. Yapay zeka yöntemleri veri analizi yapmak için kullanılan en verimli araçlardandır. Ancak makine öğrenmesi ve yapay zeka algoritmalarının başarılı sonuçlar verebilmesi için veri işleme işlemlerinin en doğru şekilde yapılması gerekir.

5.1.Veri Ön İşleme

Verilerin analiz edilebilir hale gelebilmesi için uygulanması gereken işlemlerdir.

Veri ön işleme adımları;

Verilerin toplanması, Verilerin temizlenmesi, Verilerin birleştirilmesi, Verilerin bölünmesi, Verilerin kaydedilmesi.

Mevcuttaki veri yığınına veri ön işleme adımları sırayla uygulandıktan sonra veri setine ; "Öznitelik Mühendisliği" dediğimiz, modellerin başarısını doğrudan etkileyen özniteliklerin daha başarılı şekilde çıkarılması konusu üzerinde çalışan mühendislik yöntemleri uygulanmalıdır. (Öznitelik: Verilerin özelliklerini, niteliklerini belirten değerlerdir.)

Öznitelik Mühendisliği Adımları;

Özellik seçimi, Özellik çıkarma, Yeni özellik türetme, Özellik dönüştürme, Özellik ölçeklendirme, Aykırı değerleri işleme, Eksik değerleri işleme.

6. LİTERATÜR

Son yıllarda siber saldırıda kullanılan veri setlerini ve bu veri setleri üzerinde yapılan saldırı tespit sistemlerinde kullanılan yöntemler ve elde edilen sonuçların özeti Tablo 1'de verilmiştir.

Tablo 2. *Siber güvenlikte veri setlerini ve makine öğrenimi tabanlı yaklaşımları derleyen çalışmalar ve özellikleri*

ARAŞTIRMACI/ ÇALIŞMA ADI	KULLANILAN VERİ SETİ	EN İYİ SONUÇ ALINAN MAKİNE ÖĞRENMESİ YÖNTEMİ	SONUÇ (DOĞRULUK YÜZDESİ)
Taher vd., 2019	NSLKDD	Yapay sinir ağları	%94,02
Özekes ve Karakoç, 2019	CICIDS2017	Random forest	%99,96
Uğurlu vd.,2023	CICDarknet2020	Karar ağacı	%93,32
Okur ve Dener, 2021	WSN-DS	Random forest	%99,72
M.Karaman, 2020	CSE-CIC-IDS2018	Karar Ağacı	%99,97
Kaynar vd., 2018	KDDCUP99	KNN, DVM	%99,00(KNN)
Han vd., 2022	CICIDS2017	Yapay sinir ağları	%96,55
Korkmaz, 2016	Bireysel veri seti	Yapay sinir ağları	%85,50
Şahingöz vd., 2019	Bireysel veri seti	Random Forest	%97,98
Kaya vd., 2016	KDDCUP99	KNN, Yapay sinir ağları, Karar ağacı	%100(DOS-KNN, karar ağacı, Yapay sinir ağları)
Aygün ve Yavuz, 2017	NSLKDD-test	Stokastik eşik değeri belirleme metodu	%88,28
Tang vd., 2020	NSLKDD	LightGBM	%89,82
Aksu ve Aydın, 2018	CICIDS2017	DVM, derin öğrenme	%97,80(derin öğrenme) %69,79(DVM)
Niyaz vd., 2015	NSLKDD	Derin öğrenme	%98,00
Bıçakcı ve Toklu, 2022	NSLKDD	Random forest	%99,67
Kanimozhi vd.,2019	CSE-CIC-IDS2018	Yapay sinir ağları	%99,97
Nur, 2021	NSLKDD	Yapay sinir ağları	%97,83
Nur, 2022	UNSWNB15	Yapay sinir ağları	%98,21
Türkoğlu vd., 2022	SD-VANET	Karar ağacı	%99,35
Taş, 2022	NSLKDD	LightGBM	%98,60
Karaman, 2020	CSE-CIC-IDS2018	Karar ağacı	%99,97
Ekici ve Takcı, 2022	CICIDS2017	Random forest	%94,00
Tuğrul vd., 2022	CICIDS2017	J48	%99,92
Saphezhi vd., 2022	Bireysel veri seti	Karar ağacı, Random forest, KNN	%99,00(DOS saldırıları)
Sarkar vd., 2023	NSLKDD	MLP	%89,32
Mazini vd., 2019	ISCXIDS2012	Adaboost	%98,90
Gürmen, 2020	NSLKDD	Bagging Topluluk Sınıflandırıcı	%99,78
Khempetch, 2021	CICDDOS2019	Yapay sinir ağları	%99,50(DOS saldırıları)

Selvan, 2021	CICIDS2017	SVM	%96,51
Nanda ve ark. [55]	Bireysel veri seti	Naive Bayes	%91,68
Özalp vd., 2022	NSLKDD	Random forest	%97,00
Güven, 2007	Bireysel veri seti	Çok katmanlı Yapay sinir ağları	%97,92
Aytaç, 2020	CICDDOS2019	KNN	%99,90
Benqdara vd., 2014	KDDCUP99	KM-GSA, KM-PSO, FCM	%94,47
Gaikwad vd., 2015	NSLKDD	Bagging Topluluk Sınıflandırıcı	%99,67

7. SONUÇ VE ÖNERİLER

Literatüre bakıldığında saldırı tespiti çalışmalarında en fazla tercih edilen makine öğrenmesi yöntemlerinin karar ağaçları, yapay sinir ağları ve destek vektör makinesi algoritmaları olduğu görülmüştür. En çok tercih edilen veri setleri ise NSLKDD ve UNSW veri setleridir. Bazı çalışmalarda araştırmacıların kendi veri setlerini oluşturdukları, bazı araştırmacıların da hazır veri setlerinden yararlandıkları gözlemlenmiştir. Çalışmalarda laboratuvar ortamında oluşturulmuş simülasyon verileri yerine gerçek dünya verileri ve gerçek ağ trafikleri içeren veri setleri kullanılırsa çok daha gerçekçi, özgün ve geliştirilebilir çalışmalar gerçekleştirilebileceği görülmektedir. Gerçek değerler içeren veri setlerine ulaşılamıyor ise mevcut simülasyon veri setlerinin düzenli olarak güncellenmesinin ve iyileştirilmesinin gerekliliği ve önemi görülmüştür.

KAYNAKÇA

Alloghani, M., Al-Jumeily, D., Mustafina, J., Hussain, A., ve Aljaaf, A. J. (2020). A Systematic Review on Supervised and Unsupervised Machine Learning Algorithms for Data Science. 3–21. https://doi.org/10.1007/978-3-030-22475-2_1

Arul Selvan, M. (2021). Destek Vektör Makineleriyle Güçlü Siber Saldırı Algılama: Hem Yerleşik Hem de Yeni Tehditlerle Mücadele. Bilim Teknoloji ve Araştırma Dergisi (JSTAR) 2 (1):160-165.

Aydın, 2005.Bilgisayar Ağlarında Saldırı Tespiti İçin İstatistiksel Yöntem Kullanılması, İstanbul Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi

Aytaç, T., 2020. DDOS Saldırılarının Tespitinde Makine Öğrenmesi Yöntemlerinin Uygulanması, İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi

Baykara M. ve R. Daş, "Saldırı tespit ve engelleme araçlarının incelenmesi", DÜMF MD, c. 10, sy. 1, ss. 57–75, 2019, doi: 10.24012/dumf.449059.

Benqdara, Salima & Ngadi, Md & Mohamad Sharif, Johan & Ali, Saqib. (2014). Ensemble of clustering algorithms for anomaly intrusion detection system. Journal of Theoretical and Applied Information Technology. 70. 425-431. https://www.researchgate.net/publication/286211330_Ensemble_of_clustering_algorithms_for_anomaly_intrusion_detection_system

Bıçakcı, M. S., ve Toklu, S. (2022). Bilgisayar Ağı Güvenliği için Hibrit Öznitelik Azaltma ile Makine Öğrenmesine Dayalı Bir Saldırı Tespit Sistemi Tasarımı. Journal of Gaziosmanpasa Scientific Research, 11(3), 203–220. https://dergipark.org.tr/en/pub/gbad/issue/74308/1200540

Bonaccorso, G. (2018). *Machine Learning Algorithms: Popular algorithms for data science and machine learning*. Packt Publishing Ltd.

C. Okur ve M. Dener, "Makine Öğrenme Metotları Kullanılarak KSA Ddos Saldırıları Tespiti", ECJSE, c. 8, sy. 3, ss. 1550–1564, 2021, doi: 10.31202/ecjse.971592.

D. Aksu and M. Ali Aydin, "Detecting Port Scan Attempts with Comparative Analysis of Deep Learning and Support Vector Machine Algorithms," 2018 International Congress on Big Data, Deep Learning and Fighting Cyber Terrorism (IBIGDELFT), Ankara, Turkey, 2018, pp. 77-80, doi: 10.1109/IBIGDELFT.2018.8625370.

Ekici, B., ve Takcı, H. (2022). Bilgisayar Ağlarında Anomali Tespiti Yaklaşımı ile Saldırı Tespiti. Afyon Kocatepe Üniversitesi Fen Ve Mühendislik Bilimleri Dergisi, 22(5), 1016–1027. https://doi.org/10.35414/AKUFEMUBID.1114906

Gaikwad, D. & Thool, Ravindra. (2015). Intrusion Detection System Using Bagging Ensemble Method of Machine Learning. 291-295. 10.1109/ICCUBEA.2015.61. https://www.researchgate.net/publication/283593807_Intrusion_Detection_System_Using_Bagging_Ensemble_Method_of_Machine_Learning

Gültekin, 2022. Siber Saldırılar ve Uluslararası Güvenlik, Selçuk Üniversitesi,Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Anabilim Dalı, Yüksek Lisans Tezi

Gürmen, 2020. Saldırı Tespit Sistemleri İçin Makine Öğrenmesi Yöntemlerinin Performans Karşılaştırması, Harran Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi

Güven, E. N., 2007. Zeki Saldırı Tespit Sistemlerinin İncelenmesi, Tasarımı ve Gerçekleştirilmesi, Gazi Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi

Han, H., Kim, H., ve Kim, Y. (2022). An Efficient Hyperparameter Control Method for a Network Intrusion Detection System Based on Proximal Policy Optimization. Symmetry 2022, Vol. 14, Page 161, 14(1), 161. https://doi.org/10.3390/SYM14010161

https://www.btkakademi.gov.tr/portal/course/5-1-denetimli-ogrenme-10989 erişim tarihi: 10.03.2025

http://kdd.ics.uci.edu/databases/kddcup99/kddcup99.html erişim: 18.10.2024

https://www.unb.ca/cic/datasets/nsl.html Erişim :21.10.2024

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf (erişim :12.02.2025)

https://www.unb.ca/cic/datasets/ddos-2019.html ve Erişim tarihi: 24.10.2024

https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(BT)-Kullanim-Arastirmasi-2024-53492 Erişim : 02.01.2025

https://tr.wikipedia.org/wiki/Bilgi_g%C3%BCvenli%C4%9Fi#:~:text=Bilgi%20g%C3%BCvenli%C4%9Fi%2C%20(Gizlilik%2C%20B%C3%BCt%C3%BCnl%C3%BCk,olan%20izinsiz%20eri%C5%9Fimleri%20engelleme%20i%C5%9Flemi. Erişim :22.12.2024

https://nvlpubs.nist.gov/nistpubs/legacy/sp/nistspecialpublication800-145.pdf (erişim :12.02.2025)

https://dsy.usom.gov.tr/usom/19/02/190211082958_siber_guvenlige_giris_ve_temel_kavramlar.pdf Erişim tarihi: 10.11.2024

http://ozocak.com/Dosyalar/27669f.pdf Erişim tarihi: 17.12.2024

Hussain, Jamal & Mishra, Aishwarya. (2017). Performance Analysis of Some Neural Network Algorithms using NSL-KDD Dataset. International Journal of Computer Trends and Technology. 50. 43-49. 10.14445/22312803/IJCTT-V50P107.

İ. Karabey Aksakallı, "BULUT BİLİŞİMDE GÜVENLIK ZAFİYETLERİ, TEHDİTLERI VE BU TEHDİTLERE YÖNELİK GÜVENLİK ÖNERİLERİ", UBGMD, c. 5, sy. 1, ss. 8–34, 2019, doi: 10.18640/ubgmd.544054.

Janiesch, C., Zschech, P., ve Heinrich, K. (2021). Machine learning and deep learning. Electronic Markets, 31(3), 685–695. https://doi.org/10.1007/S12525-021-00475- 2/TABLES/2,

Javaid, Ahmad & Niyaz, Quamar & Sun, Weiqing & Alam, Mansoor. (2015). A Deep Learning Approach for Network Intrusion Detection System. EAI Endorsed Transactions on Security and Safety. 3. 10.4108/eai.3-12-2015.2262516. https://www.researchgate.net/publication/288991542_A_Deep_Learning_Approach_for_Network_Intrusion_Detection_System

K. A. Taher, B. Mohammed Yasin Jisan and M. M. Rahman, "Network Intrusion Detection using Supervised Machine Learning Technique with Feature Selection," 2019 International Conference on Robotics,Electrical and Signal Processing Techniques (ICREST), Dhaka, Bangladesh, 2019, pp. 643-646, doi: 10.1109/ICREST.2019.8644161.

Kanimozhi, V., ve Prem Jacob, T. (2019). Artificial intelligence based network intrusion detection with hyper-parameter optimization tuning on the realistic cyber dataset CSE-CIC-IDS2018 using cloud computing. Proceedings of the 2019 IEEE International Conference on Communication and Signal Processing, ICCSP 2019, 33–36. https://doi.org/10.1109/ICCSP.2019.8698029

Karaman, 2020.Anomali Tabanlı Saldırı Tespit Sistemlerinde Makine Öğrenmesi Modellerinin Performans Değerlendirmesi, İstanbul Ticaret Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi

Kaya, Çetin & Yildiz, Oktay & Ay, Sinan. (2016). Performance Analysis of Machine Learning Techniques in Intrusion Detection. 10.1109/SIU.2016.7496029. https://www.researchgate.net/publication/303437737_Performance_Analysis_of_Machine_Learning_Techniques_in_Intrusion_Detection

Kaynar, O., Arslan, H., Görmez, Y., Işık, Y. E. (2018). Makine Öğrenmesi ve Öznitelik Seçim Yöntemleriyle Saldırı Tespiti. Bilişim Teknolojileri Dergisi, 11(2), 175-185. https://doi.org/10.17671/gazibtd.368583

Korkmaz, Yusuf. (2016). Developing password security system by using artificial neural networks in user log in systems.10.1109/EBBT.2016.7483682.https://www.researchgate.net/publication/303772492_Developing_password_security_system_by_using_artificial_neural_networks_in_user_log_in_systems

Koroniotis, N., Moustafa, N., Sitnikova, E., & Turnbull, B. (2019). Towards the development of realistic botnet dataset in the Internet of Things for network forensic analytics: Bot-IoT dataset. *Future Generation Computer Systems*, *100*, 779-796. https://doi.org/10.1016/j.future.2019.05.041.

Mazini, M., Shirazi, B., ve Mahdavi, I. (2019). Anomaly network-based intrusion detection system using a reliable hybrid artificial bee colony and AdaBoost algorithms. Journal of King Saud University - Computer and Information Sciences, 31(4), 541–553. https://doi.org/10.1016/J.JKSUCI.2018.03.011

Moustafa ve Slay, 2016. "The Evaluation of Network Anomaly Detection Systems: Statistical Analysis of the UNSW-NB15 Data Set and the Comparison with the KDD99 Data Set"

M. S. Elsayed, N. -A. Le-Khac, S. Dev and A. D. Jurcut, "DDoSNet: A Deep-Learning Model for Detecting Network Attacks," *2020 IEEE 21st*

International Symposium on "A World of Wireless, Mobile and Multimedia Networks" (WoWMoM), Cork, Ireland, 2020, pp. 391-396, doi: 10.1109/WoWMoM49955.2020.00072

Nur, 2021.GKO Algoritması ve YSA kullanarak Hibrit Bulut Tabanlı Saldırı Tespit ve Yanıt Sistemi, Konya Teknik Üniversitesi, Fen Bilimleri Enstitüsü, Yüksek Lisans Tezi

Özalp, Ahmet & Albayrak, Zafer. (2022). Detecting Cyber Attacks with High-Frequency Features using Machine Learning Algorithms. Acta Polytechnica Hungarica. 19. 213-233. 10.12700/APH.19.7.2022.7.12.

Özekes, S., & Karakoç, E. N. (2019). Makine Öğrenmesi Yöntemleriyle Anormal Ağ Trafiğinin Tespit Edilmesi. Duzce University Journal of Science and Technology, 7(1), 566-576. https://doi.org/10.29130/dubited.498358

Özgür, A., & Erdem, H. (2012). Saldırı Tespit Sistemlerinde Kullanılan Kolay Erişilen Makine Öğrenme Algoritmalarının Karşılaştırılması. Bilişim Teknolojileri Dergisi, 5(2), 41-48.

R. C. Aygün and A. G. Yavuz, "A stochastic data discrimination based autoencoder approach for network anomaly detection," 2017 25th Signal Processing and Communications Applications Conference (SIU), Antalya, Turkey, 2017, pp. 1-4, doi: 10.1109/SIU.2017.7960410.

Saghezchi, FB, Mantas, G., Violas, MA, de Oliveira Duarte, AM, & Rodriguez, J. (2022). Endüstri 4.0 CPPS'lerinde DDoS Saldırısı Algılama için Makine Öğrenimi. *Electronics*, *11* (4), 602. https://doi.org/10.3390/electronics11040602

Sahingoz, O. K., Çebi, C. B., Bulut, F. S., Fırat, H., vd. (2019). Saldırı Tespit Sistemlerinde Makine Öğrenmesi Modellerinin Karşılaştırılması. Erzincan University Journal of Science and Technology, 12(3), 1513-1525. https://doi.org/10.18185/erzifbed.573648

Sarkar, A., Sharma, H. S., ve Singh, M. M. (2023). A supervised machine learning-based solution for efficient network intrusion detection using ensemble learning based on hyperparameter optimization. International Journal of Information Technology (Singapore), 15(1), 423–434. https://doi.org/10.1007/S41870-022-01115- 4/TABLES/7

Shurrab, S., ve Duwairi, R. (2022). Self-supervised learning methods and applications in medical imaging analysis: a survey. PeerJ Computer Science, 8, e1045. https://doi.org/10.7717/PEERJ-CS.1045

Tang, C., Luktarhan, N., ve Zhao, Y. (2020). An Efficient Intrusion Detection Method Based on LightGBM and Autoencoder. Symmetry 2020, Vol. 12, Page 1458, 12(9), 1458. https://doi.org/10.3390/SYM12091458

Thapanarath Khempetch, Pongpisit Wuttidittachotti Department of Data Communication and Networking, King Mongkut's University of Technology North Bangkok, Thailand https://urn.fi/URN:NBN:fi-fe2015072310696 Erişim tarihi: 24.12.2024

Taş, 2022. Nesnelerin İnterneti İçin Akıllı Saldırı Tespit Ssitemleri Geliştirilmesi, İstanbul Sabahattin ZaimÜniversitesi, Fen Bilimleri Enstitüsü, Doktora Tezi

Tuğrul, B. ve Ahmed, ASA (2022). Makine öğrenme yöntemleri ile ağ trafik analizi. Niğde Ömer Halisdemir Üniversitesi Mühendislik Bilimleri Dergisi, 11(4), 862-870. https://doi.org/10.28948/ngumuh.1113956

Türkoğlu, M., Polat, H., Koçak, C., ve Polat, O. (2022). Recognition of DDoS attacks on SD-VANET based on combination of hyperparameter optimization and feature selection. Expert Systems with Applications, 203, 117500. https://doi.org/10.1016/J.ESWA.2022.117500

Uğurlu ve ark. / Journal of the Faculty of Engineering and Architecture of Gazi University 38:3 (2023) 1737-1746

DİJİTAL TEKNOLOJİLERİN ULUSLARARASI İLİŞKİLERE ETKİSİ

Sıddık ARSLAN[1]

1 Dr., siddikarslan@hotmail.com

1. GİRİŞ

Dijital teknolojilerin uluslararası ilişkilerde neden olduğu köklü dönüşüm, devletlerin güvenlik, ekonomi ve diplomasi süreçlerini yeniden şekillendirmektedir. Yapay zekâ, blok zinciri, kuantum bilişim ve siber güvenlik gibi teknolojik gelişmeler, küresel güç dengelerini ve devletlerarası rekabeti belirleyen temel unsurlar haline gelmiştir (Nye, 2021; Floridi, 2018). Bu dönüşüm süreci, geleneksel uluslararası ilişkiler teorilerinin açıklama kapasitesini zorlarken, yeni analitik çerçevelerin geliştirilmesini gerekli kılmaktadır. 21. yüzyılda devletlerin güç kapasiteleri, yalnızca askeri ve ekonomik kaynaklarıyla değil, aynı zamanda dijital teknolojilere erişimleri, bu teknolojileri geliştirme ve uygulama yetenekleri ile de ölçülmektedir.

Dijital teknolojiler, güvenlik anlayışını radikal biçimde değiştirmiştir. Geleneksel güvenlik paradigmasında askeri güç ve coğrafi konum belirleyici iken; dijital çağda siber güvenlik, veri akışı hâkimiyeti ve yapay zekâ destekli karar sistemleri ön plana çıkmaktadır. Siber savaşlar ve dezenformasyon kampanyaları, devletlerin ulusal güvenlik politikalarını yeniden şekillendirirken, uluslararası hukuk mekanizmalarının bu yeni tehditlere adaptasyonu belirsizliğini korumaktadır (Singer & Brooking, 2019; Arquilla & Ronfeldt, 2020). Dijital tehditler, fiziksel sınırları aşan, atfedilmesi zor ve asimetrik etkilere sahip olmaları nedeniyle geleneksel güvenlik anlayışlarını ve caydırıcılık teorilerini yetersiz kılmaktadır.

Dijitalleşmenin uluslararası ilişkiler üzerindeki çok boyutlu etkilerini kapsamlı bir perspektifle ele alan bu araştırma; küresel siyaset, ekonomi, güvenlik ve hukuk bağlamında dönüşüm sürecinin dinamiklerini analiz etmektedir. Teorik ve analitik bir çerçeve sunarak disiplinler arası bir değerlendirme yapmayı ve geleceğe yönelik stratejik çıkarımlar ortaya koymayı hedeflemektedir. Özellikle büyük teknoloji şirketlerinin artan etkisi ve dijital egemenlik tartışmaları bu araştırmayı daha da önemli hale getirmektedir (Choucri, 2021; Fukuyama, 2021). Google, Amazon, Facebook, Apple ve Microsoft gibi teknoloji şirketlerinin, devlet benzeri güç kapasitelerine ulaşması, uluslararası ilişkiler disiplinin temel aktör kavramını yeniden düşünmeyi gerektirmektedir.

Dijitalleşmenin uluslararası ilişkiler üzerindeki etkileri dış politika, güvenlik, ekonomi ve hukuk alanlarında kapsamlı bir dönüşüm oluşturmaktadır. Geleneksel analiz modelleri jeopolitik konum, askeri kapasite ve ekonomik büyüklük gibi somut unsurlara dayanırken; dijital teknolojilerin yaygınlaşması devletlerin etkileşim biçimlerini ve küresel sistemin işleyişini daha karmaşık hale getirmiştir (Nye, 2021; Floridi, 2018). Bu karmaşıklık yeni teorik yaklaşımların ve metodolojik araçların geliştirilmesini zorunlu kılmaktadır. Dijital dönüşümün oluşturduğu çok katmanlı ve çok aktörlü uluslararası sistem, devlet merkezli analiz modellerinin ötesinde, ağ teorisi

ve kompleksite yaklaşımları gibi yeni analitik çerçevelerin kullanılmasını gerektirmektedir.

Bu çalışma; özellikle 2000 sonrası döneme odaklanarak ABD, Avrupa Birliği, Rusya ve Çin gibi büyük güçlerin dijitalleşme stratejilerini incelemektedir. Ancak dijital teknolojilerin etkilerini değerlendirme süreci, devletlerin ulusal güvenlik politikalarına bağlı olarak sınırlıdır. Özellikle siber savaş stratejileri, yapay zekâ destekli diplomasi ve kuantum bilişim tabanlı istihbarat operasyonları gibi alanlarda kamuya açık verilerin kısıtlı olması, ampirik analizlerin kapsamını daraltmaktadır (Choucri, 2021; West, 2021). Bu nedenle çalışma büyük ölçüde akademik literatür, devletlerin strateji belgeleri ve teknoloji şirketlerinin raporları gibi ikincil kaynaklara dayanmaktadır. Bu kaynaklar, dijital dönüşümün uluslararası ilişkiler üzerindeki etkilerini anlamak için değerli bilgiler sağlarken; gizli operasyonlar ve stratejik planlar gibi alanlarda önemli kısıtlamalar içermektedir.

Dijitalleşmenin uluslararası ilişkiler üzerindeki etkileri giderek daha fazla tartışılsa da henüz sistematik bir çerçeveye oturtulmamıştır. Geleneksel uluslararası ilişkiler teorileri, güç dengelerini fiziksel kapasite ve ekonomik kaynaklarla açıklarken; dijitalleşme bu dinamikleri köklü biçimde değiştirmektedir. Siber güvenlik tehditleri, yapay zekâ destekli savaş stratejileri, blok zinciri tabanlı ekonomik sistemler ve dijital diplomasi devletlerin güç projeksiyonlarını farklı boyutlara taşımaktadır (Nye, 2021; Singer & Brooking, 2019). Ancak bu dönüşümün uluslararası sistem üzerindeki uzun vadeli etkileri tam olarak anlaşılamamıştır. Bu çalışma, dijital dönüşümün hem güncel etkilerini analiz etmeyi hem de geleceğe yönelik öngörüler sunmayı amaçlamaktadır.

Ekonomik düzlemde dijitalleşme; uluslararası ticaret ve finans sistemlerini daha önce görülmemiş bir şekilde dönüştürmektedir. Blok zinciri tabanlı finansal sistemler, merkeziyetsiz finans mekanizmaları ve dijital para birimleri devletlerin geleneksel ekonomik kontrol mekanizmalarını zayıflatmaktadır (Brynjolfsson & McAfee, 2019; Floridi, 2018). Dijital ekonominin yükselişi; uluslararası finansal sistemin temel yapı taşlarını sarsarken, küresel ekonomik yönetişimin geleceğini de belirsiz hale getirmektedir. IMF ve Dünya Bankası gibi küresel aktörler, bu değişime nasıl yanıt vereceğini tam olarak belirleyememiştir. Özellikle Çin'in dijital yuan projesi, Rusya ve İran'ın yaptırımlara karşı blok zinciri temelli çözüm arayışları dijital finans teknolojilerinin jeopolitik etkilerini göstermektedir.

Dijital teknolojiler; küresel güvenlik ve diplomasi alanlarında da derin bir dönüşüm oluşturmaktadır. Yapay zekâ destekli karar alma sistemleri, siber savaş doktrinleri ve dezenformasyon kampanyaları uluslararası güvenlik paradigmalarını değiştirmekte; ancak bu tehditlere karşı nasıl bir politika geliştirilmesi gerektiği belirsizliğini korumaktadır (Arquilla & Ronfeldt,

2020; West, 2021). Bu durum devletlerin güvenlik stratejilerini ve diplomatik araçlarını yeniden değerlendirmelerini zorunlu kılmaktadır. Siber alanın "beşinci savaş alanı" olarak tanımlanması ve NATO'nun siber saldırıları 5. Madde kapsamında kolektif savunma gerektiren eylemler olarak kabul etmesi, dijital güvenlik tehditlerine verilen stratejik önemi göstermektedir.

Dijitalleşmenin uluslararası ilişkiler üzerindeki etkileri "teorik ve metodolojik" açıdan yeni araştırma sorularının ortaya çıkmasına neden olmuştur. Çalışmanın temel sorularından biri, dijitalleşmenin devletlerarası güç dengelerini nasıl değiştirdiğidir. Siber savaşlar geleneksel askeri çatışmaların yerini alırken; yapay zekâ destekli dezenformasyon kampanyaları uluslararası güvenlik tehditlerini farklı bir boyuta taşımaktadır (Nye, 2021; Arquilla & Ronfeldt, 2020). Bu dönüşüm, güvenlik çalışmalarının teorik çerçevesinin genişletilmesini gerektirmektedir. Geleneksel güç dengesi teorileri, caydırıcılık modelleri ve kriz istikrarı kavramları dijital çağın güvenlik dinamiklerini açıklamakta yetersiz kaldığından dolayı yeni teorik çerçevelerin geliştirilmesi gerekmektedir.

Bir diğer önemli araştırma sorusu, yapay zekâ destekli karar alma süreçlerinin uluslararası güvenlik politikalarına etkisidir. Dijitalleşmenin uluslararası hukuk normlarını nasıl dönüştürdüğü, siber saldırıların savaş ilanı sayılıp sayılamayacağı gibi hukuki belirsizlikler araştırmanın kritik konuları arasında yer almaktadır (Floridi, 2018; Singer & Brooking, 2019). Bu belirsizlikler, uluslararası hukukun dijital çağa adaptasyonunu zorlaştırmaktadır. Tallinn Kılavuzu gibi girişimler, siber operasyonların uluslararası hukuk çerçevesinde nasıl değerlendirileceğine dair önemli katkılar sağlamakla birlikte, devletlerarasında siber hukuk konusunda henüz bir uzlaşı sağlanamamıştır.

Dijitalleşmenin ekonomi üzerindeki etkileri de derinlemesine sorgulanmaktadır. Blok zinciri teknolojisi "uluslararası ticaret ve finans" sistemlerini nasıl dönüştürmektedir? Dijital paralar ve merkeziyetsiz finans sistemleri devletlerin para politikalarını nasıl etkileyecektir? Bu sorular, dijitalleşmenin iktisadi kontrol mekanizmaları üzerindeki uzun vadeli etkilerini tartışmaya açmaktadır (Brynjolfsson & McAfee, 2019; West, 2021). Küresel finansal sistemin geleceği, bu soruların yanıtlarına bağlı olarak şekillenecektir. ABD dolarının küresel rezerv para birimi statüsü Merkez Bankası Dijital Para Birimleri (CBDC) ve merkeziyetsiz finans (DeFi) sistemlerinin gelişimiyle yeni zorluklarla karşı karşıya kalmaktadır.

Araştırmanın hipotezleri, dijitalleşmenin uluslararası güç dengelerini köklü bir şekilde değiştirdiği, siber savaşların geleneksel güvenlik paradigmalarını dönüştürdüğü ve blok zinciri tabanlı finansal sistemlerin uluslararası ticaret üzerindeki etkilerini derinleştirdiği üzerine kuruludur (Choucri, 2021; Fukuyama, 2021). Bu hipotezler, dijital dönüşümün çok boyutlu etkile-

rini anlamaya yönelik kapsamlı bir analitik çerçeve sunmaktadır. Çalışmanın hipotezleri, aynı zamanda "*yapay zekâ sistemlerinin stratejik karar alma süreçlerindeki artan rolünün*" devletlerin dış politika yapım süreçlerini nasıl değiştireceğini de sorgulamaktadır.

Bu araştırma, dijital teknolojilerin uluslararası ilişkiler üzerindeki etkilerini analiz etmek için nitel bir araştırma yaklaşımı benimsemektedir. Dijitalleşmenin güvenlik, ekonomi, diplomasi ve küresel yönetişim üzerindeki geniş kapsamı tek bir metodolojiyle ele alınmasını güçleştirdiğinden, disiplinler arası bir analiz gerekmektedir (Nye, 2021; Floridi, 2018). Çalışma, teknolojik gelişmelerin devletlerin dış politika, güvenlik ve ekonomik stratejilerine entegrasyonunu inceleyerek uluslararası ilişkiler teorileri ile teknoloji odaklı dönüşüm süreçlerini birleştiren özgün bir model sunmaktadır. Bu metodolojik yaklaşım dijital teknolojilerin uluslararası ilişkiler üzerindeki etkilerini bütüncül bir çerçevede değerlendirmeyi mümkün kılmaktadır.

Araştırma metodolojisi, öncelikle teorik analiz yaparak dijitalleşmenin uluslararası sistem üzerindeki etkilerini açıklayan yaklaşımları değerlendirmektedir. Teknolojik determinizm, konstrüktivizm ve eleştirel perspektifler devletlerin dijital teknolojilere uyum sağlama biçimlerini, uluslararası normlarla nasıl bütünleştiğini ve küresel eşitsizliklere etkisini analiz etmek için kullanılmaktadır (Singer & Brooking, 2019; West, 2021). Bu teorik çerçeve, dijitalleşmenin uluslararası ilişkilerde neden olduğu dönüşümü sistematik biçimde ele almayı amaçlamaktadır. *Teknolojik determinist yaklaşım*, dijital teknolojilerin kendi iç mantığı ve dinamikleriyle geliştiğini ve toplumsal yapıları şekillendirdiğini savunurken; *konstrüktivist perspektif*, bu teknolojilerin toplumsal değerler ve normlar çerçevesinde yorumlandığını ve kullanıldığını vurgulamaktadır.

Ayrıca ABD, Çin, Rusya ve Avrupa Birliği gibi büyük güçlerin dijitalleşme politikaları karşılaştırmalı olarak incelenerek bu aktörlerin siber güvenlik stratejileri, yapay zekâ politikaları ve dijital diplomasi uygulamaları değerlendirilmektedir. Bu karşılaştırmalı analiz, dijital dönüşümün farklı siyasi sistemlerde nasıl yorumlandığını ve uygulandığını anlamamıza olanak sağlamaktadır. ABD'nin teknolojik üstünlük ve açık internet yaklaşımı, Çin'in dijital egemenlik ve siber güvenlik odaklı stratejisi ve Avrupa Birliği'nin normatif ve değer temelli dijital politikaları arasındaki farklar, küresel dijital yönetişimin geleceğini şekillendiren temel dinamiklerdir.

Bu araştırma soruları ve hipotezler, dijitalleşmenin uluslararası ilişkiler üzerindeki çok boyutlu etkilerini anlamaya yönelik kapsamlı bir çerçeve sunmaktadır. Çalışma, disiplinler arası bir yaklaşımla dijital teknolojilerin küresel sistem üzerindeki etkilerini analiz ederek uluslararası ilişkiler literatürüne özgün katkılar sağlamayı amaçlamaktadır (Floridi, 2018; OECD, 2021). Bu bağlamda araştırmanın bulguları, gelecekteki akademik çalış-

malar için yeni perspektifler sunacak ve politika yapıcılar için yol gösterici olacaktır. Dijital teknolojilerin yalnızca teknik yenilikler olarak değil, aynı zamanda uluslararası sistemin temel dinamiklerini değiştiren siyasi, ekonomik ve sosyal fenomenler olarak anlaşılması gerekmektedir.

Sonuç olarak çalışma, dijital teknolojilerin uluslararası ilişkiler disiplininde neden olduğu paradigmatik dönüşümü sistematik bir şekilde ele almaktadır. Araştırmanın teorik çerçevesi ve metodolojik yaklaşımı, dijitalleşmenin çok boyutlu etkilerini anlamak için kapsamlı bir analitik model sunmaktadır. Bu model, teknoloji-toplum-politika etkileşiminin yeni boyutlarını kavramamıza olanak sağlarken, gelecekteki araştırmalar için de sağlam bir temel oluşturmaktadır. Dijital çağda uluslararası ilişkilerin dönüşümünü anlamak ve bu dönüşümü yönetebilmek için yeni teorik yaklaşımlar, metodolojik araçlar ve politika çerçeveleri geliştirmenin önemi, bu araştırmanın temel motivasyonunu oluşturmaktadır.

2. LİTERATÜR TARAMASI

2.1. Dijital Teknolojilerin Uluslararası İlişkilerdeki Evrimi

Dijital teknolojiler, uluslararası ilişkilerde köklü değişimlere yol açarak devletlerin güç projeksiyonu, güvenlik stratejileri, ekonomi ve diplomasi süreçlerini dönüştürmüştür. Geleneksel askeri ve ekonomik güç unsurlarına ek olarak bilgi üstünlüğü, siber güvenlik, veri yönetimi ve yapay zekâ destekli karar alma mekanizmaları yeni rekabet unsurları haline gelmiştir. Dijitalleşmenin ortaya çıkardığı bu yeni parametreler, devletlerin uluslararası alandaki stratejik konumlanmalarını ve etki alanlarını doğrudan şekillendirmektedir. Artan dijital bağlantılılık ve teknolojik yenilikler, aktörler arasındaki etkileşim biçimlerini kökten değiştirmiş, klasik diplomatik ilişkileri yeni bir boyuta taşımıştır (Nye, 2021; Floridi, 2018).

Dijitalleşme, devletlerin jeopolitik stratejilerini ve güvenlik politikalarını yeniden şekillendirmelerine neden olurken, küresel teknoloji şirketleri uluslararası siyasette etkin aktörler haline gelmiştir. Google, Amazon, Facebook, Apple ve Microsoft gibi şirketler, devletlerin ekonomik ve politik bağımsızlığını etkileyen veri kontrol mekanizmaları oluşturarak küresel diplomasi süreçlerinde devletlerle rekabet eden güç merkezlerine dönüşmüştür. Bu şirketlerin sahip olduğu veri işleme kapasitesi ve kullanıcı etkileşimi, geleneksel devlet aktörlerinin kontrol alanının ötesine geçen bir etki oluşturmaktadır. Dijital platformların yaygınlaşması, devlet dışı aktörlerin uluslararası karar alma süreçlerindeki rolünü artırmış ve klasik diplomatik kanalların dışında alternatif etkileşim mekanizmaları oluşturmuştur (Arquilla & Ronfeldt, 2020; Zuboff, 2019).

Bu dönüşüm, ekonomik ve siyasi dengelerin yanı sıra güvenlik stratejilerini de değiştirmiştir. Bilgi akışını yönlendirme kapasitesine sahip devletler

ve aktörler, dezenformasyon stratejileri ve bilgi savaşlarıyla küresel politikayı etkileme gücü elde etmiştir. Rusya'nın 2016 ABD seçimlerine dijital müdahalesi ve Çin'in küresel veri altyapılarına yaptığı yatırımlar, bilginin küresel etkisini artırmada stratejik bir araç olarak kullanıldığını göstermektedir. Dijital araçların politik etki oluşturmak için kullanılması, geleneksel güç projeksiyonu anlayışının ötesinde, algı yönetimi ve kamuoyu manipülasyonuna dayalı yeni müdahale biçimlerini ortaya çıkarmıştır. Toplumsal hareketlerin mobilizasyonu, siyasi kutuplaşmanın artırılması ve demokratik süreçlere müdahale, dijital teknolojilerin oluşturduğu yeni güvenlik tehditlerini oluşturmaktadır (Singer & Brooking, 2019; West, 2021).

Dijital teknolojiler, devletlerin saldırı ve savunma kapasitelerini değiştirerek uluslararası güvenlik paradigmasını dönüştürmüştür. Yapay zekâ destekli siber operasyonlar, tehdit algılama sistemleri ve büyük veri analizleri, devletlerin caydırıcılık stratejilerini yeniden şekillendirmektedir. ABD, Çin, AB ve Rusya siber güvenlik politikalarını geliştirerek devlet destekli hacker gruplarıyla istihbarat operasyonlarını daha sofistike hale getirmiştir. Otonom savunma sistemleri, ağ güvenliği protokolleri ve kritik altyapı koruma mekanizmaları, ulusal güvenlik doktrinlerinin vazgeçilmez bileşenleri haline gelmiştir. Siber saldırıların atfedilmesindeki zorluklar ve uluslararası hukuki çerçevenin yetersizliği, devletlerin örtülü operasyonlar yürütmesini kolaylaştırmış ve hesap verebilirliği zorlaştırmıştır (West, 2021; Floridi, 2018).

Kuantum bilişim ve uç bilişim sistemleri, devletlerin küresel istihbarat ağlarını yeniden inşa etmesine ve uluslararası siber güvenlik politikalarını dönüştürmesine yol açmaktadır. Kuantum bilgisayarlar, geleneksel şifreleme mekanizmalarını kırma kapasitesine ulaşarak devletlerin dijital güvenliğini tehdit etmektedir. Çin, kuantum anahtar dağıtımı (QKD) sistemleri geliştirirken, ABD, Avrupa Birliği ve Japonya kuantum şifreleme sistemlerine yatırım yaparak dijital egemenliklerini koruma altına almaktadır. Bu teknolojik rekabet, gelecekteki istihbarat üstünlüğünü belirleyecek kritik bir alan haline gelmiştir. Gelişmiş hesaplama kapasitesi, kompleks veri şifreleme mekanizmaları ve kuantum sensörler, askeri ve istihbarat uygulamalarında çığır açan yenilikler sunmaktadır (Fukuyama, 2021; Arquilla & Ronfeldt, 2020).

Blok zinciri tabanlı finansal sistemler, uluslararası ekonomik yapıları merkeziyetsiz hale getirerek devletlerin finansal mekanizmalar üzerindeki kontrolünü zayıflatmıştır. Geleneksel küresel finans sistemi dolar bazlı kontrol mekanizmalarına dayanırken, blok zinciri tabanlı merkeziyetsiz finans sistemleri (DeFi), uluslararası ticaretin finansal hegemonya süreçlerinden bağımsız hareket etmesine olanak tanımaktadır. Çin'in dijital yuan hamlesi, küresel finans sistemine entegre olarak ABD dolarına alternatif oluşturmayı amaçlarken, Rusya ve İran gibi ülkeler, blok zinciri tabanlı sis-

temlerle Batı yaptırımlarını aşmayı hedeflemektedir. Kripto paralar, akıllı kontratlar ve merkeziyetsiz borsa sistemleri, finansal işlemlerin geleneksel bankacılık sisteminin dışında gerçekleşmesini sağlayarak ekonomik ilişkilerde paradigma değişimine neden olmaktadır (Brynjolfsson & McAfee, 2019; OECD, 2021).

Yapay zekâ destekli diplomatik platformlar, devletlerarası müzakereleri yüz yüze görüşmelerin ötesine taşıyarak veri analitiği, otomatik karar destek sistemleri ve yapay zekâ tabanlı simülasyonlarla desteklenen çok boyutlu bir süreç haline getirmiştir. Yapay zekâ algoritmaları, uluslararası kriz anlarında devletlerin olası hamlelerini modelleyerek diplomatik müzakere süreçlerini daha öngörülebilir hale getirmektedir. Bu süreç, devletlere olası senaryolar üzerinden farklı stratejiler geliştirme imkânı sunmaktadır. Büyük veri analitiği, tarihsel müzakere örüntülerinin tespit edilmesini ve gelecekteki diplomatik etkileşimlerin optimize edilmesini sağlayarak uluslararası kriz yönetiminde stratejik avantaj sunmaktadır. Diplomatik iletişimin dijitalleşmesi ve sanal müzakere platformlarının yaygınlaşması, geleneksel diplomatik protokolleri ve uygulamaları yeniden şekillendirmektedir (Singer & Brooking, 2019; Choucri, 2021).

Ağ teorisi, bilgi akışlarını, güç dağılımını ve aktörler arasındaki ilişkileri analiz eden bir çerçeve sunarken, dijital söylem yönetimi ve hakikat rejimleri, uluslararası ilişkilerde bilgi manipülasyonunun nasıl gerçekleştirildiğini açıklamaktadır. Dezenformasyon kampanyaları ve sosyal medya manipülasyonları, devletlerin uluslararası kamuoyunu etkileme kapasitesini artırırken, yapay zekâ destekli veri analiz sistemleri bu süreçleri daha etkili hale getirmektedir. Bu durum, uluslararası ilişkilerde bilgi savaşlarının ve dijital propaganda tekniklerinin stratejik önemini artırmaktadır. Toplumsal algıların yönlendirilmesi, hedef kitleye özel içerik üretimi ve algoritmik filtreleme mekanizmaları, devletlerin yeni etki alanlarını oluşturmaktadır. Uluslararası haber akışının kontrolü ve dijital söylemin şekillendirilmesi, yumuşak güç projeksiyonunun temel unsurları haline gelmiştir (Floridi, 2018; Morozov, 2021).

Dijital teknolojiler, uluslararası güvenlikten küresel ekonomi politikalarına kadar geniş çaplı dönüşümler oluşturmaktadır. Devletlerin dijitalleşme politikalarını uluslararası iş birlikleri ile uyumlu hale getirmesi, siber güvenlik politikalarını güçlendirmesi ve dijital hakları koruyacak uluslararası regülasyonlar geliştirmesi gerekmektedir. Dijitalleşmenin uluslararası güvenlik, ekonomi ve diplomasi üzerindeki etkilerini inceleyen daha fazla teorik ve ampirik çalışmaya ihtiyaç duyulmaktadır. Özellikle yapay zekâ etiği, veri mahremiyeti standartları ve siber silahların kontrolü konularında küresel yönetişim mekanizmalarının geliştirilmesi kritik önem taşımaktadır. Uluslararası işbirliği olmaksızın, devletlerin dijital alandaki rekabeti

kontrolsüz bir silahlanma yarışına dönüşme riski taşımaktadır (Nye, 2021; OECD, 2021).

Dijital teknolojilerin gelişimi, uluslararası aktörlerin kimliklerini, çıkarlarını ve davranış kalıplarını dönüştürerek geleneksel uluslararası ilişkiler teorilerinin yeniden değerlendirilmesini gerektirmektedir. Güç kavramının dönüşümü, egemenlik anlayışının evrilmesi ve sınırların yeniden tanımlanması, dijital çağda uluslararası ilişkiler disiplininin karşılaştığı temel zorlukları oluşturmaktadır. Özellikle siber alanda normatif çerçevelerin oluşturulması, yapay zekâ sistemlerinin yönetişimi ve dijital küresel kamusal malların üretimi, yeni teorik yaklaşımları ve metodolojik yenilikleri gerektirmektedir. Bu bağlamda disiplinler arası çalışmalar ve çok boyutlu analiz yöntemleri, dijitalleşmenin uluslararası ilişkiler üzerindeki kompleks etkilerini kavramada kritik önem taşımaktadır (Choucri, 2021; Fukuyama, 2021).

Dijital teknolojilerin oluşturduğu paradigma değişimi, uluslararası sistem üzerindeki etkilerinin kapsamlı ve sistematik bir şekilde analiz edilmesini gerektirmektedir. Yapay zekâ, blok zinciri, bulut bilişim ve nesnelerin interneti gibi teknolojiler, sadece teknik birer yenilik değil, aynı zamanda uluslararası ilişkileri kökten dönüştüren siyasi, ekonomik ve sosyal fenomenlerdir. Devletlerin bu teknolojik gelişmelere adaptasyon kapasitesi ve bunları stratejik avantaja dönüştürme becerileri, gelecekteki küresel güç hiyerarşisini belirleyecektir. Bu nedenle, dijital dönüşümün sadece teknolojik bir süreç olarak değil, uluslararası sistemin yapısal bir transformasyonu olarak değerlendirilmesi gerekmektedir. Dijital teknolojilerin çok kutuplu bir dünya düzeninde oluşturacağı fırsatlar ve tehditler, uluslararası ilişkiler disiplininin gelecekteki araştırma gündemini şekillendirmeye devam edecektir (Nye, 2021; Zuboff, 2019).

2.2. Dijital Dönüşüm Üzerine Önceki Çalışmalar

Dijital teknolojilerin uluslararası ilişkiler üzerindeki etkileri giderek daha fazla tartışılsa da henüz sistematik bir çerçeveye oturtulmamıştır. Yapay zekâ destekli diplomasi, siber savaş stratejileri, blok zinciri tabanlı finansal sistemler ve kuantum bilişim temelli siber güvenlik mekanizmaları, devletlerin uluslararası stratejilerini doğrudan etkileyen unsurlar haline gelmiştir. Dijital egemenlik politikaları, güç mücadelesinin artık sadece askeri ve ekonomik kapasitelerle değil, aynı zamanda dijital altyapılar, veri yönetimi ve siber güvenlik stratejileri ile belirlendiğini göstermektedir. Bu teknolojik gelişmeler, devletlerin rekabet dinamiklerini ve işbirliği mekanizmalarını yeniden tanımlamakta, geleneksel diplomasi ve savunma paradigmalarını köklü biçimde dönüştürmektedir. Ayrıca uluslararası sistemin temel ilkesi olan devlet egemenliği kavramını da fiziksel alandan dijital boyuta genişletmektedir (Nye, 2021; Floridi, 2018).

Önceki akademik çalışmalar, dijitalleşmenin jeopolitik ve jeoekonomik etkilerini inceleyerek uluslararası siyasette yeni hegemonya araçlarına dönüşme sürecini analiz etmektedir. Yapay zekâ destekli diplomatik süreçler, siber savaş stratejileri ve blok zinciri tabanlı finansal sistemler, devletlerin küresel siyasetteki etki alanlarını genişleten veya sınırlandıran kritik faktörler olarak değerlendirilmektedir. Ancak mevcut akademik tartışmalar, dijitalleşmenin uluslararası ilişkilerde hangi aktörlere ne tür avantajlar sağladığını karşılaştırmalı analizlerle ele almakta yetersiz kalmaktadır. Literatürdeki bu eksiklik, dijital teknolojilerin küresel güç dengelerini nasıl yeniden şekillendirdiğini ve bunun farklı bölgelerdeki yansımalarını anlamayı zorlaştırmaktadır. Ayrıca dijital teknolojilerin oluşturduğu asimetrik güç ilişkileri ve bunların uluslararası sistem üzerindeki transformatif etkileri yeterince incelenmemiştir (Arquilla & Ronfeldt, 2020; West, 2021).

Siber güvenlik, devletlerin ulusal güvenlik stratejilerinin temel unsuru haline gelmiş, dijital egemenlik ise uluslararası ilişkilerde kritik bir güç unsuru olmuştur. Geleneksel egemenlik kavramı coğrafi sınırlar ve askeri güç üzerinden tanımlanırken, günümüzde veri akışlarının denetlenmesi ve dijital altyapının kontrolü egemenliğin yeni boyutları arasında yer almaktadır. ABD, Çin ve Rusya siber egemenliklerini güçlendirmek için ulusal ve küresel düzeyde stratejiler geliştirirken, siber savaşlar ve devlet destekli siber saldırılar uluslararası krizlerin ana tetikleyicilerinden biri haline gelmiştir. Bu kapsamda, devletlerin siber savunma kapasitelerini geliştirme çabaları, ulusal veri merkezlerinin kurulması, kritik dijital altyapıların yabancı kontrolünden korunması ve stratejik teknolojilerde dışa bağımlılığın azaltılması gibi politikalar öne çıkmaktadır. Dijital egemenlik kavramının genişleyen kapsamı, devletlerin teknoloji politikalarını ve düzenleyici çerçevelerini yeniden değerlendirmelerini gerektirmektedir (Nye, 2021; Floridi, 2018; West, 2021).

Yapay zekâ destekli diplomatik platformlar ve sanal müzakere sistemleri, uluslararası ilişkilerde etkileşim biçimlerini dönüştürerek veri analitiği, otomatik karar destek sistemleri ve simülasyonlarla desteklenen yeni bir diplomasi modeli ortaya çıkarmaktadır. Bu teknolojiler, kriz yönetimi ve müzakere süreçlerinde devletlerin karar alma kapasitesini artırmaktadır. Yapay zekâ algoritmaları, karmaşık diplomatik sorunlarda çok sayıda değişkeni analiz edebilmekte, tarihsel verilere dayanarak olası senaryoları modelleyebilmekte ve optimal müzakere stratejileri önerebilmektedir. Bu dijital dönüşüm, diplomatik iletişimin hızını ve kapsamını genişletirken, devletlerin diplomatik personel ihtiyaçlarını ve diplomatik temsilcilik yapılarını da değiştirmektedir. Sanal diplomatik platformlar ve dijital müzakere sistemleri, özellikle COVID-19 pandemisi döneminde küresel diplomasinin sürdürülmesinde kritik rol oynamıştır (Singer & Brooking, 2019; Fukuyama, 2021).

Ancak yapay zekâ destekli diplomasi, veri manipülasyonu ve dezenformasyon gibi riskler de taşımaktadır. Özellikle Çin ve Rusya'nın yapay zekâ destekli dezenformasyon kampanyaları, Batılı devletlerin diplomatik müzakere süreçlerini zorlaştırarak büyük güçler arasındaki bilgi savaşlarını daha karmaşık hale getirmektedir. Yapay zekâ algoritmalarının geliştirdiği deepfake teknolojileri, diplomatik iletişimde manipülasyon riskini artırmakta ve uluslararası krizlerin tetiklenmesine yol açabilmektedir. Ayrıca yapay zekâ sistemlerinin kullandığı veri setlerindeki önyargılar ve algoritmik şeffaflık eksikliği, diplomatik karar alma süreçlerinde etik ve güvenilirlik sorunlarını gündeme getirmektedir. Bu nedenle, yapay zekâ destekli diplomatik sistemlerin geliştirilmesinde etik standartların ve denetim mekanizmalarının oluşturulması kritik önem taşımaktadır (Arquilla & Ronfeldt, 2020).

Blok zinciri teknolojisi, merkeziyetsiz finans sistemleri aracılığıyla küresel ekonomik yapıyı dönüştürerek devletlerin finansal kontrol mekanizmalarını zayıflatmaktadır. Geleneksel küresel finans sistemi dolar bazlı bir kontrol mekanizmasına dayanırken, blok zinciri tabanlı sistemler, finansal akışları merkezî otoritelerden bağımsız hale getirmektedir. Çin'in dijital yuan hamlesi, küresel finans sisteminde ABD dolarına alternatif oluşturmayı amaçlarken, Rusya ve İran, Batı yaptırımlarını aşmak için blok zinciri tabanlı sistemleri kullanmaktadır. Bu teknolojik dönüşüm, uluslararası para transferlerini daha hızlı, şeffaf ve düşük maliyetli hale getirirken, merkez bankalarının para politikası kontrolünü zorlaştırmakta ve geleneksel finansal aracıların rolünü azaltmaktadır. Merkeziyetsiz finans (DeFi) uygulamaları, akıllı kontratlar ve dijital varlıklar, yeni bir finansal ekosistem oluşturmakta ve uluslararası ticaretin yapısını değiştirmektedir (Brynjolfsson & McAfee, 2019; OECD, 2021).

Kuantum bilişim teknolojileri, devletlerin istihbarat kapasitelerini ve siber güvenlik politikalarını yeniden şekillendirmektedir. Kuantum bilgisayarlar, mevcut tüm şifreleme sistemlerini kırabilme kapasitesine sahip olduğundan, devletlerin veri güvenliği stratejilerinde köklü değişikliklere yol açmaktadır. ABD, Çin ve Avrupa Birliği gibi büyük güçler, kuantum destekli güvenlik sistemlerine yatırım yaparak ulusal istihbarat mekanizmalarını daha güvenli hale getirmeye çalışmaktadır. Kuantum bilişim alanındaki rekabet, yalnızca teknolojik üstünlük için değil, aynı zamanda stratejik istihbarat avantajı elde etmek için de sürdürülmektedir. Kuantum bilgisayarların sağladığı üstün hesaplama gücü, kompleks şifreleme sistemlerini kırma, büyük veri setlerini daha hızlı analiz etme ve gelişmiş simülasyonlar oluşturma kapasitesi, ulusal güvenlik açısından çığır açan uygulamalara olanak tanımaktadır (West, 2021; Floridi, 2018).

Bu teknolojik dönüşüm, devletlerin sadece savunma mekanizmalarını değil, saldırı kapasitelerini de artırmalarına neden olmuş, kuantum bilişim destekli istihbarat savaşlarını uluslararası güvenlik politikasının ayrılmaz

bir parçası haline getirmiştir. Örneğin Çin'in Mozi adlı kuantum iletişim uydusu, devletlerin istihbarat faaliyetlerini gizli tutmasını sağlayan önemli bir güvenlik aracı olarak öne çıkmaktadır. Kuantum kriptografi ve kuantum anahtar dağıtımı (QKD) sistemleri, teorik olarak kırılamaz şifreleme mekanizmaları sunarak hassas diplomatik ve askeri iletişimin güvenliğini artırmaktadır. Aynı zamanda, kuantum bilişim teknolojileri, yapay zekâ algoritmalarının performansını önemli ölçüde artırarak istihbarat analizi, tehdit modelleme ve karar destek sistemlerinde çığır açan gelişmelere olanak tanımaktadır (Singer & Brooking, 2019; Arquilla & Ronfeldt, 2020).

Dijitalleşmenin uluslararası ilişkiler üzerindeki etkileri giderek daha fazla akademik ilgi görmekle birlikte, bu dönüşüm sürecinin teorik bir çerçeveye oturtulması konusunda önemli boşluklar bulunmaktadır. Mevcut akademik çalışmalar genellikle siber güvenlik, yapay zekâ destekli diplomasi, kuantum bilişim ve blok zinciri tabanlı finans sistemlerine odaklanırken, bu teknolojilerin birbirleriyle nasıl etkileşim içinde olduğu ve devletlerarası ilişkileri nasıl çok boyutlu bir yapıya dönüştürdüğü yeterince incelenmemektedir. Bu teknolojilerin birbiriyle kesişen ve birbirini güçlendiren etkileri, uluslararası sistem üzerinde kümülatif ve sinerjetik bir dönüşüm oluşturmaktadır. Örneğin yapay zekâ ve blok zinciri teknolojilerinin kombinasyonu, tamamen yeni dijital yönetişim modellerinin ortaya çıkmasına neden olurken, kuantum bilişim ve siber güvenlik teknolojilerinin birleşimi, istihbarat toplama ve korunma stratejilerini kökten değiştirmektedir (Nye, 2021; Floridi, 2018).

Teknoloji merkezli uluslararası ilişkiler teorilerinin eksikliği, dijitalleşmenin küresel güç dengeleri üzerindeki uzun vadeli etkilerinin kavramsallaştırılmasını zorlaştırmaktadır. Klasik uluslararası ilişkiler teorileri, devlet merkezli ve fiziksel güç odaklı yaklaşımlarıyla dijital çağın karmaşık ve çok aktörlü yapısını açıklamakta yetersiz kalmaktadır. Özellikle teknoloji şirketlerinin devlet benzeri güç kazanması, sanal topluluklara ulus-ötesi kimliklerin oluşması ve dijital etki alanlarının fiziksel sınırlardan bağımsızlaşması, mevcut teorik çerçevelerle tam olarak açıklanamamaktadır. Bu nedenle, dijital teknolojilerin uluslararası ilişkiler disiplinine entegrasyonu için yeni teorik yaklaşımlar ve kavramsal modeller geliştirilmesi gerekmektedir. Dijital realizm, siber liberalizm ve teknolojik konstrüktivizm gibi yeni teorik yaklaşımlar, dijital çağın dinamiklerini daha kapsamlı bir şekilde analiz etmeye olanak sağlayabilir (West, 2021; Floridi, 2018).

Dijital egemenlik ve uluslararası hukuk açısından literatürdeki eksiklikler, devletlerin siber alan üzerindeki kontrolünü ve veri yönetimi süreçlerini ifade ederken, uluslararası hukuk çerçevesinde bu kavramın nasıl tanımlanacağı ve düzenleneceği konusunda önemli boşluklar bulunmaktadır. Özellikle siber saldırıların uluslararası hukukta nasıl sınıflandırılacağı, devlet destekli siber operasyonların meşruiyeti ve yapay zekâ destekli askeri

sistemlerin hukuki statüsü gibi konular küresel ölçekte netlik kazanmamıştır. Bu hukuki belirsizlikler, devletlerin siber operasyonlarının sınırlarını belirlemeyi ve dijital çatışmaların yönetimini zorlaştırmaktadır. Tallinn Kılavuzu gibi uluslararası girişimler, siber operasyonlara yönelik hukuki çerçeveleri netleştirmeyi amaçlasa da, henüz geniş çaplı uluslararası konsensüs oluşturulamamıştır. Dijital egemenliğin sınırları, veri lokalizasyonu politikaları ve dijital sınır ötesi operasyonların meşruiyeti, uluslararası hukuk literatüründe daha fazla incelenmesi gereken alanlar arasındadır (Floridi, 2018; Arquilla & Ronfeldt, 2020).

Bu boşluklar, devletlerin dijital egemenlik politikalarını bireysel olarak geliştirmelerine ve uluslararası sistemde farklı yaklaşımların ortaya çıkmasına yol açmaktadır. Örneğin Çin'in "dijital sınırları" koruma stratejisi ile Batı'nın açık internet politikaları arasındaki farklılıklar, bu alandaki teorik çerçevenin eksikliğini ortaya koymaktadır. Çin'in siber egemenlik doktrini, internet içeriklerinin devlet kontrolü altında tutulmasını ve dijital altyapıların ulusal güvenlik perspektifiyle yönetilmesini savunurken, ABD ve Avrupa Birliği daha açık, çok paydaşlı ve serbest bir internet ekosistemine öncelik vermektedir. Bu yaklaşım farklılıkları, küresel internet yönetişimi ve dijital haklar konusunda derin ayrışmalara yol açmakta, uluslararası dijital rejimin parçalanmasına neden olmaktadır. Dijital teknolojilerin düzenlenmesindeki bu farklı yaklaşımlar, uluslararası sistemin ideolojik ve stratejik kutuplaşmasını derinleştirerek "dijital demir perde" olarak nitelendirilen yeni bir ayrışma oluşturmaktadır (Singer & Brooking, 2019; Floridi, 2018).

2.3. Literatürdeki Boşluklar ve Yeni Yaklaşımlar

Dijitalleşmenin uluslararası ilişkiler üzerindeki etkileri giderek daha fazla akademik ilgi görmekle birlikte, bu dönüşüm sürecinin teorik bir çerçeveye oturtulması konusunda önemli boşluklar bulunmaktadır. Mevcut akademik çalışmalar genellikle siber güvenlik, yapay zekâ destekli diplomasi, kuantum bilişim ve blok zinciri tabanlı finans sistemlerine odaklanırken, bu teknolojilerin birbirleriyle nasıl etkileşim içinde olduğu ve devletlerarası ilişkileri nasıl çok boyutlu bir yapıya dönüştürdüğü yeterince incelenmemektedir. Dijital teknolojilerin yalnızca teknik yenilikler olarak değil, uluslararası sistemi yapısal olarak dönüştüren siyasi ve ekonomik fenomenler olarak incelenmesi gerekmektedir. Bu bağlamda dijitalleşmenin devletlerin güç kapasitelerini, egemenlik anlayışlarını ve dış politika araçlarını nasıl yeniden tanımladığına dair daha kapsamlı teorik modellere ihtiyaç duyulmaktadır. Özellikle dijital teknolojilerin küresel güç dağılımını asimetrik biçimde etkileme potansiyeli ve bunun uluslararası düzen üzerindeki uzun vadeli sonuçları detaylı olarak araştırılmalıdır (Nye, 2021; Floridi, 2018).

Teknoloji merkezli uluslararası ilişkiler teorilerinin eksikliği, dijitalleşmenin küresel güç dengeleri üzerindeki uzun vadeli etkilerinin kavramsal-

laştırılmasını zorlaştırmaktadır. Geleneksel uluslararası ilişkiler teorileri, dijital teknolojilerin oluşturduğu yeni güç dinamiklerini, çok katmanlı aktör etkileşimlerini ve sanal-fiziksel alanların iç içe geçmişliğini açıklamakta yetersiz kalmaktadır. Realizm, liberalizm ve konstrüktivizm gibi klasik teoriler, dijital çağın güç konseptlerini anlamlandırmak için revizyona ihtiyaç duymaktadır. Örneğin dijital realizm, siber uzaydaki güç mücadelesini ve dijital alandaki güvenlik ikilemlerini analiz ederken, dijital liberalizm, teknolojik karşılıklı bağımlılığın ve sanal toplulukların uluslararası işbirliği üzerindeki etkilerine odaklanabilir. Teknolojik konstrüktivizm ise, dijital kimliklerin, normların ve söylemlerin uluslararası politikayı nasıl şekillendirdiğini inceleyebilir. Bu yeni teorik yaklaşımlar, dijitalleşmenin çok boyutlu ve dinamik doğasını daha iyi kavramaya olanak sağlayacaktır (West, 2021; Choucri, 2021).

Dijital egemenlik ve uluslararası hukuk açısından literatürdeki eksiklikler, devletlerin siber alan üzerindeki kontrolünü ve veri yönetimi süreçlerini ifade ederken, uluslararası hukuk çerçevesinde bu kavramın nasıl tanımlanacağı ve düzenleneceği konusunda önemli boşluklar bulunmaktadır. Özellikle siber saldırıların uluslararası hukukta nasıl sınıflandırılacağı, devlet destekli siber operasyonların meşruiyeti ve yapay zekâ destekli askeri sistemlerin hukuki statüsü gibi konular küresel ölçekte netlik kazanmamıştır. Dijital egemenlik kavramının fiziksel egemenlikten farklı olarak sınırları aşan veri akışları, bulut hizmetleri ve dijital platformlar üzerindeki kontrol yetkilerini içermesi, geleneksel uluslararası hukuk ilkelerinin yeniden yorumlanmasını gerektirmektedir. Veri lokalizasyonu, sınır ötesi veri transferleri ve devletlerin kendi vatandaşlarının verilerine erişim hakları gibi konularda uluslararası normlar henüz tam olarak oluşmamıştır. Bu durum, dijital alanda hukuki belirsizliklere ve devletlerin birbiriyle çatışan yaklaşımlar geliştirmesine yol açmaktadır (Floridi, 2018; Singer & Brooking, 2019).

Bu boşluklar, devletlerin dijital egemenlik politikalarını bireysel olarak geliştirmelerine ve uluslararası sistemde farklı yaklaşımların ortaya çıkmasına yol açmaktadır. Örneğin Çin'in "dijital sınırları" koruma stratejisi ile Batı'nın açık internet politikaları arasındaki farklılıklar, bu alandaki teorik çerçevenin eksikliğini ortaya koymaktadır. Bu farklı yaklaşımlar, internetin parçalanması (splinternet) olarak adlandırılan, birbirine bağlantısı sınırlı ve farklı normlara, kurallara tabi dijital alanların oluşmasına neden olmaktadır. Küresel internet yönetişimi, veri koruma standartları ve dijital ticaret rejimlerindeki bu ayrışma, uluslararası sistemin dijital fragmantasyonunu hızlandırmakta ve devletlerarasında dijital bölünmeleri derinleştirmektedir. Dijital egemenlik yaklaşımları arasındaki bu çatışma, yalnızca teknolojik bir ayrışmayı değil, aynı zamanda ideolojik ve jeopolitik bir rekabeti de yansıtmaktadır (Arquilla & Ronfeldt, 2020; Morozov, 2021).

Dijital teknolojilerin diplomasi üzerindeki etkileri yeterince incelenmemiş bir alan olarak öne çıkmaktadır. Yapay zekâ destekli müzakere sistemlerinin uluslararası diplomaside nasıl kullanılacağı, tarafsızlık sorunu ve uluslararası hukuk bağlamında dijital müzakerelerin nasıl ele alınması gerektiği konuları hâlâ netlik kazanmamıştır. Özellikle otoriter devletlerin yapay zekâ destekli diplomasi sistemlerini manipülasyon aracı olarak kullanma potansiyeli, demokratik devletlerin bu teknolojiyi nasıl düzenlemesi gerektiği konusunda küresel bir uzlaşı eksikliğini göstermektedir. Diplomatik süreçlerin dijitalleşmesi, yeni diplomatik protokollerin ve uygulamaların geliştirilmesini gerektirmektedir. Sanal diplomatik platformlar, e-konsolosluk hizmetleri ve dijital müzakere ortamları, geleneksel diplomatik etkileşim modellerini dönüştürmekte, ancak bu dönüşümün nasıl yönetileceği ve standardize edileceği konusunda kapsamlı çalışmalar bulunmamaktadır. Ayrıca yapay zekâ destekli diplomatik analiz sistemlerinin etik kullanımı, algoritmik önyargıların yönetimi ve karar alma süreçlerindeki insan faktörünün korunması gibi konularda daha fazla araştırmaya ihtiyaç duyulmaktadır (Singer & Brooking, 2019; Nye, 2021).

Blok zinciri teknolojisi ve merkeziyetsiz finans sistemlerinin, devletlerarası ekonomik rekabet üzerindeki etkileri yeterince analiz edilmemiştir. Bu teknolojilerin geleneksel finansal yapıları nasıl dönüştüreceği ve devletlerin ekonomik kontrolünü nasıl sınırlayacağı konusunda daha fazla araştırmaya ihtiyaç duyulmaktadır. ABD ve Batılı müttefikler, dolara dayalı küresel finansal sistemin sürdürülebilirliğini korumaya çalışırken, Çin ve Rusya gibi ülkeler, blok zinciri tabanlı finansal ağlar geliştirerek Batı'nın ekonomik yaptırımlarını aşmayı hedeflemektedir. Dijital para birimlerinin, özellikle merkez bankası dijital para birimlerinin (CBDC) uluslararası finansal sistemdeki rolü, rezerv para birimlerinin statüsüne etkileri ve küresel ticaret modellerini nasıl değiştireceği henüz kapsamlı olarak incelenmemiştir. Merkeziyetsiz finans sistemlerinin yaygınlaşması, uluslararası finansal istikrarı nasıl etkileyeceği, ekonomik krizlerin yönetimi ve sistemik risklerin kontrolü açısından yeni zorluklar oluşturmaktadır. Bu teknolojilerin regülasyonu, vergilendirilmesi ve uluslararası standartlarının oluşturulması konularında daha fazla disiplinler arası araştırmaya ihtiyaç vardır (Brynjolfsson & McAfee, 2019; OECD, 2021).

Kuantum bilişim teknolojilerinin uluslararası güvenlik ve istihbarat üzerindeki etkileri literatürde yeterince ele alınmamıştır. Özellikle kuantum bilgisayarların şifreleme sistemlerini etkisiz hale getirme potansiyeli ve devletlerin istihbarat kapasitelerini nasıl dönüştüreceği konularında daha fazla araştırmaya ihtiyaç duyulmaktadır. Kuantum üstünlüğünün (quantum supremacy) elde edilmesinin stratejik sonuçları, kuantum teknolojilerinin silahlanma yarışına etkisi ve kuantum güvenliğinin uluslararası normları henüz yeterince incelenmemiştir. Kuantum kriptografinin yaygınlaşmasıy-

la birlikte, devletlerin istihbarat toplama yöntemlerinin köklü biçimde değişeceği ve bu durumun küresel güvenlik dengelerini nasıl etkileyeceği önemli bir araştırma alanıdır. Kuantum sensörlerin askeri uygulamaları, kuantum radarlar ve kuantum navigasyon sistemleri gibi yenilikler, konvansiyonel askeri dengeleri ve caydırıcılık stratejilerini dönüştürme potansiyeline sahiptir. Bu teknolojilerin gelişimi ve yayılımının kontrolü, uluslararası güvenlik rejimleri açısından ciddi zorluklar oluşturmaktadır (West, 2021; Floridi, 2018).

Dijital haklar ve küresel insan hakları rejiminin dijital çağa adaptasyonu konusunda literatürde önemli boşluklar bulunmaktadır. İnternet erişiminin temel insan hakkı olarak tanımlanması, dijital mahremiyet standartlarının geliştirilmesi ve çevrimiçi ifade özgürlüğünün korunması gibi konularda uluslararası normların oluşturulması henüz tamamlanmamıştır. Yapay zekâ sistemlerinin insan haklarına saygılı biçimde geliştirilmesi ve kullanılması için gerekli etik çerçevelerin belirlenmesi, veri koruma rejimlerinin harmonizasyonu ve dijital gözetimin sınırlandırılması konuları daha fazla incelenmelidir. Dijital teknolojilerin demokratikleşme süreçlerine etkisi, otoriter rejimlerin dijital kontrol mekanizmalarının analizi ve sivil toplumun dijital alandaki direnç stratejileri, uluslararası ilişkiler literatürünün daha fazla odaklanması gereken alanlar arasındadır. Özellikle yapay zekâ destekli gözetim sistemleri, yüz tanıma teknolojileri ve sosyal kredi sistemleri gibi uygulamaların insan hakları üzerindeki etkileri ve bunların uluslararası standartlarla nasıl düzenleneceği kritik araştırma konuları olarak öne çıkmaktadır (Zuboff, 2019; Morozov, 2021).

Dijital bölünme ve teknolojik eşitsizliklerin uluslararası sisteme etkileri konusundaki literatür sınırlıdır. Dijital teknolojilere erişimdeki küresel eşitsizlikler, teknolojik kapasitelerin geliştirilmesindeki asimetri ve dijital altyapı yatırımlarındaki dengesizlikler, uluslararası güç dengelerini ve ekonomik gelişme modellerini derinden etkilemektedir. Gelişmiş ülkeler ile gelişmekte olan ülkeler arasındaki teknolojik uçurum, küresel eşitsizlikleri derinleştirme ve uluslararası sistemdeki hiyerarşik yapıları pekiştirme potansiyeline sahiptir. Dijital teknolojilerin yayılımındaki bu asimetri, teknolojik bağımlılık ilişkilerini güçlendirmekte ve dijital kolonizasyon olarak tanımlanan yeni bağımlılık biçimlerini ortaya çıkarmaktadır. Bu bağlamda teknoloji transferi politikaları, kapasite geliştirme programları ve dijital kalkınma yardımlarının etkinliği, daha fazla incelenmesi gereken araştırma alanlarıdır. Ayrıca dijital teknolojilerin sürdürülebilir kalkınma hedeflerine katkısı ve çevresel etkileri de literatürde yeterince ele alınmamış konular arasındadır (Brynjolfsson & McAfee, 2019; OECD, 2021).

Dijital teknolojilerin devlet dışı aktörler üzerindeki etkileri ve bu aktörlerin uluslararası sistem içindeki rollerinin dönüşümü, literatürde derinlemesine incelenmesi gereken bir diğer alandır. Teknoloji şirketlerinin devlet

benzeri güç kazanması, dijital platformların küresel normları şekillendirme kapasitesi ve sanal toplulukların uluslararası politikadaki artan etkisi, geleneksel devlet merkezli uluslararası ilişkiler yaklaşımlarını zorlamaktadır. Bu aktörlerin meşruiyeti, hesap verebilirliği ve devletlerle olan karmaşık ilişkileri, uluslararası sistemi daha çok katmanlı ve çok merkezli bir yapıya dönüştürmektedir. Özellikle büyük teknoloji şirketlerinin veri kontrolü, içerik moderasyonu ve algoritmik yönetişim alanlarındaki kritik rolleri, yeni tür bir özel sektör otoritesi oluşturmakta ve devletlerin bu aktörlerle nasıl ilişki kuracağı konusunda önemli sorular ortaya çıkarmaktadır. Ayrıca hacktivist gruplar, dijital sivil toplum örgütleri ve sanal diaspora toplulukları gibi yeni tür aktörlerin uluslararası politikadaki mobilizasyon kapasitesi ve etki potansiyeli daha detaylı analiz edilmelidir (Zuboff, 2019; Fukuyama, 2021).

Dijital dönüşümün uluslararası çatışma dinamikleri üzerindeki etkisi konusunda literatürde önemli boşluklar bulunmaktadır. Siber savaş stratejileri, hibrit tehditler ve bilgi savaşlarının geleneksel çatışma paradigmalarını nasıl dönüştürdüğü, daha kapsamlı teorik ve ampirik çalışmalarla incelenmelidir. Özellikle siber saldırıların atfedilmesi problemi, çatışma eşiğinin belirlenmesi ve orantılı karşılık ilkesinin dijital alanda uygulanması gibi konular, uluslararası güvenlik literatüründe daha fazla araştırılmalıdır. Dijital teknolojilerin terörizm, organize suç ve asimetrik tehditler üzerindeki etkisi, devletlerin bu tehditlere karşı geliştirdiği yeni güvenlik stratejileri ve uluslararası işbirliği mekanizmaları da detaylı olarak incelenmelidir. Ayrıca dijital silahların yayılımının kontrolü, siber silahsızlanma anlaşmalarının potansiyeli ve kitle imha silahlarının dijital versiyonları olarak tanımlanabilecek teknolojilerin regülasyonu gibi konularda akademik literatürde önemli eksiklikler bulunmaktadır (Singer & Brooking, 2019; Arquilla & Ronfeldt, 2020).

Dijital teknolojilerin çevresel etkileri ve küresel iklim politikaları üzerindeki yansımaları, uluslararası ilişkiler literatüründe yeterince incelenmemiş bir diğer alandır. Veri merkezlerinin enerji tüketimi, dijital altyapıların karbon ayak izi ve elektronik atıkların yönetimi gibi konular, küresel sürdürülebilirlik hedefleri açısından kritik öneme sahiptir. Blok zinciri teknolojilerinin, özellikle madencilik süreçlerinin çevresel maliyetleri ve bu maliyetlerin devletlerin enerji politikalarına etkileri daha detaylı incelenmelidir. Bununla birlikte, dijital teknolojilerin iklim değişikliğiyle mücadelede sunduğu fırsatlar, akıllı şehirler, sürdürülebilir enerji sistemleri ve yeşil dijital dönüşüm stratejilerinin uluslararası işbirliği potansiyeli de literatürde daha fazla yer bulmalıdır. Dijital teknolojiler ve çevre politikaları arasındaki etkileşim, uluslararası ilişkilerin yeni ve önemli bir kesişim noktasını oluşturmaktadır ve bu alandaki araştırmaların derinleştirilmesi gerekmektedir (OECD, 2021; Brynjolfsson & McAfee, 2019).

2.4. Dijital Dönüşümün Uluslararası İlişkilerdeki Yansımaları ve Gelecek Perspektifi: Dijital dönüşüm, devletlerin stratejik önceliklerini ve küresel güç rekabetini yeniden şekillendirmiştir. Geleneksel güç unsurları askeri kapasite ve ekonomik üstünlüğe dayanırken, dijitalleşme bilgi yönetimi, siber güvenlik, yapay zekâ destekli karar alma mekanizmaları ve blok zinciri tabanlı ekonomik sistemleri küresel rekabetin merkezine taşımıştır. Devletler, dijital teknolojileri dış politika stratejilerinin temel bileşeni haline getirerek uluslararası alanda avantaj sağlamaya çalışmaktadır. Bu paradigma değişimi, jeopolitik rekabeti yeni teknolojik alanları kapsayacak şekilde genişletmekte ve dijital egemenlik kavramını ulusal güvenliğin ayrılmaz bir parçası haline getirmektedir. Özellikle veri hâkimiyeti, algoritmik kapasite ve teknolojik standartların belirlenmesi, devletlerin stratejik rekabet alanlarını oluşturmaktadır. Bu bağlamda dijital altyapı yatırımları, teknoloji transferi politikaları ve siber kapasite geliştirme programları, devletlerin dış politika araçları arasında ön plana çıkmaktadır (Nye, 2021; Floridi, 2018).

Yapay zekâ alanındaki gelişmeler, uluslararası ilişkilerde devrim niteliğinde değişimlere yol açmaktadır. Büyük veri analitiği, makine öğrenmesi ve derin öğrenme algoritmalarının diplomatik süreçlere entegrasyonu, devletlerin karar alma mekanizmalarını daha sofistike ve veri odaklı hale getirmektedir. Yapay zekâ destekli istihbarat analizi, diplomatik müzakere simülasyonları ve kriz modellemeleri, dış politika stratejilerinin formülasyonunda giderek daha fazla kullanılmaktadır. Bu teknolojilerin gelişimi, diplomatik süreçlerde insan faktörünün rolünü değiştirmekte ve geleneksel diplomatik yöntemleri dijital platformlarla bütünleştirmektedir. Bununla birlikte, yapay zekâ algoritmalarının şeffaflığı, hesap verebilirliği ve etik kullanımı konularında uluslararası standartların geliştirilmesi gerekmektedir. Yapay zekâ destekli dış politika kararlarının meşruiyeti ve algoritmaların önyargılardan arındırılması, küresel yönetişimin kritik konuları arasında yer almaktadır (Choucri, 2021; Fukuyama, 2021).

Blok zinciri teknolojisi ve merkeziyetsiz finans sistemleri, uluslararası ekonomik yapıları köklü biçimde dönüştürme potansiyeline sahiptir. Devletlerin para politikaları üzerindeki tekelini zayıflatan bu teknolojiler, küresel finans sisteminde merkez bankalarının ve uluslararası finans kuruluşlarının rolünü yeniden tanımlamaktadır. Dijital para birimleri, akıllı kontratlar ve merkeziyetsiz borsalar, uluslararası ticaretin yapısını değiştirerek finansal işlemlerin hızını, şeffaflığını ve maliyetini optimize etmektedir. Özellikle merkez bankası dijital para birimleri (CBDC), devletlerin para politikası kontrolünü dijital çağa uyarlamasının bir yolu olarak öne çıkmaktadır. Çin'in dijital yuan projesi, Avrupa Birliği'nin dijital euro girişimi ve diğer ülkelerin benzer projeleri, küresel rezerv para birimi rekabetinin dijital boyutunu oluşturmaktadır. Bu teknolojiler, uluslararası ekonomik yaptırımların etkinliğini azaltma, sermaye kontrolleri ve vergi düzenlemeleri-

ni aşma potansiyeli taşımakta, dolayısıyla ekonomik hegemonya araçlarını yeniden şekillendirmektedir (Brynjolfsson & McAfee, 2019; OECD, 2021).

Kuantum bilişim teknolojileri, uluslararası ilişkilerde güvenlik ve istihbarat paradigmalarını devrimsel biçimde değiştirme potansiyeline sahiptir. Geleneksel bilgisayarların işlem kapasitesini eksponansiyel olarak aşan kuantum bilgisayarlar, mevcut şifreleme sistemlerini kırabilme, karmaşık simülasyonlar oluşturabilme ve devasa veri setlerini analiz edebilme kapasitesiyle devletlerin stratejik avantaj elde etmesini sağlayabilir. Kuantum üstünlüğü (quantum supremacy) yarışı ABD, Çin, Rusya ve Avrupa Birliği gibi büyük güçler arasında yeni bir teknolojik rekabet alanı oluşturmaktadır. Kuantum iletişim sistemleri ve kuantum kriptografi, teorik olarak kırılamaz şifreleme mekanizmaları sunarak diplomatik ve askeri haberleşmenin güvenliğini artırmaktadır. Kuantum sensörler, radarlar ve navigasyon sistemleri ise, askeri istihbarat ve gözetim kapasitelerini geliştirerek stratejik dengeyi değiştirebilecek yenilikler sunmaktadır. Bu teknolojilerin gelişimi ve yayılımı, uluslararası güvenlik rejimlerinin yeniden tasarlanmasını gerektirecek büyük zorluklar oluşturmaktadır (West, 2021; Singer & Brooking, 2019).

Siber güvenlik stratejileri ve dijital savunma kapasiteleri, ulusal güvenliğin ayrılmaz bir parçası haline gelmiştir. Kritik altyapıların korunması, siber saldırılara karşı caydırıcılık politikalarının geliştirilmesi ve dijital varlıkların güvenliğinin sağlanması, devletlerin öncelikli güvenlik konuları arasındadır. Siber saldırıların atfedilmesi problemi, orantılı karşılık ilkesinin dijital alanda uygulanması ve siber operasyonların uluslararası hukuk çerçevesinde tanımlanması gibi konular, uluslararası güvenlik rejimlerinin karşılaştığı temel zorluklardır. Devlet destekli siber operasyonlar, kritik altyapılara yönelik saldırılar ve geniş çaplı veri ihlalleri, uluslararası krizleri tetikleyebilecek ve geleneksel çatışmalara dönüşebilecek yeni risk faktörleri oluşturmaktadır. Bu bağlamda devletlerin siber kapasite geliştirme yarışı, dijital silahlanma olarak tanımlanabilecek yeni bir rekabet alanı oluşturmaktadır. Siber silahların yayılımının kontrolü, siber silahsızlanma anlaşmalarının potansiyeli ve güven artırıcı önlemlerin geliştirilmesi, uluslararası güvenlik mimarisinin güncel zorlukları arasında yer almaktadır (Arquilla & Ronfeldt, 2020; Floridi, 2018).

Dijital dezenformasyon ve bilgi savaşları, uluslararası ilişkilerde ülkelerin iç siyasetini etkileme ve kamuoyu algılarını yönlendirme aracı olarak giderek daha fazla kullanılmaktadır. Sosyal medya platformları, yapay zekâ destekli içerik üretimi (deepfake) ve hedefli reklamcılık teknikleri, kamuoyu manipülasyonu, siyasi kutuplaşma ve demokratik süreçlere müdahale için güçlü araçlar sunmaktadır. Devletlerin stratejik iletişim ve kamu diplomasisi yaklaşımları, dijital kanaat teknolojilerinin kapasitesine bağlı olarak evrilmektedir. İnternet üzerinden yürütülen etki operasyonları, seçimlere

müdahale ve toplumsal hareketleri mobilize etme gibi faaliyetler, uluslararası çatışmaların yeni boyutlarını oluşturmaktadır. Bu bağlamda medya okuryazarlığı, dijital içerik doğrulama mekanizmaları ve platformların düzenlenmesi konuları, demokratik toplumların karşılaştığı temel zorluklar haline gelmektedir. Dezenformasyon kampanyalarına karşı uluslararası işbirliği ve koordinasyon ihtiyacı, dijital çağın diplomasi gündeminde üst sıralarda yer almaktadır (Singer & Brooking, 2019; Morozov, 2021).

Dijital teknolojilerin küresel kalkınma üzerindeki etkileri, fırsatlar ve zorluklar açısından çift yönlü bir süreci ifade etmektedir. Bir yandan, yapay zekâ, büyük veri ve nesnelerin interneti gibi teknolojiler, sürdürülebilir kalkınma hedeflerine ulaşmak için yenilikçi çözümler sunmaktadır. Akıllı şehirler, telemedicine, dijital eğitim ve hassas tarım uygulamaları, kalkınma sorunlarına teknoloji odaklı yaklaşımlar getirmektedir. Öte yandan, gelişmiş ve gelişmekte olan ülkeler arasındaki dijital uçurum, teknolojik bağımlılık ve dijital kolonizasyon riskleri, küresel eşitsizlikleri derinleştirme potansiyeli taşımaktadır. Dijital altyapı yatırımları, teknoloji transferi ve kapasite geliştirme programları, sürdürülebilir kalkınmanın temel unsurları haline gelmektedir. Bu bağlamda "Dijital İpek Yolu" gibi girişimler, teknoloji diplomasisinin ve jeopolitik rekabetin kesiştiği noktada yer almaktadır. Dijital teknolojilerin kapsayıcı ve sürdürülebilir bir şekilde geliştirilmesi ve yaygınlaştırılması, uluslararası kalkınma gündeminin öncelikli konuları arasında yer almaktadır (OECD, 2021; Brynjolfsson & McAfee, 2019).

Dijital haklar ve siber alanın yönetişimi, uluslararası hukuk ve insan hakları rejimlerinin evriminde kritik önem taşımaktadır. İnternet erişiminin temel hak olarak tanımlanması, çevrimiçi ifade özgürlüğünün korunması ve dijital mahremiyet standartlarının geliştirilmesi, küresel dijital haklar gündeminin başlıca konularıdır. Veri lokalizasyonu, sınır ötesi veri transferleri ve dijital gözetim uygulamaları, devletlerin egemenlik hakları ile bireysel özgürlükler arasında yeni gerilim alanları oluşturmaktadır. Özellikle yapay zekâ sistemlerinin etik kullanımı, algoritmik ayrımcılığın önlenmesi ve otomatik karar alma sistemlerinin şeffaflığı, uluslararası standartların geliştirilmesini gerektiren alanlardır. Dijital platformların içerik moderasyonu, kullanıcı haklarının korunması ve hesap verebilirlik mekanizmalarının oluşturulması, dijital çağın yönetişim yapılarının temel unsurlarıdır. Bu bağlamda küresel, çok paydaşlı internet yönetişimi modeli ile devlet merkezli siber egemenlik yaklaşımı arasındaki gerilim, uluslararası dijital düzenin şekillenmesinde belirleyici olmaktadır (Zuboff, 2019; Floridi, 2018).

Çok uluslu teknoloji şirketlerinin artan gücü ve etkisi, devlet-şirket ilişkilerinin dinamiklerini yeniden tanımlamaktadır. Google, Apple, Facebook, Amazon ve Microsoft gibi büyük teknoloji şirketleri, sahip oldukları ekonomik kaynaklar, teknolojik kapasite ve veri kontrolü sayesinde devlet benzeri

güç projeksiyonu yapabilmektedir. Bu şirketler, küresel standartların belirlenmesi, uluslararası normların şekillendirilmesi ve dijital altyapının kontrolü konularında kritik roller üstlenmektedir. Özellikle veri toplama, işleme ve monetizasyon süreçlerindeki merkezi konumları, bu şirketleri uluslararası ilişkilerin önemli aktörleri haline getirmektedir. Devletlerin bu şirketleri regüle etme çabaları, dijital vergilendirme politikaları ve anti-tröst düzenlemeleri, devlet-şirket ilişkilerinin güncel gerilim alanlarını oluşturmaktadır. Teknoloji şirketlerinin dijital diplomasi süreçlerindeki rolleri, devletlerin dış politika uygulamalarında özel sektörle işbirliği yapmasını gerektirmektedir. Bu bağlamda teknoloji şirketlerinin meşruiyeti, hesap verebilirliği ve uluslararası sorumluluklarının tanımlanması, dijital yönetişimin temel zorluklarından biridir (Zuboff, 2019; West, 2021).

Dijital teknolojilerin çevresel etkileri ve sürdürülebilirlik zorlukları, uluslararası ilişkilerin yeni kesişim noktalarını oluşturmaktadır. Veri merkezlerinin enerji tüketimi, elektronik atıkların yönetimi ve dijital altyapıların karbon ayak izi, küresel iklim politikalarının güncel konuları arasındadır. Özellikle kripto para madenciliği gibi yüksek enerji tüketen dijital süreçler, ülkelerin enerji politikaları ve karbon emisyonu hedefleri üzerinde baskı oluşturmaktadır. Bununla birlikte, dijital teknolojiler, enerji verimliliğini artırma, akıllı şebekeler geliştirme ve yenilenebilir enerji kaynaklarını optimize etme potansiyelleriyle, sürdürülebilir kalkınmaya katkı sağlayabilmektedir. Yeşil dijital dönüşüm stratejileri, yapay zekâ destekli iklim modelleme ve çevresel izleme sistemleri, sürdürülebilirlik hedeflerine ulaşmak için teknolojik çözümler sunmaktadır. Bu bağlamda dijital teknolojilerin çevresel etkilerinin yönetilmesi ve sürdürülebilir dijital altyapıların geliştirilmesi, uluslararası işbirliğinin öncelikli alanlarından biri haline gelmektedir (OECD, 2021; Brynjolfsson & McAfee, 2019).

Gelecekte yapay zekâ destekli diplomasi, kuantum bilişim tabanlı istihbarat sistemleri ve blok zinciri teknolojileri daha yaygın hale gelecek ve devletlerin bu alanlara yönelik stratejik yaklaşımlarını yeniden şekillendirmesini zorunlu kılacaktır. Yapay zekâ sistemleri, diplomatik müzakereleri optimize etme, karmaşık uluslararası krizleri modelleme ve stratejik iletişimi kişiselleştirme kapasiteleriyle diplomasi pratiğini dönüştürecektir. Kuantum bilgisayarlar, şifreleme sistemlerini kırma, yeni güvenlik protokolleri geliştirme ve istihbarat analizi kapasitelerini artırma potansiyelleriyle, güvenlik paradigmalarını yeniden şekillendirecektir. Blok zinciri teknolojileri ise, uluslararası finansal işlemleri, tedarik zincirlerini ve diplomatik belge yönetimini merkeziyetsiz ve şeffaf bir yapıya kavuşturacaktır. Bu teknolojilerin birbirleriyle etkileşimi ve sinerjisi, uluslararası ilişkilerde öngörülemeyen dönüşümlere yol açabilecektir. Bu bağlamda teknolojik gelişmelerin hızı ve kapsamı, devletlerin adaptasyon kapasitesini ve stratejik öngörü yeteneğini test edecektir (Arquilla & Ronfeldt, 2020; OECD, 2021).

Bu dönüşüm sürecinin yönetilebilmesi için devletlerin dijitalleşme politikalarını uluslararası iş birlikleri ile uyumlu hale getirmesi ve küresel regülasyon mekanizmalarını geliştirmesi gerekmektedir. Dijital teknolojilerin sınır aşan doğası ve küresel etkileri, tek taraflı ulusal yaklaşımlarla etkin bir şekilde yönetilemez. Dijital alandaki zorlukların üstesinden gelmek için çok taraflı, çok paydaşlı ve kapsayıcı işbirliği mekanizmalarının güçlendirilmesi gerekmektedir. Siber güvenlik standartları, dijital ticaret kuralları, veri koruma rejimleri ve yapay zekâ etiği gibi alanlarda uluslararası normların ve düzenleyici çerçevelerin geliştirilmesi, dijital çağın küresel yönetişim mimarisinin temel unsurlarıdır. Aynı zamanda, dijital teknolojilerin potansiyel risklerinin yönetilmesi ve olumsuz etkilerinin azaltılması için ulusal ve uluslararası düzeyde proaktif politikaların oluşturulması gerekmektedir. Bu bağlamda teknolojik gelişmelerin sosyal, etik ve politik boyutlarını dikkate alan bütüncül yaklaşımların benimsenmesi kritik önem taşımaktadır (Nye, 2021; OECD, 2021).

Büyük güçler arasındaki dijital rekabet, uluslararası sistemin geleceğini belirleyen en önemli faktörlerden biri olmaya devam edecektir. ABD, Çin, Rusya ve Avrupa Birliği arasındaki teknolojik rekabet, yalnızca ekonomik veya askeri bir yarış değil, aynı zamanda farklı yönetişim modellerinin, değer sistemlerinin ve jeopolitik vizyonların çatıştığı bir alan haline gelmektedir. Çin'in "Dijital İpek Yolu" girişimi ve teknoloji ihracatı stratejisi, ABD'nin "Temiz Ağ" (Clean Network) yaklaşımı ve Avrupa Birliği'nin "Dijital Egemenlik" vizyonu, bu rekabetin farklı boyutlarını yansıtmaktadır. Teknolojik standartların belirlenmesi, stratejik teknolojilerin kontrolü ve dijital altyapının şekillendirilmesi konularındaki rekabet, küresel güç dengelerini derinden etkilemektedir. Bu bağlamda dijital teknolojilere hâkim olan ve bu alandaki standartları belirleyen aktörler, 21. yüzyılın küresel liderliğinde öne çıkacaktır. Dijital rekabetin yönetilmesi, teknolojik bölünmelerin önlenmesi ve küresel dijital alanın parçalanmasının (splinternet) engellenmesi, uluslararası istikrar açısından kritik önem taşımaktadır (Fukuyama, 2021; Morozov, 2021).

3. TEORİK ÇERÇEVE VE ANALİTİK YAKLAŞIM

3.1. Ağ Teorisi, Bilgi Akışı ve Dijital Güç Dengesi

Dijital teknolojilerin uluslararası ilişkiler üzerindeki etkilerini analiz etmek için kullanılan teorik çerçeveler, dijitalleşmenin küresel sistemde nasıl bir dönüşüm oluşturduğunu anlamada farklı bakış açıları sunmaktadır. Ağ teorisi, bilgi akışı ve dijital güç dengesi kavramları, uluslararası ilişkilerde geleneksel güç unsurlarının dijital dünyaya nasıl adapte olduğunu ve devletlerarası rekabetin hangi eksende devam edeceğini anlamayı zorunlu hale getirmiştir. Özellikle yapay zekâ, blok zinciri, kuantum bilişim ve siber güvenlik gibi teknolojik gelişmeler, devletlerin jeopolitik ve ekonomik strate-

jilerini belirleyen en önemli faktörler arasında yer alacaktır. Bu teknolojiler, yalnızca devletlerin askeri ve ekonomik kapasitelerini değil, aynı zamanda karar alma süreçlerini, diplomatik etkileşimlerini ve küresel nüfuz alanlarını da doğrudan etkilemektedir. Dijitalleşme süreci, uluslararası ilişkilerin temel parametrelerini yeniden tanımlarken, aktörler arasındaki güç dinamiklerinin daha karmaşık ve çok boyutlu bir yapıya dönüşmesine neden olmaktadır (Nye, 2021; Floridi, 2018).

Ağ teorisi, uluslararası ilişkilerde aktörlerin birbiriyle nasıl bağlantı kurduğunu, bilgi akışının nasıl şekillendiğini ve küresel güç dinamiklerinin nasıl inşa edildiğini anlamak için kritik bir çerçeve sunmaktadır. Geleneksel uluslararası ilişkiler analizleri, büyük ölçüde devlet merkezli ve hiyerarşik yapılar üzerinden yürütülürken, ağ teorisi, devletlerin, devlet dışı aktörlerin, teknoloji şirketlerinin ve sivil toplum kuruluşlarının birbiriyle nasıl etkileşim kurduğunu modellemeye olanak tanımaktadır. Özellikle siber güvenlik, yapay zekâ destekli iletişim ağları, büyük veri analitiği ve blok zinciri sistemleri, uluslararası ilişkilerde bilginin nasıl dolaştığını, nasıl kontrol edildiğini ve hangi aktörlerin küresel bilgi yönetiminde merkezi bir konuma sahip olduğunu analiz etmeyi mümkün kılmaktadır. Ağ teorisinin sunduğu analiz çerçevesi, dijital çağda devletlerin gücünün yalnızca sahip oldukları maddi kaynaklarla değil, aynı zamanda küresel ağlar içindeki merkeziyet dereceleri, bağlantı yoğunlukları ve ağ kontrolü kapasiteleriyle de belirlendiğini ortaya koymaktadır. Bu bağlamda ağ merkeziliği yüksek olan aktörler, bilgi akışını yönlendirme ve kontrol etme kapasitesine sahip olarak küresel sistemde daha etkili bir konuma ulaşmaktadır (Castells, 2020; Morozov, 2021).

Devletler, bilgi akışlarını yönlendirmek ve küresel dezenformasyon stratejileri oluşturmak için gelişmiş yapay zekâ destekli veri analiz sistemleri kullanarak bilgi savaşlarını daha karmaşık bir hale getirmektedir. Bu durum, uluslararası ilişkilerde güç dağılımının yeniden şekillenmesine ve geleneksel diplomatik süreçlerin dönüşmesine neden olmaktadır. Özellikle büyük veri analitiği ve makine öğrenmesi algoritmaları, devletlerin hedef kitlelere yönelik özelleştirilmiş dezenformasyon kampanyaları yürütmesine olanak tanımaktadır. Sosyal medya platformları üzerinden yürütülen algı yönetimi operasyonları, seçimlere müdahale, toplumsal kutuplaşmayı artırma ve demokratik süreçleri zayıflatma amaçlı kullanılabilmektedir. Bu dijital müdahale teknikleri, fiziksel sınırları aşarak küresel ölçekte etki oluşturabilmekte ve geleneksel diplomatik koruma mekanizmalarını etkisiz hale getirebilmektedir. Bilgi savaşlarının bu yeni formu, uluslararası güvenlik doktrilerinin ve diplomatik savunma stratejilerinin yeniden değerlendirilmesini gerektirmektedir (Zuboff, 2019; Arquilla & Ronfeldt, 2020).

Bilgi akışı, uluslararası ilişkilerde aktörlerin stratejik konumlarını ve güç kapasitelerini belirleyen temel unsurlardan biri haline gelmiştir. Dijitalleş-

me süreci, bilgiyi üretme, saklama ve yayma yeteneğini yalnızca devletlerin tekelinden çıkararak teknoloji şirketleri, uluslararası örgütler ve bireysel aktörlerin de bu süreçte etkin roller üstlenmesine olanak tanımıştır. Yapay zekâ destekli veri analiz sistemleri, devletlerin küresel kamuoyunu nasıl yönlendirdiğini ve uluslararası krizleri nasıl manipüle edebildiğini göstermektedir. Örneğin 2016 ABD seçimlerinde Rusya'nın sosyal medya platformları üzerinden bilgi akışlarını manipüle ederek kamuoyunu yönlendirmeye çalışması, bilgi savaşlarının uluslararası siyasetteki etkisini ortaya koymuştur. Dijital bilgi ekosistemindeki bu dönüşüm, geleneksel medya kontrolü ve propaganda tekniklerinin ötesinde, çok daha sofistike ve hedef odaklı etki operasyonlarının geliştirilmesine olanak tanımıştır. Algoritmik içerik dağıtımı, mikro-hedefleme teknikleri ve otomatik bot ağları, bilgi akışlarının manipülasyonunda kullanılan yeni araçlar olarak öne çıkmaktadır. Bu teknolojik gelişmeler, bilginin küresel dolaşımını kontrol etme kapasitesini, uluslararası güç projeksiyonunun temel bir bileşeni haline getirmiştir (Nye, 2021; Choucri, 2021).

Dijital güç dengesi, devletlerin ulusal ve küresel ölçekte dijital sistemler üzerinde ne kadar kontrol sahibi olduğu ile doğrudan ilişkilidir. Veri yönetimi, siber güvenlik stratejileri, yapay zekâ temelli karar alma sistemleri ve kuantum bilişim destekli istihbarat mekanizmaları, devletlerin dijital kapasitesini belirleyen en önemli unsurlar arasında yer almaktadır. Özellikle büyük teknoloji şirketleri (GAFAM), küresel bilgi akışlarının büyük bir bölümünü kontrol ederek devletlerden bağımsız bir ekonomik ve stratejik güç unsuru haline gelmiştir. Bu şirketler, devletlerarası güç mücadelesine doğrudan etki edebilmekte, diplomatik krizlerde taraf olarak konumlanabilmekte ve küresel politika süreçlerinde belirleyici bir rol oynayabilmektedir. Teknoloji şirketlerinin bu artan gücü, devlet egemenliği kavramının yeniden tanımlanmasını gerektirmekte ve geleneksel egemenlik anlayışının sınırlarını zorlamaktadır. Veri lokalizasyonu politikaları, kritik teknolojilerin millileştirilmesi ve teknoloji şirketlerinin düzenlenmesine yönelik yeni hukuki çerçeveler, devletlerin dijital egemenliklerini koruma çabalarını yansıtmaktadır. Bu bağlamda dijital güç dengesinin nasıl şekillendiği, gelecekteki uluslararası sistemin yapısını doğrudan etkileyecek kritik bir faktör olarak öne çıkmaktadır (Zuboff, 2019; Morozov, 2021).

Dijital güç dengesindeki bu dönüşüm, geleneksel diplomatik süreçleri ve uluslararası güvenlik stratejilerini de etkilemektedir. Devletler, dijital altyapılarını güçlendirerek ve veri yönetimi kapasitelerini artırarak küresel rekabette avantaj sağlamaya çalışırken, aynı zamanda siber saldırılara karşı savunma mekanizmalarını da geliştirmek zorunda kalmaktadır. Bu durum, uluslararası sistemde yeni ittifak modellerinin oluşmasına ve dijital güvenlik politikalarının ön plana çıkmasına neden olmaktadır. Dijital teknolojiler alanında gelişmiş olan devletler, bu avantajlarını uluslararası

nüfuzlarını artırmak ve stratejik çıkarlarını korumak için kullanmaktadır. Örneğin ABD'nin küresel internet altyapısı üzerindeki kontrolü, istihbarat toplama ve stratejik iletişim alanlarında önemli bir avantaj sağlarken, Çin'in 5G teknolojisi ve dijital altyapı yatırımları yoluyla küresel nüfuzunu genişletme çabaları, dijital güç mücadelesinin farklı boyutlarını göstermektedir. Bu teknolojik rekabet, yalnızca ekonomik ve askeri alanlarda değil, aynı zamanda normatif ve ideolojik düzlemlerde de sürdürülmekte, dijital teknolojilerin gelişimi ve kullanımına yönelik farklı değer sistemleri ve yönetişim modelleri arasında bir mücadele yaşanmaktadır (Arquilla & Ronfeldt, 2020; West, 2021).

Kuantum bilişim ve yapay zekâ gibi ileri teknolojiler, dijital güç dengesini köklü biçimde değiştirme potansiyeline sahiptir. Kuantum bilgisayarların mevcut şifreleme sistemlerini kırabilme kapasitesi, istihbarat toplama ve veri güvenliği alanlarında stratejik bir üstünlük sağlayacaktır. Yapay zekâ sistemlerinin karar alma süreçlerine entegrasyonu ise, askeri operasyonlardan kriz yönetimine, diplomatik müzakerelerden ekonomik tahminlere kadar geniş bir alanda devletlere rekabet avantajı sunacaktır. Bu ileri teknolojilerin geliştirilmesi ve kontrolü için yürütülen rekabet, yeni nesil bir silahlanma yarışı olarak değerlendirilmektedir. Özellikle yapay zekâ ve kuantum teknolojileri alanında üstünlük elde eden aktörler, uluslararası sistemde önemli bir stratejik avantaj kazanacaktır. Bu nedenle, devletler yalnızca bu teknolojilerin geliştirilmesine yatırım yapmakla kalmayıp, aynı zamanda bunların yayılımını kontrol etmeye ve stratejik rakiplerin erişimini kısıtlamaya yönelik politikalar da geliştirmektedir. Bu teknolojik rekabet, dijital güç dengesini şekillendiren en önemli dinamiklerden biri olarak öne çıkmaktadır (Singer & Brooking, 2019; Fukuyama, 2021).

Dijital güç dengesi, uluslararası norm oluşturma süreçleri ve küresel yönetişim mekanizmaları üzerinde de belirleyici bir etkiye sahiptir. Dijital teknolojilerin düzenlenmesine yönelik küresel standartları ve normatif çerçeveleri şekillendirme kapasitesi, devletlerin dijital güç projeksiyonunun önemli bir boyutunu oluşturmaktadır. Özellikle veri koruma standartları, içerik düzenleme politikaları, yapay zekâ etiği ve siber güvenlik normları gibi alanlarda, farklı aktörlerin kendi değerlerini ve stratejik çıkarlarını yansıtan modelleri küresel standart haline getirme çabaları gözlemlenmektedir. Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR) ve dijital hizmetler yasası gibi düzenlemeler, veri mahremiyeti ve dijital haklar alanında küresel normatif çerçeveyi şekillendirirken, Çin'in siber egemenlik doktrini alternatif bir model sunmaktadır. Bu normatif rekabet, yalnızca teknolojik standartları değil, aynı zamanda dijital dünyada hangi değerlerin ve ilkelerin hâkim olacağını da belirlemektedir. Dijital teknolojilerin yönetişimine yönelik bu farklı yaklaşımlar, uluslararası sistemin ideolojik ve stratejik kutup-

laşmasını derinleştirerek internetin ve dijital ekosistemin parçalanmasına (splinternet) yol açma potansiyeli taşımaktadır (Floridi, 2018; OECD, 2021).

Dijital teknolojilerin yaygınlaşması ve bilgi akışlarının küreselleşmesi, devletlerin geleneksel kontrol mekanizmalarını zorlayarak dijital egemenlik kavramının yeniden tanımlanmasını gerektirmektedir. Dijital egemenlik, bir devletin kendi sınırları içindeki dijital altyapılar, veri akışları ve teknolojik sistemler üzerindeki kontrol kapasitesini ifade etmekte ve ulusal güvenlik stratejilerinin ayrılmaz bir parçası haline gelmektedir. Devletler, dijital egemenliklerini güçlendirmek için veri lokalizasyonu politikaları, ulusal teknoloji şampiyonlarının desteklenmesi, kritik teknolojilerde dışa bağımlılığın azaltılması ve siber savunma kapasitelerinin geliştirilmesi gibi stratejiler izlemektedir. Bu dijital egemenlik yaklaşımları, bir yandan ulusal güvenliği ve stratejik özerkliği güçlendirmeyi amaçlarken, diğer yandan küresel teknoloji ekosisteminin parçalanmasına ve uluslararası işbirliğinin zorlaşmasına neden olabilmektedir. Dijital egemenlik ile açık internet arasındaki denge, uluslararası sistemin geleceğini şekillendirecek kritik bir faktör olarak öne çıkmaktadır. Bu bağlamda dijital güç dengesinin nasıl şekilleneceği ve dijital teknolojilerin uluslararası ilişkilerde nasıl bir rol oynayacağı, küresel sistemin yapısal dönüşümünü belirleyecek temel dinamiklerden biri olacaktır (Nye, 2021; Choucri, 2021).

3.2. Teknolojik Determinizm, Konstrüktivizm ve Eleştirel Perspektifler

Dijital teknolojilerin uluslararası ilişkiler üzerindeki etkilerini anlamak için farklı teorik perspektiflerin karşılaştırmalı bir çerçevede ele alınması gerekmektedir. Teknolojik gelişmelerin devletler, uluslararası örgütler, küresel şirketler ve bireyler üzerindeki etkileri, uluslararası ilişkiler disiplininde farklı teorik yaklaşımlar aracılığıyla analiz edilmektedir. Teknolojik determinizm, teknolojinin insan davranışlarını ve toplumların gelişimini belirleyen ana unsur olduğunu savunurken, konstrüktivizm, teknolojinin sosyal yapıların bir parçası olarak geliştiğini öne sürmektedir. Eleştirel perspektifler ise, dijitalleşmenin küresel güç dengesini nasıl şekillendirdiğini ve teknolojik gelişmelerin hangi aktörler tarafından nasıl yönlendirildiğini sorgulamaktadır. Bu teorik çerçeveler, dijital teknolojilerin uluslararası ilişkiler üzerindeki etkilerini farklı açılardan aydınlatarak bu dönüşüm sürecinin derinlemesine anlaşılmasına katkıda bulunmaktadır. Her bir teorik yaklaşım teknoloji-toplum-politika etkileşiminin farklı boyutlarını ön plana çıkararak dijitalleşmenin çok boyutlu doğasını kavramaya yardımcı olmaktadır (Nye, 2021; Floridi, 2018).

Teknolojik determinizm, teknolojinin toplumsal, ekonomik ve politik değişimleri belirleyen ana itici güç olduğunu savunan bir yaklaşımdır. Bu teoriye göre, teknolojik gelişmeler kendi başlarına bağımsız bir değişken olarak ilerler ve toplumsal yapılar, politik sistemler ve uluslararası ilişkiler

bu teknolojik dönüşüme uyum sağlamak zorunda kalır. Özellikle dijitalleşme çağında, yapay zekâ, blok zinciri, kuantum bilişim ve siber güvenlik gibi teknolojiler, devletlerin uluslararası sistemdeki konumlarını doğrudan etkilemekte ve küresel rekabet dinamiklerini şekillendirmektedir. Teknolojik deterministyaklaşım dijital devrim olarak adlandırılan bu sürecin kaçınılmaz ve kontrolü zor bir evrimsel güç olduğunu, toplumların ve devletlerin bu teknolojik dalgaya adapte olmaları gerektiğini vurgulamaktadır. Bu perspektife göre, teknolojik yenilikler kendi iç mantığı ve dinamikleriyle ilerlemekte, toplumsal ve politik yapılar ise bu teknolojik gelişmelerin sonuçlarına uyum sağlamak zorunda kalmaktadır. Dijital teknolojilerin yayılma hızı ve transformatif etkisi, bu deterministyaklaşımı destekler nitelikte görünse de, bu teorinin teknolojinin sosyal, kültürel ve politik bağlamından bağımsız olarak değerlendirilmesi önemli bir eleştiri konusudur (Smith & Marx, 1994; Brynjolfsson & McAfee, 2019).

Bu yaklaşım devletlerin ve küresel aktörlerin bu sürece yalnızca adapte olmak zorunda kaldığını ve teknolojik gelişmelerin kontrol edilmesinin imkânsız olduğunu öne sürer. Bu bağlamda uluslararası ilişkilerde güç dağılımı, devletlerin teknolojiyi ne ölçüde benimsediğine ve entegre ettiğine bağlı hale gelmiştir. Teknolojik deterministperspektife göre, dijital teknolojilere erişim ve bu teknolojileri etkin kullanma kapasitesi, devletlerin küresel hiyerarşideki konumlarını belirlemektedir. Yapay zekâ, kuantum bilişim ve blok zinciri gibi ileri teknolojilere yatırım yapan ve bunları ulusal güvenlik, ekonomi ve diplomasi alanlarına entegre eden devletler, uluslararası sistemde üstünlük elde edecektir. Bu yaklaşım teknolojik gelişmelerin uluslararası sistemde oluşturacağı dönüşümün kaçınılmazlığını vurgularken, devletlerin ve diğer aktörlerin bu süreçteki etkilerini ve seçimlerini yeterince dikkate almamakla eleştirilmektedir. Ayrıca teknolojik determinizm, teknolojinin sosyal ve kültürel bağlamdan bağımsız olarak geliştiği varsayımıyla teknolojik yeniliklerin belirli değerler, çıkarlar ve güç ilişkileri çerçevesinde şekillendiği gerçeğini göz ardı etmektedir (West, 2021; Floridi, 2018).

Konstrüktivizm, uluslararası ilişkilerde aktörlerin davranışlarının yalnızca maddi güç unsurlarıyla değil, aynı zamanda sosyal yapılar, normlar ve kimlikler aracılığıyla şekillendiğini savunan bir teorik çerçeve sunmaktadır. Bu yaklaşıma göre, dijital teknolojiler kendi başlarına belirleyici bir faktör değil, toplumlar, devletler ve bireyler tarafından nasıl anlamlandırıldıklarına bağlı olarak şekillenen dinamik unsurlardır. Örneğin bir ülke blok zinciri tabanlı finansal sistemleri ekonomik bağımsızlığın bir aracı olarak görürken, başka bir ülke aynı teknolojiyi finansal düzeni tehdit eden bir unsur olarak değerlendirebilir. Konstrüktivist perspektif, teknolojinin kendisinin değil, teknolojiye yüklenen anlamların ve bu teknolojinin kullanım biçimlerinin toplumsal ve politik sonuçları belirlediğini vurgulamaktadır. Bu bağlamda dijital teknolojiler, devletlerin ve toplumların kimlik-

lerini, çıkarlarını ve normlarını yansıtan sosyal inşa süreçleri çerçevesinde gelişmekte ve kullanılmaktadır. Teknolojik yenilikler, belirli sosyal, politik ve kültürel bağlamlarda anlam kazanmakta ve bu bağlamlar tarafından şekillendirilmektedir (Wendt, 1999; Finnemore & Sikkink, 1998).

Dijitalleşmenin uluslararası ilişkilerdeki rolü, devletlerin ve diğer aktörlerin bu teknolojilere yüklediği anlamlar ve inşa ettikleri kimlikler tarafından şekillendirilmektedir. Örneğin Çin'in "Dijital İpek Yolu" stratejisi, yalnızca teknolojik yatırımlarla ilgili bir hamle değil, aynı zamanda Çin'in küresel liderlik iddiasını güçlendiren bir kimlik inşası sürecidir. Konstrüktivist yaklaşım dijital teknolojilerin belirli değerler, normlar ve kimlikler çerçevesinde geliştiğini ve kullanıldığını vurgulayarak teknolojik gelişmelerin sosyal ve politik bağlamdan bağımsız olmadığını göstermektedir. Bu perspektife göre, dijital teknolojiler ve bunların uluslararası ilişkiler üzerindeki etkileri, devletlerin ve diğer aktörlerin karşılıklı etkileşimleri ve müzakereleri sonucunda oluşan paylaşılan anlamlar ve normlar çerçevesinde şekillenmektedir. Dijital teknolojilerin gelişimi ve kullanımına ilişkin normlar, kurallar ve uygulamalar, aktörlerin etkileşimleri sonucunda sosyal olarak inşa edilmekte ve zamanla değişebilmektedir. Bu sosyal inşa süreci, dijital teknolojilerin uluslararası politikadaki rolünü ve etkilerini anlamada kritik öneme sahiptir (Checkel, 1998; Fukuyama, 2021).

Konstrüktivist yaklaşım aynı zamanda dijital kimlikler, dijital diplomasi ve siber normların oluşumu gibi konularda da önemli analitik araçlar sunmaktadır. Dijital kimliklerin nasıl oluştuğu, hangi değerlerle ilişkilendirildiği ve uluslararası siyasetteki etkileşimlerde nasıl bir rol oynadığı, konstrüktivist perspektifle daha derinlemesine analiz edilebilir. Örneğin "siber güç", "dijital egemenlik" veya "siber savaş" gibi kavramların nasıl tanımlandığı ve bu tanımların aktörler arasındaki etkileşimleri nasıl şekillendirdiği, konstrüktivist bir çerçevede incelenebilir. Siber normların gelişimi, devletlerin ve diğer aktörlerin siber alandaki "uygun davranış" standartları üzerine müzakereleri ve uzlaşıları olarak görülebilir. Bu normların oluşumu ve değişimi, aktörlerin kimliklerinden, çıkarlarından ve güç ilişkilerinden etkilenmekte, ancak aynı zamanda bu unsurları da şekillendirmektedir. Konstrüktivist yaklaşım dijital teknolojilerin gelişimi ve etkilerine ilişkin deterministik varsayımları sorgulayarak teknoloji-toplum-politika etkileşiminin karmaşık ve dinamik doğasını vurgulamaktadır (Choucri, 2021; Arquilla & Ronfeldt, 2020).

Dijitalleşme süreci, eleştirel perspektiflerden bakıldığında, uluslararası ilişkilerde güç dengelerini yeniden şekillendiren ve belirli aktörlerin gücünü pekiştiren bir araç olarak değerlendirilmektedir. Özellikle büyük teknoloji şirketlerinin, uluslararası sistemin geleneksel aktörleri olan devletler kadar etkili hale gelmesi ve bilgi kontrol mekanizmalarını yönetme kapasitesinin artması, dijital dönüşümün yalnızca teknolojik bir ilerleme olmadığını, aynı

zamanda küresel siyasetteki güç asimetrilerini derinleştiren bir süreç olduğunu göstermektedir. Eleştirel teoriler, dijital teknolojilerin gelişimini ve kullanımını mevcut güç ilişkileri ve hegemonik yapılar çerçevesinde analiz etmekte, bu teknolojilerin kimin çıkarlarına hizmet ettiğini ve hangi değerleri yansıttığını sorgulamaktadır. Bu perspektife göre, dijital teknolojiler nötr araçlar değil, belirli güç ilişkilerini ve hegemonik yapıları yeniden üreten veya güçlendiren politik enstrümanlardır. Eleştirel yaklaşımlar, dijital teknolojilerin gelişimi ve kullanımının arkasındaki güç dinamiklerini, ekonomik çıkarları ve ideolojik motivasyonları açığa çıkararak bu teknolojilerin toplumsal etkilerini daha kapsamlı bir şekilde anlamaya çalışmaktadır (Zuboff, 2019; Fuchs, 2020).

Dijital kapitalizm kavramı, küresel teknoloji şirketlerinin veri ekonomisi üzerindeki hâkimiyetini eleştirel bir çerçevede inceleyerek dijitalleşmenin neo-liberal politikalarla nasıl iç içe geçtiğini sorgulamaktadır. Teknoloji devleri, büyük veri setlerini toplayarak küresel piyasaları yönlendirmekte ve devletlerin ekonomik politikalarına yön verebilmektedir. Eleştirel perspektifler, veri kolonizasyonu olarak adlandırılan bu süreci, yeni bir sömürü biçimi olarak değerlendirmekte ve dijital teknolojilerin küresel eşitsizlikleri nasıl derinleştirdiğini analiz etmektedir. Örneğin veri madenciliği ve gözetim kapitalizmi kavramları, teknoloji şirketlerinin kullanıcı verilerini nasıl metalaştırdığını ve bu verileri kâr amaçlı kullandığını açıklamaktadır. Bu süreç, yalnızca ekonomik eşitsizlikleri değil, aynı zamanda bilgiye erişim, dijital okuryazarlık ve teknolojik altyapı gibi alanlardaki küresel asimetrileri de derinleştirmektedir. Eleştirel perspektifler, dijital teknolojilerin demokratikleşme potansiyelini kabul etmekle birlikte, bu teknolojilerin mevcut güç yapılarını güçlendirme ve yeni kontrol mekanizmaları oluşturma risklerine de dikkat çekmektedir (Mosco, 2017; Couldry & Mejias, 2019).

Ayrıca eleştirel perspektifler, dijital teknolojilerin demokrasi, insan hakları ve ifade özgürlüğü üzerindeki etkilerini de sorgulamaktadır. Dijitalleşmenin, küresel demokratikleşme sürecini destekleyici bir unsur olarak görülebileceği iddia edilse de, otoriter rejimlerin dijital teknolojileri toplumsal gözetim ve kontrol mekanizmalarını güçlendirmek için kullanması, bu argümanın sorgulanmasına neden olmuştur. Eleştirel teoriler, dijital gözetim, algoritma tabanlı ayrımcılık ve içerik sansürü gibi uygulamaların, demokratik değerleri ve insan haklarını nasıl tehdit ettiğini incelemektedir. Özellikle yapay zekâ algoritmaları ve büyük veri analitiği gibi ileri teknolojilerin, otoriter rejimlerin gözetim kapasitelerini artırdığı ve muhalif sesleri bastırmak için kullanılabildiği vurgulanmaktadır. Bu bağlamda eleştirel perspektifler, dijital teknolojilerin demokratikleşme ve özgürleşme potansiyelini gerçekleştirmek için bu teknolojilerin gelişimi ve kullanımına ilişkin normatif çerçevelerin ve demokratik denetim mekanizmalarının önemine dikkat çekmektedir (Morozov, 2011; Singer & Brooking, 2019).

Eleştirel yaklaşımlar, aynı zamanda dijital teknolojilerin çevresel etkileri ve sürdürülebilirlikle ilişkisini de sorgulamaktadır. Veri merkezlerinin enerji tüketimi, elektronik atıkların artışı ve dijital altyapıların karbon ayak izi gibi konular, dijitalleşmenin çevresel maliyetlerini gündeme getirmektedir. Eleştirel teoriler, teknolojik ilerleme söyleminin çoğu zaman bu çevresel etkileri göz ardı ettiğini ve dijital teknolojilerin sürdürülebilir kalkınma hedeflerine katkısının sorgulanması gerektiğini vurgulamaktadır. Ayrıca dijital teknolojilerin kaynak çıkarma, üretim ve atık yönetimi süreçlerindeki küresel eşitsizlikleri nasıl yeniden ürettiği de eleştirel perspektiflerden analiz edilmektedir. Eleştirel yaklaşımlar, dijital teknolojilerin gelişimi ve kullanımına ilişkin politikaların, yalnızca ekonomik verimlilik ve teknolojik yenilik odaklı değil, aynı zamanda sosyal adalet, eşitlik ve çevresel sürdürülebilirlik gibi değerleri de gözetmesi gerektiğini savunmaktadır. Bu bağlamda dijital teknolojilerin uluslararası ilişkiler üzerindeki etkilerini anlamak için teknoloji-toplum-politika-çevre etkileşimini bütünsel bir çerçevede ele almak gerekmektedir (Klein, 2020; OECD, 2021).

3.3. Yapay Zekâ, Blok Zinciri ve Kuantum Teknolojileri Üzerine Teorik Değerlendirme

Dijital teknolojilerin uluslararası ilişkiler üzerindeki etkilerini anlamak için kullanılan teorik çerçeveler, dijitalleşmenin küresel sistemde nasıl bir dönüşüm oluşturduğunu anlamada farklı bakış açıları sunmaktadır. Teknolojik determinizm, dijital dönüşümün kaçınılmaz bir süreç olduğunu ve devletlerin bu dönüşüme ayak uydurmak zorunda kaldığını savunurken, konstrüktivizm, dijitalleşmenin sosyal ve politik yapıların bir yansıması olarak şekillendiğini öne sürmektedir. Eleştirel perspektifler ise, dijital teknolojilerin küresel güç dengelerini nasıl değiştirdiğini ve bu dönüşüm sürecinin belirli aktörler tarafından nasıl yönlendirildiğini sorgulamaktadır. Özellikle yapay zekâ, blok zinciri ve kuantum bilişim gibi öncü teknolojiler, uluslararası ilişkilerde güç, güvenlik, ekonomi ve diplomasi alanlarında köklü dönüşümlere yol açmakta ve geleneksel uluslararası ilişkiler teorilerinin bu yeni dinamikleri açıklama kapasitesini zorlamaktadır. Bu teknolojilerin gelişimi ve küresel yayılımı, devletler, uluslararası örgütler ve teknoloji şirketleri arasındaki etkileşimleri yeniden şekillendirerek uluslararası sistemin yapısal bir transformasyonuna neden olmaktadır (Nye, 2021; Floridi, 2018).

Yapay zekâ (YZ), uluslararası ilişkilerde diplomasi, güvenlik, ekonomi ve küresel yönetişim alanlarında köklü değişimlere neden olan en önemli teknolojik gelişmelerden biri olarak öne çıkmaktadır. Devletlerarası güç rekabeti artık yalnızca askeri ve ekonomik kapasiteler üzerinden değil, yapay zekâ destekli büyük veri analitiği, otonom sistemler ve algoritmik karar alma mekanizmaları aracılığıyla da şekillenmektedir. YZ'nin uluslararası ilişkiler disiplininde nasıl konumlandırılacağı, devletlerin bu teknolojiyi nasıl benimsediği ve dijital hegemonya süreçlerinde nasıl bir araç olarak

kullanıldığı konularında teorik çerçevelerin geliştirilmesi gerekmektedir. Teknolojik determinist yaklaşımlar, yapay zekânın gelişimini kaçınılmaz bir süreç olarak görüp, devletlerin bu teknolojik dalgaya uyum sağlaması gerektiğini vurgularken, konstrüktivist perspektifler, yapay zekânın toplumsal değerler, normlar ve kimlikler çerçevesinde şekillendiğini ve farklı kültürel bağlamlarda farklı biçimlerde geliştiğini öne sürmektedir. Eleştirel yaklaşımlar ise, yapay zekâ teknolojilerinin ardındaki güç dinamiklerini, ekonomik çıkarları ve ideolojik motivasyonları sorgulayarak bu teknolojilerin belirli aktörlerin hegemonik pozisyonlarını güçlendirme potansiyeline dikkat çekmektedir (Nye, 2021; Brynjolfsson & McAfee, 2019).

YZ destekli diplomatik platformlar ve karar alma mekanizmaları, devletlerin dış politika stratejilerini ve kriz yönetim kapasitelerini köklü biçimde değiştirmektedir. Ancak bu sistemlerin insan faktörünü devre dışı bırakması ve kararların otomatikleştirilmesi, uluslararası ilişkilerde öngörülemeyen sonuçlar doğurabilir. Yapay zekânın diplomatik süreçlere entegrasyonu, karar alma mekanizmalarının hızlanması ve veri odaklı politika geliştirme süreçlerinin güçlenmesi gibi avantajlar sunarken, algoritmik önyargılar, veri manipülasyonu ve sistemik risklerin artması gibi sorunları da beraberinde getirmektedir. Uluslararası ilişkiler teorileri, yapay zekânın diplomatik müzakereleri, kriz yönetimini ve stratejik planlamayı nasıl dönüştürdüğünü anlamak için yeni analitik çerçeveler geliştirmelidir. Yapay zekâ diplomasisinin etik boyutları, hesap verebilirlik mekanizmaları ve demokratik denetim süreçleri, bu alandaki teorik tartışmaların önemli bileşenleri olmalıdır. Ayrıca yapay zekâ sistemlerinin karar alma süreçlerinde artan rolü, uluslararası ilişkilerdeki insani boyutu ve diplomatik etkileşimlerin sosyal ve kültürel dinamiklerini nasıl etkileyeceği de teorik düzeyde incelenmelidir (West, 2021; Choucri, 2021).

Yapay zekânın askeri uygulamaları, uluslararası güvenlik teorilerini ve stratejik düşünceyi yeniden şekillendirmektedir. Otonom silah sistemleri, yapay zekâ destekli istihbarat analizi ve siber savunma mekanizmaları, güvenlik doktrinlerini ve caydırıcılık stratejilerini dönüştürmektedir. Güvenlik çalışmaları, yapay zekânın savaşın doğasını nasıl değiştirdiğini, insan faktörünün azalmasının stratejik istikrar üzerindeki etkilerini ve otonom sistemlerin uluslararası insancıl hukuk açısından oluşturduğu zorlukları analiz etmelidir. Yapay zekâ silahlanma yarışının dinamikleri, güvenlik ikilemi teorileri çerçevesinde incelenebilir, ancak bu teknolojilerin belirsizliği, atfedilme zorluğu ve stratejik öngörülemezliği, mevcut teorik modellerin genişletilmesini gerektirmektedir. Yapay zekânın askeri alandaki uygulamaları, geleneksel güç dengesi teorilerini, caydırıcılık stratejilerini ve kriz istikrarı modellerini önemli ölçüde etkilemektedir. Bu bağlamda yapay zekâ destekli sistemlerin güvenlik politikalarındaki artan rolü, uluslararası ilişkiler teorisyenlerini yeni kavramsal çerçeveler ve analitik modeller geliş-

tirmeye yönlendirmektedir. Özellikle otonom silah sistemlerinin proliferasyonu, yapay zekâ algoritmalarının stratejik karar alma süreçlerindeki rolü ve yapay zekâ teknolojilerinin asimetrik güç dağılımına etkileri, uluslararası güvenlik teorilerinin güncel araştırma alanları olarak öne çıkmaktadır (Arquilla & Ronfeldt, 2020; Singer & Brooking, 2019).

Blok zinciri teknolojisi, merkeziyetsiz ve güvenli veri kayıt sistemleri oluşturma kapasitesi ile uluslararası ilişkiler, ekonomi ve güvenlik alanlarında köklü dönüşümlere yol açmaktadır. Geleneksel finansal ve yönetişim mekanizmalarına olan bağımlılığı azaltan bu teknoloji, küresel ölçekte devletlerin ve uluslararası örgütlerin ekonomik, diplomatik ve güvenlik stratejilerini yeniden şekillendirmelerine neden olmaktadır. Özellikle merkeziyetsiz finans sistemleri, herhangi bir merkezi otoriteye ihtiyaç duymadan güvenli ve şeffaf işlem kayıtları sağlayarak devletlerarası finansal ilişkileri, veri güvenliğini ve yönetişim süreçlerini köklü biçimde değiştirme potansiyeline sahiptir. Uluslararası ilişkiler teorileri, blok zinciri teknolojisinin devlet egemenliği, uluslararası işbirliği ve küresel yönetişim yapıları üzerindeki etkilerini açıklamak için yeni teorik çerçeveler geliştirmelidir. Teknolojik determinist yaklaşımlar, blok zincirinin finansal sistemleri merkeziyetsizleştirme ve aracıları ortadan kaldırma kapasitesini kaçınılmaz bir süreç olarak görürken, konstrüktivist perspektifler, bu teknolojinin farklı sosyal, kültürel ve politik bağlamlarda nasıl anlamlandırıldığını ve uygulandığını incelemektedir (Brynjolfsson & McAfee, 2019; OECD, 2021).

Blok zinciri tabanlı sistemlerin uluslararası hukuk çerçevesinde nasıl düzenleneceği ve devletlerin ekonomik kontrol mekanizmalarını nasıl etkileyeceği konusunda teorik tartışmalar devam etmektedir. Özellikle Çin'in dijital yuan projesi ve Avrupa Birliği'nin dijital euro girişimleri, devletlerin blok zinciri teknolojisine yönelik farklı yaklaşımlarını göstermektedir. Uluslararası politik ekonomi teorileri, blok zinciri tabanlı finansal sistemlerin küresel ekonomik yapıları nasıl dönüştürdüğünü, merkeziyetsiz finans platformlarının uluslararası para politikalarını nasıl etkilediğini ve dijital para birimlerinin küresel rezerv para birimleri üzerindeki potansiyel etkilerini analiz etmelidir. Blok zinciri teknolojisi, uluslararası ticaret, sermaye hareketleri ve ekonomik yaptırımlar gibi alanlarda devletlerin kontrolünü azaltarak geleneksel ekonomik güç anlayışını dönüştürmektedir. Bu teknolojinin ekonomik egemenlik, finansal bağımsızlık ve parasal kontrol gibi kavramları nasıl yeniden tanımladığı, uluslararası politik ekonomi teorilerinin güncel araştırma konuları arasındadır. Ayrıca blok zinciri tabanlı sistemlerin uluslararası örgütlerin yapısı, işleyişi ve meşruiyeti üzerindeki etkileri de teorik düzeyde incelenmelidir (Floridi, 2018; Fukuyama, 2021).

Blok zinciri teknolojisinin küresel yönetişim üzerindeki etkilerine ilişkin teorik değerlendirmeler, bu teknolojinin merkeziyetsiz yapısının uluslararası işbirliği ve koordinasyon süreçlerini nasıl dönüştürdüğüne odaklanmalı-

dır. Merkeziyetsiz otonom organizasyonlar (DAO) ve akıllı kontratlar gibi blok zinciri tabanlı yönetişim modelleri, geleneksel uluslararası örgütlerin yapısına ve işleyişine alternatif oluşturabilir. Bu yeni yönetişim formları, katılımcılık, şeffaflık ve hesap verebilirlik açısından farklı dinamikler sunarak küresel kamusal malların üretimi ve yönetimi için yeni mekanizmalar sağlayabilir. Uluslararası ilişkiler teorileri, blok zinciri teknolojisinin uluslararası rejimler, normlar ve kurumlar üzerindeki dönüştürücü etkilerini anlamak için yeni teorik perspektifler geliştirmelidir. Özellikle küresel yönetişim teorileri, blok zinciri tabanlı sistemlerin çok aktörlü, şeffaf ve ademi merkeziyetçi yapısının, mevcut hiyerarşik ve merkeziyetçi küresel yönetişim modelleriyle nasıl etkileşime girdiğini incelemelidir. Bu bağlamda blok zinciri teknolojisinin uluslararası örgütlerin meşruiyeti, etkinliği ve demokratikliği üzerindeki potansiyel etkileri, küresel yönetişim literatürünün güncel araştırma alanları arasında yer almaktadır (Zuboff, 2019; West, 2021).

Kuantum teknolojileri, geleneksel bilgi işlem paradigmasını köklü biçimde değiştirerek devletlerin istihbarat toplama ve siber güvenlik stratejilerini yeniden şekillendirmesine neden olmuştur. Geleneksel bilgisayarlar, verileri sıralı işlem kapasitesine sahip bitler üzerinden işlerken, kuantum bilgisayarlar süperpozisyon ve dolaşıklık prensipleri sayesinde çok daha yüksek hızda ve karmaşık hesaplamalar gerçekleştirebilmektedir. Bu teknoloji, devletlerin istihbarat faaliyetlerinde veri analitiği, şifreleme kırma süreçleri ve tehdit modelleme mekanizmalarında radikal değişiklikler oluşturmaktadır. Teknolojik determinist yaklaşımlar, kuantum teknolojilerinin gelişimini kaçınılmaz bir süreç olarak görüp, devletlerin bu teknolojik dalgaya uyum sağlaması gerektiğini vurgularken, konstrüktivist perspektifler, bu teknolojilerin farklı stratejik kültürler ve güvenlik anlayışları çerçevesinde nasıl yorumlandığını ve uygulandığını incelemektedir. Eleştirel yaklaşımlar ise, kuantum teknolojilerinin gelişimi ve kontrolü sürecindeki güç asimetrilerini ve bunların küresel eşitsizlikleri derinleştirme potansiyelini sorgulamaktadır. Uluslararası ilişkiler teorileri, kuantum teknolojilerinin güvenlik, ekonomi ve diplomasi alanlarındaki dönüştürücü etkilerini anlamak için disiplinler arası bir yaklaşım benimsemelidir (West, 2021; Singer & Brooking, 2019).

Kuantum bilişimin en kritik etkilerinden biri, mevcut tüm şifreleme protokollerini kırabilme potansiyelidir. Bu durum, devletlerin ulusal güvenlik stratejilerini yeniden gözden geçirmesini zorunlu hale getirmiş ve uluslararası güvenlik dengelerini tamamen değiştirebilecek bir tehdit unsuru olarak değerlendirilmesine yol açmıştır. ABD, Çin ve Avrupa Birliği gibi büyük güçler, kuantum teknolojilerine yönelik stratejik yatırımlarını artırırken, bu alandaki rekabet giderek yoğunlaşmaktadır. Güvenlik teorileri, kuantum teknolojilerinin stratejik istikrar, nükleer caydırıcılık ve kriz yönetimi üzerindeki potansiyel etkilerini analiz etmelidir. Kuantum bilgisayarların şifreleme sistemlerini kırma kapasitesi, özellikle nükleer komuta-kontrol sistem-

leri ve stratejik iletişim ağları için ciddi güvenlik riskleri oluşturmaktadır. Bu durum, nükleer strateji teorilerinin ve caydırıcılık modellerinin kuantum çağına adapte edilmesini gerektirmektedir. Ayrıca kuantum sensörler, kuantum radarlar ve kuantum iletişim ağları gibi yeni teknolojiler, askeri istihbarat ve gözetim kapasitelerini kökten değiştirerek stratejik denge ve güvenlik ikilemlerini yeniden şekillendirmektedir. Uluslararası güvenlik teorileri, kuantum teknolojilerinin oluşturduğu bu yeni dinamikleri açıklamak için mevcut kavramsal çerçeveleri genişletmelidir (Arquilla & Ronfeldt, 2020; Fukuyama, 2021).

Kuantum teknolojileri alanında uluslararası işbirliği ve rekabet dinamikleri, uluslararası ilişkiler teorilerinin önemli araştırma konuları arasında yer almaktadır. Kuantum üstünlüğü yarışı, büyük güçler arasında yeni bir soğuk savaş dinamiği oluşturma potansiyeline sahipken, aynı zamanda ortak güvenlik tehditlerine karşı işbirliği fırsatları da sunmaktadır. Kuantum-sonrası kriptografi standartlarının geliştirilmesi, kuantum teknolojilerinin silahlanma kontrolü ve kuantum internet altyapısının küresel yönetişimi gibi alanlarda uluslararası işbirliği mekanizmalarının oluşturulması, teorik ve pratik düzeyde önemli zorluklar oluşturmaktadır. Uluslararası rejim teorileri, kuantum teknolojileri alanındaki işbirliği ve düzenleme süreçlerini analiz etmek için yeni perspektifler geliştirmelidir. Özellikle kuantum teknolojilerinin çift kullanımlı doğası (hem sivil hem askeri uygulamalara sahip olması), bu alandaki uluslararası rejim oluşturma çabalarını daha da karmaşık hale getirmektedir. Kuantum teknolojilerinin yayılmasının kontrolü, kuantum silahsızlanma anlaşmalarının olasılığı ve kuantum destekli askeri sistemlerin uluslararası hukuk çerçevesinde nasıl düzenleneceği, uluslararası ilişkiler disiplininin güncel araştırma alanları arasında yer almaktadır. Bu bağlamda kuantum teknolojilerinin uluslararası sistem üzerindeki dönüştürücü etkisi, hem teorik hem de ampirik düzeyde daha fazla incelemeyi gerektirmektedir (Choucri, 2021; Morozov, 2021).

4. METODOLOJİ

4.1. Araştırma Tasarımı ve Yöntemi

Bu çalışma, dijital teknolojilerin uluslararası ilişkiler üzerindeki etkilerini analiz etmek amacıyla nitel bir araştırma yaklaşımı benimsemektedir. Dijitalleşmenin güvenlik, ekonomi, diplomasi ve küresel yönetişim üzerindeki geniş etkisi, disiplinler arası bir analiz gerektirmektedir. Çalışma, dijital dönüşüm süreçlerini uluslararası ilişkiler teorileri ile birleştiren bir model sunmaktadır. Araştırma tasarımı, dijital teknolojilerin çok boyutlu doğasını kapsayacak şekilde oluşturulmuş; yapay zekâ, blok zinciri, kuantum bilişim ve siber güvenlik gibi temel dijital teknolojilerin uluslararası sistem üzerindeki transformatif etkilerini sistematik bir çerçevede incelemeyi amaçlamaktadır. Bu nitel yaklaşım dijitalleşme sürecinin karmaşık ve çok

katmanlı yapısını anlamak için en uygun metodolojik çerçeveyi sunmaktadır. Çalışma; teknolojik determinizm, konstrüktivizm ve eleştirel teori perspektiflerini birleştirerek dijital teknolojilerin uluslararası ilişkilerdeki rolünü çok boyutlu bir şekilde analiz etmektedir.

Araştırmada literatür taraması, vaka analizi ve içerik analizi yöntemleri kullanılacaktır. Dijitalleşmenin uluslararası ilişkiler üzerindeki etkilerini inceleyen akademik çalışmalar analiz edilerek literatürdeki boşluklar ve güncel yaklaşımlar değerlendirilecektir. Siber savaşlar, yapay zekâ destekli dış politika stratejileri ve blok zinciri tabanlı finansal sistemlerin devletlerarası rekabette nasıl kullanıldığına dair somut örnekler incelenecektir. Vaka analizi yöntemi, özellikle büyük güçlerin dijital stratejilerini ve bunların uluslararası sistem üzerindeki etkilerini derinlemesine incelemek için kullanılacaktır. Rusya'nın seçimlere dijital müdahale operasyonları, Çin'in Dijital İpek Yolu girişimi ve ABD'nin yapay zekâ destekli güvenlik stratejileri gibi örnek vakalar, dijital teknolojilerin uluslararası ilişkilerdeki pratik uygulamalarını göstermek amacıyla analiz edilecektir. İçerik analizi ise devletlerin dijital stratejilerini ve politika belgelerini incelemek, dijital söylemlerdeki temaları ve öncelikleri belirlemek için kullanılacaktır. Bu çok yönlü metodolojik yaklaşım dijital teknolojilerin uluslararası ilişkiler üzerindeki etkilerini kapsamlı bir şekilde anlamamıza olanak tanıyacaktır.

Çalışmanın teorik çerçevesi; realizm, liberalizm ve inşacılık gibi klasik uluslararası ilişkiler teorilerini dijitalleşme bağlamında yeniden ele almaktadır. Ayrıca teknolojik determinizm gibi dijitalleşmeye özgü teorik yaklaşımlar da incelenerek yapay zekâ destekli dış politika karar alma süreçlerinin devletler arası ilişkileri nasıl etkilediği analiz edilecektir. *Realist perspektif*, dijital teknolojilerin devletlerin güç maksimizasyonu ve güvenlik stratejileri üzerindeki etkilerini incelerken; *liberal yaklaşım*, dijitalleşmenin uluslararası işbirliği, küresel yönetişim ve karşılıklı bağımlılık üzerindeki rolüne odaklanmaktadır. *İnşacı perspektif* ise dijital teknolojilerin normların, kimliklerin ve sosyal yapıların oluşumu ve dönüşümü üzerindeki etkilerini analiz etmektedir. Bu teorik çeşitlilik, dijitalleşmenin uluslararası ilişkiler üzerindeki çok boyutlu etkilerini anlamak için bütünsel bir çerçeve sunmaktadır. Araştırma metodolojisi, teorik perspektiflerin ampirik verilerle bütünleştirilmesini sağlayarak dijital teknolojilerin uluslararası sistem üzerindeki dönüştürücü etkilerine ilişkin kapsamlı bir anlayış geliştirmeyi amaçlamaktadır.

Ayrıca ABD, Çin ve Avrupa Birliği gibi büyük güçlerin dijitalleşme politikaları karşılaştırmalı olarak incelenerek bu aktörlerin siber güvenlik stratejileri, yapay zekâ politikaları ve dijital diplomasi uygulamaları değerlendirilecektir. *Karşılaştırmalı vaka analizi yöntemi*, farklı siyasi sistemlere, teknolojik kapasitelere ve stratejik kültürlere sahip devletlerin dijitalleşme süreçlerini nasıl yönettiklerini ve bu süreçlerin uluslararası politikalarını

nasıl şekillendirdiğini anlamak için kullanılacaktır. Bu bağlamda devletlerin dijital stratejilerini belirleyen iç faktörler (politik yapı, teknolojik altyapı, sosyo-ekonomik koşullar) ve dış faktörler (uluslararası rekabet, güvenlik tehditleri, küresel normlar) arasındaki etkileşim incelenecektir. Karşılaştırmalı analiz, aynı zamanda devletlerin dijital teknolojilere yönelik farklı düzenleyici yaklaşımlarını, veri yönetimi politikalarını ve teknolojik bağımsızlık stratejilerini de değerlendirerek küresel dijital yönetişimin geleceğine ilişkin çıkarımlar sunacaktır. Bu metodolojik yaklaşım dijital dönüşümün uluslararası politikalara etkisini bütüncül bir şekilde ele almayı amaçlamaktadır.

4.2. Veri Toplama Süreçleri ve Kaynak Seçimi

Bu araştırma, dijital teknolojilerin uluslararası ilişkiler üzerindeki etkilerini analiz etmek için çok yönlü bir veri toplama süreci benimsemekte ve geniş bir kaynak yelpazesine dayanmaktadır. Uluslararası sistemin dijitalleşme sürecini bütüncül bir şekilde incelemek amacıyla hem birincil hem de ikincil kaynaklar kullanılacaktır. Veri toplama süreci, dijital teknolojilerin uluslararası güvenlik, diplomasi, ekonomi ve yönetişim alanlarındaki çok boyutlu etkilerini kapsamlı bir şekilde incelemek için tasarlanmıştır. Çalışma; akademik literatür, resmi belge ve raporlar, düşünce kuruluşu analizleri, teknoloji şirketlerinin raporları ve uluslararası örgütlerin yayınlarından oluşan geniş bir kaynak havuzundan yararlanmaktadır. Bu çeşitlilik, dijital teknolojilerin uluslararası ilişkiler üzerindeki etkilerine ilişkin farklı perspektifleri ve yaklaşımları bir araya getirerek araştırmanın kapsamlılığını ve derinliğini artırmaktadır. Veri toplama sürecinde, kaynak güvenilirliği, güncellik ve kapsayıcılık kriterleri göz önünde bulundurulmuş; dijital dönüşümün hızlı doğası dikkate alınarak sürekli güncellenen bir kaynak havuzu oluşturulmuştur.

Birincil kaynaklar, devletlerin dijital stratejilerini ve politikalarını değerlendirmek açısından önem taşımaktadır. Bu kapsamda ulusal güvenlik belgeleri, dış politika strateji dokümanları ve siber güvenlik politikaları analiz edilerek dijitalleşmenin küresel sistem üzerindeki etkileri değerlendirilecektir. Özellikle ABD, Çin, Avrupa Birliği ve Rusya gibi büyük güçlerin dijital politika belgeleri, yapay zekâ stratejileri ve blok zinciri düzenlemeleri incelenecektir. ABD'nin Ulusal Yapay Zekâ Stratejisi, Çin'in Yeni Nesil Yapay Zekâ Geliştirme Planı, Avrupa Birliği'nin Dijital Tek Pazar Stratejisi ve Rusya'nın Dijital Ekonomi Programı gibi resmi belgeler, bu devletlerin dijital teknolojilere yaklaşımlarını ve stratejik önceliklerini anlamak için kritik öneme sahiptir. Ayrıca Birleşmiş Milletler, NATO, OECD ve Dünya Ticaret Örgütü gibi uluslararası kuruluşların dijital teknolojilere ilişkin politika belgeleri ve raporları da incelenecektir. Bu birincil kaynaklar, devletlerin ve uluslararası örgütlerin dijital dönüşüme nasıl yanıt verdiğini, bu teknolojileri nasıl düzenlediğini ve küresel dijital yönetişimin geleceğini nasıl şekillendirdiğini anlamak için değerli veriler sunmaktadır.

İkincil kaynaklar, akademik literatür, teknoloji raporları ve uluslararası örgütlerin yayınladığı belgelerden oluşmaktadır. Devletlerin yayımladığı strateji belgeleri ve güvenlik politikaları "*dijital güç stratejileri*" hakkında önemli bilgiler sunmaktadır. Buna ek olarak teknoloji şirketlerinin raporları ve özel sektör analizleri de veri kaynakları arasında yer almaktadır. Bu ikincil kaynaklar "*akademik, politika ve sektör*" perspektiflerini bir araya getirerek dijital teknolojilerin uluslararası ilişkiler üzerindeki çok boyutlu etkilerini kapsamlı bir şekilde anlamamıza olanak tanımaktadır.

Kaynak seçimi sürecinde "*güvenilirlik, geçerlilik ve güncellik*" kriterleri dikkate alınarak titiz bir değerlendirme yapılmıştır. Dijital teknolojilerin hızla gelişen doğası göz önüne alındığında, en güncel verilerin ve analizlerin kullanılması özellikle önemlidir. Çalışmada kullanılan kaynaklar, dijital teknolojilerin uluslararası ilişkiler üzerindeki etkilerini incelemede uzmanlaşmış akademisyenler, politika yapıcılar ve teknoloji uzmanları tarafından üretilen güvenilir ve saygın kaynaklardan seçilmiştir. Ayrıca kaynak çeşitliliği sağlanarak farklı perspektiflerin ve yaklaşımların araştırmaya dâhil edilmesi amaçlanmıştır. Batı, Çin ve Rusya kaynaklı literatürün dengeli bir şekilde incelenmesi, dijital teknolojilere ilişkin farklı jeopolitik ve kültürel perspektifleri anlamamıza olanak tanımaktadır. Veri toplama sürecinde, aynı zamanda disiplinler arası bir yaklaşım benimsenerek uluslararası ilişkiler literatürünün yanı sıra bilgisayar bilimleri, hukuk, ekonomi ve sosyoloji gibi alanlardan da kaynaklar dâhil edilmiştir. Bu disiplinler arası yaklaşım, dijital teknolojilerin uluslararası ilişkiler üzerindeki çok boyutlu etkilerini daha kapsamlı bir şekilde anlamamıza yardımcı olmaktadır.

4.3. Veri Analiz Yöntemleri

Bu araştırma, dijital teknolojilerin uluslararası güvenlik, diplomasi, ekonomi ve hukuk üzerindeki etkilerini analiz etmek için nitel veri analiz yöntemlerini kullanmaktadır. Karşılaştırmalı analiz, içerik analizi, söylem analizi ve ağ analizi gibi yöntemler bir arada uygulanarak dijitalleşmenin çok boyutlu etkileri incelenecektir. Bu metodolojik çoğulculuk, dijital teknolojilerin uluslararası ilişkilerdeki karmaşık ve çok katmanlı etkilerini derinlemesine anlamak için kapsamlı bir analitik çerçeve sunmaktadır. Veri analiz süreci, toplandıktan sonra sistematik bir kodlama ve kategorizasyon aşamasından geçirilerek temel temalar, örüntüler ve ilişkiler belirlenecektir. Bu analitik yaklaşım dijital teknolojilerin uluslararası ilişkilerdeki dönüştürücü etkilerini farklı boyutlarıyla kavramaya olanak tanımaktadır. *Nitel analiz yöntemleri*, hem teorik çerçevenin geliştirilmesine hem de ampirik bulguların değerlendirilmesine katkıda bulunarak dijitalleşme sürecinin uluslararası sistem üzerindeki etkilerine ilişkin kapsamlı bir anlayış sunmaktadır (Nye, 2021; Floridi, 2018).

Karşılaştırmalı analiz yöntemi, devletlerin dijitalleşme politikalarını kıyaslayarak farklı stratejilerin uluslararası sisteme etkilerini analiz etmeyi amaçlamaktadır. ABD, Çin, Avrupa Birliği ve Rusya gibi büyük güçlerin dijital stratejileri karşılaştırmalı bir perspektifle incelenerek bu aktörlerin teknolojik kapasiteleri, düzenleyici yaklaşımları ve stratejik öncelikleri arasındaki benzerlikler ve farklılıklar belirlenecektir. Bu karşılaştırmalı çerçeve, farklı politik sistemlerin ve stratejik kültürlerin dijital teknolojileri nasıl yorumladığını ve uyguladığını anlamak için değerli bir analitik araç sunmaktadır. Örneğin Çin'in dijital egemenlik odaklı yaklaşımı ile Avrupa Birliği'nin değer temelli düzenleyici modeli arasındaki farklar, dijital teknolojilerin yönetişimine ilişkin farklı normatif vizyonları ortaya koymaktadır. Karşılaştırmalı analiz, aynı zamanda devletlerin dijital teknolojilere adaptasyon hızını, teknolojik yenilik kapasitelerini ve küresel dijital standartları şekillendirme güçlerini de değerlendirerek uluslararası sistemdeki güç dinamiklerinin nasıl evrildiğine dair içgörüler sunmaktadır. Bu yöntem, devletlerin ve bölgelerin dijital stratejileri arasındaki farklılıkların altında yatan faktörleri anlamak ve dijital teknolojilerin küresel yayılımının jeopolitik ve jeoekonomik etkilerini değerlendirmek için kullanılacaktır.

İçerik analizi yöntemi, devletlerin dijital politikalarına yönelik strateji belgeleri, uluslararası örgüt raporları ve büyük teknoloji şirketlerinin yönetişim stratejilerini inceleyerek dijitalleşme yaklaşımlarını değerlendirmektedir. Bu yöntem, dokümanların sistematik ve objektif bir şekilde analiz edilmesini sağlayarak belirli temaların, kavramların ve önceliklerin tanımlanmasına olanak tanımaktadır. İçerik analizi, ulusal güvenlik stratejileri, yapay zekâ politika belgeleri, siber güvenlik doktrinleri ve dijital ekonomi planları gibi resmi belgelerdeki anahtar temaları ve söylemsel örüntüleri belirlemek için kullanılacaktır. Örneğin *dijital egemenlik*, *siber güvenlik*, *teknolojik bağımsızlık* ve *veri koruma* gibi kavramların farklı aktörler tarafından nasıl yorumlandığı ve politika belgelerinde ne sıklıkla vurgulandığı incelenecektir. Bu analiz, devletlerin ve uluslararası örgütlerin dijital teknolojilere yaklaşımlarındaki stratejik öncelikleri, değer yönelimlerini ve potansiyel çatışma alanlarını belirlemek için değerli veriler sunmaktadır. İçerik analizi aynı zamanda, dijital politikaların zaman içindeki evrimini ve belirli olaylara (örneğin büyük siber saldırılar veya teknolojik atılımlar) nasıl yanıt verdiğini anlamak için de kullanılacaktır. Bu analitik yaklaşım dijital teknolojilerin uluslararası ilişkilerdeki rolüne ilişkin resmi söylem ve politikaların sistematik bir şekilde incelenmesine olanak tanımaktadır.

Söylem analizi ve ağ analizi yöntemleri de çalışmada önemli bir rol oynamaktadır. *Söylem analizi*, dijitalleşmenin uluslararası politika söylemlerine etkisini incelemekte; devlet liderlerinin konuşmaları, diplomatik açıklamalar ve politik tartışmalardaki dijital teknolojilere ilişkin dil ve retorik yapıları analiz etmektedir. Bu yöntem, dijital teknolojilerin nasıl güvenlikleşti-

rildiğini, ekonomik fırsatlar veya tehditler olarak nasıl çerçevelendiğini ve jeopolitik rekabette nasıl konumlandırıldığını anlamak için kullanılacaktır. Örneğin Çin liderlerinin "siber egemenlik" söylemi ile ABD yetkililerinin "açık internet" vurgusu arasındaki ideolojik ve stratejik farklılıklar söylem analizi aracılığıyla incelenecektir. *Ağ analizi* ise dijitalleşmenin uluslararası ilişkilerde çok aktörlü yapısını anlamaya yönelik olarak kullanılmaktadır. Bu yöntem; devletler, uluslararası örgütler, teknoloji şirketleri ve sivil toplum kuruluşları arasındaki karmaşık ilişkileri ve etkileşimleri haritalandırarak dijital yönetişimin çok katmanlı yapısını görselleştirmeye olanak tanımaktadır. Dijital teknoloji alanındaki işbirliği ağları, stratejik ortaklıklar ve rekabet dinamikleri ağ analizi aracılığıyla incelenerek uluslararası sistemdeki yeni güç dağılımları ve etki mekanizmaları belirlenecektir. Bu analitik yaklaşımlar, dijital teknolojilerin uluslararası ilişkilerdeki rolünü ve etkilerini daha kapsamlı ve derinlemesine anlamak için tamamlayıcı perspektifler sunmaktadır.

4.4. Güvenilirlik, Geçerlilik ve Etik Hususlar

Bu araştırma, dijitalleşmenin uluslararası ilişkiler üzerindeki etkilerini analiz ederken güvenilirlik, geçerlilik ve etik hususlara büyük önem vermektedir. Verilerin güvenilirliği ve analiz yöntemlerinin geçerliliği, araştırmanın bilimsel tutarlılığını sağlamak açısından kritik bir unsurdur. Özellikle yapay zekâ, blok zinciri, kuantum bilişim ve siber güvenlik gibi hızla gelişen alanlarda kullanılan verilerin kaynağı ve analitik yöntemlerin doğruluğu dikkatle değerlendirilmelidir. Araştırmanın güvenilirliğini artırmak için veri toplama ve analiz süreçlerinde metodolojik üçgenleme uygulanmıştır. Farklı veri kaynakları (akademik literatür, resmi belgeler, teknoloji raporları), çeşitli analiz yöntemleri (karşılaştırmalı analiz, içerik analizi, söylem analizi) ve farklı teorik perspektifler (realizm, liberalizm, konstrüktivizm, eleştirel teori) bir arada kullanılarak araştırma bulgularının güvenilirliği güçlendirilmiştir. Bu metodolojik çeşitlilik, dijital teknolojilerin uluslararası ilişkiler üzerindeki etkilerini daha kapsamlı ve derinlemesine anlamamıza olanak tanırken, aynı zamanda tek bir metodolojik yaklaşıma veya teorik perspektife bağlı kalmanın potansiyel sınırlılıklarını aşmamıza yardımcı olmaktadır.

Veri toplama sürecinde, yanlı ve manipülatif bilgilerin elenmesi, güvenilir ve doğrulanabilir kaynaklardan elde edilen verilerin kullanılması esastır. Dijitalleşme süreçlerinin doğru analiz edilebilmesi için çalışmada büyük ölçüde uluslararası kuruluş raporları, hükümetlerin yayımladığı resmi dokümanlar ve akademik olarak denetlenmiş makaleler kullanılacaktır. Kaynakların güvenilirliğini değerlendirmek için sistematik bir inceleme süreci uygulanmış; verilerin doğruluğu ve güncelliği çapraz kontrollerle teyit edilmiştir. Özellikle dijital teknolojiler alanında dezenformasyon ve yanıltıcı bilgilerin yaygınlığı göz önüne alındığında, kaynak değerlendirme

sürecinin titizlikle yürütülmesi büyük önem taşımaktadır. Resmi belgeler ve akademik kaynaklar kullanılırken, bunların politik yönelimler, kurumsal çıkarlar veya metodolojik sınırlılıklar nedeniyle içerebileceği potansiyel önyargılar dikkate alınmış; kaynakların çeşitlendirilmesi ve dengelenmesi yoluyla bu sınırlılıklar aşılmaya çalışılmıştır. Ayrıca farklı ülkelerin ve kurumların kaynaklarından yararlanılarak araştırmanın kültürel ve jeopolitik çeşitliliği sağlanmış; tek bir perspektifin veya yaklaşımın hâkimiyeti önlenmiştir. Bu kapsamlı kaynak değerlendirme süreci, araştırma bulgularının güvenilirliğini ve geçerliliğini güçlendirmektedir.

Araştırmanın geçerliliğini sağlamak için iç geçerlilik ve dış geçerlilik unsurları dikkatle değerlendirilmiştir. *İç geçerlilik*, araştırma bulgularının tutarlılığını ve mantıksal bütünlüğünü ifade ederken; *dış geçerlilik*, bulguların genellenebilirliğine işaret etmektedir. İç geçerliliği güçlendirmek için teorik çerçeve ile ampirik bulgular arasında güçlü bir ilişki kurulmuş; kavramsal tanımlar netleştirilmiş ve metodolojik adımlar sistematik bir şekilde uygulanmıştır. Dış geçerliliği artırmak amacıyla farklı bölgelerden ve farklı teknolojik gelişmişlik düzeylerinden örnekler incelenmiş; araştırma bulguları karşılaştırmalı bir perspektifle değerlendirilmiştir. Araştırmanın geçerliliğini test etmek için uzman değerlendirmesi ve katılımcı doğrulaması gibi teknikler kullanılmıştır. Uzman değerlendirmesi kapsamında dijital teknolojiler ve uluslararası ilişkiler alanında uzmanlaşmış akademisyenler ve pratisyenlerden araştırma tasarımı, metodoloji ve bulgular hakkında geri bildirimler alınmıştır. Bu çok boyutlu değerlendirme süreci, araştırmanın geçerliliğini güçlendirerek dijital teknolojilerin uluslararası ilişkiler üzerindeki etkilerine ilişkin daha sağlam ve güvenilir sonuçlar elde etmemize olanak tanımaktadır.

Etik açıdan veri gizliliği ve kişisel verilerin korunması konularında uluslararası etik standartlar dikkate alınmaktadır. Özellikle yapay zekâ destekli karar alma mekanizmalarının diplomasi süreçlerine entegrasyonu ve blok zinciri tabanlı finansal sistemlerin küresel ekonomik dinamiklere etkileri gibi konular etik riskler barındırmaktadır. Bu nedenle, araştırmada etik standartlara tam uyum sağlanarak analizler yürütülmektedir. Özellikle dijital güvenlik konularında, kritik altyapılara yönelik potansiyel güvenlik açıklarına ilişkin detaylar gibi duyarlı bilgilerin ele alınmasında etik ilkeler gözetilmiştir. Araştırmada, dijital teknolojilerin potansiyel zararlı kullanımlarının tartışılması durumunda bile bu tür uygulamaların nasıl gerçekleştirileceğine dair teknik detaylar verilmemiş; bunun yerine bu tehditlere karşı koruyucu politikaların ve önlemlerin geliştirilmesine odaklanılmıştır. Ayrıca dijital teknolojilerin sosyal, ekonomik ve politik etkilerinin değerlendirilmesinde normatif tarafsızlık sağlanmaya çalışılmış; farklı değer sistemlerinin ve yaklaşımların adil bir şekilde temsil edilmesine dikkat edilmiştir. Bu etik duyarlılık, araştırmanın bilimsel bütünlüğünü ve toplumsal sorum-

luluğunu güçlendirerek dijital teknolojilerin uluslararası ilişkiler üzerindeki etkilerinin dengeli ve kapsamlı bir şekilde anlaşılmasına katkıda bulunmaktadır.

5. BULGULAR

5.1. Dijital Teknolojilerin Uluslararası Güvenlik ve Siber Savaş Üzerindeki Etkisi

Dijital teknolojilerin gelişimi, uluslararası güvenlik paradigmalarını köklü bir biçimde değiştirmiş ve savaşın doğasını geleneksel askeri yöntemlerden siber savaş alanına taşımıştır. Devletlerin ulusal güvenlik politikaları, siber tehditleri öncelikli bir tehdit unsuru olarak ele almaya başlamış, siber saldırılara karşı caydırıcılık politikaları geliştirilmiş ve dijital altyapıların korunmasına yönelik büyük yatırımlar yapılmıştır. Özellikle ulusal güvenlik stratejilerinde yapay zekâ destekli siber savunma sistemleri, otonom tehdit tespit algoritmaları ve büyük veri analitiği gibi teknolojiler giderek daha fazla kullanılmaktadır. Devletlerin siber güvenlik politikaları ve stratejileri, ulusal savunma doktrinlerinin ayrılmaz bir parçası haline gelmiş, siber komutanlıklar ve savunma birimleri kurularak kurumsal yapılanmalar güçlendirilmiştir. ABD'nin Siber Komutanlığı, Çin'in Stratejik Destek Kuvvetleri ve Rusya'nın siber savaş birimleri, dijital tehditlere karşı geliştirilen kurumsal yanıtların en belirgin örnekleri arasında yer almaktadır. Bu kurumsal dönüşüm, devletlerin dijital tehditleri ne kadar ciddi ele aldığını ve siber alanı yeni bir savaş domeni olarak nasıl benimsediğini göstermektedir (Nye, 2021; Floridi, 2018).

Siber savaş, artık devletlerarası rekabetin en önemli bileşenlerinden biri haline gelmiştir. Geleneksel savaş anlayışından farklı olarak siber savaş fiziksel sınırları aşarak devletlerin kritik altyapılarını hedef almakta, ekonomik sistemleri çökertmekte ve dezenformasyon stratejileri ile kamuoylarını manipüle etmektedir. Bu bağlamda devlet destekli hacker grupları, düşman devletlerin iletişim ağlarını, elektrik altyapısını, bankacılık sistemlerini ve savunma sanayi veritabanlarını hedef alarak düşman ülkelerin ulusal güvenliğini tehdit etmektedir. Bu durum, devletlerin yalnızca askeri caydırıcılığa değil, aynı zamanda siber savunma yeteneklerine de yatırım yapmasını gerektirmektedir. Siber savaşın en belirgin özelliklerinden biri, saldırganın kimliğinin belirlenmesindeki zorluktur. "Atfetme problemi" olarak bilinen bu durum, siber saldırıların kaynağının kesin olarak tespit edilmesindeki teknik zorlukları ifade etmekte ve geleneksel caydırıcılık stratejilerinin uygulanmasını zorlaştırmaktadır. Rusya'nın 2007 yılında Estonya'ya, 2008'de Gürcistan'a ve 2014'te Ukrayna'ya yönelik siber saldırıları, devlet destekli siber operasyonların uluslararası krizlerdeki stratejik rolünü gösteren önemli örneklerdir. Bu saldırılar, kritik altyapıları hedef alarak modern toplumla-

rın dijital sistemlere bağımlılığını stratejik bir zayıflık olarak kullanmışlardır (Arquilla & Ronfeldt, 2020; Singer & Brooking, 2019).

Siber güvenlik politikaları, yalnızca devletlerarası rekabeti değil, aynı zamanda uluslararası hukukun nasıl şekilleneceğini de belirlemektedir. Siber saldırıların uluslararası hukuk çerçevesinde savaş ilanı olarak değerlendirilip değerlendirilmeyeceği, devletlerin siber saldırılara karşı nasıl yanıt vermesi gerektiği gibi konular halen netlik kazanmamıştır. NATO, büyük çaplı bir siber saldırının 5. madde kapsamında kolektif savunma mekanizmasını harekete geçirebileceğini açıklamış olsa da, siber savaşın hukuki boyutları hâlâ devletlerarasında ciddi görüş ayrılıklarına neden olmaktadır. Tallinn Kılavuzu, siber operasyonların uluslararası hukuktaki yerini netleştirmeye yönelik önemli bir girişim olsa da, bu belgenin bağlayıcılığı sınırlıdır ve tüm devletler tarafından kabul edilmemektedir. Siber saldırıların ne zaman "silahlı saldırı" kategorisine gireceği, hangi koşullarda meşru müdafaa hakkı doğuracağı ve orantılı karşılık ilkesinin siber alanda nasıl uygulanacağı gibi kritik hukuki sorular halen tartışılmaktadır. Bu hukuki belirsizlik, siber alanda devletlerin davranışlarını düzenleyen normların ve kuralların geliştirilmesini zorlaştırmakta, potansiyel çatışmaların önlenmesi için gerekli uluslararası işbirliğinin kurulmasını engellemektedir (West, 2021; OECD, 2021).

Yapay zekâ teknolojilerinin siber güvenlik alanına entegrasyonu, hem savunma hem de saldırı kapasitelerini önemli ölçüde artırmaktadır. Yapay zekâ destekli siber savunma sistemleri, anomali tespiti, tehdit istihbaratı ve otomatik müdahale alanlarında devletlere benzeri görülmemiş kapasiteler sunmaktadır. Makine öğrenmesi algoritmaları, normal ağ trafiği örüntülerini analiz ederek potansiyel tehditleri gerçek zamanlı olarak tespit edebilmekte ve otomatik savunma mekanizmalarını harekete geçirebilmektedir. Aynı zamanda, yapay zekâ teknolojileri, siber saldırıları daha sofistike ve etkili hale getirmektedir. Otonom kötü amaçlı yazılımlar, hedef sistemlerin zayıflıklarını kendi kendine keşfedebilmekte ve adaptif saldırı stratejileri geliştirebilmektedir. Deepfake teknolojisi gibi yapay zekâ uygulamaları, sosyal mühendislik saldırılarını ve dezenformasyon kampanyalarını daha inandırıcı ve etkili hale getirmektedir. Bu teknolojik gelişmeler, siber güvenlik alanında yeni bir yarışı başlatmış, büyük güçler yapay zekâ destekli siber savunma ve saldırı kapasitelerini geliştirmek için büyük yatırımlar yapmaya başlamıştır. DARPA'nın Siber Grand Challenge programı ve Çin'in Stratejik Destek Kuvvetleri'nin yapay zekâ destekli siber savunma araştırmaları, bu alandaki rekabeti gösteren önemli örneklerdir (Singer & Brooking, 2019; Arquilla & Ronfeldt, 2020).

Siber caydırıcılık stratejileri, geleneksel nükleer caydırıcılıktan önemli ölçüde farklılık göstermektedir. Nükleer caydırıcılık, "garanti edilmiş karşılıklı yıkım" ilkesine dayanırken, siber caydırıcılık çok daha karmaşık ve belirsiz bir yapıya sahiptir. Siber saldırıların atfedilmesindeki zorluklar, et-

kilerinin değişkenliği ve devlet dışı aktörlerin artan kapasiteleri, geleneksel caydırıcılık teorilerinin siber alana doğrudan uygulanmasını zorlaştırmaktadır. Devletler, bu zorlukları aşmak için çeşitli stratejiler geliştirmektedir. İlk olarak, "cezalandırma yoluyla caydırıcılık" stratejisi, siber saldırılara karşı güçlü ve orantılı karşılık verme taahhüdüne dayanmaktadır. Bu yaklaşım ABD'nin "Calculated Response" doktrini ve İsrail'in "aktif savunma" stratejisinde görülmektedir. İkinci olarak, "inkâr yoluyla caydırıcılık" stratejisi, siber savunma kapasitelerini güçlendirerek potansiyel saldırıların başarı şansını azaltmayı amaçlamaktadır. Üçüncü olarak, "normatif caydırıcılık" yaklaşımı, uluslararası normlar ve kurallar geliştirerek siber alanda kabul edilemez davranışları tanımlamaya ve bunlara yönelik kolektif tepkiler oluşturmaya çalışmaktadır. Birleşmiş Milletler Hükümet Uzmanları Grubu (UN GGE) ve Açık Uçlu Çalışma Grubu (OEWG) gibi girişimler, bu normatif çerçevenin geliştirilmesine katkıda bulunmaktadır. Ancak siber caydırıcılık stratejilerinin etkinliği halen sınırlıdır ve devletlerarasında siber saldırılar devam etmektedir (Nye, 2021; West, 2021).

Kritik altyapı sistemlerinin dijitalleşmesi, yeni güvenlik kırılganlıkları oluşturmakta ve devletlerin ulusal güvenlik politikalarını derinden etkilemektedir. Enerji şebekeleri, su arıtma tesisleri, ulaşım sistemleri, sağlık hizmetleri ve finansal ağlar gibi kritik altyapılar, giderek daha fazla dijital sistemlere ve internete bağımlı hale gelmektedir. Bu dijitalleşme, operasyonel verimlilik ve yönetim kolaylığı sağlarken, aynı zamanda bu sistemleri siber saldırılara karşı daha savunmasız hale getirmektedir. 2015 yılında Ukrayna'nın elektrik şebekesine yönelik gerçekleştirilen ve 230.000'den fazla insanı elektriksiz bırakan siber saldırı, 2017 yılında İsveç'in ulaşım sistemlerine yönelik saldırı ve 2021 yılında ABD'nin Colonial Pipeline'ına yönelik fidye yazılımı saldırısı, kritik altyapıların siber saldırılara karşı ne kadar savunmasız olabileceğini gösteren çarpıcı örneklerdir. Bu tehditlere yanıt olarak devletler kritik altyapıların siber güvenliğini artırmak için yasal ve düzenleyici çerçeveler geliştirmektedir. ABD'nin Kritik Altyapı Güvenliği ve Dayanıklılık Ajansı (CISA), Avrupa Birliği'nin NIS Direktifi ve Japonya'nın Kritik Altyapı Koruma programı, bu alandaki önemli girişimlerdir. Ayrıca kamu-özel sektör işbirliği modelleri, kritik altyapı koruması için giderek daha fazla benimsenmekte, devletler ve özel sektör arasında tehdit istihbaratı paylaşımı ve ortak savunma stratejileri geliştirilmektedir. Bu işbirliği modelleri, kritik altyapıların büyük ölçüde özel sektör tarafından işletildiği günümüz dünyasında, siber güvenliğin sağlanması için vazgeçilmez bir unsur haline gelmiştir (Floridi, 2018; Fukuyama, 2021).

Nesnelerin İnterneti (IoT), 5G teknolojileri ve akıllı şehir uygulamaları gibi yeni dijital teknolojiler, siber güvenlik tehditlerinin kapsamını ve karmaşıklığını artırmaktadır. IoT cihazlarının yaygınlaşması, saldırı yüzeyini önemli ölçüde genişleterek daha önce izole olan fiziksel sistemlerin dijital

saldırılara açık hale gelmesine neden olmaktadır. Zayıf güvenlik standartlarıyla üretilen milyarlarca IoT cihazı, botnet saldırıları ve dağıtık hizmet engelleme (DDoS) saldırıları için potansiyel araçlar haline gelmektedir. 2016 yılında Mirai botnet saldırısı, binlerce IoT cihazını kullanarak Dyn DNS sağlayıcısını hedef almış ve Twitter, Netflix ve CNN gibi popüler web sitelerinin erişimini engellemişti. 5G teknolojilerinin yaygınlaşması, veri aktarım hızlarını ve bağlantı kapasitesini artırırken, aynı zamanda yeni güvenlik zorlukları da oluşturmaktadır. Özellikle Huawei gibi Çinli telekomünikasyon şirketlerinin 5G altyapılarındaki rolü, ABD ve müttefikleri tarafından ulusal güvenlik tehdidi olarak görülmekte, bu durum teknolojik rekabet ile jeopolitik gerilimlerin nasıl iç içe geçtiğini göstermektedir. Akıllı şehir uygulamaları, kentsel yaşamı iyileştirmek için büyük miktarda veri toplarken, bu verilerin korunması ve güvenliği giderek daha önemli bir endişe kaynağı haline gelmektedir. Bu teknolojik gelişmeler, sadece teknik güvenlik önlemleriyle değil, aynı zamanda uluslararası standartlar, düzenleyici çerçeveler ve diplomatik girişimlerle ele alınması gereken karmaşık güvenlik sorunları oluşturmaktadır. Devletler ve uluslararası örgütler, bu yeni teknolojilerin güvenli bir şekilde geliştirilmesi ve kullanılması için işbirliği yapmalı, ortak standartlar ve normlar geliştirmelidir (Zuboff, 2019; OECD, 2021).

5.2. Yapay Zekâ Destekli Askerî Stratejiler ve Otonom Sistemler

Dijitalleşmenin uluslararası güvenlik üzerindeki en önemli etkilerinden biri, yapay zekâ destekli askerî stratejilerin ve otonom sistemlerin savaş doktrinlerinde ve operasyonel kapasitede köklü değişiklikler oluşturmasıdır. Geleneksel savaş yöntemlerinin yerini, daha düşük maliyetli, hızlı, esnek ve insan hatasını minimize eden yapay zekâ tabanlı silah sistemleri almaktadır. Yapay zekâ destekli askeri stratejiler, düşman unsurların hareketlerini tahmin edebilme, gerçek zamanlı veri analizi yapma ve operasyonları otomatikleştirme kapasitesiyle, devletlerin savaş gücünü artırmaktadır. Bu teknolojiler, savaş alanlarında karar alma süreçlerini optimize ederek insan faktörünü minimize etmekte ve askeri etkinliği artırmaktadır. ABD'nin "Üçüncü Offset Stratejisi", Çin'in "Akıllı Savaş" doktrini ve Rusya'nın "Yeni Nesil Savaş" konsepti, yapay zekâ teknolojilerinin askeri stratejilere entegrasyonunu öngören önemli örneklerdir. Bu stratejik yaklaşımlar, dijital teknolojilerin savaşın doğasını köklü biçimde değiştireceğini ve gelecekteki askeri üstünlüğün yapay zekâ kapasitesiyle doğrudan ilişkili olacağını öngörmektedir. Askeri alandaki yapay zekâ uygulamaları, sensör verilerinin işlenmesi, hedef tespiti, lojistik planlaması, istihbarat analizi ve karar destek sistemleri gibi çeşitli alanlarda hızla gelişmektedir (Nye, 2021; Floridi, 2018).

Otonom savaş sistemleri, yapay zekâ tabanlı algoritmalar sayesinde insansız hava araçları (İHA), kara araçları, denizaltılar ve robotik askerî birimlerle savaş operasyonlarını insan müdahalesine gerek kalmadan yürütme kapasitesine sahiptir. Özellikle ABD, Çin ve Rusya gibi büyük askeri

güçler, yapay zekâ destekli otonom sistemleri savaş doktrinlerine entegre ederek askeri operasyonlarını daha verimli ve hızlı hale getirmektedir. Bu sistemler, hedef tespitinde, tehdit analizi yapmada ve otomatik saldırı stratejileri geliştirmede gelişmiş algoritmalara sahiptir. İnsansız hava araçları, özellikle MQ-9 Reaper ve İsrail'in Harop kamikaze droneları gibi sistemler, savaş alanlarında giderek daha fazla otonom özellikler kazanmaktadır. Deniz kuvvetlerinde, ABD'nin Sea Hunter otonom savaş gemisi ve Çin'nin insansız denizaltı programları, otonom deniz sistemlerinin gelişimini göstermektedir. Kara kuvvetlerinde ise, Rusya'nın Uran-9 robotik tankı ve Güney Kore'nin DMZ sınırında kullandığı otonom gözetim sistemleri dikkat çekmektedir. Bu sistemler, insan askerlerinin hayatını riske atmadan, tehlikeli ve zorlu görevlerin yürütülmesine olanak tanımaktadır. Ayrıca sürekli operasyonel kalabilme, yorulma faktörünün olmaması ve insan duygularından etkilenmeme gibi avantajlar sunmaktadır. Ancak bu sistemlerin güvenilirliği, dayanıklılığı ve karmaşık senaryolarda karar alma kapasiteleri hala önemli sınırlamalara tabidir (Arquilla & Ronfeldt, 2020; Singer & Brooking, 2019).

Ancak bu tür sistemlerin karar alma süreçlerinde insan faktörünün devre dışı kalması, savaşlarda etik sorumluluğun nasıl belirleneceği konusunda uluslararası hukukta ciddi tartışmalara yol açmaktadır. "İnsan-in-the-loop" (insanın karar döngüsünde olduğu), "insan-on-the-loop" (insanın karar döngüsünü denetlediği) ve "insan-out-of-the-loop" (insanın karar döngüsünün dışında kaldığı) sistemler arasındaki ayrım, otonom silah sistemlerinin düzenlenmesi konusundaki tartışmaların merkezinde yer almaktadır. Tam otonom silah sistemlerinin (killer robots olarak da adlandırılır) kullanımı, etik, hukuki ve stratejik açıdan önemli sorunlar oluşturmaktadır. Birincisi, bu sistemlerin hedef seçimi ve saldırı kararlarında insan muhakemesinin yerini alması, orantılılık ve ayrım ilkelerinin uygulanmasını zorlaştırmaktadır. İkincisi, komuta zincirindeki sorumluluğun belirlenmesi ve potansiyel savaş suçlarının hesap verebilirliği konularında belirsizlikler oluşturmaktadır. Üçüncüsü, otonom silah sistemlerinin proliferasyonu, terörist gruplar ve devlet dışı aktörler tarafından kötüye kullanım riskini artırmaktadır. Bu endişeler, BM Belli Konvansiyonel Silahlar Sözleşmesi (CCW) çerçevesinde otonom silah sistemlerinin düzenlenmesine yönelik uluslararası müzakereleri tetiklemiştir. "Campaign to Stop Killer Robots" gibi sivil toplum girişimleri, tam otonom silah sistemlerinin yasaklanması için kampanyalar yürütmektedir. Ancak büyük askeri güçler arasında bu konuda henüz bir uzlaşı sağlanamamıştır (West, 2021; OECD, 2021).

Yapay zekâ destekli komuta-kontrol sistemleri, askeri karar alma süreçlerini kökten değiştirmektedir. Geleneksel komuta-kontrol yapıları, hiyerarşik ve merkezi bir yapıya sahipken, yapay zekâ destekli sistemler daha dağıtık, esnek ve adaptif bir yapı sunmaktadır. Bu sistemler, büyük miktarda

veriyi gerçek zamanlı olarak işleyebilmekte, muhtemel tehditleri öngörebilmekte ve optimal müdahale stratejileri geliştirebilmektedir. ABD Savunma Bakanlığı'nın "Proje Maven" girişimi, görüntü tanıma ve hedef belirleme için makine öğrenmesi algoritmaları geliştirerek istihbarat analizini önemli ölçüde hızlandırmayı amaçlamaktadır. Çin'in "Akıllı Komuta Platformu" ve İsrail'in "Yönetilen Olay Analiz Sistemi", benzer şekilde yapay zekâ destekli karar destek sistemlerine örnektir. Bu sistemler, savaş alanındaki sensörlerden, istihbarat kaynaklarından ve açık kaynaklardan toplanan verileri entegre ederek komutanlara kapsamlı bir durum farkındalığı ve karar destek mekanizması sunmaktadır. Yapay zekâ destekli komuta-kontrol sistemleri, özellikle hızlı değişen ve karmaşık savaş ortamlarında, insan komutanların bilişsel sınırlamalarını aşarak daha hızlı ve daha etkili kararlar alınmasına olanak tanımaktadır. Ayrıca bu sistemler, siber savaş ve elektronik harp gibi geleneksel insan algı kapasitesinin ötesindeki alanlarda özellikle değerli olabilmektedir. Ancak yapay zekâ sistemlerinin önyargıları, teknik sınırlamaları ve güvenilirlik sorunları, tamamen otomatikleştirilmiş komuta-kontrol sistemlerine geçişin önündeki önemli engellerdir (Singer & Brooking, 2019; Fukuyama, 2021).

Yapay zekâ teknolojilerinin askeri alandaki bir diğer önemli uygulaması, istihbarat, gözetleme ve keşif (ISR) sistemleridir. Geleneksel ISR sistemleri, büyük miktarda veri toplarken, bu verilerin analizi ve anlamlı istihbarata dönüştürülmesi zaman alıcı ve insan gücüne dayalı bir süreçti. Yapay zekâ destekli ISR sistemleri, veri toplama, analiz ve yorumlama süreçlerini önemli ölçüde hızlandırmakta ve otomatikleştirmektedir. Görüntü tanıma algoritmaları, uydu görüntülerinden ve İHA kameralarından toplanan verileri anında analiz ederek hedefleri, tehditleri ve ilgi alanlarını tespit edebilmektedir. Doğal dil işleme teknolojileri, iletişim istihbaratını (COMINT) ve açık kaynak istihbaratını (OSINT) otomatik olarak analiz edebilmekte, anahtar bilgileri çıkarabilmekte ve tehdit göstergelerini belirleyebilmektedir. Örüntü tanıma algoritmaları, elektronik istihbarat (ELINT) verilerinden anormallikler ve potansiyel tehditler tespit edebilmektedir. ABD'nin "Algoritmik Savaş Merkezi", Çin'in "Akıllı Gözetim Sistemi" ve İsrail'in "Derinleştirilmiş İstihbarat Programı", yapay zekâ destekli ISR sistemlerine yönelik önemli yatırımları temsil etmektedir. Bu sistemler, özellikle büyük coğrafi alanların gözetlenmesi, sürekli izleme gerektiren hedeflerin takibi ve karmaşık tehdit ortamlarının analizi için kritik öneme sahiptir. Ayrıca daha az insan gücüyle daha geniş alanlara yönelik istihbarat toplamayı mümkün kılarak askeri operasyonlarda önemli bir maliyet avantajı sağlamaktadır. Ancak yapay zekâ destekli ISR sistemleri aynı zamanda gözetim kapasitelerinin dramatik bir şekilde artmasına ve potansiyel olarak sivil gizliliğin ihlal edilmesine yol açabilecek endişeler de oluşturmaktadır (Arquilla & Ronfeldt, 2020; Choucri, 2021).

Askeri simülasyon ve eğitim alanında yapay zekâ uygulamaları, askeri personelin daha etkili ve gerçekçi bir şekilde eğitilmesine olanak tanımaktadır. Yapay zekâ destekli sanal ve artırılmış gerçeklik sistemleri, gerçek savaş koşullarını simüle ederek askerlerin risk almadan taktiklerini geliştirmelerine ve senaryoları test etmelerine imkân vermektedir. ABD Ordusu'nun "Synthetic Training Environment" programı, geniş ölçekli, çok alanlı ve gerçekçi sanal eğitim ortamları oluşturmak için yapay zekâ teknolojilerini kullanmaktadır. Benzer şekilde Çin Halk Kurtuluş Ordusu'nun "Dijital Savaş Simülasyonu" ve Rusya'nın "Sanal Muharebe Eğitim Sistemi", yapay zekâ destekli askeri eğitim programlarına örnektir. Bu sistemler, düşman kuvvetlerini ve davranışlarını gerçekçi bir şekilde modelleyebilmekte, çeşitli savaş senaryolarını simüle edebilmekte ve askeri personelin performansını değerlendirerek geri bildirim sağlayabilmektedir. Yapay zekâ destekli simülasyon sistemleri, aynı zamanda yeni silah sistemlerinin ve taktiklerin test edilmesi, savaş planlarının değerlendirilmesi ve potansiyel çatışma senaryolarının analiz edilmesi için de kullanılmaktadır. Bu sistemler, gerçek dünya testlerinin maliyetli ve riskli olduğu durumlarda, silah sistemlerinin etkinliğini ve güvenilirliğini değerlendirmek için değerli araçlar sunmaktadır. Ayrıca yapay zekâ destekli simülasyonlar, savaş oyunları (wargaming) ve stratejik planlama süreçlerini de geliştirmekte, karar alıcılara farklı stratejik seçeneklerin potansiyel sonuçlarını analiz etme imkânı vermektedir (Zuboff, 2019; West, 2021).

Yapay zekâ destekli askerî sistemlerin gelecekte daha da yaygınlaşması beklenmektedir. Bu süreç, geleneksel askeri doktrinlerin yeniden tanımlanmasını ve uluslararası güvenlik politikalarının yapay zekâ teknolojilerine uyum sağlamasını gerektirecektir. Devletlerin otonom silah sistemlerini nasıl regüle edeceği ve bu sistemlerin uluslararası çatışmalarda nasıl kullanılacağı konusunda hukuki düzenlemelere duyulan ihtiyaç giderek artmaktadır. Aynı zamanda, yapay zekâ destekli askeri sistemlerin etik kullanımı ve insan kontrolü altında tutulması konusunda uluslararası standartların geliştirilmesi de önem kazanmaktadır. Yapay zekâ teknolojilerinin askeri alandaki artan rolü, aynı zamanda stratejik istikrar ve silahlanma kontrolü açısından yeni zorluklar oluşturmaktadır. Yapay zekâ destekli saldırı sistemleri, savunma sistemlerinden daha etkili olduğunda, bu durum "ilk vuruş" avantajını artırabilir ve kriz anlarında istikrarsızlığa yol açabilir. Nükleer komuta-kontrol sistemlerine yapay zekânın entegrasyonu, karar süreçlerini hızlandırabilir ve potansiyel olarak yanlış alarm riskini artırabilir. Bu endişeler, yapay zekâ silahlanma yarışının kontrolü ve otonom silah sistemlerinin düzenlenmesi için uluslararası işbirliğinin önemini vurgulamaktadır. Birleşmiş Milletler, NATO ve diğer uluslararası örgütler, yapay zekâ destekli askeri sistemlerin sorumlu kullanımı için ilkeler ve normlar geliştirmeye başlamıştır. Ancak bu alandaki uluslararası düzenlemeler hala başlangıç

aşamasındadır ve hızla gelişen teknolojileri takip etmekte zorlanmaktadır (OECD, 2021; Floridi, 2018).

5.3. Blok Zinciri Teknolojisi ve Küresel Veri Güvenliği

Blok zinciri teknolojisi, güvenli, şeffaf ve merkeziyetsiz veri yönetimi mekanizmaları sunarak küresel ölçekte bilgi güvenliğini sağlamada yeni bir paradigma oluşturmuştur. Verilerin şifrelenmiş ve değiştirilemez bir şekilde saklanmasını sağlayan blok zinciri, uluslararası güvenlik ve dijital egemenlik açısından büyük önem taşımaktadır. Özellikle finans, tedarik zinciri yönetimi, diplomasi ve siber güvenlik alanlarında devletlerin blok zinciri tabanlı çözümler geliştirmesi, veri güvenliği politikalarını ve uluslararası ilişkilerdeki rekabeti derinden etkilemektedir. Bu teknoloji, yalnızca ekonomik sistemleri değil, aynı zamanda devletlerin ulusal güvenlik mekanizmalarını ve uluslararası istihbarat stratejilerini de yeniden şekillendirmektedir. Blok zincirinin en temel özelliklerinden olan dağıtık defter teknolojisi (distributed ledger technology - DLT), merkezi bir otoriteye ihtiyaç duymadan verilerin bir ağdaki tüm katılımcılar tarafından doğrulanmasını ve saklanmasını sağlamaktadır. Bu yapı, tek bir merkezi veri tabanına dayalı geleneksel sistemlere kıyasla çok daha güvenli ve dayanıklıdır, çünkü sistemin tek bir noktadan siber saldırıya uğraması veya manipüle edilmesi neredeyse imkânsız hale gelmektedir. Ayrıca blok zinciri teknolojisinin sağladığı kriptografik güvenlik, verilerin bütünlüğünü ve gizliliğini koruyarak hassas bilgilerin güvenli bir şekilde saklanmasını ve paylaşılmasını mümkün kılmaktadır (Brynjolfsson & McAfee, 2019; Floridi, 2018).

Blok zinciri tabanlı sistemler, verilerin değiştirilmesini veya manipüle edilmesini önleyen merkeziyetsiz bir yapı sunduğundan, özellikle devletlerin dijital güvenlik politikalarında güçlü bir unsur haline gelmiştir. Siber saldırıların artmasıyla birlikte, devletler ve uluslararası kuruluşlar, hassas verilerin korunması ve güvenli bilgi paylaşımı için blok zinciri çözümlerine yönelmektedir. Örneğin NATO ve Avrupa Birliği, askeri ve diplomatik iletişimde blok zinciri tabanlı sistemleri kullanarak bilgi güvenliğini artırmayı ve kritik verilerin siber saldırılara karşı korunmasını sağlamayı amaçlamaktadır. NATO'nun Siber Savunma Mükemmeliyet Merkezi (CCDCOE), blok zinciri teknolojisinin askeri ağlarda ve komuta-kontrol sistemlerinde kullanımını araştırmaktadır. Benzer şekilde ABD Savunma Bakanlığı'nın Savunma İleri Araştırma Projeleri Ajansı (DARPA), blok zinciri tabanlı güvenli mesajlaşma ve veri paylaşım platformları geliştirmektedir. Çin'in Blok Zinciri-temelli Hizmet Ağı (BSN) projesi ise, ulusal güvenlik ve dijital egemenlik açısından stratejik bir girişim olarak görülmektedir. Bu projeler, blok zinciri teknolojisinin ulusal güvenlik stratejilerinin ayrılmaz bir parçası haline geldiğini göstermektedir. Blok zinciri tabanlı sistemlerin sağladığı değiştirilemezlik (immutability) ve merkezi olmayan doğrulama mekanizmaları, özellikle kritik altyapıların korunması ve siber saldırılara karşı da-

yanıklılığın artırılması açısından devletlere önemli avantajlar sunmaktadır (West, 2021; Singer & Brooking, 2019).

Blok zinciri teknolojisinin uluslararası diplomasi üzerindeki etkisi de giderek artmaktadır. Diplomatik belgelerin güvenli bir şekilde saklanması ve uluslararası anlaşmaların şeffaf ve doğrulanabilir bir şekilde yönetilmesi için blok zinciri tabanlı sistemler önerilmektedir. Özellikle uluslararası örgütler, dijitalleşen diplomasi süreçlerinde blok zinciri teknolojisini kullanarak sahte belgeler ve manipülatif bilgilerin diplomatik ilişkiler üzerindeki etkisini azaltmayı hedeflemektedir. Birleşmiş Milletler'in Blok Zinciri İçin Çok Taraflı Araştırma Merkezi ve Dünya Ekonomik Forumu'nun Blok Zinciri ve Dağıtık Defter Teknolojileri Küresel Konseyi gibi girişimler, diplomatik süreçlerde blok zinciri kullanımını teşvik etmektedir. Blok zinciri tabanlı dijital kimlik sistemleri, diplomatik pasaportların doğrulanması, vize işlemlerinin güvenli bir şekilde yürütülmesi ve diplomatik personelin güvenli erişiminin sağlanması için potansiyel uygulamalar sunmaktadır. Ayrıca blok zinciri tabanlı oylama sistemleri, uluslararası örgütlerdeki karar alma süreçlerini daha şeffaf ve güvenilir hale getirebilir. Örneğin G20 zirvelerinde veya BM Genel Kurulu'nda blok zinciri tabanlı güvenli oylama mekanizmaları, kararların meşruiyetini artırabilir ve manipülasyon iddialarını azaltabilir. Bununla birlikte, bu teknolojinin diplomatik süreçlere entegrasyonu konusunda henüz uluslararası düzeyde kabul edilen bir model geliştirilmemiştir. Diplomatik verilerin gizliliği, ulusal egemenlik endişeleri ve teknolojik altyapı farklılıkları, blok zinciri tabanlı diplomatik sistemlerin yaygınlaşmasının önündeki önemli engellerdir (Arquilla & Ronfeldt, 2020; OECD, 2021).

Blok zinciri teknolojisinin tedarik zinciri güvenliği üzerindeki etkisi, uluslararası ticaretin güvenliğini ve şeffaflığını artırmaktadır. Küreselleşen tedarik zincirleri, artan karmaşıklık ve siber tehditler nedeniyle giderek daha savunmasız hale gelmektedir. Blok zinciri tabanlı tedarik zinciri yönetim sistemleri, ürünlerin kaynağından son kullanıcıya kadar izlenmesini sağlayarak sahtecilik, kaçakçılık ve tedarik zinciri manipülasyonu risklerini azaltmaktadır. Bu özellikle askeri teçhizat, kritik altyapı bileşenleri ve stratejik hammaddeler gibi ulusal güvenlik açısından kritik ürünlerin tedarikinde büyük önem taşımaktadır. ABD Savunma Bakanlığı'nın "Blok Zinciri Tabanlı Tedarik Zinciri Güvenliği" programı, askeri malzemelerin tedarik zincirini güvence altına almak ve sahte parçaların savunma sistemlerine girmesini önlemek için blok zinciri teknolojisini kullanmaktadır. Benzer şekilde Avrupa Birliği'nin "Blok Zinciri Tabanlı Güvenli Tedarik Zincirleri" projesi, kritik altyapı bileşenlerinin güvenliğini sağlamayı amaçlamaktadır. Diğer bir önemli uygulama alanı, nükleer malzemelerin ve silahların izlenmesi ve kontrolüdür. Uluslararası Atom Enerjisi Ajansı (IAEA), nükleer malzemelerin izlenmesi ve nükleer silahların yayılmasının önlenmesi için

blok zinciri tabanlı izleme sistemleri geliştirmektedir. Bu sistemler, nükleer malzemelerin üretimden imhaya kadar tüm yaşam döngüsünün şeffaf ve değiştirilemez bir kaydını tutarak nükleer silahların yayılmasını önleme rejimini güçlendirmektedir (Fukuyama, 2021; Nye, 2021).

Blok zinciri teknolojisinin veri koruma ve gizlilik alanındaki uygulamaları, kişisel ve kurumsal verilerin güvenliğini artırmaktadır. Geleneksel merkezi veri tabanları, tek bir noktadan saldırıya açık olmaları ve veri ihlali risklerini artırmaları nedeniyle eleştirilmektedir. Blok zinciri tabanlı veri koruma sistemleri, verilerin dağıtık ve şifrelenmiş bir şekilde saklanmasını sağlayarak bu riskleri önemli ölçüde azaltmaktadır. Zero-knowledge proofs (sıfır bilgi ispatları) gibi kriptografik tekniklerle birleştirildiğinde, blok zinciri teknolojisi, verilerin içeriğini ifşa etmeden doğruluğunu kanıtlamaya olanak tanımaktadır. Bu özellik, özellikle istihbarat paylaşımı ve diplomatik iletişim gibi yüksek güvenlik gerektiren alanlarda değerlidir. Devletler ve uluslararası örgütler, yalnızca belirli aktörlerin erişebileceği izin tabanlı blok zinciri sistemleri (permissioned blockchains) geliştirerek hassas verilerin güvenliğini sağlamaktadır. Örneğin NATO Müttefik Komutanlığı Dönüşüm Komutanlığı (ACT), üye ülkeler arasında güvenli istihbarat paylaşımı için izin tabanlı blok zinciri platformları oluşturmaktadır. ABD İç Güvenlik Bakanlığı'nın "Siber Güvenlik için Blok Zinciri" programı, kritik altyapı verilerinin korunması için blok zinciri tabanlı çözümler geliştirmektedir. Ayrıca Estonya gibi dijital öncü ülkeler, vatandaşların kişisel verilerinin korunması ve e-devlet hizmetlerinin güvenliğinin sağlanması için blok zinciri teknolojisini kullanmaktadır. Bu uygulamalar, blok zinciri teknolojisinin veri güvenliği ve gizlilik alanında sunduğu potansiyeli göstermektedir (Floridi, 2018; Choucri, 2021).

Blok zinciri teknolojisi, kritik altyapı sistemlerinin siber güvenliğini güçlendirmek için de kullanılmaktadır. Enerji şebekeleri, su arıtma tesisleri, ulaşım ağları ve telekom altyapıları gibi kritik sistemler, giderek daha fazla dijitalleşmekte ve bu nedenle siber saldırılara karşı daha savunmasız hale gelmektedir. Blok zinciri tabanlı güvenlik çözümleri, bu sistemlerin bütünlüğünü korumak ve yetkisiz erişimi önlemek için önemli avantajlar sunmaktadır. Dağıtık yapısı sayesinde, blok zinciri teknolojisi, merkezi kontrol noktalarını ortadan kaldırarak kritik altyapılara yönelik "tek noktadan başarısızlık" (single point of failure) riskini azaltmaktadır. Akıllı şebeke (smart grid) sistemlerinde, blok zinciri teknolojisi, enerji üretimi, dağıtımı ve tüketimi verilerinin güvenli bir şekilde kaydedilmesini ve doğrulanmasını sağlamaktadır. Bu, şebeke manipülasyonlarını tespit etmeyi ve önlemeyi kolaylaştırmaktadır. ABD Enerji Bakanlığı'nın "Blok Zinciri Tabanlı Akıllı Şebeke Güvenliği" projesi, enerji altyapısının korunması için blok zinciri teknolojisini kullanmaktadır. Benzer şekilde Avrupa Birliği'nin "Kritik Altyapı Koruma için Blok Zinciri" girişimi, ulaşım, enerji ve telekom altyapı-

larının güvenliğini artırmayı amaçlamaktadır. Bu projeler, blok zinciri teknolojisinin kritik altyapı güvenliğindeki potansiyel rolünü göstermektedir. Ayrıca Nesnelerin İnterneti (IoT) cihazlarının güvenliği açısından da blok zinciri önemli avantajlar sunmaktadır. IoT cihazlarının kimlik doğrulaması, güvenli iletişimi ve davranış denetimi için blok zinciri tabanlı çözümler geliştirilmektedir. Bu, özellikle endüstriyel kontrol sistemleri ve akıllı şehir uygulamaları gibi kritik IoT ekosistemlerinin güvenliğini artırmak için önemlidir (West, 2021; Zuboff, 2019).

Blok zinciri teknolojisinin uluslararası güvenlik ve veri koruma alanındaki potansiyeline rağmen, çeşitli zorluklar ve sınırlamalar da bulunmaktadır. İlk olarak, blok zinciri teknolojisinin ölçeklenebilirlik sorunu, büyük miktarda veri işlemesi gereken ulusal güvenlik uygulamaları için bir engel oluşturabilir. Mevcut blok zinciri sistemlerinin işlem hızı ve kapasitesi, geleneksel merkezi sistemlere kıyasla sınırlı kalabilmektedir. İkinci olarak, kuantum bilişim teknolojilerinin gelişimi, mevcut blok zinciri sistemlerinde kullanılan kriptografik algoritmaların güvenliğini tehdit edebilir. Kuantum bilgisayarların gelişmesiyle, RSA ve ECC gibi mevcut kriptografik algoritmaların kırılması mümkün hale gelebilir, bu da blok zinciri tabanlı güvenlik sistemlerinin etkinliğini azaltabilir. Üçüncü olarak, blok zinciri teknolojisinin düzenlenmesi ve standartlaştırılması konusunda uluslararası bir uzlaşı eksikliği bulunmaktadır. Farklı devletlerin ve bölgelerin farklı düzenleyici yaklaşımları, blok zinciri tabanlı güvenlik çözümlerinin küresel ölçekte uygulanmasını zorlaştırmaktadır. Son olarak, blok zinciri teknolojisinin enerji tüketimi, özellikle proof-of-work (iş ispatı) mekanizması kullanan sistemlerde, önemli bir endişe kaynağı oluşturmaktadır. Yüksek enerji tüketimi, hem ekonomik hem de çevresel açıdan sürdürülebilirlik sorunları oluşturmaktadır. Bu zorluklar ve sınırlamalar, blok zinciri teknolojisinin uluslararası güvenlik ve veri koruma alanındaki potansiyelini tam olarak gerçekleştirmesi için aşılması gereken engelleri temsil etmektedir (OECD, 2021; Brynjolfsson & McAfee, 2019).

Blok zinciri teknolojisinin uluslararası güvenlik ve veri koruma alanındaki geleceği, teknolojik gelişmeler, düzenleyici çerçeveler ve uluslararası işbirliği tarafından şekillendirilecektir. Teknolojik açıdan, blok zinciri sistemlerinin ölçeklenebilirliği, enerji verimliliği ve güvenliği sürekli olarak geliştirilmektedir. Proof-of-stake (hisse ispatı) ve sharding gibi yeni konsensüs mekanizmaları ve mimari yaklaşımlar, blok zinciri sistemlerinin performansını ve verimliliğini artırmaktadır. Kuantum-dayanıklı kriptografik algoritmaların geliştirilmesi, gelecekteki kuantum bilgisayar tehditlerine karşı blok zinciri sistemlerinin güvenliğini sağlamak için kritik öneme sahiptir. Düzenleyici açıdan, uluslararası standartların ve en iyi uygulamaların geliştirilmesi, blok zinciri tabanlı güvenlik çözümlerinin yaygınlaşması için önemlidir. ISO TC 307 (Blok Zinciri ve Dağıtık Defter Teknolojileri için

Teknik Komite) gibi uluslararası standartlaştırma girişimleri, bu alanda ilerlemeler sağlamaktadır. Uluslararası işbirliği açısından, blok zinciri teknolojisinin güvenlik ve veri koruma alanındaki potansiyelini tam olarak gerçekleştirmek için devletler, uluslararası örgütler, özel sektör ve akademik kurumlar arasında daha fazla işbirliği gerekmektedir. Birleşmiş Milletler, NATO, OECD ve diğer uluslararası örgütler, blok zinciri teknolojisinin güvenlik ve veri koruma alanındaki kullanımı için ortak yaklaşımlar ve normlar geliştirmeye başlamıştır. Bu çok paydaşlı işbirliği, blok zinciri teknolojisinin uluslararası güvenlik ve veri koruma alanındaki potansiyelini realize etmek için kritik öneme sahiptir (Singer & Brooking, 2019; Floridi, 2018).

5.4. Dijital Teknolojiler ve Algı Yönetimi (Sosyal Mühendislik, Dezenformasyon)

Dijital teknolojiler, algı yönetimi ve dezenformasyon stratejilerinin etkinliğini artırarak uluslararası ilişkilerde kamuoyunun yönlendirilmesini daha sofistike hale getirmiştir. Devletler, politik aktörler ve siber gruplar, yapay zekâ destekli veri analizleri, sosyal medya manipülasyonu ve psikolojik operasyonlar aracılığıyla kamuoyunu etkileme kapasitesine ulaşmıştır. Özellikle sosyal mühendislik ve dezenformasyon teknikleri, toplumsal algıları manipüle etmek, seçim süreçlerine müdahale etmek ve rakip devletlerin siyasi istikrarını zayıflatmak için etkili bir araç olarak kullanılmaktadır. Bu süreç, geleneksel propaganda yöntemlerinden farklı olarak hedef kitlelere özel olarak uyarlanabilen ve büyük veri destekli psikolojik analizlere dayanan bir yapı oluşturmuştur. Devletlerin yürüttüğü bilgi operasyonları artık sadece doğrudan propagandaya değil, aynı zamanda çok daha incelikli teknikler kullanarak toplumsal kutuplaşmayı artırmaya, güveni sarsmaya ve gerçeklik algısını bulanıklaştırmaya odaklanmaktadır. Rusya'nın Bilgi Savaşı Doktrini, Çin'in Üç Savaş Stratejisi (psikolojik savaş, medya savaşı ve hukuki savaş) ve ABD'nin Stratejik İletişim yaklaşımı, dijital teknolojilerin algı yönetimi alanında nasıl sistemli bir şekilde kullanıldığını gösteren örneklerdir (Nye, 2021; Singer & Brooking, 2019).

Yapay zekâ destekli dezenformasyon kampanyaları, yanlış bilgilerin yayılmasını otomatikleştiren ve etkisini artıran bir faktör olarak öne çıkmaktadır. Gelişmiş yapay zekâ algoritmaları, büyük veri analitiği aracılığıyla hangi tür içeriklerin hangi hedef kitleler üzerinde daha etkili olacağını belirleyerek dezenformasyonun etkisini maksimize etmektedir. Örneğin deepfake teknolojileri ile sahte video ve ses kayıtları üretilerek devlet liderleri ve önemli siyasi figürler hakkında yanıltıcı içerikler oluşturulmakta ve kamuoyunun güveni sarsılmaktadır. Bu tür yapay içerikler, özellikle seçim süreçlerinde ve uluslararası krizlerde manipülasyon amacıyla kullanılabilmekte, küresel güvenliği tehdit edebilecek boyutlara ulaşabilmektedir. Deepfake videoların kalitesi ve gerçekçiliği hızla artmakta, bu içeriklerin gerçek olmadığını tespit etmek giderek zorlaşmaktadır. 2018'de Jordan Pee-

le ve BuzzFeed tarafından yayınlanan Barack Obama deepfake videosu, bu teknolojinin potansiyel tehlikelerini göstermiştir. Avrupa'da 2019 yılında meydana gelen "Ibizagate" skandalı sırasında, Avusturyalı politikacı Heinz-Christian Strache'nin manipüle edilmiş bir videosu politik kriz oluşturmuştur. Yapay zekâ destekli metin üretimi sistemleri (GPT-3, GPT-4 gibi) ise, insan yazarlardan ayırt edilmesi neredeyse imkânsız içerikler üreterek makale, blog yazısı ve sosyal medya gönderileri şeklinde dezenformasyon kampanyalarını desteklemektedir. Bu teknolojiler, az sayıda operatörün çok sayıda sahte hesap ve içerik oluşturmasına olanak tanıyarak dezenformasyon kampanyalarının ölçeğini ve etkinliğini önemli ölçüde artırmaktadır (Floridi, 2018; Arquilla & Ronfeldt, 2020).

Sosyal medya platformları, algı yönetimi ve dezenformasyon kampanyalarının yürütülmesinde merkezi bir rol oynamaktadır. Bu platformların algoritmik içerik dağıtım sistemleri, duygusal tepki uyandıran ve kutuplaştırıcı içeriklerin daha hızlı ve geniş bir şekilde yayılmasını teşvik etmektedir. Cambridge Analytica skandalı, Facebook üzerinden toplanan kullanıcı verilerinin 2016 ABD Başkanlık Seçimleri ve Brexit referandumu gibi kritik seçimlerde seçmenlerin davranışlarını etkilemek için nasıl kullanıldığını göstermiştir. Benzer şekilde Oxford Internet Enstitüsü'nün Hesaplanabilir Propaganda Projesi, sosyal medya platformlarının sistematik dezenformasyon kampanyaları için nasıl kullanıldığını belgelemiştir. Algoritmik içerik dağıtımı, yankı odaları ve filtre baloncukları, kullanıcıların yalnızca kendi görüşlerini doğrulayan içeriklere maruz kalmalarına yol açarak toplumsal kutuplaşmayı derinleştirmektedir. Bot ağları ve koordineli inauthentic behavior (koordineli sahte davranış) olarak bilinen teknikler, belirli içeriklerin ve hashtag'lerin trend olmasını sağlayarak kamusal söylemin manipüle edilmesine olanak tanımaktadır. Facebook, Twitter ve YouTube gibi büyük platformlar, bu tür manipülatif aktivitelere karşı çeşitli önlemler geliştirmiş olsa da, bu tekniklerin sofistikasyonu ve ölçeği sürekli artmaktadır. Araştırmalar, sosyal medya platformlarında yayılan yanlış bilgilerin gerçek bilgilerden daha hızlı, daha geniş ve daha derinlemesine yayıldığını göstermektedir, ki bu durum dezenformasyon kampanyalarının etkinliğini artırmaktadır (West, 2021; Zuboff, 2019).

Mikro-hedefleme (micro-targeting) teknikleri, dijital dezenformasyon kampanyalarının etkinliğini önemli ölçüde artırmaktadır. Büyük veri analitiği ve makine öğrenmesi algoritmaları, kullanıcıların demografik özellikleri, psikolojik profilleri, siyasi eğilimleri ve kişisel ilgi alanları gibi faktörlere dayalı olarak son derece özelleştirilmiş içerikler sunulmasına olanak tanımaktadır. Cambridge Analytica'nın kullandığı OCEAN modeli (Açıklık, Sorumluluk, Dışadönüklük, Uyumluluk, Nevrotiklik) gibi psikolojik profilleme teknikleri, bireylerin hangi tür mesajlara daha duyarlı olacağını tahmin etmek için kullanılmaktadır. Bu teknikler, seçmenlerin davranış-

larını etkilemek, toplumsal kutuplaşmayı artırmak veya belirli politikalara yönelik kamuoyu desteğini manipüle etmek için kullanılabilmektedir. Mikro-hedefleme, geleneksel kitle iletişim araçlarına kıyasla çok daha etkili olabilmektedir, çünkü mesajlar kişiselleştirilmiş ve hedef kitlenin özgül hassasiyetlerine göre uyarlanmıştır. Ayrıca bu tür hedefli kampanyalar genellikle kamuoyunun ve düzenleyici kurumların görüş alanı dışında gerçekleştiğinden, tespit edilmeleri ve düzenlenmeleri daha zordur. Facebook ve Google gibi büyük teknoloji şirketlerinin reklam platformları, bu tür mikro-hedefleme tekniklerini kolaylaştırmakta ve dezenformasyon kampanyalarının etkinliğini artırmaktadır. Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR) ve Kaliforniya Tüketici Gizliliği Yasası (CCPA) gibi düzenlemeler, bu tür veri tabanlı mikro-hedefleme uygulamalarını sınırlamayı amaçlasa da, teknolojik gelişmeler genellikle düzenleyici çerçevelerden daha hızlı ilerlemektedir (Morozov, 2021; Fukuyama, 2021).

Uluslararası örgütler ve devletler, dezenformasyonun küresel güvenlik üzerindeki etkilerini azaltmak amacıyla çeşitli önlemler almaktadır. Avrupa Birliği, sahte haberlerle mücadele etmek için "Dijital Hizmetler Yasası" gibi yeni regülasyonlar geliştirmiş, NATO ise bilgi güvenliğini artırmak amacıyla siber savunma mekanizmalarını güçlendirmeye yönelik stratejiler geliştirmiştir. Ancak dezenformasyonun küresel ölçekte nasıl düzenleneceği ve hangi mekanizmalar aracılığıyla kontrol edileceği konusunda devletlerarasında ortak bir çerçeve oluşturulamamıştır. Avrupa Birliği'nin Dezenformasyonla Mücadele Eylem Planı, Dijital Hizmetler Yasası ve Uygulama Kuralları (Code of Practice on Disinformation) gibi girişimler, dezenformasyonla mücadele için önemli adımlar olsa da, küresel ölçekte bir etkinliğe sahip değildir. NATO'nun Stratejik İletişim Mükemmeliyet Merkezi (NATO StratCom COE) ve NATO-AB Dezenformasyonla Mücadele İşbirliği, transatlantik alanda dezenformasyona karşı ortak yaklaşımlar geliştirmeyi amaçlamaktadır. BM Genel Sekreteri'nin Dijital İşbirliği Yol Haritası, küresel dijital yönetişim ve bilgi bütünlüğü konularında uluslararası işbirliğini teşvik etmektedir. Ancak Çin ve Rusya gibi ülkelerin "bilgi egemenliği" ve "internet egemenliği" kavramlarına dayalı yaklaşımları, küresel düzeyde ortak düzenleyici çerçevelerin oluşturulmasını zorlaştırmaktadır. Bu farklı yaklaşımlar, dezenformasyonla mücadelede küresel işbirliğinin önündeki önemli engellerden biridir (OECD, 2021; Choucri, 2021).

Sivil toplum kuruluşları, akademik kurumlar ve teknoloji şirketleri, dezenformasyon ve algı yönetimi tekniklerine karşı çeşitli karşı önlemler geliştirmektedir. Doğruluk kontrol (fact-checking) platformları, dezenformasyonu tespit etmek ve kamusal farkındalığı artırmak için önemli roller üstlenmektedir. First Draft, PolitiFact, Faktograf gibi bağımsız doğrulama platformları, şüpheli içerikleri analiz ederek kamuoyunu bilgilendirmektedir. Deepfake tespit teknolojileri, yapay zekâ üretimi sahte içerikleri ta-

nımlamak için geliştirilmektedir. DARPA'nın Media Forensics programı ve Microsoft'un Video Authenticator gibi girişimler, deepfake videoları tespit etmek için teknikler geliştirmektedir. Medya okuryazarlığı eğitim programları, vatandaşların yanıltıcı bilgileri tanıma ve eleştirel düşünme becerilerini geliştirmeyi amaçlamaktadır. UNESCO'nun Bilgi ve Medya Okuryazarlığı girişimi ve AB'nin DigComp çerçevesi, bu alandaki önemli eğitim programlarıdır. Blok zinciri tabanlı içerik doğrulama sistemleri, dijital içeriklerin orijinalliğini ve değiştirilmemiş olduğunu garantilemek için kullanılmaktadır. The New York Times'ın News Provenance Project ve Microsoft'un Project Origin gibi girişimler, içerik kaynağının güvenilir bir şekilde takip edilmesini sağlamayı amaçlamaktadır. Çapraz platform dezenformasyon izleme sistemleri, farklı sosyal medya platformları arasında yayılan dezenformasyon kampanyalarını tespit etmeye yardımcı olmaktadır. Ancak bu karşı önlemlerin etkinliği, dezenformasyon tekniklerinin sürekli evrimleşmesi nedeniyle sınırlı kalmaktadır. Dezenformasyon ve algı yönetimi teknikleriyle etkili bir şekilde mücadele etmek için teknolojik çözümler, düzenleyici yaklaşımlar ve eğitim girişimlerinin koordineli bir şekilde uygulanması gerekmektedir (Singer & Brooking, 2019; Floridi, 2018).

Algı yönetimi ve dezenformasyon teknikleri, gelecekte yapay zekâ ve diğer dijital teknolojilerin gelişmesiyle daha da sofistike hale gelecektir. Yapay zekâ destekli içerik üretim sistemleri, deepfake teknolojileri ve otomatik metin oluşturma sistemleri giderek daha gerçekçi ve inandırıcı içerikler üretebilecektir. Bu teknolojik gelişmeler, dezenformasyonu tespit etmeyi ve ona karşı koymayı daha da zorlaştıracaktır. GPT-4 ve DALL-E gibi büyük dil modelleri ve görüntü oluşturma sistemleri, manuel içerik üretiminin ötesinde, tamamen otomatikleştirilmiş dezenformasyon kampanyalarının yürütülmesine olanak tanıyabilir. Ayrıca arttırılmış gerçeklik (AR) ve sanal gerçeklik (VR) teknolojilerinin yaygınlaşması, yeni tür dezenformasyon ve algı manipülasyonu tekniklerinin ortaya çıkmasına neden olabilir. Bu teknolojik gelişmeler, dezenformasyonla mücadele için yeni yaklaşımların ve teknolojilerin geliştirilmesini gerektirecektir. Yapay zekâ destekli içerik doğrulama sistemleri, dijital içerik kimlik doğrulama sistemleri ve blok zinciri tabanlı güven mekanizmaları, gelecekteki dezenformasyon tehditlerini azaltmada kritik rol oynayabilir. Ayrıca uluslararası toplumun dezenformasyona karşı ortak normlar, standartlar ve düzenleyici çerçeveler geliştirmesi de önemli olacaktır. Ancak teknoloji ile dezenformasyon arasındaki yarış devam ettikçe, tamamen teknolojik veya düzenleyici bir çözüm yerine, eleştirel düşünme, medya okuryazarlığı ve kurumsal güvenin güçlendirilmesi gibi daha temel yaklaşımların önemi artacaktır. Dezenformasyon ve algı yönetimi tekniklerinin uluslararası güvenlik ve istikrar üzerindeki etkileri, gelecekte devletler ve uluslararası örgütler için önemli bir endişe kaynağı olmaya devam edecektir (West, 2021; Zuboff, 2019).

5.5. Dijital Paralar ve Merkeziyetsiz Finansın (DeFi) Uluslararası Ekonomi Üzerindeki Etkisi

Dijital paralar ve merkeziyetsiz finans (DeFi) sistemleri, uluslararası ekonomi üzerinde büyük bir dönüşüm oluşturarak devletlerin ekonomik kontrol mekanizmalarını yeniden şekillendirmelerine neden olmuştur. Geleneksel finans sistemleri, uzun yıllardır devletlerin merkez bankaları, uluslararası finans kuruluşları ve büyük ölçekli bankalar tarafından yönetilirken, blok zinciri tabanlı finansal sistemlerin yükselişi, bu merkezi yapıları zayıflatarak finansal işlemlerin merkeziyetsiz ve küresel ölçekte gerçekleşmesine olanak tanımaktadır. Bu süreç, devletlerin finansal politikalarını ve para üzerindeki kontrol mekanizmalarını değiştirerek ekonomik güç dengelerinde yeni kırılmalara neden olmaktadır. Özellikle Bitcoin, Ethereum ve diğer kripto varlıklar, devletlerin kontrol ettiği merkezî finansal sistemlere karşı bağımsız bir yapı oluşturarak bireylerin ve kurumların finansal işlemlerini daha özgür bir şekilde gerçekleştirmesine olanak tanımaktadır. Bitcoin'in 2009 yılında ortaya çıkışından bu yana, kripto para piyasası dramatik bir büyüme göstermiş, toplam piyasa değeri 2 trilyon doları aşmıştır. Bu hızlı büyüme, geleneksel finans sisteminin dışında gelişen paralel bir ekonomik ekosistemin oluşmasına yol açmış, devletlerin para politikalarını kontrol etme ve ekonomik yaptırımlar uygulama kapasitelerini zorlamıştır. Özellikle ABD dolarının küresel rezerv para birimi olarak sahip olduğu ayrıcalıklı statü, kripto paraların yaygınlaşmasıyla potansiyel olarak tehdit altına girmiştir (Brynjolfsson & McAfee, 2019; OECD, 2021).

DeFi sistemleri, geleneksel bankacılık sistemlerini baypas ederek finansal aracılara olan ihtiyacı ortadan kaldıran yeni nesil finansal işlemleri mümkün kılmaktadır. Akıllı kontratlar aracılığıyla yapılan finansal işlemler, güvenli, merkeziyetsiz ve manipülasyona kapalı bir yapı sunarak finansal işlemlerin hızlanmasını ve maliyetlerin düşmesini sağlamaktadır. Ancak bu sistemlerin düzenlenmesi ve kontrol altına alınması konusundaki belirsizlikler, uluslararası ekonomi açısından ciddi riskler doğurmaktadır. Özellikle kara para aklama, terörün finansmanı ve vergilendirme gibi konular, devletlerin DeFi sistemlerini nasıl yöneteceği konusunda ciddi endişeler oluşturmaktadır. Ethereum blok zinciri üzerinde geliştirilen DeFi protokolleri, borç verme, likidite sağlama, türev ürünler ve varlık yönetimi gibi geleneksel finansal hizmetlerin merkeziyetsiz alternatiflerini sunmaktadır. Compound, Aave, Uniswap ve MakerDAO gibi protokoller, kullanıcıların aracı kurumlara ihtiyaç duymadan finansal işlemler gerçekleştirmelerine olanak tanımaktadır. Bu merkeziyetsiz borsa ve kredi platformları, geleneksel finansal kurumların işlem ücretleri, sınır ötesi transfer maliyetleri ve bürokratik süreçler gibi dezavantajlarını ortadan kaldırmaktadır. DeFi sistemlerinin "toplam kilitli değeri" (Total Value Locked - TVL), 2021 yılında 100 milyar doları aşarak bu alternatif finansal ekosistemin hızlı bü-

yümesini göstermiştir. Ancak DeFi sistemlerinin yasal ve düzenleyici belirsizlikler, teknik güvenlik açıkları, likidite riskleri ve piyasa manipülasyonu gibi önemli zorlukları bulunmaktadır (Fukuyama, 2021; Singer & Brooking, 2019).

Merkez Bankası Dijital Para Birimleri (CBDC), devletlerin dijital para ekosistemindeki kontrol ve etkilerini koruma çabalarının bir parçası olarak ortaya çıkmıştır. Çin'in dijital yuan (e-CNY) projesi, Avrupa Merkez Bankası'nın dijital euro girişimi ve İsveç'in e-krona projesi, bu alandaki önemli örneklerdir. CBDC'ler, devletlerin merkezi kontrolü altında bulunan dijital para birimleri olarak kripto paraların merkeziyetsiz yapısına alternatif sunmaktadır. Çin, dijital yuan projesini 2014 yılında başlatmış ve 2020 yılından itibaren çeşitli şehirlerde pilot uygulamaları hayata geçirmiştir. Bu girişim, Çin'in küresel finans sisteminde dolar hegemonyasına karşı stratejik bir hamle olarak değerlendirilmektedir. Dijital yuan, Çin'in uluslararası ödemelerde dolar bağımlılığını azaltma, Kuşak ve Yol İnisiyatifi çerçevesinde ticari işlemleri kolaylaştırma ve ülke içindeki finansal aktiviteleri daha etkin bir şekilde izleme amaçlarına hizmet etmektedir. Benzer şekilde Avrupa Merkez Bankası'nın dijital euro projesi, Avrupa'nın dijital finans alanındaki teknolojik rekabet gücünü artırma, finansal egemenliğini koruma ve ABD ile Çin arasındaki dijital para rekabetinde üçüncü bir alternatif sunma hedeflerini taşımaktadır. CBDC'ler, devletlere para politikalarını uygulama, mali suçlarla mücadele ve finansal istikrarı koruma konularında yeni araçlar sunmaktadır. Ancak bu sistemlerin gizlilik kaygıları, siber güvenlik riskleri ve mevcut bankacılık sistemleri üzerindeki potansiyel etkileri, önemli tartışma konularıdır (West, 2021; Floridi, 2018).

Dijital paralar ve DeFi sistemleri, uluslararası ticaret ve ödemeler sistemini de dönüştürmektedir. Sınır ötesi ödemeler, geleneksel bankacılık sisteminde yüksek maliyetli, yavaş ve karmaşık bir süreç olarak bilinirken, blok zinciri tabanlı dijital para sistemleri bu işlemleri daha hızlı, daha ucuz ve daha şeffaf hale getirmektedir. Ripple, Stellar ve Algorand gibi ödeme odaklı blok zincirleri, bankalar ve finansal kurumlar arasında gerçek zamanlı ve düşük maliyetli sınır ötesi transferleri mümkün kılmaktadır. Bu sistemler, özellikle gelişmekte olan ülkelerdeki bireyler ve işletmeler için finansal sisteme erişimi kolaylaştırarak küresel ekonomik kapsayıcılığı artırma potansiyeline sahiptir. Dünya Bankası verilerine göre, geleneksel sistemlerle gönderilen uluslararası havalelerin ortalama maliyeti %6'nın üzerindeyken, blok zinciri tabanlı sistemler bu maliyeti %1'in altına düşürebilmektedir. Bu maliyet avantajı, özellikle göçmen işçilerin ülkelerine gönderdikleri havalelerde önemli bir tasarruf sağlamaktadır. Ayrıca dijital paralar, uluslararası ticaret finansmanında da önemli avantajlar sunmaktadır. Akıllı kontratlar aracılığıyla ithalat-ihracat işlemlerinde kullanılan akreditifler ve diğer ticaret finansmanı araçları otomatikleştirilebilmekte, bu da işlem süreçlerini

hızlandırmakta ve maliyetleri düşürmektedir. IBM ve Maersk'in geliştirdiği TradeLens platformu, blok zinciri teknolojisini kullanarak küresel tedarik zincirlerini dijitalleştirme ve uluslararası ticaret süreçlerini optimize etme amacını taşımaktadır. Ancak bu sistemlerin yaygın kabulü için düzenleyici belirsizliklerin giderilmesi, teknik standartların geliştirilmesi ve geleneksel finans sistemleriyle entegrasyonun sağlanması gerekmektedir (Brynjolfsson & McAfee, 2019; Choucri, 2021).

Dijital paralar ve DeFi sistemleri, ekonomik yaptırımlar ve küresel finansal gözetim mekanizmaları üzerinde de önemli etkilere sahiptir. SWIFT gibi geleneksel uluslararası ödeme sistemleri, ABD ve diğer Batılı ülkeler tarafından ekonomik yaptırım aracı olarak kullanılabilmektedir. İran, Kuzey Kore ve Venezuela gibi yaptırıma tabi ülkeler, bu yaptırımları aşmak için kripto para ve blok zinciri tabanlı alternatif ödeme sistemlerine yönelmektedir. Örneğin Venezuela'nın Petro kripto para girişimi, ABD yaptırımlarını aşma ve ülkenin petrol rezervlerini monetize etme amacını taşımaktadır. Benzer şekilde İran ve Rusya gibi ülkeler, SWIFT sistemine alternatif oluşturmak için blok zinciri tabanlı ödeme sistemleri geliştirmektedir. Bu gelişmeler, ABD dolarının küresel rezerv para birimi statüsüne ve ABD'nin finansal yaptırımları küresel politika aracı olarak kullanma kapasitesine potansiyel bir tehdit oluşturmaktadır. Ayrıca merkeziyetsiz finans sistemleri, finansal gözetim mekanizmalarını da zorlamaktadır. Geleneksel finans sistemlerinde, Kara Paranın Aklanmasının Önlenmesi (AML) ve Müşterini Tanı (KYC) düzenlemeleri, mali suçlarla mücadele için kritik öneme sahiptir. Ancak DeFi protokollerinin çoğu, bu tür düzenleyici gereklilikleri uygulamamakta veya uygulayamamaktadır. Bu durum, terör finansmanı, kara para aklama ve vergi kaçakçılığı gibi mali suçlar açısından endişe oluşturmaktadır. ABD Hazine Bakanlığı, Finansal Eylem Görev Gücü (FATF) ve diğer uluslararası düzenleyici kurumlar, kripto para ekosistemini düzenlemek için çeşitli girişimlerde bulunmaktadır. Ancak DeFi sistemlerinin merkeziyetsiz ve sınır ötesi doğası, bu düzenlemelerin uygulanmasını zorlaştırmaktadır (Arquilla & Ronfeldt, 2020; OECD, 2021).

Dijital paralar ve DeFi sistemleri, finansal kapsayıcılık ve ekonomik gelişim açısından önemli fırsatlar sunmaktadır. Dünya genelinde 1.7 milyar yetişkin birey hala temel finansal hizmetlere erişememektedir. Dijital paralar ve mobil ödeme sistemleri, geleneksel bankacılık altyapısının yetersiz olduğu bölgelerde finansal kapsayıcılığı artırma potansiyeline sahiptir. Kenya'nın M-Pesa mobil para sistemi, bankası olmayan milyonlarca insana finansal hizmetlere erişim sağlayarak ülkenin ekonomik gelişimine katkıda bulunmuştur. Benzer şekilde blok zinciri tabanlı finansal sistemler, özellikle gelişmekte olan ülkelerde finansal altyapı eksikliklerini "atlayarak" (leapfrogging) daha gelişmiş finansal hizmetlere erişim sağlayabilir. Dijital kimlik çözümleri ile entegre edildiğinde, bu sistemler bankası olmayan

bireylerin finansal sisteme güvenli bir şekilde erişmelerini kolaylaştırabilir. Ayrıca mikro finansman, küçük işletme kredileri ve sigorta gibi finansal hizmetler, DeFi protokolleri aracılığıyla daha erişilebilir hale gelebilir. Dünya Ekonomik Forumu'nun raporlarına göre, blok zinciri teknolojisinin finansal kapsayıcılık alanında uygulanması, 2025 yılına kadar küresel GSYİH'ya 3.7 trilyon dolar katkı sağlayabilir. Ancak dijital paralar ve DeFi sistemlerinin finansal kapsayıcılık potansiyelinin tam olarak gerçekleşmesi için dijital okuryazarlık, internet erişimi ve teknolojik altyapı gibi alanlarda önemli ilerlemelerin kaydedilmesi gerekmektedir. Ayrıca bu sistemlerin kullanıcı dostu arayüzler ve güvenlik önlemleriyle desteklenmesi, geniş kitlelerce benimsenmesi için kritik öneme sahiptir (Zuboff, 2019; Fukuyama, 2021).

Dijital paralar ve DeFi sistemlerinin geleceği, teknolojik gelişmeler, düzenleyici yaklaşımlar ve kullanıcı benimseme dinamikleri tarafından şekillendirilecektir. Teknolojik açıdan, ölçeklenebilirlik, enerji verimliliği ve güvenlik alanlarında sürekli iyileştirmeler yapılmaktadır. Ethereum 2.0 gibi güncellemeler, blok zinciri ağlarının işlem kapasitesini ve enerji verimliliğini artırmayı amaçlamaktadır. Layer-2 çözümleri, zk-rollup'lar ve sidechain'ler gibi ölçeklendirme teknolojileri, blok zinciri sistemlerinin kullanılabilirliğini ve erişilebilirliğini artırmaktadır. Düzenleyici açıdan, devletler ve uluslararası kuruluşlar, dijital para ekosistemini düzenlemek için çeşitli yaklaşımlar geliştirmektedir. Bazı ülkeler, inovasyon dostu düzenleyici çerçeveler oluştururken, diğerleri daha kısıtlayıcı politikalar benimsemektedir. Avrupa Birliği'nin Kripto Varlık Piyasaları Yönetmeliği (MiCA), ABD'nin Dijital Varlık Düzenleme Girişimleri ve Japonya'nın Sanal Para Birimi Yasası, bu alandaki önemli düzenleyici gelişmelerdir. Bu düzenleyici çerçevelerin gelişimi, dijital para ekosisteminin meşruiyetini ve güvenilirliğini artırabilir, ancak aynı zamanda bu teknolojilerin merkeziyetsiz ve sınır ötesi doğasını koruma dengesini sağlamak önemlidir. Kullanıcı benimseme açısından, dijital paraların ve DeFi sistemlerinin yaygın kullanımı için kullanıcı deneyiminin iyileştirilmesi, güvenlik önlemlerinin güçlendirilmesi ve eğitim girişimlerinin artırılması gerekmektedir. Kurumsal benimseme, özellikle büyük şirketlerin ve finansal kurumların dijital para ve DeFi ekosistemlerine girişi, bu teknolojilerin geleceği açısından kritik öneme sahiptir. Tesla, Square, MicroStrategy ve PayPal gibi şirketlerin Bitcoin ve diğer dijital varlıkları kurumsal rezervlerinin bir parçası olarak benimsemesi, bu alandaki önemli gelişmelerdir. Dijital paralar ve DeFi sistemleri, uluslararası ekonomik sistemdeki önemlerini artırmaya devam ederken, geleneksel finans sistemleri ile bu yeni teknolojiler arasında bir denge ve entegrasyon sağlanması, küresel finansal istikrar ve ekonomik gelişim açısından kritik öneme sahiptir (West, 2021; Floridi, 2018).

5.6. Dijital Haklar ve Küresel İnsan Hakları Perspektifi

Dijital teknolojilerin yaygınlaşması, bireylerin temel haklarını ve özgürlüklerini koruma gerekliliğini gündeme getirerek uluslararası insan hakları normlarının dijitalleşme süreciyle nasıl uyum sağlayacağını tartışmaya açmıştır. Dijital haklar, bireylerin internet erişimi, çevrimiçi gizlilik, veri güvenliği ve bilgiye erişim gibi haklarını kapsayan geniş bir kavram olup, küresel insan hakları rejiminde giderek daha fazla önem kazanmaktadır. Devletlerin ve teknoloji şirketlerinin veri yönetim süreçleri üzerindeki etkisi, bireylerin mahremiyetini tehdit edebileceği gibi, ifade özgürlüğü ve bilgiye erişim gibi temel hakları da kısıtlayabilir. Özellikle otoriter rejimler, dijital hakları sınırlayan politikalar geliştirerek internet sansürü ve devlet destekli gözetim sistemleri ile bireylerin bilgiye erişim hakkını ihlal edebilmektedir. BM İnsan Hakları Konseyi'nin 2012 yılında aldığı karar, internet erişiminin temel bir insan hakkı olduğunu kabul etmiş ve çevrimdışı dünyada geçerli olan insan hakları korumalarının çevrimiçi dünyada da eşit şekilde uygulanması gerektiğini vurgulamıştır. Bu karar, dijital haklar kavramının uluslararası insan hakları çerçevesinde resmi olarak tanınması açısından önemli bir dönüm noktası olmuştur. Dijital hakların kapsamı, teknolojik gelişmelerle birlikte genişlemekte, yapay zekâ, büyük veri, algoritmik karar alma sistemleri ve biyometrik tanıma teknolojileri gibi yeni teknolojilerin oluşturduğu etik ve hukuki zorlukları da içermektedir (Floridi, 2018; Fukuyama, 2021).

Dijital hakların korunması ve geliştirilmesi konusunda küresel çapta ortak bir yaklaşım oluşturulması gerekmektedir. Avrupa Birliği'nin Genel Veri Koruma Tüzüğü (GDPR), bireylerin dijital verilerini koruma ve veri güvenliği standartlarını artırma amacıyla önemli bir adım olarak değerlendirilmektedir. Ancak farklı ülkelerin dijital haklar konusunda farklı yaklaşımlar benimsemesi, küresel düzeyde bir standardizasyon sağlanmasını zorlaştırmaktadır. Örneğin ABD'nin teknoloji şirketlerine daha fazla özgürlük tanıyan politikaları ile Avrupa Birliği'nin birey odaklı veri koruma stratejileri arasında ciddi farklılıklar bulunmaktadır. Bu durum, dijital hakların korunması için uluslararası düzeyde daha kapsamlı ve bağlayıcı düzenlemelere ihtiyaç duyulduğunu göstermektedir. GDPR, bireylere kişisel verilerinin nasıl toplandığı, işlendiği ve paylaşıldığı konusunda kontrol sağlayan "unutulma hakkı", "veri taşınabilirliği hakkı" ve "açık rıza" gibi önemli haklar tanımıştır. Bu düzenleme, küresel dijital haklar standardı oluşturma yolunda önemli bir adım olmuş, Kaliforniya Tüketici Gizlilik Yasası (CCPA) ve Brezilya'nın Genel Veri Koruma Kanunu (LGPD) gibi benzer düzenlemelere ilham kaynağı olmuştur. Avrupa Konseyi'nin Kişisel Verilerin Otomatik İşlenmesi Karşısında Bireylerin Korunması Sözleşmesi (Sözleşme 108) ve BM İnsan Hakları Yüksek Komiserliği'nin dijital gizlilik konusundaki rehber ilkeleri, uluslararası alanda dijital hakların korunma-

sına yönelik diğer önemli girişimlerdir. Ancak bu düzenlemelerin küresel ölçekte uygulanması ve etkili bir şekilde yaptırıma bağlanması hala önemli zorluklar içermektedir (Singer & Brooking, 2019; West, 2021).

Yapay zekâ ve algoritmik karar alma sistemlerinin yaygınlaşması, dijital haklar bağlamında yeni zorluklar oluşturmaktadır. Bu sistemler, kredi başvuruları, istihdam kararları, sosyal yardım tahsisi ve hatta ceza adalet sistemindeki kararlar gibi bireylerin hayatını doğrudan etkileyen süreçlerde giderek daha fazla kullanılmaktadır. Algoritmik önyargı ve ayrımcılık riskleri, şeffaflık eksikliği ve hesap verebilirlik sorunları, bu teknolojilerin insan hakları üzerindeki potansiyel etkilerine ilişkin endişeleri artırmaktadır. Örneğin ABD'de COMPAS adlı risk değerlendirme algoritmasının, Afro-Amerikan sanıklar aleyhine önyargılı sonuçlar ürettiği tespit edilmiştir. Benzer şekilde işe alım algoritmalarının cinsiyet temelli ayrımcılığa yol açtığı birçok vakada belgelenmiştir. Avrupa Konseyi'nin "Yapay Zekâ Sistemlerinin İnsan Hakları, Demokrasi ve Hukukun Üstünlüğü Üzerindeki Etkileri" raporu ve UNESCO'nun "Yapay Zekâ Etiği Tavsiye Kararı", algoritmik sistemlerin insan hakları standartlarına uygun şekilde geliştirilmesi ve kullanılması için rehber ilkeler sunmaktadır. Avrupa Birliği'nin Yapay Zekâ Yasası taslağı, yapay zekâ sistemlerini risk düzeylerine göre sınıflandıran ve yüksek riskli uygulamalar için sıkı düzenlemeler getiren kapsamlı bir yasal çerçeve önermektedir. Bu düzenleyici girişimler, yapay zekâ ve algoritmik sistemlerin insan hakları üzerindeki potansiyel olumsuz etkilerini azaltmayı amaçlamaktadır. Ancak teknolojik gelişmelerin hızı ve karmaşıklığı, düzenleyici çerçevelerin sürekli güncellenmesini ve adaptasyonunu gerektirmektedir (West, 2021; OECD, 2021).

Dijital gözetim teknolojilerinin devletler ve özel sektör aktörleri tarafından artan kullanımı, mahremiyet hakkı ve ifade özgürlüğü gibi temel dijital haklar üzerinde önemli tehditler oluşturmaktadır. Edward Snowden'ın 2013 yılında ABD Ulusal Güvenlik Ajansı'nın (NSA) küresel gözetim programlarını ifşa etmesi, devletlerin dijital gözetim kapasitelerini ve bunların insan hakları üzerindeki potansiyel etkilerini gözler önüne sermiştir. Çin'in Sosyal Kredi Sistemi ve Xinjiang bölgesindeki gözetim uygulamaları, dijital teknolojilerin toplumsal kontrol amacıyla nasıl kullanılabileceğini gösteren çarpıcı örneklerdir. Öte yandan, özel sektör aktörlerinin veri toplama ve profilleme uygulamaları da mahremiyet hakkı açısından endişe verici boyutlara ulaşmıştır. Facebook-Cambridge Analytica skandalı, özel şirketlerin topladığı kişisel verilerin politik manipülasyon amacıyla nasıl kullanılabileceğini göstermiştir. BM İnsan Hakları Yüksek Komiserliği'nin "Dijital Çağda Mahremiyet Hakkı" raporu ve BM Özel Raportörü'nün gözetim teknolojileri üzerine raporları, dijital gözetimin insan hakları üzerindeki etkilerine dikkat çekmekte ve devletlere bu alanda düzenleyici çerçeveler geliştirmeleri için çağrıda bulunmaktadır. Avrupa İnsan Hakları Mahkemesi'nin Big

Brother Watch ve Diğerleri v. Birleşik Krallık (2018) kararı, kitle gözetim programlarının insan hakları standartlarına uygunluğunun yargısal denetimi açısından önemli bir emsal oluşturmuştur. Bu karar, devletlerin ulusal güvenlik gerekçesiyle bile olsa, dijital gözetim uygulamalarının belirli yasal sınırlar içinde kalması ve etkin denetim mekanizmalarına tabi olması gerektiğini vurgulamıştır (Arquilla & Ronfeldt, 2020; Zuboff, 2019).

İfade özgürlüğü ve bilgiye erişim hakları, dijital çağda yeni zorluklarla karşı karşıyadır. İnternet ve sosyal medya platformları, bireyler için benzeri görülmemiş bir ifade ve bilgi paylaşım imkânı sunarken, aynı zamanda bu hakların kullanımını kısıtlayan yeni kontrol mekanizmalarının da ortaya çıkmasına neden olmuştur. Devletlerin internet sansürü, içerik engelleme ve sosyal medya kısıtlamaları, ifade özgürlüğü ve bilgiye erişim haklarını ciddi şekilde sınırlandırmaktadır. Freedom House'un "İnternette Özgürlük" raporuna göre, dünya nüfusunun yalnızca %20'si tamamen özgür bir internet ortamında yaşamaktadır. Rusya, İran ve Çin gibi ülkelerin uyguladığı kapsamlı internet sansürü rejimleri, vatandaşların bilgiye erişimini önemli ölçüde kısıtlamaktadır. Çin'in "Büyük Güvenlik Duvarı" (Great Firewall), dünyanın en kapsamlı internet sansürü sistemlerinden biri olarak uluslararası web sitelerine erişimi engellemekte ve çevrimiçi içeriği yoğun bir şekilde filtrelemektedir. Türkiye, Mısır ve Suudi Arabistan gibi ülkelerde, sosyal medya platformları ve haber siteleri düzenli olarak engellenmekte veya kısıtlanmaktadır. Öte yandan, teknoloji şirketlerinin içerik moderasyon politikaları ve algoritmik filtreleme sistemleri de ifade özgürlüğü üzerinde önemli etkiler oluşturmaktadır. Facebook, Twitter ve YouTube gibi platformların içerik kaldırma kararları, milyarlarca kullanıcının ifade özgürlüğünü doğrudan etkilemektedir. BM İfade Özgürlüğü Özel Raportörü'nün dijital platformlar üzerine raporları, hem devletlerin hem de özel sektör aktörlerinin ifade özgürlüğüne ilişkin sorumluluklarını vurgulamakta ve bu alanda insan hakları temelli bir yaklaşımın benimsenmesi için çağrıda bulunmaktadır (Morozov, 2021; Choucri, 2021).

Dijital teknolojilere erişim eşitsizliği, yeni bir dijital bölünme ve insan hakları sorunu olarak ortaya çıkmaktadır. İnternet ve dijital teknolojilere erişim, eğitim, sağlık, finansal hizmetler ve demokratik katılım gibi temel insan haklarından yararlanmak için giderek daha kritik hale gelmektedir. Ancak Uluslararası Telekomünikasyon Birliği (ITU) verilerine göre, dünya nüfusunun yaklaşık %40'ı hala internet erişimine sahip değildir. Bu dijital bölünme, gelişmiş ve gelişmekte olan ülkeler arasında, kırsal ve kentsel bölgeler arasında, sosyoekonomik gruplar arasında ve cinsiyet hatları boyunca belirgin şekilde gözlenmektedir. Afrika'da internet penetrasyon oranı %40 civarındayken, Avrupa'da bu oran %85'in üzerindedir. Kırsal bölgelerde yaşayan bireyler, kentsel alanlardaki vatandaşlara kıyasla önemli ölçüde daha düşük internet erişim oranlarına sahiptir. Dünya genelinde 327 milyon

daha az kadın internet kullanıcısı bulunmakta, bu da önemli bir toplumsal cinsiyet dijital uçurumuna işaret etmektedir. COVID-19 pandemisi, dijital erişim eşitsizliğinin sonuçlarını daha da belirgin hale getirmiş, uzaktan eğitim ve çalışma imkânlarından yararlanma konusunda dezavantajlı gruplar ciddi zorluklar yaşamıştır. BM Sürdürülebilir Kalkınma Hedefleri (SDG) kapsamında dijital erişim eşitsizliklerinin azaltılması ve 2030 yılına kadar evrensel internet erişiminin sağlanması hedeflenmektedir. Dijital kapsayıcılık girişimleri, altyapı yatırımları, yenilikçi bağlantı çözümleri ve dijital okuryazarlık programları, dijital bölünmeyi kapatmak için uygulanan stratejiler arasındadır. Ancak dijital erişim eşitliğinin sağlanması için daha kapsamlı ve koordineli küresel çabalara ihtiyaç duyulmaktadır (Brynjolfsson & McAfee, 2019; OECD, 2021).

Çocuklar, engelliler, yaşlılar ve diğer savunmasız gruplar için dijital hakların korunması, özel dikkat gerektiren bir alandır. Dijital teknolojiler bu gruplar için önemli fırsatlar sunarken, aynı zamanda özgün riskler ve zorluklar da oluşturmaktadır. Çocuklar, çevrimiçi ortamlarda siber zorbalık, cinsel istismar, yasa dışı içeriğe maruz kalma ve kişisel verilerin kötüye kullanılması gibi risklere karşı özellikle savunmasızdır. BM Çocuk Hakları Sözleşmesi'nin dijital bağlamda uygulanması, çocukların dijital ortamlarda hem korunma hem de katılım haklarının dengelenmesini gerektirmektedir. UNICEF'in "Dijital Dünyada Çocuklar" raporu ve Çocukların Çevrimiçi Mahremiyeti ve İfade Özgürlüğü üzerine Genel Yorum, bu alanda rehberlik sağlayan önemli dokümanlardır. Engelli bireyler için dijital teknolojilere erişilebilirlik, Engelli Hakları Sözleşmesi kapsamında bir hak olarak tanınmaktadır. Web İçeriği Erişilebilirlik Kılavuzu (WCAG) gibi standartlar, dijital içerik ve hizmetlerin engelli bireyler için erişilebilir olmasını sağlamayı amaçlamaktadır. Yaşlılar için dijital okuryazarlık ve teknolojik dışlanma ile mücadele, dijital hakların gerçekleştirilmesi için önemli konulardır. Dijital teknolojilerin gelişimi ve yaygınlaşması, bu savunmasız gruplar için erişilebilirlik, güvenlik ve katılım haklarının korunmasını sağlayacak şekilde yönlendirilmelidir. Avrupa Konseyi'nin "Dijital Ortamda Çocuk Hakları Kılavuz İlkeleri" ve AB'nin "Web Erişilebilirlik Direktifi", savunmasız grupların dijital haklarının korunması için geliştirilen normatif çerçevelere örnektir. Ancak bu standartların küresel ölçekte uygulanması ve farklı toplumsal ve kültürel bağlamlara adapte edilmesi, önemli zorluklar içermektedir (Floridi, 2018; Fukuyama, 2021).

Dijital hakların geleceği, teknolojik gelişmeler, düzenleyici çerçeveler ve çok paydaşlı yönetişim modelleri tarafından şekillendirilecektir. Metaverse, artırılmış gerçeklik, nöro-teknolojiler ve yapay genel zekâ gibi gelişmekte olan teknolojiler, dijital haklar alanında yeni zorluklar ve fırsatlar oluşturacaktır. Bu teknolojilerin insan hakları standartlarına uygun şekilde geliştirilmesi ve düzenlenmesi için proaktif yaklaşımlar gerekmektedir. BM Diji-

tal İşbirliği Yol Haritası, dijital teknolojilerin insan haklarını koruyacak ve geliştirecek şekilde yönetilmesi için küresel işbirliği çağrısında bulunmaktadır. İnternetin yönetişimi konusunda çok paydaşlı modeller (multi-stakeholder models), devletler, özel sektör, sivil toplum ve teknik toplulukların karar alma süreçlerine katılımını sağlayarak dijital hakların korunmasında daha kapsayıcı ve etkili stratejilerin geliştirilmesine olanak tanımaktadır. İnternet Yönetişim Forumu (IGF) ve Dünya İnternet Konferansı gibi platformlar, dijital haklar konusunda küresel diyaloğu teşvik etmektedir. Ayrıca "dijital anayasacılık" (digital constitutionalism) olarak adlandırılan yaklaşımlar, dijital ortamda temel hakların korunmasına yönelik anayasal güvenceler sağlamayı önermektedir. Dijital hakların etkili bir şekilde korunması ve geliştirilmesi için ulusal ve uluslararası düzeyde güçlü yasal çerçeveler, etkin denetim mekanizmaları, sivil toplum katılımı ve dijital okur-yazarlık girişimleri gibi çok boyutlu bir yaklaşım gerekmektedir. Dijital haklar, insan haklarının dijital çağda korunması ve geliştirilmesi için kritik öneme sahip olup, küresel toplumun ortak sorumluluğunu gerektirmektedir (Singer & Brooking, 2019; West, 2021).

6. TARTIŞMA VE ANALİZ

6.1. Bulguların Teorik Perspektifle Değerlendirilmesi

Dijital teknolojilerin uluslararası ilişkiler üzerindeki etkilerini analiz etmek için kullanılan teorik çerçeveler, dijitalleşmenin küresel sistemde nasıl bir dönüşüm oluşturduğunu anlamada farklı bakış açıları sunmaktadır. Teknolojik determinizm, dijital dönüşümün kaçınılmaz bir süreç olduğunu ve devletlerin bu dönüşüme ayak uydurmak zorunda kaldığını savunurken, konstrüktivizm, dijitalleşmenin sosyal ve politik yapıların bir yansıması olarak şekillendiğini öne sürmektedir. Eleştirel perspektifler ise, dijital teknolojilerin küresel güç dengelerini nasıl değiştirdiğini ve bu dönüşüm sürecinin belirli aktörler tarafından nasıl yönlendirildiğini sorgulamaktadır. Bu farklı teorik yaklaşımlar, dijitalleşmenin uluslararası güvenlik, ekonomi ve diplomasi alanlarındaki etkilerinin nasıl kavramsallaştırılabileceğini anlamada kritik bir rol oynamaktadır. Teknolojik determinist perspektif, yapay zekâ, blok zinciri ve kuantum bilişim gibi teknolojilerin uluslararası ilişkilerde oluşturduğu dönüşümün kaçınılmaz olduğunu ve devletlerin bu teknolojik gelişmelere adapte olmaları gerektiğini savunurken, konstrüktivist yaklaşım bu teknolojilerin geliştirilmesi, benimsenmesi ve kullanılmasının sosyal, kültürel ve politik bağlamlara göre farklılaştığını vurgulamaktadır. Eleştirel teoriler ise dijital teknolojilerin gelişiminin ve kullanımının mevcut güç yapılarını nasıl pekiştirdiğini ve yeni eşitsizlikler oluşturduğunu analiz etmektedir (Nye, 2021; Floridi, 2018).

Araştırmanın bulguları, dijital teknolojilerin uluslararası sistem üzerindeki etkilerinin çok boyutlu ve karmaşık olduğunu göstermektedir. Yapay

zekâ destekli diplomatik süreçler, siber savaş stratejileri, blok zinciri tabanlı finansal sistemler ve kuantum bilişim teknolojileri, devletlerin güç kapasitelerini ve uluslararası rekabet dinamiklerini köklü bir şekilde değiştirmektedir. Bu dönüşüm sürecinin teorik çerçevede değerlendirilmesi, geleneksel uluslararası ilişkiler teorilerinin dijital çağın karmaşıklıklarını açıklamada yetersiz kaldığını ve yeni teorik yaklaşımlara ihtiyaç duyulduğunu ortaya koymaktadır. Özellikle teknoloji merkezli uluslararası ilişkiler teorilerinin geliştirilmesi ve disiplinler arası yaklaşımların benimsenmesi, dijitalleşmenin küresel sistem üzerindeki etkilerini daha iyi anlamamızı sağlayacaktır. Realist perspektiften bakıldığında, dijital teknolojiler devletlerin güç maksimizasyonu ve güvenlik arayışları için yeni araçlar sunmaktadır. Siber saldırı kapasiteleri, yapay zekâ destekli askeri sistemler ve kuantum bilişim teknolojileri, devletlerin güç projeksiyonlarını genişleten ve ulusal güvenlik stratejilerini yeniden şekillendiren unsurlar olarak karşımıza çıkmaktadır. Liberal yaklaşım açısından, dijital teknolojiler karşılıklı bağımlılığı artırarak ve ulus-ötesi bağlantıları güçlendirerek devletlerarası işbirliği için yeni fırsatlar sunabilir. Ancak aynı zamanda bu teknolojilerin güvenli ve şeffaf bir şekilde yönetilmesi için uluslararası rejimlere ve normatif çerçevelere olan ihtiyacı da artırmaktadır (Singer & Brooking, 2019; West, 2021).

Konstrüktivist teorik perspektif, dijital teknolojilerin nasıl anlamlandırıldığı ve toplumsal olarak inşa edildiğine odaklanarak farklı devletlerin ve toplumların bu teknolojilere yönelik farklı yaklaşımlarını anlamamıza yardımcı olmaktadır. Örneğin "siber güvenlik", "dijital egemenlik" ve "yapay zekâ etiği" gibi kavramların farklı bağlamlarda nasıl yorumlandığı ve bu yorumların devletlerin politikalarını nasıl şekillendirdiği, konstrüktivist bir çerçevede analiz edilebilir. Çin'in "siber egemenlik" kavramını internet kontrolü ve ulusal güvenlik bağlamında yorumlarken, Batılı ülkelerin "açık internet" ve "çevrimiçi özgürlükler" kavramlarını vurgulaması, bu konstrüktivist yaklaşımın önemini göstermektedir. Kimlikler, normlar ve söylemler, dijital teknolojilerin geliştirilmesi, düzenlenmesi ve kullanılmasında belirleyici faktörler olarak öne çıkmaktadır. Ayrıca konstrüktivist yaklaşım dijital diplomasi, siber normlar ve teknolojik yönetişim rejimlerinin nasıl oluştuğunu ve zamanla nasıl evrildiğini anlamada değerli içgörüler sunmaktadır. Uluslararası siber güvenlik normlarının gelişimi, dijital hakların tanımlanması ve yapay zekâ etiği konusundaki küresel müzakereler, devletler, uluslararası örgütler, teknoloji şirketleri ve sivil toplum kuruluşları arasındaki etkileşimler sonucunda şekillenmektedir. Bu etkileşimler, dijital teknolojilerin uluslararası ilişkilerde nasıl kullanılacağına dair paylaşılan anlayışların ve normların ortaya çıkmasına katkıda bulunmaktadır (Arquilla & Ronfeldt, 2020; Fukuyama, 2021).

Eleştirel teorik perspektifler, dijital teknolojilerin mevcut güç yapılarını nasıl pekiştirdiğini ve yeni eşitsizlikler oluşturduğunu sorgulayarak bu tek-

nolojilerin gelişimi ve kullanımının ardındaki ekonomik, politik ve ideolojik motivasyonları analiz etmektedir. Dijital kapitalizm kavramı, büyük teknoloji şirketlerinin veriler üzerindeki kontrolünü ve bu kontrolün ekonomik ve politik güce nasıl dönüştüğünü incelemektedir. Gözetim kapitalizmi teorisi, kullanıcı verilerinin ticari ve politik amaçlarla nasıl metalaştırıldığını ve yeni bir sermaye birikimi biçiminin nasıl ortaya çıktığını açıklamaktadır. Dijital kolonizasyon kavramı ise, Küresel Kuzey'in teknoloji şirketlerinin Küresel Güney üzerindeki teknolojik hâkimiyetini ve bunun oluşturduğu bağımlılık ilişkilerini sorgulamaktadır. Teknolojik sistemlerin geliştirilmesi ve kullanılmasında gömülü olan değerler, önyargılar ve iktidar ilişkileri, eleştirel teorinin odak noktasıdır. Örneğin yapay zekâ sistemlerindeki algoritmaların algoritmik önyargı ve ayrımcılık sorunları, bu sistemlerin geliştirilmesinde ve eğitilmesinde var olan toplumsal eşitsizliklerin teknolojik sistemlere nasıl yansıdığını göstermektedir. Ayrıca dijital teknolojilerin çevresel etkileri, bu teknolojilerin üretimi ve kullanımının küresel ölçekte oluşturduğu ekolojik ayak izi de eleştirel perspektiflerden analiz edilmektedir. Eleştirel teoriler, dijital teknolojilerin potansiyel olarak demokratikleştirici ve özgürleştirici etkilerini kabul etmekle birlikte, bu potansiyelin gerçekleşmesi için mevcut güç yapılarının ve hegemonik ilişkilerin dönüştürülmesi gerektiğini vurgulamaktadır (Zuboff, 2019; Morozov, 2021).

Disiplinler arası teorik yaklaşımlar, dijital teknolojilerin uluslararası ilişkiler üzerindeki çok boyutlu etkilerini daha kapsamlı bir şekilde anlamamıza olanak tanımaktadır. Bilim ve teknoloji çalışmaları (STS), sosyo-teknik sistemler teorisi, tekno-politik yaklaşımlar ve ağ teorisi gibi disiplinler arası perspektifler, dijital teknolojilerin sosyal, politik ve ekonomik boyutlarını bütüncül bir çerçevede incelemeye imkân vermektedir. Bu yaklaşımlar, teknoloji ile toplum arasındaki karşılıklı ilişkiyi vurgulayarak teknolojik gelişmelerin basit bir determinizm ile açıklanamayacağını, teknoloji ve toplumun birbirini karşılıklı olarak şekillendirdiğini göstermektedir. Aktör-ağ teorisi, uluslararası ilişkilerde insan ve insan olmayan aktörlerin (teknolojik sistemler, algoritmalar, dijital platformlar) karmaşık etkileşimlerini analiz etmek için değerli bir çerçeve sunmaktadır. Kompleksite teorisi, dijital teknolojilerin oluşturduğu karmaşık, öngörülemeyen ve doğrusal olmayan etkileri anlamada yardımcı olmaktadır. Tekno-jeopolitik perspektifler, dijital teknolojilerin küresel güç mücadelesindeki rolünü ve teknolojik üstünlük için verilen rekabeti incelemektedir. Ayrıca feminist ve post-kolonyal teorik yaklaşımlar, dijital teknolojilerin toplumsal cinsiyet, ırk ve sınıf boyutlarını ve küresel eşitsizlikler üzerindeki etkilerini analiz etmek için önemli çerçeveler sunmaktadır. Bu disiplinler arası teorik yaklaşımların benimsenmesi, dijital teknolojilerin uluslararası ilişkiler üzerindeki çok boyutlu etkilerini daha derinlemesine anlamamıza ve bu teknolojilerin insani, sosyal ve çevresel değerlerle uyumlu bir şekilde geliştirilmesi ve kullanılması için daha

kapsayıcı politikalar geliştirmemize yardımcı olacaktır (Choucri, 2021; OECD, 2021).

6.2. Dijital Dönüşümün Uluslararası İlişkilerde Oluşturduğu Stratejik Değişimler

Dijital dönüşüm, uluslararası ilişkilerin temel parametrelerini değiştirerek devletlerin stratejik önceliklerini ve küresel güç rekabetini köklü bir dönüşüme uğratmıştır. Geleneksel güç unsurları, askeri kapasiteler ve ekonomik üstünlük gibi maddi faktörlere dayanırken, dijitalleşme süreci, bilgi yönetimi, siber güvenlik, yapay zekâ destekli karar alma mekanizmaları ve blok zinciri tabanlı ekonomik sistemler gibi yeni güç unsurlarını küresel rekabetin merkezine yerleştirmiştir. Devletler, dijital dönüşümü dış politika stratejilerinin merkezine koyarak uluslararası ilişkilerde rekabet avantajı elde etmeye çalışmaktadır. Bu süreç, geleneksel uluslararası ilişkiler teorilerinin genişletilmesini ve dijitalleşmenin çok boyutlu etkilerinin kapsamlı bir şekilde analiz edilmesini gerektirmektedir. Büyük güçler arasındaki rekabet, artık yalnızca konvansiyonel askeri kapasiteler ve ekonomik üstünlük üzerinden değil, aynı zamanda teknolojik inovasyon, dijital altyapı kontrolü ve veri hâkimiyeti üzerinden de yürütülmektedir. Çin'in "Made in China 2025" ve "Dijital İpek Yolu" girişimleri, ABD'nin "Ulusal Yapay Zekâ Girişimi" ve Avrupa Birliği'nin "Dijital Tek Pazar Stratejisi", büyük güçlerin dijital teknolojiler alanındaki stratejik konumlanmalarını göstermektedir. Bu stratejik girişimler, dijital teknolojilerin artık yalnızca ekonomik büyümenin değil, aynı zamanda jeopolitik üstünlüğün ve ulusal güvenliğin de kritik bileşenleri olarak görüldüğünü ortaya koymaktadır (Nye, 2021; Floridi, 2018).

Dijital dönüşümün en büyük etkilerinden biri, devletlerin ulusal güvenlik stratejilerini ve savunma politikalarını yeniden şekillendirmesi olmuştur. Siber savaşlar, yapay zekâ destekli istihbarat operasyonları ve otonom silah sistemleri, devletlerin askeri caydırıcılık anlayışlarını değiştirmiştir. Özellikle büyük güçler, dijitalleşen savaş alanlarında avantaj sağlamak amacıyla yapay zekâ destekli savunma mekanizmalarını entegre etmeye başlamıştır. ABD'nin "Joint Artificial Intelligence Center" projesi ve Çin'in "Military-Civil Fusion" politikası, dijitalleşmenin güvenlik doktrinlerine nasıl entegre edildiğini gösteren önemli örneklerdir. Siber alanın "beşinci savaş alanı" olarak tanımlanması ve NATO'nun siber saldırıları 5. Madde kapsamında kolektif savunma gerektiren eylemler olarak kabul etmesi, dijital tehditlerin geleneksel güvenlik paradigmalarını nasıl dönüştürdüğünü göstermektedir. Rusya'nın hibrit savaş doktrini, dijital teknolojileri geleneksel askeri operasyonlar ile bilgi savaşı ve siber operasyonları birleştiren bütünleşik bir stratejik yaklaşım içinde konumlandırmaktadır. Bu yeni güvenlik ortamında, devletler siber saldırı ve savunma kapasitelerini geliştirmek, kritik dijital altyapılarını korumak ve dijital tehditlere hızlı yanıt verebilecek kurumsal yapılar oluşturmak için kapsamlı stratejiler geliştirmektedir. Ulusal Siber

Güvenlik Stratejileri, Dijital Savunma Planları ve Siber Komutanlıkların kurulması, devletlerin bu yeni güvenlik ortamına adaptasyonunun somut göstergeleridir (Arquilla & Ronfeldt, 2020; Singer & Brooking, 2019).

Dijitalleşme süreci aynı zamanda, devletlerin uluslararası yönetişim süreçlerinde daha fazla dijital araç kullanmaya başlamasını sağlamıştır. Dijital diplomasi, devletlerin uluslararası toplantılara katılımını ve kriz yönetim süreçlerini hızlandırmış, devletlerarası iletişimi daha verimli hale getirmiştir. Ancak bu teknolojilerin kullanımı, uluslararası güvenlik politikalarının nasıl regüle edileceği konusunda büyük tartışmalara neden olmaktadır. Devletlerin dijital teknolojileri bir hegemonya aracı olarak kullanma eğilimi, uluslararası sistemde yeni gerilimlerin ortaya çıkmasına yol açmaktadır. Dijital diplomasi, yalnızca diplomatik iletişimin dijitalleşmesi olarak değil, aynı zamanda dijital platformlar aracılığıyla kamuoyu diplomasisi yürütme, dijital koalisyonlar oluşturma ve küresel dijital politikaları şekillendirme aracı olarak da kullanılmaktadır. ABD'nin "Dijital Dış Politika Stratejisi", Fransa'nın "Dijital Diplomasi Yol Haritası" ve İngiltere'nin "Dijital Strateji" belgeleri, dijital diplomasinin stratejik bir dış politika aracı olarak nasıl kurumsallaştığını göstermektedir. Sosyal medya platformları, diplomatlar ve dışişleri bakanlıkları tarafından resmi iletişim kanalları olarak kullanılmakta, hashtag diplomasisi ve dijital kampanyalar aracılığıyla küresel kamuoyu etkilenmeye çalışılmaktadır. Ayrıca yapay zekâ destekli diplomatik analiz sistemleri, büyük veri analitiği kullanarak diplomatik müzakereleri optimize etmekte ve kriz yönetimi süreçlerinde karar alıcılara destek sağlamaktadır. Dijital diplomasi alanındaki bu gelişmeler, diplomatik ilişkilerin doğasını ve diplomatik personelin rolünü yeniden tanımlamakta, geleneksel diplomatik uygulamaların dijital çağa adaptasyonunu gerektirmektedir (West, 2021; OECD, 2021).

Dijital teknolojiler, devletlerin ekonomik politikalarını ve uluslararası ticaret stratejilerini de köklü bir şekilde dönüştürmektedir. Dijital ekonomi, veri odaklı iş modelleri, e-ticaret, platform ekonomisi ve dijital hizmetler, küresel ekonominin en hızlı büyüyen sektörleri haline gelmiştir. Devletler, bu dijital ekonomik dönüşümden maksimum fayda sağlamak ve stratejik dijital endüstrilerde rekabet avantajı elde etmek için kapsamlı stratejiler geliştirmektedir. ABD'nin "Amerikan Yapay Zekâ Girişimi", Çin'in "Yeni Nesil Yapay Zekâ Geliştirme Planı", Avrupa Birliği'nin "Dijital Tek Pazar Stratejisi" ve Japonya'nın "Toplum 5.0" girişimi, dijital ekonomik dönüşümü ulusal öncelik haline getiren stratejik yaklaşımlardır. Ayrıca dijital teknolojiler uluslararası ticaret ve yatırım kalıplarını da değiştirmektedir. Dijital hizmet ticareti, geleneksel mal ticaretinden daha hızlı büyümekte, dijital platformlar ve e-ticaret marketleri küresel ticaret akışlarını yeniden yapılandırmaktadır. Blok zinciri teknolojisi, uluslararası ödeme sistemlerini ve tedarik zincirlerini dönüştürerek ticaret işlemlerini daha verimli, şeffaf ve

güvenli hale getirmektedir. Merkez bankası dijital para birimleri (CBDC), küresel finansal sistemi yeniden şekillendirme potansiyeline sahiptir. Bu gelişmeler, uluslararası ekonomik düzenin temel dinamiklerini değiştirmekte ve devletlerin ekonomik egemenliklerini korumak için yeni stratejiler geliştirmelerini gerektirmektedir. Dijital ticaret anlaşmaları, veri lokalizasyonu politikaları, dijital vergilendirme stratejileri ve teknoloji transferi düzenlemeleri, devletlerin dijital ekonomi alanındaki politika araçları haline gelmiştir (Brynjolfsson & McAfee, 2019; Fukuyama, 2021).

Büyük teknoloji şirketlerinin uluslararası politikadaki artan etkisi, dijital dönüşümün oluşturduğu bir diğer stratejik değişimdir. Apple, Google, Amazon, Facebook ve Microsoft gibi Amerikan teknoloji devleri ve Baidu, Alibaba, Tencent ve Huawei gibi Çin teknoloji şirketleri, yalnızca ekonomik aktörler değil, aynı zamanda küresel politikayı etkileyen stratejik oyuncular haline gelmiştir. Bu şirketlerin kullanıcı verileri, dijital altyapılar ve yapay zekâ teknolojileri üzerindeki kontrolü, devletlerin geleneksel güç kapasitelerini zorlayan bir faktör olarak ortaya çıkmaktadır. Teknoloji şirketleri, milyarlarca kullanıcının verilerini kontrol ederek küresel bilgi akışlarını yönlendirme ve kamuoyu algılarını şekillendirme kapasitesine sahiptir. Bu durum, "teknoloji diplomasisi" olarak adlandırılan yeni bir diplomatik alanın ortaya çıkmasına neden olmuştur. Devletler, teknoloji şirketleriyle stratejik ortaklıklar kurarak ve bu şirketlerin faaliyetlerini düzenleyerek dijital alandaki etki kapasitelerini artırmaya çalışmaktadır. Teknoloji şirketlerinin küresel politikadaki artan etkisi, devlet egemenliği, demokratik hesap verebilirlik ve dijital haklar konularında önemli soruları gündeme getirmektedir. Devletler, bu şirketleri düzenlemek ve dijital egemenliklerini korumak için çeşitli stratejiler geliştirmektedir. Avrupa Birliği'nin Dijital Hizmetler Yasası ve Dijital Piyasalar Yasası, ABD'nin anti-tröst soruşturmaları ve Çin'in teknoloji şirketlerine yönelik düzenleyici müdahaleleri, bu stratejik yaklaşımların örnekleridir. Teknoloji şirketlerinin küresel politikadaki rolü ve devletlerle ilişkileri, dijital çağda uluslararası ilişkilerin anlaşılması için kritik öneme sahip bir faktör haline gelmiştir (Zuboff, 2019; Choucri, 2021).

Dijital dönüşümün uluslararası ilişkilerde oluşturduğu stratejik değişimler, küresel yönetişim mekanizmalarının ve uluslararası işbirliği modellerinin de yeniden şekillenmesini gerektirmektedir. Siber güvenlik, veri koruma, yapay zekâ etiği, dijital ticaret ve dijital haklar gibi alanlarda uluslararası normların ve rejimlerin geliştirilmesi, dijital çağda uluslararası istikrarın ve işbirliğinin sağlanması için kritik öneme sahiptir. Birleşmiş Milletler Hükümetler Arası Siber Güvenlik Uzmanlar Grubu (UN GGE) ve Açık Uçlu Çalışma Grubu (OEWG), siber alanda sorumlu devlet davranışı normlarının geliştirilmesi için önemli platformlardır. BM Genel Sekreteri'nin Dijital İşbirliği Yol Haritası, dijital çağda küresel yönetişimin temel prensiplerini ve önceliklerini belirlemektedir. G20 Dijital Ekonomi Çalışma Grubu, yapay

zekâ ilkeleri ve dijital ekonomi konularında uluslararası koordinasyonu teşvik etmektedir. Ayrıca çok paydaşlı yönetişim modelleri (multi-stakeholder governance), dijital teknolojilerin düzenlenmesi ve yönetilmesi için devletler, özel sektör, sivil toplum ve teknik toplulukların katılımını sağlayan yenilikçi yaklaşımlar sunmaktadır. İnternet Yönetişim Forumu (IGF), bu çok paydaşlı yönetişim modelinin önemli bir örneğidir. Dijital teknolojilerin yönetişimi konusundaki bu uluslararası girişimler, dijital çağda küresel işbirliğinin ve istikrarın sağlanması için kritik öneme sahiptir. Ancak devletlerin dijital egemenlik yaklaşımları ve stratejik rekabet dinamikleri, bu işbirliği çabalarını zorlaştırmaktadır. Dijital teknolojilerin etkin bir şekilde yönetilmesi ve düzenlenmesi için devletlerin ulusal güvenlik kaygıları ile küresel işbirliği gereklilikleri arasında bir denge kurması gerekmektedir (Morozov, 2021; OECD, 2021).

6.3. Gelecekte Dijital Teknolojilerin Küresel Sistem Üzerindeki Olası Etkileri

Dijital teknolojilerin hızla ilerlemesi, küresel güç dengelerini, ekonomik yapıların işleyişini, güvenlik paradigmasını ve diplomatik süreçleri dönüştürmektedir. Yapay zekâ, blok zinciri, kuantum bilişim ve siber güvenlik, devletlerin jeopolitik ve ekonomik stratejilerini belirleyen en önemli faktörler arasına girmektedir. Bu teknolojiler, uluslararası yönetişim mekanizmalarını, egemenlik anlayışlarını ve devletlerarası iş birliklerini yeniden tanımlamaya zorlayacaktır. Önümüzdeki on yılda, yapay zekâ teknolojilerinin daha otonom, daha yetenekli ve daha yaygın hale gelmesi beklenmektedir. Yapay genel zekâ (AGI) ve yapay süper zekâ (ASI) gibi ileri yapay zekâ formlarının geliştirilmesi, uluslararası güvenlik, ekonomi ve diplomasi alanlarında radikal değişimlere yol açabilir. Yapay zekâ sistemleri, askeri operasyonlardan diplomatik müzakerelere, ekonomik tahminlerden istihbarat analizine kadar geniş bir yelpazede insanlardan daha üstün kapasitelere ulaşabilir. Bu gelişme, yapay zekâ sistemlerinin kontrolü konusunda uluslararası rekabeti şiddetlendirebilir ve stratejik istikrarı tehdit edebilir. Ayrıca yapay zekâ destekli siber silahlar, otomatik hedef tanıma ve saldırı kapasiteleriyle siber savaşın doğasını değiştirebilir. Devletler, bu teknolojilerin gelişimini ve kullanımını düzenlemek için yeni uluslararası rejimlere ve normlara ihtiyaç duyacaktır. Yapay Zekâ Silahlanma Kontrol Anlaşmaları, Yapay Zekâ Etik Standartları ve Uluslararası Yapay Zekâ Araştırma İşbirliği Çerçeveleri, gelecekte uluslararası diplomasinin önemli konuları haline gelebilir (Nye, 2021; Floridi, 2018).

Dijital teknolojilerin en büyük etkisi, uluslararası güvenlik ve diplomasi alanında olacaktır. Yapay zekâ destekli askeri sistemler, kuantum bilişim tabanlı istihbarat operasyonları ve siber savaş stratejileri, devletlerin güvenlik politikalarını köklü biçimde değiştirecektir. Blok zinciri teknolojilerinin yaygınlaşması ise, finansal sistemleri merkeziyetsiz hale getirerek devletle-

rin ekonomik kontrol mekanizmalarını zayıflatacaktır. Bu dönüşüm, yeni ittifak modellerinin oluşmasına, dijital egemenliğin yeniden tanımlanmasına ve küresel yönetişim yapılarının değişmesine yol açacaktır. Kuantum bilişim ve kuantum kriptografi, geleneksel şifreleme sistemlerini etkisiz hale getirerek ulusal güvenlik ve istihbarat stratejilerinde devrim oluşturabilir. Kuantum üstünlüğü (quantum supremacy) elde eden devletler, rakiplerinin şifreli iletişimlerini kırabilir ve hassas bilgilere erişebilir. Bu teknolojik üstünlük, uluslararası istihbarat ve siber operasyonlar alanında dramatik bir güç değişimine neden olabilir. Aynı zamanda, kuantum-dayanıklı şifreleme sistemleri, devletlerin ve kurumların kritik verilerini korumak için vazgeçilmez hale gelecektir. Kuantum sensörler ve kuantum radarlar, askeri keşif ve gözetleme kapasitelerini artırarak denizaltıların tespiti gibi daha önce imkânsız olan görevleri mümkün kılabilir. Bu gelişmeler, stratejik caydırıcılık dengelerini bozabilir ve yeni bir silahlanma yarışına yol açabilir. Kuantum teknolojileri alanında küresel işbirliği ve düzenleme rejimleri, gelecekteki uluslararası güvenlik mimarisinin kritik bileşenleri olacaktır (Singer & Brooking, 2019; West, 2021).

Metaverse ve üç boyutlu internet, dijital diplomasi ve uluslararası müzakereler için yeni platformlar sunarak diplomatik etkileşimlerin doğasını dönüştürebilir. Sanal diplomatik misyonlar, üç boyutlu uluslararası toplantılar ve avatarlar aracılığıyla gerçekleştirilen diplomatik görüşmeler, geleneksel yüz yüze diplomasiye alternatif veya tamamlayıcı olabilir. Bu gelişmeler, diplomatik temsil, protokol ve müzakere kavramlarını yeniden tanımlayabilir. Holografik telepresence (holografik uzaktan bulunma) teknolojileri, devlet liderlerinin ve diplomatların fiziksel olarak bulunmadan uluslararası toplantılara katılmalarını mümkün kılabilir. Yapay zekâ destekli diplomatik asistanlar, diplomatların bilgi toplama, analiz ve müzakere hazırlıklarında artan rol oynayabilir. Dijital teknolojiler ayrıca sivil toplum, özel sektör ve uluslararası örgütlerin diplomatik süreçlere katılımını artırarak diplomasinin daha kapsayıcı ve çok aktörlü bir yapıya evrilmesine katkıda bulunabilir. Sanal diplomatik platformların siber güvenliği ve diplomatik verilerin korunması, bu yeni diplomatik ortamın önemli endişeleri arasında yer alacaktır. Devletler ve uluslararası örgütler, bu sanal diplomatik ekosistemin güvenliğini ve bütünlüğünü korumak için yeni protokoller ve güvenlik standartları geliştirmeye ihtiyaç duyacaktır (Arquilla & Ronfeldt, 2020; OECD, 2021).

Dijital teknolojiler, küresel ekonomik yapıyı da köklü bir şekilde dönüştürecektir. Merkez bankası dijital para birimleri (CBDC), merkeziyetsiz finans (DeFi) sistemleri ve blok zinciri tabanlı ekonomik altyapılar, uluslararası finans ve ticaret sistemlerini yeniden şekillendirebilir. ABD dolarının küresel rezerv para birimi olarak hâkimiyeti, dijital yuan gibi büyük ekonomilerin CBDC'leri tarafından zorlanabilir. Merkeziyetsiz finans sis-

temlerinin yaygınlaşması, geleneksel bankacılık ve finans kuruluşlarının rolünü azaltabilir ve küresel finans akışlarını bankacılık sistemleri dışına yönlendirebilir. Akıllı kontratlar, uluslararası ticaret ve yatırım anlaşmalarının otomatik olarak uygulanmasını sağlayabilir ve mevcut hukuki ve finansal aracılık mekanizmalarını dönüştürebilir. Tokenizasyon, fiziksel ve dijital varlıkların blok zinciri üzerinde temsil edilmesi ve alınıp satılması, küresel varlık piyasalarını daha erişilebilir ve likit hale getirebilir. Küresel dijital vergiler, veri hakları ve dijital ticaret rejimleri, uluslararası ekonomik sistemin yeni düzenleyici çerçeveleri olarak ortaya çıkabilir. Bu ekonomik dönüşüm, hem fırsatlar hem de riskler sunmaktadır: Bir yandan finansal kapsayıcılığı ve ekonomik verimliliği artırabilirken, diğer yandan finansal istikrarı tehdit edebilir ve yeni eşitsizlikler oluşturabilir. Küresel ekonomik yönetişim kurumları, IMF, Dünya Bankası ve WTO gibi, dijital çağa uyum sağlamak ve etkinliklerini korumak için köklü reformlara ihtiyaç duyabilir (Brynjolfsson & McAfee, 2019; Fukuyama, 2021).

Dijital teknolojilerin gelecekteki etkisi, kaçınılmaz olarak devletler ve diğer aktörler arasındaki stratejik tercihler ve politika kararları tarafından şekillendirilecektir. Teknolojik determinizm yerine, teknoloji-toplum etkileşiminin karmaşık ve çok boyutlu doğasını kabul eden bir yaklaşım benimsenmelidir. Dijital teknolojiler, içsel olarak ne iyi ne de kötüdür; bunların etkileri, nasıl geliştirildikleri, düzenlendikleri ve kullanıldıklarına bağlıdır. Devletler, uluslararası örgütler, teknoloji şirketleri, sivil toplum kuruluşları ve vatandaşlar, bu teknolojilerin insani değerler, özgürlükler, eşitlik ve sürdürülebilirlikle uyumlu bir şekilde geliştirilmesini ve kullanılmasını sağlamak için aktif rol oynamalıdır. Dijital teknolojilerin küresel sistem üzerindeki potansiyel olumlu etkileri arasında, sürdürülebilir kalkınmayı destekleme, hastalıkları tedavi etme, iklim değişikliğiyle mücadele etme ve uzay keşfini hızlandırma kapasiteleri yer alır. Ancak bu teknolojilerin kontrolsüz gelişimi ve kullanımı, artan eşitsizlikler, demokratik kurumların zayıflaması, kitle imha silahlarının yayılması ve hatta insan türünün geleceğini tehdit eden varoluşsal riskler gibi ciddi tehlikeler de oluşturabilir. Dijital teknolojilerin küresel sistem üzerindeki nihai etkisi, kolektif stratejik zekâmızın ve etik değerlerimizin, teknolojik gelişme hızına ayak uydurabilme kapasitesine bağlı olacaktır. Uluslararası işbirliği, çok paydaşlı yönetişim ve ortak etik çerçeveler, dijital teknolojilerin insanlığın yararına kullanılmasını sağlamak için kritik öneme sahiptir (Zuboff, 2019; Choucri, 2021).

6.4. Araştırmanın Sınırlılıkları ve Alternatif Açıklamalar

Bu araştırma, dijital teknolojilerin uluslararası ilişkiler üzerindeki etkilerini kapsamlı bir teorik ve metodolojik çerçevede ele almaktadır. Ancak hızla değişen dijitalleşme dinamikleri ve bu dönüşümün uzun vadeli etkilerinin tam olarak öngörülememesi, araştırmanın bazı sınırlılıklarını ortaya çıkarmaktadır. Dijital teknolojilerin gelişme hızı, araştırma bulgularının

zamanla güncelliğini yitirme riskini artırmakta ve teorik çerçevenin ilerleyen yıllarda revize edilmesini gerektirmektedir. Özellikle siber savaş stratejileri, yapay zekâ destekli diplomasi ve kuantum bilişim tabanlı istihbarat operasyonları gibi alanlarda devletlerin kamuya açık veri paylaşımında sınırlamalar getirmesi, ampirik analizlerin kapsamını daraltmaktadır. Yapay zekâ, kuantum bilişim ve blok zinciri teknolojilerinin gelişim hızı, akademik araştırmaların bu teknolojilerin en güncel durumunu yansıtmasını zorlaştırmaktadır. Araştırma tamamlandığında, teknolojik gelişmeler çalışmanın bazı bulgularını ve öngörülerini geçersiz kılabilir veya değiştirebilir. Bu durum, dijital teknolojilerin uluslararası ilişkiler üzerindeki etkilerini inceleyen araştırmaların sürekli olarak güncellenmesini ve yeni gelişmeleri dikkate alacak şekilde revize edilmesini gerektirmektedir. Ayrıca devletlerin dijital teknoloji stratejilerine ilişkin verilerin çoğu, ulusal güvenlik gerekçesiyle kısıtlı veya gizlidir, bu da özellikle siber operasyonlar, istihbarat faaliyetleri ve savunma kapasiteleri gibi hassas alanlarda kapsamlı analizleri sınırlandırmaktadır (Nye, 2021; Floridi, 2018).

Bölgesel ve ekonomik farklılıklar da dijitalleşmenin etkilerini homojen bir şekilde değerlendirmeyi zorlaştırmaktadır. Gelişmiş ülkeler dijital dönüşüme büyük yatırımlar yaparken, Afrika ve Güney Asya'daki bazı ülkeler altyapı eksiklikleri nedeniyle bu dönüşüme tam olarak adapte olamamaktadır. Bu durum, dijitalleşmenin küresel etkilerinin farklı coğrafyalarda değişiklik göstermesine neden olmaktadır. Araştırmanın kapsamı, öncelikle ABD, Çin, Rusya ve Avrupa Birliği gibi büyük güçlerin dijitalleşme stratejilerine odaklanmakta; ancak bu durum küresel Güney'deki ülkelerin deneyimlerini ve perspektiflerini yeterince temsil etmeme riskini taşımaktadır. Dijital uçurum (digital divide), yalnızca ülkeler arasında değil, aynı zamanda ülkeler içindeki farklı demografik gruplar arasında da önemli eşitsizlikler oluşturmaktadır. Araştırmanın makro düzeydeki odağı, bu mikro düzeydeki eşitsizlikleri ve bunların sosyo-politik etkilerini kapsamlı bir şekilde incelemeyi zorlaştırmaktadır. Farklı bölgelerin ve ülkelerin dijital teknolojilere yaklaşımlarındaki kültürel, kurumsal ve tarihi farklılıklar, dijitalleşmenin uluslararası ilişkiler üzerindeki etkisinin tek bir teorik çerçeve ile açıklanmasını imkânsız kılmaktadır. Bu, araştırmanın bulgularının genelleştirilebilirliğini sınırlandıran önemli bir faktördür. Ayrıca gelişmekte olan ülkelerdeki dijitalleşme süreçleri, gelişmiş ülkelerden farklı dinamikler ve öncelikler gösterebilir, bu da araştırmanın teorik çerçevesinin evrensel geçerliliğini sorgulanır hale getirebilir (Singer & Brooking, 2019; West, 2021).

Metodolojik sınırlılıklar da araştırmanın kapsamını ve derinliğini etkilemektedir. Dijital teknolojilerin karmaşık ve çok boyutlu doğası, tek bir metodolojik yaklaşımla kapsamlı bir şekilde analiz edilmesini zorlaştırmaktadır. Nitel analize dayalı yaklaşımlar, dijitalleşmenin uluslararası ilişkiler üzerindeki etkilerine ilişkin derinlemesine içgörüler sağlarken, nicel

verilerin ve ampirik analizlerin sınırlı olması, bulgulara ilişkin niceliksel değerlendirmeleri ve kesin etki ölçümlerini zorlaştırmaktadır. Yapay zekâ, kuantum bilişim ve blok zinciri gibi teknolojilerin teknik karmaşıklığı, bu teknolojilerin uluslararası ilişkiler araştırmacıları tarafından kapsamlı bir şekilde anlaşılmasını ve analiz edilmesini zorlaştırmaktadır. Disiplinler arası işbirliği eksikliği, teknolojik gelişmelerin politik, stratejik ve sosyal sonuçlarının tam olarak değerlendirilmesini engelleyebilir. Araştırma, genellikle resmi belgeler, akademik literatür ve uzman görüşlerine dayanmaktadır, ancak bu kaynaklar devletlerin ve aktörlerin gerçek niyetlerini, gizli stratejilerini ve operasyonel kapasitelerini tam olarak yansıtmayabilir. Özellikle siber operasyonlar, yapay zekâ destekli istihbarat faaliyetleri ve dijital etki operasyonları gibi alanlarda, kamuya açık bilgilerin sınırlı ve bazen yanıltıcı olabileceği dikkate alınmalıdır (Arquilla & Ronfeldt, 2020; OECD, 2021).

Teknolojik determinizm ve sosyal inşacılık arasındaki teorik gerilim, araştırmanın dijital teknolojilerin uluslararası ilişkiler üzerindeki etkilerini açıklama kapasitesini etkilemektedir. Teknolojik determinist yaklaşımlar, dijital teknolojilerin kendi iç mantığıyla geliştiğini ve toplumları şekillendirdiğini savunurken, sosyal inşacı perspektifler, teknolojinin sosyal, kültürel ve politik bağlamlarda inşa edildiğini ve bu bağlamlara göre farklı anlamlar kazandığını vurgulamaktadır. Araştırmanın teorik çerçevesinin bu iki yaklaşım arasında dengeyi sağlaması ve teknoloji-toplum etkileşiminin karşılıklı ve dinamik doğasını yansıtması gerekmektedir. Ayrıca dijital teknolojilerin uluslararası ilişkiler üzerindeki etkilerini analiz ederken, devlet merkezli yaklaşımların sınırlılıkları da dikkate alınmalıdır. Devletlerin merkezi rolüne odaklanan geleneksel uluslararası ilişkiler teorileri, teknoloji şirketleri, uluslararası örgütler, sivil toplum kuruluşları ve bireysel aktörler gibi devlet dışı aktörlerin dijital dönemdeki artan önemini tam olarak açıklayamayabilir. Küresel teknoloji şirketlerinin, milyarlarca kullanıcının verilerini kontrol etme ve sınır ötesi dijital altyapıları yönetme kapasitesi, devlet egemenliği ve uluslararası sistemin yapısı hakkındaki geleneksel anlayışları zorlamaktadır. Bu karmaşık aktör etkileşimlerini ve güç dinamiklerini analiz etmek için daha kapsayıcı teorik modellere ihtiyaç vardır (Zuboff, 2019; Fukuyama, 2021).

Alternatif açıklamalar, dijital dönüşümün yalnızca devletlerarası rekabetle sınırlı kalmadığını, büyük teknoloji şirketleri, uluslararası örgütler ve sivil toplum kuruluşlarının da dijitalleşme süreçlerinde giderek daha fazla etkili hale geldiğini öne sürmektedir. Bu bağlamda dijital egemenlik kavramının nasıl yeniden şekilleneceği ve devletlerin dijitalleşme süreçlerindeki rollerinin nasıl değişeceği üzerine daha fazla araştırmaya ihtiyaç duyulmaktadır. Uluslararası ilişkilerin geleneksel devlet merkezli analiz modeli, dijital çağda önemini korumakla birlikte, teknoloji şirketlerinin artan gücü, bu modelin yeniden değerlendirilmesini gerektirmektedir. Google, Amazon,

Facebook, Apple ve Microsoft gibi şirketler, milyarlarca kullanıcının verilerini kontrol etmekte, küresel dijital altyapıları yönetmekte ve yapay zekâ gibi stratejik teknolojilerin gelişimini yönlendirmektedir. Bu şirketlerin sahip olduğu ekonomik, teknolojik ve politik etki, devletlerin geleneksel güç kapasitelerini zorlamakta ve uluslararası ilişkilerde yeni bir aktör kategorisi oluşturmaktadır. Teknoloji şirketlerinin faaliyetleri ve stratejileri, devletlerin dış politika ve güvenlik hedeflerini destekleyebileceği gibi, bu hedeflerle çatışabilir veya bunları engelleyebilir de. Bu karmaşık etkileşimleri anlamak için devlet-şirket ilişkilerini ve bunların uluslararası sistemi nasıl şekillendirdiğini inceleyen yeni teorik modellere ihtiyaç vardır. Ayrıca sivil toplum aktörlerinin, hacker gruplarının ve dijital aktivistlerin artan önemi, dijital teknolojilerin demokratikleştirici potansiyelini vurgulamakta ve güç dağılımının daha yatay hale gelebileceğini göstermektedir (West, 2021; Choucri, 2021).

Bir diğer alternatif açıklama, dijital teknolojilerin uluslararası ilişkilerde köklü değişimler oluşturmaktan ziyade, mevcut güç yapılarını ve jeopolitik dinamikleri pekiştirdiği yönündedir. Bu görüşe göre, dijital teknolojilerin geliştirilmesi ve kontrol edilmesi süreci, zaten güçlü olan devletlerin ve aktörlerin avantajlı konumlarını güçlendirmekte ve mevcut küresel eşitsizlikleri derinleştirmektedir. Örneğin yapay zekâ ve büyük veri analitiği gibi ileri teknolojilerin geliştirilmesi, önemli miktarda sermaye, teknik uzmanlık ve veri gerektirir, bu da bu kaynaklara zaten sahip olan gelişmiş ülkelere ve büyük teknoloji şirketlerine avantaj sağlar. Dijital teknolojilerin küresel Güney ülkeleri üzerindeki etkisi, bu nedenle, teknolojik bağımlılık ve yeni sömürgecilik biçimleri oluşturabilir. Bu "dijital kolonizasyon" perspektifi, dijital teknolojilerin küresel güç ilişkilerindeki yapısal eşitsizlikleri yeniden ürettiğini ve pekiştirdiğini öne sürer. Ayrıca devletlerin dijital teknolojileri gözetim, kontrol ve ulusal güvenlik amaçlarıyla kullanması, bu teknolojilerin özgürleştirici ve demokratikleştirici potansiyelini sınırlandırabilir. Bu alternatif açıklama, dijital teknolojilerin mevcut güç yapılarını ve jeopolitik rekabeti dönüştürmekten çok, bu yapıları ve rekabeti yeni biçimlerde yeniden ürettiğini savunur. Bu perspektif, araştırmanın dijital teknolojilerin dönüştürücü etkilerine yönelik daha iyimser değerlendirmelerine önemli bir karşı argüman sunmaktadır (Morozov, 2021; OECD, 2021).

7. SONUÇ

Dijital teknolojilerin uluslararası ilişkiler disiplininde oluşturduğu epistemolojik dönüşüm, geleneksel teorik yaklaşımların açıklama kapasitesini zorlamaktadır. Bu araştırma, sosyo-teknik sistemlerin devlet davranışlarını nasıl şekillendirdiğini inceleyerek neo-realist paradigmanın ötesinde yeni bir analitik çerçeve önermektedir. Özellikle siber-ontolojik güvenlik, dijital-diplomatik hibridizasyon ve kuantum-algoritmik rekabet gibi olgular, disiplinin kavramsal araçlarının güncellenmesini gerektirmektedir (Nye,

2021; Floridi, 2018). Bulgularımız, yapay zekâ, blok zinciri ve kuantum bilişim teknolojilerinin uluslararası sistem üzerindeki dönüştürücü etkisinin, yalnızca teknik gelişmelerin bir sonucu değil, aynı zamanda siyasi, ekonomik ve sosyal faktörlerin karmaşık bir etkileşimi olduğunu göstermektedir.

Çalışmada benimsenen metodolojik çoğulculuk, dijital dönüşümün çok katmanlı yapısını kavramaya olanak sağlamıştır. Nitel ve yorumlayıcı yöntemlerin, vaka analizleri ve karşılaştırmalı incelemelerle desteklenmesi, araştırmanın analitik derinliğini artırmıştır. Özellikle büyük güçlerin dijital strateji dokümanlarının söylem analizi, teknopolitik dönüşümün jeostratejik boyutlarını aydınlatmıştır (Arquilla & Ronfeldt, 2020; West, 2021). ABD, Çin, Avrupa Birliği ve Rusya'nın dijitalleşme stratejilerinin karşılaştırmalı analizi, bu aktörlerin farklı teknolojik yaklaşımlarını ve dijital egemenlik anlayışlarını ortaya koymuştur.

Post-Vestfalyan dijital düzende, devlet egemenliğinin parametreleri radikal biçimde değişmektedir. Veri hâkimiyeti, algoritma kontrolü ve kuantum üstünlüğü yarışı, klasik güç projeksiyonu araçlarının ötesinde yeni rekabet alanları oluşturmaktadır (Singer & Brooking, 2019; Zuboff, 2019). Platform devletleri ve dijital imparatorluklar gibi yeni aktör tipolojileri, uluslararası sistemin yapısal dönüşümünü hızlandırmaktadır. Devletlerin dijital egemenlik anlayışlarındaki farklılıklar, internetin parçalanması (splinternet) riskini artırmakta ve küresel dijital yönetişim için çok paydaşlı modellerin geliştirilmesini zorunlu kılmaktadır.

Bulgular, yapay zekâ destekli diplomasinin uluslararası müzakere süreçlerini nasıl dönüştürdüğünü ortaya koymaktadır. Algoritmik karar destek sistemleri, stratejik öngörü mekanizmaları ve simülasyon tabanlı senaryo analizleri, diplomatik pratiğin dijital-analog hibritleşmesine yol açmaktadır (Choucri, 2021; Fukuyama, 2021). Bu dönüşüm, diplomatik teorinin temel varsayımlarının yeniden değerlendirilmesini gerektirmektedir. Yapay zekâ destekli diplomatik analiz sistemleri, büyük miktarda veriyi işleyerek diplomatların karar alma süreçlerini optimize etmekte, ancak aynı zamanda algoritmik önyargı ve şeffaflık sorunu gibi yeni etik zorluklar da oluşturmaktadır.

Meta-uzay diplomasisi ve siber-fiziksel çatışma yönetimi, güvenlik çalışmalarında yeni araştırma gündemleri oluşturmaktadır. Özellikle otonom silah sistemleri, kuantum sensörler ve yapay zekâ destekli istihbarat analizi, stratejik düşüncenin evrimini hızlandırmaktadır (Arquilla & Ronfeldt, 2020; Singer & Brooking, 2019). Bu gelişmeler, caydırıcılık teorisinin dijital çağa adaptasyonunu zorunlu kılmaktadır. Siber saldırıların atfedilmesindeki zorluklar, orantılı karşılık ilkesinin uygulanmasındaki belirsizlikler ve siber-nükleer etkileşim riskleri, güvenlik teorisyenlerinin ele alması gereken kritik konular haline gelmiştir.

Blok zinciri teknolojilerinin oluşturduğu merkeziyetsiz yönetişim mimarisi, uluslararası finansal sistemin onto-politik temellerini sarsmaktadır. Bretton Woods sonrası para politikası araçları ve merkez bankacılığı pratikleri, dijital değer transfer protokolleri karşısında etkinliğini yitirmektedir (Brynjolfsson & McAfee, 2019; Floridi, 2018). Küresel finans sisteminin bu tekno-politik dönüşümü, ekonomik diplomasinin geleneksel enstrümanlarını yetersiz kılmaktadır. Merkez Bankası Dijital Para Birimleri (CBDC) ile merkeziyetsiz finans (DeFi) sistemleri arasındaki rekabet, para politikası kontrolü ve finansal egemenlik kavramlarını yeniden tanımlamaktadır.

Araştırmanın özgün katkılarından biri, kuantum enformasyon sistemlerinin uluslararası güvenlik paradigması üzerindeki dönüştürücü etkisini kavramsallaştırmasıdır. Post-kuantum kriptografi yarışı, devletlerin istihbarat kapasitelerini ve siber savunma doktrinlerini kökten değiştirmektedir (West, 2021; Nye, 2021). Bu dönüşüm, güvenlik çalışmalarında yeni bir teorik çerçeveyi gerekli kılmaktadır. Kuantum bilgisayarların gelişimi ve kuantum kriptografinin ilerlemesi, siber güvenlik stratejilerini, şifreleme standartlarını ve istihbarat toplama yöntemlerini temelden değiştirme potansiyeline sahiptir.

Dijital haklar rejiminin gelişimi, uluslararası hukuk teorisinde normatif bir dönüşümü tetiklemektedir. Veri egemenliği, algoritmik şeffaflık ve yapay zekâ etiği gibi yeni nesil haklar, küresel yönetişimin normatif altyapısını yeniden şekillendirmektedir (Floridi, 2018; West, 2021). Bu süreç, insan hakları hukukunun dijital çağa adaptasyonunu zorunlu kılmaktadır. Özellikle yapay zekâ sistemlerinde gömülü olan önyargıların ve ayrımcılığın önlenmesi, algoritmaların hesap verebilirliğinin sağlanması ve dijital gözetim teknolojilerinin insan hakları standartlarına uygun şekilde düzenlenmesi, hukuki çerçevelerin geliştirilmesini gerektirmektedir.

Teknolojik bağımlılık ve dijital kırılganlık, devletlerin stratejik özerklik arayışlarını derinleştirmektedir. Yarı iletken tedarik zincirleri, bulut altyapıları ve yapay zekâ ekosistemlerindeki bağımlılıklar, yeni bir jeopolitik rekabet alanı oluşturmaktadır (Fukuyama, 2021; Choucri, 2021). Dijital endüstri politikaları ve teknolojik milliyetçilik, bu rekabetin temel parametrelerini oluşturmaktadır. ABD, Çin ve AB arasındaki teknolojik rekabet yalnızca ekonomik üstünlük için değil, aynı zamanda gelecekteki uluslararası sistemin normlarını ve kurallarını belirlemek için de yürütülmektedir.

Siber-uzayın militarizasyonu, uluslararası hukukta yeni doktrinel yaklaşımları gerekli kılmaktadır. Siber saldırıların atfedilebilirliği, dijital misilleme hakları ve otonom sistemlerin kullanımına ilişkin normlar, jus ad bellum ve jus in bello prensiplerinin yeniden yorumlanmasını gerektirmektedir (Singer & Brooking, 2019; Arquilla & Ronfeldt, 2020). Tallinn Kılavuzu gibi girişimler, siber alanın uluslararası hukuk çerçevesinde nasıl düzenle-

neceğine dair önemli katkılar sağlamakla birlikte, devletlerarasında bu konuda henüz bir uzlaşı sağlanamamıştır.

Araştırmanın metodolojik kısıtları arasında, dijital teknolojilerin hızlı evrimi nedeniyle bulguların geçerlilik süresinin sınırlı olması ve devletlerin siber kapasitelerine ilişkin verilerin güvenilirlik sorunları bulunmaktadır (Nye, 2021; OECD, 2021). Bu kısıtlar, gelecek araştırmacıların daha dinamik ve adaptif metodolojik yaklaşımlar geliştirmesini gerektirmektedir. Ayrıca disiplinler arası yaklaşımların güçlendirilmesi, dijital teknolojilerin teknik, sosyal, politik ve etik boyutlarının bütüncül bir şekilde anlaşılması için hayati önem taşımaktadır.

Platform kapitalizmi ve dijital gözetim pratikleri, uluslararası politik ekonominin yapısal dönüşümünü hızlandırmaktadır. Veri ekstraktivizmi, algoritmik değer üretimi ve dijital emek süreçleri, küresel ekonomi politiğin yeni analitik kategorilerini oluşturmaktadır (Zuboff, 2019; Morozov, 2021). Gözetim kapitalizmi olarak adlandırılan bu yeni ekonomik model, büyük teknoloji şirketlerinin veri toplama ve işleme kapasitelerini kullanarak insan deneyimini metalaştırma sürecini ifade etmektedir.

Meta-sistem dönüşümü yaşanan bu dönemde, politik uygulayıcılar için dört stratejik öncelik öne çıkmaktadır: dijital ekosistem direncinin güçlendirilmesi, kuantum-güvenli altyapıların geliştirilmesi, algoritmik yönetişim standartlarının oluşturulması ve dijital haklar rejiminin kurumsallaştırılması (Floridi, 2018; OECD, 2021). Bu öncelikler, dijital teknolojilerin yıkıcı potansiyelini sınırlarken, olumlu etkilerini maksimize etmeyi amaçlamaktadır.

Gelecek araştırmacılar için özellikle üç alan kritik önem taşımaktadır: kuantum diplomasinin uluslararası müzakere süreçlerine etkisi, yapay zekâ sistemlerinin stratejik karar alma mekanizmalarını dönüştürme biçimleri ve blok zinciri teknolojilerinin küresel yönetişim mimarisini yeniden yapılandırma potansiyeli (Brynjolfsson & McAfee, 2019; West, 2021). Bu alanlar, disiplinler arası yaklaşımlarla incelenmesi gereken kompleks araştırma konuları sunmaktadır.

Dijital çağın normatif altyapısının inşası, uluslararası toplumun en acil gündemlerinden birini oluşturmaktadır. Siber silahların kontrolü, yapay zekâ etiği ve veri koruma standartları gibi alanlarda küresel bir uzlaşının sağlanması, dijital barış ve istikrar için hayati önem taşımaktadır (Singer & Brooking, 2019; Floridi, 2018). Bu normatif altyapı, devletlerin, teknoloji şirketlerinin, sivil toplum kuruluşlarının ve uluslararası örgütlerin katılımıyla çok paydaşlı bir süreçte geliştirilmelidir.

Disiplinler arası diyaloğun güçlendirilmesi, dijital dönüşümün çok boyutlu etkilerinin kavranması için elzemdir. Bilgisayar bilimleri, sibernetik,

kuantum fiziği ve politik teorinin kesişiminde yeni bir epistemolojik çerçevenin geliştirilmesi gerekmektedir (Choucri, 2021; Fukuyama, 2021). Bu epistemolojik çerçeve, teknolojinin yalnızca bir araç değil, aynı zamanda politik, sosyal ve ontolojik dönüşümün aktif bir ajanı olduğunu kabul etmelidir.

Çalışmanın en önemli teorik katkısı, dijital dönüşümün uluslararası ilişkiler disiplininde oluşturduğu paradigmatik kırılmayı sistematik biçimde kavramsallaştırmasıdır. Önerilen analitik çerçeve, teknoloji-toplum-politika etkileşiminin yeni boyutlarını anlamamıza olanak sağlamaktadır (Nye, 2021; Zuboff, 2019). Bu çerçeve, dijital teknolojilerin gelişiminin yalnızca teknik bir süreç değil, aynı zamanda sosyal, kültürel ve politik faktörlerle şekillenen kompleks bir fenomen olduğunu vurgulamaktadır.

Sonuç olarak, dijital çağda uluslararası ilişkilerin dönüşümü, disiplinin teorik araçlarının ve metodolojik yaklaşımlarının kapsamlı bir revizyonunu gerektirmektedir. Bu dönüşümün başarılı yönetimi, akademik araştırmaların, politik uygulamaların ve kurumsal adaptasyonun eşgüdümlü gelişimini zorunlu kılmaktadır (Floridi, 2018; Choucri, 2021). Dijital teknolojilerin şekillendirdiği dünyada barış, güvenlik ve refah için yeni bir uluslararası sistem mimarisinin oluşturulması, 21. yüzyılın en önemli politik ve entelektüel zorluklarından biri olmaya devam edecektir.

KAYNAKÇA

Kitaplar

Akçay, B. (2021). Dijital Diplomasi ve Uluslararası İlişkilerde Yeni Paradigmalar. İstanbul: Beta Yayınları.

Arı, T. (2019). Uluslararası İlişkiler Teorileri ve Günümüz Dünyası. İstanbul: Der Yayınları.

Arquilla, J., & Ronfeldt, D. (2020). The Cyberwarfare Age: Strategic Perspectives. Oxford: Oxford University Press.

Balcı, A. (2020). Dış Politika Analizi. İstanbul: Küre Yayınları.

Bayraktutan, Y. (2022). Siber Güvenlik ve Uluslararası Politika. Ankara: Nobel Yayıncılık.

Brynjolfsson, E., & McAfee, A. (2019). The Second Machine Age: Work, Progress, and Prosperity in a Time of Brilliant Technologies. New York: W.W. Norton & Company.

Castells, M. (2020). Networks of Outrage and Hope in the Digital Age. Cambridge: Polity Press.

Choucri, N. (2021). Cyberpolitics in International Relations. Cambridge, MA: MIT Press.

Çınar, Ö. (2021). Blok Zinciri ve Dijital Ekonomi: Hukuki ve Ekonomik Perspektifler. İstanbul: Seçkin Yayıncılık.

Floridi, L. (2018). The Fourth Revolution: How the Infosphere is Reshaping Human Reality. Oxford: Oxford University Press.

Fuchs, C. (2020). Social Media: A Critical Introduction. SAGE Publications.

Gök, M. (2020). Uluslararası Hukukta Dijitalleşme ve Devlet Egemenliği. Ankara: Yetkin Yayınları.

Kahraman, S. (2018). Siber Savaş ve Dijital Güvenlik Politikaları. Ankara: Palme Yayıncılık.

Kardaş, Ş. (2019). Büyük Veri ve Uluslararası İlişkiler. İstanbul: Bilgi Üniversitesi Yayınları.

Morozov, E. (2021). The Geopolitics of Digital Sovereignty. PublicAffairs.

Nye, J. (2020). The Future of Power. New York: PublicAffairs.

Öztürk, M. (2021). Yapay Zekâ Çağında Uluslararası Siyaset. Ankara: Siyasal Kitabevi.

Schwab, K. (2018). The Fourth Industrial Revolution. Geneva: World Economic Forum.

Singer, P. W., & Brooking, E. T. (2019). LikeWar: The Weaponization of Social Media. Boston: Houghton Mifflin Harcourt.

Smith, M. R., & Marx, L. (1994). Does Technology Drive History? The Dilemma of Technological Determinism. MIT Press.

Taş, M. (2017). Küreselleşme, Teknoloji ve Uluslararası Politikalar. İstanbul: Alfa Yayınları.

West, D. M. (2021). The Future of Work: Robots, AI, and Automation. Washington, D.C.: Brookings Institution Press.

Wendt, A. (1999). Social Theory of International Politics. Cambridge University Press.

Zuboff, S. (2019). The Age of Surveillance Capitalism: The Fight for a Human Future at the New Frontier of Power. PublicAffairs.

Akademik Makaleler

Abrahams, R. (2022). "Artificial Intelligence in Global Politics," International Security Review, 45(1), 112-137.

Aydın, Z. (2022). "Dijitalleşme ve Küresel Güç Dengeleri," Uluslararası İlişkiler Dergisi, 19(3), 55-78.

Cohen, B. J. (2021). "Cryptocurrencies and the Future of International Finance," Financial Policy Journal, 28(2), 90-118.

Demir, E. (2021). "Yapay Zekânın Uluslararası Güvenlik Politikalarına Etkisi," Güvenlik Bilimleri Dergisi, 14(2), 101-125.

Erdem, T. (2020). "Siber Saldırılar ve Uluslararası Hukuk," Türkiye Barolar Birliği Dergisi, 12(4), 33-57.

Floridi, L. (2018). "Ethics of AI and Big Data in International Relations," Ethics & Information Technology, 20(3), 95-112.

Fukuyama, F. (2021). "AI and the Future of Global Order," Foreign Affairs, 100(3), 118-132.

Kılıç, B. (2019). "Blok Zinciri Teknolojisinin Küresel Finans Üzerindeki Etkileri," İktisat ve Yönetim Araştırmaları Dergisi, 17(2), 85-110.

Morozov, E. (2021). "The Geopolitics of Digital Sovereignty," Foreign Affairs, 99(6), 22-49.

Öner, H. (2021). "Sosyal Medya ve Dijital Propaganda," Siyasal Araştırmalar Dergisi, 10(1), 44-72.

Şahin, R. (2018). "Metaverse ve Uluslararası İlişkiler," İletişim Bilimleri Dergisi, 15(3), 67-89.

Tekin, C. (2022). "Kuantum Bilişim ve Dijital Dönüşüm," Teknoloji ve Toplum Araştırmaları Dergisi, 9(2), 30-50.

Williams, R. (2019). "Quantum Computing and Global Security," Strategic Studies Quarterly, 13(2), 33-57.

Yılmaz, D. (2020). "Dijital Haklar ve Uluslararası Hukuk," Hukuk ve İnsan Hakları Dergisi, 14(3), 92-116.

Resmi Raporlar ve Çalışmalar

Brookings Institution. (2020). Disinformation and AI-Driven Propaganda Mechanisms.

BTK. (2020). Siber Güvenlik Raporu: Türkiye ve Dünya Trendleri.

European Commission. (2021). Digital Transformation and Policy Implications for EU.

IMF. (2021). The Economic Impact of AI and Blockchain on Global Finance.

NATO. (2021). Cyber Security Strategies in a Multipolar World.

OECD. (2022). AI, Big Data, and International Governance Trends.

RAND Corporation. (2021). Strategic AI Applications in Defense and Security.

SETA. (2022). Dijital Diplomasi ve Geleceğin Uluslararası Politikaları.

TEPAV. (2020). Türkiye'de Dijital Finansın Geleceği ve Düzenleyici Çerçeve.

TÜBİTAK. (2021). Dijital Ekonomi ve Blok Zinciri Teknolojisi Üzerine Analizler.

Türkiye Cumhuriyeti Dışişleri Bakanlığı. (2021). Dijital Dönüşüm ve Dış Politika Stratejileri.

Türkiye Cumhuriyeti Sanayi ve Teknoloji Bakanlığı. (2022). Türkiye'nin Yapay Zekâ Yol Haritası.

UNDP Türkiye. (2021). Dijitalleşme ve İnsan Hakları Üzerine Rapor.

United Nations. (2022). Artificial Intelligence and Human Rights.

World Economic Forum. (2020). The Future of Digital Currencies and Global Trade.