



T.C.
BANDIRMA ONYEDİ EYLÜL ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİM DALI

Yüksek Lisans Tezi

SİBER SAVUNMA STRATEJİLERİNDE YAPAY ZEKA
ENTEGRASYONUN ETKİSİ

Nisa KEFELİOĞLU
2215052016

Tez Danışmanı:
Dr. Öğr. Üyesi Zeynep ÖZER

Bandırma 2025

T.C.
BANDIRMA ONYEDİ EYLÜL ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
YÖNETİM BİLİŞİM SİSTEMLERİ ANABİLİM DALI

Yüksek Lisans Tezi

SİBER SAVUNMA STRATEJİLERİNDE YAPAY ZEKA
ENTEGRASYONUN ETKİSİ

NİSA KEFELİOĞLU
2215052016

Tez Danışmanı:
Dr. Öğr. Üyesi Zeynep ÖZER

Bandırma 2025

ETİK BEYAN
TÜRKİYE CUMHURİYETİ
BANDIRMA ONYEDİ EYLÜL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Bu belge ile, bu tezdeki bütün bilgilerin akademik kurallara ve etik ilkelere uygun olarak toplanıp sunulduğunu beyan ederim. Bu kural ve ilkelerin gereği olarak, çalışmada bana ait olmayan tüm veri, düşünce ve sonuçları andığımı ve kaynağını gösterdiğimi ayrıca beyan ederim. (24/06/2025)

Nisa KEFELİOĞLU

ÖZET

SİBER SAVUNMA STRATEJİLERİNDE YAPAY ZEKA ENTEGRASYONUN ETKİSİ

Nisa KEFELİOĞLU

Bu çalışmada siber savunma stratejilerinde yapay zeka entegrasyonunun etkileri incelenmiştir. Günümüzde dijitalleşmenin hızla artmasıyla birlikte siber tehditlerin karmaşıklığı ve etkinliği önemli ölçüde yükselmiştir. Bu bağlamda geleneksel siber güvenlik önlemlerinin yetersiz kaldığı durumlar ortaya çıkmış ve yapay zeka tabanlı çözümlerin siber savunma sistemlerine entegrasyonu kaçınılmaz bir gereklilik haline gelmiştir. Çalışmada yapay zeka teknolojilerinin siber tehditlerin tespiti, analizi, sınıflandırılması ve bertaraf edilmesi süreçlerindeki rolü ele alınmış ve bu teknolojilerin savunma sistemlerine sağladığı avantajlar ortaya konmuştur. Özellikle makine öğrenimi, derin öğrenme ve doğal dil işleme gibi yapay zeka yöntemlerinin, anomali tespiti, tehdit istihbaratı, otomatik yanıt mekanizmaları ve saldırı tahmini konularında nasıl bir dönüşüm sağladığı incelenmiştir. Çalışmanın teorik çerçevesi oluşturulurken, yapay zekanın siber güvenlikteki kullanım alanları ve bu alandaki güncel literatür değerlendirilmiştir. Yapay zekanın siber savunmadaki etkinliğini artıran faktörler ve bu entegrasyonun zorlukları ele alınmıştır. Yapılan incelemelerde yapay zeka destekli güvenlik sistemlerinin, büyük hacimli verileri analiz edebilme, bilinmeyen tehditleri tespit edebilme ve saldırılara gerçek zamanlı tepki verme gibi yetenekleri sayesinde geleneksel yöntemlere kıyasla daha güçlü bir koruma sağladığı gözlemlenmiştir. Çalışmada ayrıca farklı ülkelerin ve kurumların yapay zeka destekli siber güvenlik stratejileri karşılaştırmalı olarak incelenmiş ve başarılı uygulama örnekleri analiz edilmiştir. Bu çerçevede yapay zeka entegrasyonunun siber savunma stratejilerinde devrim niteliğinde değişiklikler yarattığı ve gelecekte daha sofistike saldırı ve savunma mekanizmalarının ortaya çıkacağı sonucuna varılmıştır.

Anahtar Sözcükler: Entegrasyon, Savunma, Siber, Strateji, Yapay Zeka

ABSTRACT

THE IMPACT OF ARTIFICIAL INTELLIGENCE INTEGRATION IN CYBER DEFENSE STRATEGIES

Nisa KEFELİOĞLU

In this study, the implications of artificial intelligence integration into cyber defense systems are examined. Nowadays, with the rapid expansion in digitalization, the complexity and effectiveness of cyber attacks have increased exponentially. In this context, there have been scenarios in which traditional cyber security mechanisms are not sufficient and artificial intelligence-based solution integration into cyber defense systems becomes an inevitable necessity. In the study, the application of artificial intelligence technologies in detection, analysis, classification and elimination of cyber threats is described and the advantages of these technologies to defense systems are revealed. In particular, it is examined how artificial intelligence methods such as machine learning, deep learning and natural language processing reshape anomaly detection, threat intelligence, automated response systems and attack prediction. While developing the research theoretical framework, the fields of application of artificial intelligence in cyber security and the literature available in this field were studied. The factors facilitating the performance of artificial intelligence in cyber defense and the difficulties of their integration are discussed. In the tests, it was observed that artificial intelligence-supported security systems are more secure than traditional methods because of their capabilities such as processing high volumes of data, detecting unknown threats, and reacting to attacks in real time. In the study, artificial intelligence-supported cyber security policies of different countries and institutions were comparatively examined and successful implementation examples were researched. In this context, it has been established that the use of artificial intelligence has come up with groundbreaking changes in cyber defense systems and that even more sophisticated attack and defense systems will be created in the future.

Keywords: Artificial Intelligence, Cyber, Defense, Integration, Strategy

ÖNSÖZ

Bu tez çalışması, Siber Savunma Stratejilerinde Yapay Zeka Entegrasyonun Etkilerini, ele alarak siber tehditlerin tespiti, analizi, sınıflandırılması ve bertaraf edilmesi süreçlerindeki rolü ele alınmış ve bu teknolojilerin savunma sistemlerine sağladığı avantajlar ortaya konmuştur. Makine öğrenimi, derin öğrenme ve doğal dil işleme gibi yapay zeka yöntemlerinin, anomali tespiti, tehdit istihbaratı, otomatik yanıt mekanizmaları ve saldırı tahmini konularında nasıl bir dönüşüm sağladığı incelenmiştir. Bu çalışmayı hazırlarken, alanın güncel dinamiklerini takip etmek ve akademik bir bakış açısıyla değerlendirme yapmak, benim için hem öğretici hem de ilham verici bir süreç oldu. Tez süreci boyunca bana rehberlik eden, bilgi ve tecrübeleriyle yolumu aydınlatan değerli danışmanım Dr. Öğr. Üyesi Zeynep ÖZER'e teşekkürlerimi sunarım. Ayrıca akademik yolculuğumda bana destek olan aileme, arkadaşlarıma ve katkı sağlayan tüm paydaşlara minnettarım.

Bu tezin, hem akademik literatüre katkı sağlaması hem de uygulayıcılar için yol gösterici olması dileğiyle.

Nisa KEFELİOĞLU

Bandırma 2025

İÇİNDEKİLER

ETİK BEYAN	i
ÖZET.....	ii
ABSTRACT	iii
ÖNSÖZ.....	iv
İÇİNDEKİLER	v
TABLolar.....	vii
ŞEKİLLER	ix
KISALTMALAR.....	x
1. GİRİŞ	1
1.1. Çalışmanın Amacı	2
1.2. Çalışmanın Önemi.....	3
1.3. Çalışmanın Kapsamı	4
1.4. Çalışmanın Sınırlılıkları	5
2. KAVRAMSAL ÇERÇEVE.....	6
2.1. Siber Güvenlik ve Savunma Stratejileri.....	6
2.1.1. Siber Güvenlik Kavramı	8
2.1.2. Siber Saldırıları ve Tehdit Türleri	9
2.1.3. Geleneksel Siber Savunma Yöntemleri.....	11
2.2. Yapay Zeka ve Siber Güvenlik.....	13
2.2.1. Yapay Zekanın Tanımı ve Gelişim Süreci	16
2.2.2. Yapay Zeka Türleri ve Uygulama Alanları	17
2.2.3. Siber Güvenlikte Yapay Zeka Kullanımı	19
2.3. Siber Savunmada Yapay Zeka Entegrasyonu.....	22
2.3.1. Yapay Zeka Destekli Tehdit Tespit Sistemleri.....	24
2.3.2. Otomasyon ve Anomali Tespiti	26
2.3.3. Makine Öğrenimi ile Saldırı Önleme	29
2.4. Siber Savunma Stratejilerinde Yapay Zeka Örnekleri.....	30
2.4.1. Dünyada Siber Güvenlik	33
2.4.2. Türkiye'de Siber Güvenlik	36

3. YÖNTEM.....	39
3.1. Araştırma Deseni.....	39
3.2. Evren ve Örneklem	39
3.3. Veri Toplama Süreci	40
3.4. Veri Toplama Araçları	40
3.5. Veri Analizi.....	41
4. BULGULAR.....	42
5. TARTIŞMA.....	93
6. SONUÇ VE ÖNERİLER.....	98
KAYNAKÇA.....	100

TABLÖLAR

Tablo 1: Siber Güvenlik Farkındalığı ve Davranışları	42
Tablo 2: Verinin Faktör Analizine Uygunluğu	44
Tablo 3: Siber Güvenlik Farkındalığı ve Davranışları Ölçeğine Ait Açıklayıcı Faktör Analizi ve Güvenilirlik Sonuçları	44
Tablo 4: Risk Algısı ve Yapay Zeka Destekli Güvenlik Önlemleri.....	45
Tablo 5: Verinin Faktör Analizine Uygunluğu	47
Tablo 6: Risk Algısı ve Yapay Zeka Destekli Güvenlik Önlemleri Ölçeğine Ait Açıklayıcı Faktör Analizi ve Güvenilirlik Sonuçları.....	47
Tablo 7: Kurumsal ve Bireysel Siber Güvenlik Politikaları.....	49
Tablo 8: Verinin Faktör Analizine Uygunluğu	50
Tablo 9: Kurumsal ve Bireysel Siber Güvenlik Politikaları Ölçeğine Ait Açıklayıcı Faktör Analizi ve Güvenilirlik Sonuçları	51
Tablo 10: Siber Zorbalık ve Dijital Güvenlik.....	52
Tablo 11: Verinin Faktör Analizine Uygunluğu	54
Tablo 12: Siber Zorbalık ve Dijital Güvenlik Ölçeğine Ait Açıklayıcı Faktör Analizi ve Güvenilirlik Sonuçları	54
Tablo 13: Siber Güvenlik Tehdit Farkındalığı.....	56
Tablo 14: Verinin Faktör Analizine Uygunluğu	57
Tablo 15: Siber Güvenlik Tehdit Farkındalığı Ölçeğine Ait Açıklayıcı Faktör Analizi ve Güvenilirlik Sonuçları	58
Tablo 16: Yapay Zeka ile Desteklenen Güvenlik Çözümleri	59
Tablo 17: Verinin Faktör Analizine Uygunluğu	61
Tablo 18: Yapay Zeka ile Desteklenen Güvenlik Çözümleri Ölçeğine Ait Açıklayıcı Faktör Analizi ve Güvenilirlik Sonuçları	62
Tablo 19: Siber Güvenlik Stratejileri ve Politikalar	64
Tablo 20: Verinin Faktör Analizine Uygunluğu	65
Tablo 21: Siber Güvenlik Stratejileri ve Politikalar Ölçeğine Ait Açıklayıcı Faktör Analizi ve Güvenilirlik Sonuçları.....	66
Tablo 22: Siber Güvenlik Tehditleri ve Savunma Mekanizmaları	68
Tablo 23: Verinin Faktör Analizine Uygunluğu	69
Tablo 24: Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeğine Ait Açıklayıcı Faktör Analizi ve Güvenilirlik Sonuçları.....	70
Tablo 25: Katılımcıların Demografik Özelliklerine Ait Dağılımlar.....	72
Tablo 26: Ölçek ve Alt Boyutlara Ait Tanımlayıcı İstatistikler (n = 132).....	73

Tablo 27: Cinsiyete Göre Ölçek ve Alt Boyutların Karşılaştırılması (Mann-Whitney U Testi Sonuçları).....	76
Tablo 28: Yaş Gruplarına Göre Ölçek ve Alt Boyutların Karşılaştırılması (Kruskal-Wallis Testi Sonuçları)	77
Tablo 29: Eğitim Düzeyine Göre Ölçek ve Alt Boyutların Karşılaştırılması (Kruskal-Wallis Testi Sonuçları)	79
Tablo 30: Mesleğe Göre Ölçek ve Alt Boyutların Karşılaştırılması (Kruskal-Wallis Testi Sonuçları)	80
Tablo 31: Siber Güvenlik Eğitimi Alıp Almama Durumuna Göre Ölçek ve Alt Boyutların Karşılaştırılması	82
Tablo 32: Ölçek ve Alt Boyutlar Arasındaki Korelasyonlar (Spearman Korelasyon Katsayıları).....	85

ŞEKİLLER

Şekil 1: Risk Algısı ve Yapay Zeka Destekli Güvenlik Önlemleri Ölçeğine Ait Açımlayıcı Faktör Analizi Grafiği	47
Şekil 2: Siber Zorbalık ve Dijital Güvenlik Ölçeğine Ait Açımlayıcı Faktör Analizi Grafiği	54
Şekil 3: Siber Güvenlik Tehdit Farkındalığı Ölçeğine Ait Açımlayıcı Faktör Analizi Grafiği	58
Şekil 4: Yapay Zeka ile Desteklenen Güvenlik Çözümleri Ölçeğine Ait Açımlayıcı Faktör Analizi Grafiği	62
Şekil 5: Siber Güvenlik Stratejileri ve Politikalar Ölçeğine Ait Açımlayıcı Faktör Analizi Grafiği	66
Şekil 6: Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeğine Ait Açımlayıcı Faktör Analizi Grafiği	70

KISALTMALAR

AI	: Artificial Intelligence
APT	: Gelişmiş Kalıcı Tehdit
BTK	: Bilgi Teknolojileri ve İletişim Kurumu
CSS	: Center for Security Studies
DARPA	: Defense Advanced Research Projects Agency
DDoS	: Dağıtılmış Hizmet Dışı Bırakma Saldırısı
ENISA	: European Union Agency for Cybersecurity
GDPR	: Genel Veri Koruma Yönetmeliği
GCHQ	: Government Communications Headquarters
HAVELSAN	: Hava Elektronik Sanayi ve Ticaret A.Ş.
IBM	: International Business Machines Corporation
IDS/IPS	: Intrusion Detection System / Intrusion Prevention System
IoT	: Nesnelerin İnterneti
KVKK	: Kişisel Verileri Koruma Kurumu
NATO	: North Atlantic Treaty Organization
NSA	: National Security Agency
SOC	: Security Operations Center
TÜBİTAK	: Türkiye Bilimsel ve Teknolojik Araştırma Kurumu
USOM	: Ulusal Siber Olaylara Müdahale Merkezi

1. GİRİŞ

Dijitalleşmenin hızla yayılmasıyla birlikte bireylerin, kurumların ve devletlerin siber tehditlere karşı korunma gereksinimi giderek artmaktadır. Günümüzde siber saldırılar, yalnızca bireysel veya kurumsal güvenliği tehdit etmekle kalmamakta, aynı zamanda ulusal güvenlik politikalarının da öncelikli konularından biri haline gelmektedir (Abdulhussein, 2024). Bilgi teknolojilerinin gelişmesi, dijital altyapının genişlemesi ve internet tabanlı hizmetlerin yaygınlaşmasıyla birlikte, siber güvenlik stratejileri daha karmaşık ve çok boyutlu bir hal almaktadır. Geleneksel siber güvenlik yaklaşımları, artan ve evrilen tehditlere karşı yetersiz kalmakta, bu nedenle yapay zeka tabanlı çözümler, savunma sistemlerine entegre edilerek güvenliği daha etkin bir şekilde sağlama amacı taşımaktadır. Bu çerçevede Araya ve King (2022) çalışmasında yapay zekanın askeri savunma ve güvenlik üzerindeki etkileri analiz edilmiştir. Çalışma, yapay zekanın askeri stratejilerdeki potansiyelini ve siber güvenlikle olan etkileşimini değerlendirerek güvenlik alanındaki gelecekteki uygulamalara ışık tutmaktadır. Bu kapsamda Bhardwaj (2023) çalışmasında askeri ve savunma alanındaki siber güvenlik uygulamaları ile yapay zekanın entegrasyonu incelenmiştir. Çalışma, askeri savunma stratejilerinde yapay zekanın nasıl kritik bir rol oynayabileceği ve bu teknolojilerin siber güvenlikteki potansiyelini araştırmaktadır.

Yapay zeka, tehditlerin tespit edilmesi, analiz edilmesi ve bunlara karşı önlemler alınması noktasında kritik bir rol oynamakta, siber saldırıların önceden tahmin edilmesi ve otomatik olarak bertaraf edilmesi süreçlerinde önemli avantajlar sunmaktadır. Siber tehditlerin çeşitlenmesi ve karmaşıklığının artması, savunma mekanizmalarının da sürekli olarak güncellenmesini gerektirmektedir (Aldasoro vd., 2024). Geleneksel güvenlik sistemleri, genellikle imza tabanlı tehdit algılama yöntemlerine dayanmakta ve yalnızca bilinen tehditlere karşı etkili olmaktadır. Bu noktada yapay zeka, makine öğrenimi ve derin öğrenme gibi alt disiplinleri sayesinde bilinmeyen tehditleri öngörebilmekte ve büyük veri analizi ile saldırı paternlerini tanımlayarak hızlı bir şekilde müdahalede bulunabilmektedir (Abdulhussein, 2024; Aldasoro vd., 2024). Bu konu bağlamında Abdulhussein (2024) çalışmasında yapay zeka ve makine öğrenmesinin organizasyonların siber güvenliği üzerindeki etkisi

incelenmiştir. Çalışma, bu teknolojilerin organizasyonlarda nasıl siber güvenlik stratejilerini dönüştürdüğünü ve bu alandaki potansiyel uygulamalarını detaylandırmaktadır. Siber savunma sistemleri, tehdit istihbaratı oluşturma, anomali tespiti yapma ve olaylara otomatik yanıt verme gibi fonksiyonları sayesinde daha güvenli ve sürdürülebilir bir yapı kazanabilmektedir. Yapay zeka destekli siber savunma sistemlerinin sağladığı en büyük avantajlardan biri, büyük hacimli verilerin hızlı ve etkin bir şekilde analiz edilmesidir (Aldhamer, 2024). Geleneksel yöntemlerle bir saldırının tespit edilmesi ve müdahale edilmesi zaman alırken, yapay zeka tabanlı sistemler tehditleri gerçek zamanlı olarak değerlendirebilmekte ve saldırılara karşı proaktif önlemler alabilmektedir. Bu çerçevede algoritmik önyargılar, yanlış pozitif veya negatif tespitler, etik ve hukuki sorunlar gibi konular, yapay zekanın siber güvenlik alanında uygulanabilirliğini ve etkinliğini doğrudan etkilemektedir (Alowaidi vd., 2023). Bu kapsamda Das ve Sandhane (2021) çalışmasında yapay zekanın siber güvenlikteki kullanım alanları ele alınmıştır. Çalışma, AI'nın siber güvenlikteki uygulamalarını ve bu teknolojinin güvenlik süreçlerini nasıl iyileştirdiğini incelemektedir. Tüm bunlarla beraber yönetim bilişim sistemleri kurumların bilgi altyapılarını etkin bir şekilde yönetmelerini, stratejik karar alma süreçlerini desteklemelerini ve operasyonel verimliliklerini artırmalarını sağlayan çok disiplinli bir alandır. Bu bağlamda siber güvenlik unsurları YBS'nin ayrılmaz bir parçası haline gelmektedir. Kurumların dijital varlıklarını koruma yükümlülüğü, yalnızca teknik bir mesele olarak değil, aynı zamanda yönetsel ve organizasyonel bir sorumluluk olarak da değerlendirilmektedir. YBS perspektifinden bakıldığında, siber güvenlik yalnızca bilişim teknolojilerinin değil, aynı zamanda risk yönetimi, bilgi yönetimi, iç kontrol sistemleri ve politika geliştirme süreçlerinin de merkezinde yer almaktadır. Günümüzde kurumlar, veri güvenliği, sistem bütünlüğü ve bilgiye yetkisiz erişimin önlenmesi gibi temel ilkeleri, YBS çerçevesinde yapılandırılmış güvenlik protokolleri ile sağlamaktadır.

1.1. Çalışmanın Amacı

Bu çalışmanın temel amacı, siber savunma stratejilerinde yapay zeka entegrasyonunun etkilerini kapsamlı bir şekilde incelemek ve bu entegrasyonun siber güvenlik sistemlerine sağladığı avantajları, karşılaştığı zorlukları ve geleceğe yönelik

potansiyel gelişim alanlarını değerlendirmektir. Günümüzde siber saldırılar giderek daha karmaşık hale gelmekte ve geleneksel güvenlik sistemleri bu tehditlere karşı yeterli seviyede koruma sağlayamamaktadır. Bu bağlamda yapay zeka tabanlı çözümler, siber güvenlik sistemlerini daha proaktif, hızlı ve etkili hale getirmekte ve saldırıların önceden tespit edilmesini, analiz edilmesini ve otomatik olarak önlenmesini sağlamaktadır. Çalışmada yapay zekanın siber güvenlikte kullanım alanları ve bu teknolojinin tehdit istihbaratı, anomali tespiti, otomatik savunma mekanizmaları ve saldırı önleme sistemleri üzerindeki etkisi değerlendirilmektedir. Makine öğrenimi, derin öğrenme ve doğal dil işleme gibi yapay zeka alt disiplinlerinin siber güvenlik süreçlerine nasıl entegre edildiği, bu entegrasyonun mevcut güvenlik sistemlerinin verimliliğini nasıl artırdığı ele alınmaktadır.

Genel olarak çalışmanın bir diğer amacı, farklı ülkelerde ve kurumsal yapılarda kullanılan yapay zeka tabanlı siber güvenlik stratejilerini karşılaştırmalı olarak incelemek ve başarılı uygulama örnekleri üzerinden bu sistemlerin etkinliğini değerlendirmektir. Farklı sektörlerde ve devlet kurumlarında yapay zeka destekli siber savunma sistemlerinin nasıl uygulandığı, bu sistemlerin ne tür avantajlar sunduğu ve ne gibi zorluklarla karşılaştığı detaylı bir şekilde ele alınmaktadır. Ayrıca siber güvenlik alanında geleceğe yönelik olası gelişmeler ve yapay zeka tabanlı güvenlik sistemlerinin sürdürülebilirliğini artırmak için yapılması gereken iyileştirmeler üzerinde durulmaktadır. Yapay zekanın siber güvenlik sistemlerine entegrasyonunun sağladığı fırsatları ve bu süreçte karşılaşılan temel sorunları ortaya koyarak araştırmacılara, siber güvenlik uzmanlarına ve politika yapıcılara yol göstermektedir. Çalışmanın bulgularının siber güvenlik stratejilerinin geliştirilmesine ve daha güvenli dijital altyapılar oluşturulmasına katkı sağlaması beklenmektedir.

1.2. Çalışmanın Önemi

Siber güvenlik, günümüzün en kritik konularından biri haline gelmekte ve dijitalleşmenin hız kazanmasıyla birlikte önemi giderek artmaktadır. Bilgi teknolojilerinin yaygınlaşması, bireylerin, kurumların ve devletlerin giderek daha fazla dijital platformlara bağımlı hale gelmesine yol açmakta, bu durum ise siber tehditlerin kapsamını genişletmektedir. Geleneksel siber güvenlik yöntemleri, artan saldırı çeşitliliği ve sofistikasyonu karşısında yetersiz kalmakta, bu nedenle daha etkin

ve akıllı çözümlere olan ihtiyaç her geçen gün daha da belirgin hale gelmektedir. Bu noktada yapay zeka tabanlı sistemler, büyük veri analizinden tehdit tespiti, anomali belirlemeden otomatik savunma mekanizmalarına kadar geniş bir yelpazede kritik roller üstlenmekte ve siber savunma stratejilerinin dönüşümüne öncülük etmektedir. Bu çalışmanın önemi, yapay zeka entegrasyonunun siber güvenlik alanındaki etkilerini kapsamlı bir şekilde ele alarak bu teknolojinin sunduğu avantajları ve karşılaşılabileceği zorlukları ortaya koymasından kaynaklanmaktadır.

Yapay zeka destekli sistemlerin saldırıları tespit etme, analiz etme ve önleme süreçlerinde nasıl daha etkili sonuçlar ortaya koyduğu incelenmekte, geleneksel yöntemlerle kıyaslandığında sağladığı katkılar değerlendirilmektedir. Özellikle makine öğrenimi, derin öğrenme ve doğal dil işleme gibi tekniklerin siber tehditlere karşı nasıl kullanıldığı ve gelecekte bu alandaki potansiyel gelişmelerin neler olabileceği üzerine detaylı bir analiz sunulmaktadır. Çalışmanın bir diğer önemli boyutu, siber güvenlikte yapay zeka kullanımının yalnızca teknik avantajlarını değil, aynı zamanda etik, hukuki ve yönetsel etkilerini de ele almasıdır. Yapay zeka destekli güvenlik sistemlerinin önyargılı kararlar verebilmesi, yanlış pozitif veya negatif sonuçlar üretebilmesi gibi potansiyel riskler, güvenlik politikalarının ve algoritmaların nasıl geliştirileceği konusunda kritik sorular ortaya çıkarmaktadır.

1.3. Çalışmanın Kapsamı

Bu çalışma, siber savunma stratejilerinde yapay zeka entegrasyonunun etkilerini kapsamlı bir şekilde ele almakta ve bu entegrasyonun siber güvenlik alanındaki rolünü teorik ve pratik açılardan incelemektedir. Çalışmanın temel odağı, yapay zeka destekli güvenlik sistemlerinin siber tehditleri tespit etme, analiz etme ve bertaraf etme süreçlerindeki etkinliğini değerlendirmek, bu sistemlerin sağladığı avantajları ve karşılaşılabileceği zorlukları ortaya koymaktır. Araştırma, hem teknik hem de yönetsel açılardan siber güvenlik ile yapay zeka ilişkisini detaylandırmakta ve bu alandaki güncel gelişmeleri akademik bir çerçevede tartışmaktadır. Çalışmanın kapsamı içerisinde yapay zeka tabanlı siber güvenlik yaklaşımlarının geleneksel yöntemlerle karşılaştırılması önemli bir yer tutmaktadır. Geleneksel imza tabanlı tehdit algılama sistemlerinin sınırlılıkları analiz edilmekte, yapay zeka ve makine öğrenimi tekniklerinin bu sınırlılıkları nasıl aşabileceği üzerinde durulmaktadır.

Araştırma, farklı sektörlerde ve devlet kurumlarında uygulanan yapay zeka destekli siber güvenlik stratejilerine de odaklanmaktadır. Farklı ülkelerde geliştirilen yapay zeka tabanlı siber savunma sistemleri analiz edilmekte ve bu sistemlerin etkinliği, uygulanabilirliği ve sürdürülebilirliği değerlendirilmektedir. Bu bağlamda, ulusal güvenlik stratejileri kapsamında yapay zeka kullanımına yönelik politikalar ve düzenlemeler de incelenmektedir. Özellikle devlet destekli siber saldırılar, kritik altyapı güvenliği ve siber savaş konularında yapay zekanın rolü, araştırmanın kapsamı dahilinde ele alınmaktadır. Çalışmada teorik çerçevenin yanı sıra güncel akademik çalışmalar ve uygulamalar da incelenmektedir. Mevcut literatür üzerinden yapılan analizlerle, yapay zeka tabanlı siber güvenlik sistemlerinin etkinliği hakkında kapsamlı bir değerlendirme sunulmaktadır. Yapay zekanın siber güvenlikte kullanımına dair akademik araştırmalar, teknik raporlar ve sektörel analizler incelenmekte, bu bağlamda mevcut bilgi birikimine katkı sağlanmaktadır.

1.4. Çalışmanın Sınırlılıkları

Bu çalışma, siber savunma stratejilerinde yapay zeka entegrasyonunun etkilerini kapsamlı bir şekilde ele almayı amaçlamakta olsa da, çeşitli sınırlılıklara tabi olmaktadır. Farklı ülkeler ve kurumlar tarafından geliştirilen siber savunma stratejileri analiz edilmekte, ancak her bir stratejinin uygulanabilirliği ve etkinliği, yerel düzenlemelere, teknoloji altyapısına ve kurumların kaynaklarına bağlı olarak değişiklik göstermektedir. Bu nedenle çalışmada sunulan değerlendirmeler, genel eğilimler ve teorik çerçeve üzerinden yapılmakta olup belirli bir sistem veya ülkeye özgü ayrıntılı vaka analizlerini içermemektedir. Çalışmanın bir diğer sınırlılığı, yapay zeka destekli siber güvenlik sistemlerinin sürekli değişen ve gelişen doğasıdır. Siber tehditler dinamik bir yapı sergilemekte ve saldırganlar, yeni güvenlik teknolojilerini aşmak için sürekli olarak yeni yöntemler geliştirmektedir. Yapay zeka tabanlı güvenlik sistemleri de bu tehditlere karşı kendini güncellemekte ve değişen saldırı tekniklerine uyum sağlamakta fakat araştırma süreci belirli bir zaman dilimi içinde gerçekleştirildiğinden, çalışmada ele alınan teknolojiler, yöntemler ve tehditler, zamanla geçerliliğini yitirebilecek nitelikte olabilmektedir. Bu durum, araştırmanın sonuçlarının ilerleyen yıllarda değişebileceği ve yeni tehdit türlerinin yapay zeka destekli sistemlerin etkinliğini etkileyebileceği anlamına gelmektedir.

2. KAVRAMSAL ÇERÇEVE

2.1. Siber Güvenlik ve Savunma Stratejileri

Siber güvenlik, dijital sistemlerin, ağların, cihazların ve verilerin yetkisiz erişim, saldırı ve zarar görmesine karşı korunmasını amaçlayan bir alan olarak öne çıkmaktadır. Günümüzde siber güvenlik, yalnızca bireysel ve kurumsal düzeyde değil, aynı zamanda ulusal güvenlik politikalarının da temel bileşenlerinden biri haline gelmektedir. Dijitalleşmenin hızlanmasıyla birlikte bireylerin işletmelerin ve devlet kurumlarının internet tabanlı hizmetlere olan bağımlılığı artmakta ve bu durum, siber tehditlerin çeşitlenmesine ve daha karmaşık hale gelmesine neden olmaktadır (Araya ve King, 2022; Arroyo-Figueroa, 2023). Bu bağlamda siber güvenlik stratejileri, siber tehditleri önlemek, saldırılara karşı direnç geliştirmek, saldırı anında hızlı müdahale etmek ve saldırı sonrası sistemleri eski haline döndürmek gibi çok boyutlu bir yapıya sahip bulunmaktadır. Siber güvenlik stratejileri, proaktif ve reaktif yaklaşımlar çerçevesinde şekillenmektedir. Proaktif güvenlik stratejileri, potansiyel tehditleri önceden tespit etmeyi ve önlem almayı amaçlamakta olup, sürekli izleme, tehdit istihbaratı toplama ve güvenlik açıklarını önceden kapatma gibi uygulamaları içermektedir (Bhardwaj, 2023). Bu süreç çerçevesinde Roshanaei vd., (2024) çalışmasında siber güvenliği artırmak için yapay zeka ve makine öğrenmesinin nasıl kullanılabileceği, karşılaşılan zorluklar ve gelecekteki yönelimler ele alınmıştır. Çalışma, bu teknolojilerin siber güvenlikteki potansiyelini değerlendirerek AI ve ML'nin tehdit tespitinde nasıl bir devrim yaratabileceğini inceler. Ayrıca Temara (2024) çalışmasında yapay zekanın gelecekteki siber güvenlik sistemlerinde nasıl kullanılabileceği üzerine odaklanılmıştır. Çalışma, AI'nin siber güvenliği iyileştirecek potansiyel kullanımlarını ve bu alanın gelecekte nasıl şekilleneceğini tartışmaktadır.

Öte yandan reaktif güvenlik stratejileri, bir saldırı gerçekleştikten sonra devreye girerek saldırının etkilerini minimize etmeye ve sistemlerin güvenli bir şekilde yeniden işler hale getirilmesine odaklanmaktadır. Etkili bir siber güvenlik politikası, hem proaktif hem de reaktif yaklaşımları entegre ederek tehditlere karşı kapsamlı bir koruma sağlamaktadır (Binhammad vd., 2024). Modern siber güvenlik stratejileri, çok katmanlı bir yapı üzerine inşa edilmekte olup, ağ güvenliği, uç nokta güvenliği,

veri koruma, kimlik doğrulama sistemleri ve güvenlik duvarları gibi çeşitli bileşenleri içermektedir. Genel olarak Binhammad vd., (2024) çalışmasında yapay zekanın dijital kimlik güvenliğini sağlamak için siber güvenlik alanındaki rolü ele alınmıştır. Çalışma, dijital kimliklerin korunmasında yapay zekanın nasıl bir savunma mekanizması oluşturduğunu ve bu teknolojinin güvenlik sistemlerini nasıl iyileştirdiğini tartışmaktadır. Geleneksel güvenlik önlemleri, genellikle imza tabanlı tehdit algılama sistemlerine dayalı olarak çalışmakta ve bilinen tehditleri tespit ederek engellemeye yönelik çözümler sunmakta ama gelişmiş saldırı yöntemleri, mevcut güvenlik önlemlerini aşma konusunda giderek daha başarılı olmakta ve bu durum, geleneksel güvenlik anlayışının yetersiz kalmasına yol açmaktadır. Bu bağlamda Salem vd., (2024) çalışmasında yapay zeka destekli tespit tekniklerinin siber güvenlik alanındaki gelişmelerinin kapsamlı bir şekilde gözden geçirilmesi yapılmıştır. Çalışma, AI'nin siber güvenlikteki rolünü güçlendiren tespit tekniklerini ve bu teknolojilerin savunma stratejilerindeki yenilikçi kullanımlarını tartışmaktadır.

Günümüzde siber saldırganlar, yapay zeka destekli teknikler, sosyal mühendislik yöntemleri ve sıfır gün açıklarını hedefleyen saldırılar gibi sofistike yaklaşımlar kullanarak savunma sistemlerini devre dışı bırakmaya çalışmaktadır (Bhardwaj, 2023; Binhammad vd., 2024). Siber savunma stratejileri, yalnızca teknik önlemleri değil, aynı zamanda insan faktörünü ve organizasyonel süreçleri de içermektedir. Ayrıca Bonfanti ve Kohler (2020) çalışmasında yapay zekanın siber güvenlikteki rolü ele alınmıştır. Çalışma, yapay zekanın tehdit algılama, siber saldırılara müdahale ve savunma stratejilerinde nasıl bir araç olarak kullanılabileceğini analiz etmektedir. İnsan hatası, siber saldırıların başarıya ulaşmasında önemli bir rol oynamakta ve güvenlik açıklarının büyük bir kısmı, zayıf şifre kullanımı, dikkatsiz veri paylaşımı veya sosyal mühendislik saldırılarına karşı bilinçsiz yaklaşımlar gibi insan kaynaklı faktörlerden kaynaklanmaktadır. Bu nedenle etkili bir siber güvenlik stratejisi oluşturulurken teknik tedbirlerin yanı sıra farkındalık eğitimleri, güvenlik politikaları ve prosedürleri gibi insan odaklı önlemlerin de uygulanması gerekmektedir (Bonfanti, 2020).

2.1.1. Siber Güvenlik Kavramı

Siber güvenlik, bilgi ve iletişim teknolojileri ekosisteminde yer alan dijital varlıkların sistemlerin, ağların ve verilerin kötü niyetli saldırılara, yetkisiz erişimlere, bozulmalara, çalınmalara veya zarar görmeye karşı korunmasını amaçlayan çok disiplinli bir alan olarak tanımlanmaktadır. Günümüzde bireylerden devletlere kadar her seviyede kullanıcı, siber tehditlere maruz kalmakta ve bu tehditler, finansal kayıplardan ulusal güvenlik krizlerine kadar geniş çaplı sonuçlar doğurabilmektedir (Bonfanti ve Kohler, 2020). Siber güvenlik kavramı, yalnızca teknik önlemleri değil, aynı zamanda hukuki, yönetsel, etik ve stratejik yaklaşımları da içermekte ve modern toplumların dijitalleşme sürecinde vazgeçilmez bir unsur haline gelmektedir. Bununla beraber Arroyo-Figueroa (2023) çalışmasında yapay zekanın siber güvenlikte stratejik bir anahtar olarak kullanımı ele alınmıştır. Çalışma, yapay zekanın siber tehditleri tanıma ve bunlara yanıt verme kapasitesini artırarak güvenliği nasıl iyileştirdiğini tartışmaktadır. Siber güvenliğin temel amacı, dijital sistemlerde gizlilik, bütünlük ve erişilebilirlik prensiplerini sağlamaktır. Gizlilik ilkesi, yetkisiz kişilerin verilere erişimini engellemeyi ve bilgi güvenliğini korumayı hedeflemektedir. Bütünlük ilkesi, verilerin izinsiz değiştirilmesini veya bozulmasını önlemekte ve sistemlerin doğruluğunu garanti altına almaktadır. Erişilebilirlik ilkesi ise yetkili kullanıcıların bilgilere ihtiyaç duyduklarında kesintisiz bir şekilde ulaşmasını sağlamaktadır (Bonfanti, 2020; Bonfanti ve Kohler, 2020).

Siber güvenlik kavramı, geleneksel güvenlik anlayışından farklı olarak, dinamik ve sürekli değişen bir tehdit ortamına karşı sürekli güncellenen savunma mekanizmalarını gerektirmektedir (Bonfanti, 2022). Dijitalleşmenin hızla yayılması, saldırganlara daha geniş bir saldırı yüzeyi sunmakta ve siber güvenlik önlemlerinin de giderek daha sofistike hale gelmesini zorunlu kılmaktadır. Siber saldırılar, bireysel düzeyde kişisel verilerin çalınması, kimlik avı saldırıları veya fidye yazılımlarından başlayarak kurumsal düzeyde veri ihlalleri, kritik altyapılara yönelik saldırılar ve devlet destekli siber casusluk faaliyetlerine kadar geniş bir yelpazeye yayılmaktadır. Siber güvenlik kavramı, yalnızca savunma stratejilerini değil, aynı zamanda saldırı ve tehdit aktörlerini de kapsamaktadır (Center for Security Studies, 2019). Siber saldırılar, bireysel hackerlar, organize suç grupları, ideolojik motivasyonla hareket

eden hacktivist gruplar ve devlet destekli siber casusluk operasyonları tarafından gerçekleştirilebilmektedir. Uluslararası arenada siber güvenlik kavramı giderek daha fazla önem kazanmakta ve devletler, siber tehditlerle mücadele etmek amacıyla ulusal güvenlik politikalarına siber savunma stratejilerini entegre etmektedir. NATO, Avrupa Birliği ve Birleşmiş Milletler gibi uluslararası kuruluşlar, siber güvenlik konusunda ortak standartlar belirlemekte ve ülkeler arasında iş birliğini teşvik etmektedir (Bonfanti, 2022; Center for Security Studies, 2019).

2.1.2. Siber Saldırıları ve Tehdit Türleri

Siber saldırılar, bilgisayar sistemlerine, ağlara, yazılımlara veya dijital altyapılara zarar vermek, yetkisiz erişim sağlamak, veri çalmak veya işleyişi bozmak amacıyla gerçekleştirilen kötü niyetli faaliyetler olarak tanımlanmaktadır. Dijitalleşmenin hızla ilerlemesiyle birlikte siber saldırılar giderek daha karmaşık bir hal almakta ve saldırganlar gelişmiş teknikler kullanarak güvenlik açıklarını istismar etmektedir (Chouraik vd., 2024). Ayrıca Özkurt (2020) çalışmasında savunma sanayindeki dijitalleşmenin kurumsal niteliklere etkisi yapay zeka yöntemleri ile öngörülmüştür. Çalışma, Sakarya ili örneği üzerinden savunma sanayi kuruluşlarında dijitalleşmenin nasıl bir etki yarattığını, AI'nın bu dönüşümdeki rolünü ve kurumsal stratejilerin nasıl şekillendiğini araştırmaktadır.

Günümüzde siber saldırılar, bireyleri, şirketleri, devletleri ve kritik altyapıları hedef olarak küresel ölçekte ciddi güvenlik riskleri oluşturmaktadır. Bu saldırılar, finansal kayıplardan itibar zedelenmesine, devletler arası siyasi krizlerden kamu hizmetlerinin aksamasına kadar geniş kapsamlı etkiler yaratmaktadır. Siber saldırılar, farklı teknikler ve motivasyonlarla gerçekleştirilmekte olup saldırganların amaçlarına göre değişiklik göstermektedir. Bazı saldırılar doğrudan finansal kazanç sağlamak amacıyla düzenlenirken, bazıları ise ideolojik, politik veya casusluk amacı taşımaktadır (Çalışkan, 2024). Devlet destekli saldırılar, genellikle rakip ülkelerin bilgi sistemlerini hedef almakta ve siber savaş unsuru olarak kullanılmaktadır. Bunun yanı sıra organize suç grupları, bireysel hackerlar ve hacktivist gruplar da siber saldırıları gerçekleştiren aktörler arasında yer almaktadır. Bu çerçevede Bonfanti (2022) çalışmasında yapay zekanın siber güvenlikteki saldırı ve savunma dengesine olan etkisi incelenmiştir. Çalışma, yapay zekanın siber savaşta nasıl bir denge unsuru olarak

işlev görebileceğini ve bu teknolojinin savaş stratejilerini nasıl dönüştürebileceğini tartışmaktadır.

Günümüzde en yaygın siber saldırı türleri arasında kötü amaçlı yazılımlar, fidye yazılımları, kimlik avı saldırıları, hizmet dışı bırakma saldırıları, iç tehditler ve gelişmiş kalıcı tehditler yer almaktadır. Kötü amaçlı yazılımlar, hedef sistemlere sızarak verileri bozmak, çalmak veya sistemleri işlevsiz hale getirmek için tasarlanmaktadır. Bu yazılımlar, truva atları, solucanlar, casus yazılımlar ve fidye yazılımları gibi farklı türlerde ortaya çıkmaktadır (Chouraik vd., 2024; Çalışkan, 2024). Özellikle fidye yazılımları, sistemleri kilitleyerek veya dosyaları şifreleyerek kullanıcılardan fidye talep etmekte ve büyük ölçekli finansal kayıplara neden olmaktadır. Kimlik avı saldırıları, kullanıcıları kandırarak hassas bilgilerini ele geçirmek amacıyla gerçekleştirilmektedir. Saldırganlar, genellikle sahte e-posta, mesaj veya web siteleri kullanarak kullanıcıları yanıltmakta ve oturum açma bilgileri, kredi kartı bilgileri veya kişisel verileri ele geçirmektedir. Bu tür saldırılar, özellikle sosyal mühendislik teknikleriyle birleştirildiğinde son derece etkili olabilmektedir (Das ve Sandhane, 2021). Sosyal mühendislik saldırıları, bireylerin güvenini kötüye kullanarak gizli bilgileri elde etmeye yönelik manipülasyon tekniklerini içermektedir. Hizmet dışı bırakma saldırıları (DDoS), hedef sistemlerin aşırı yüklenmesini sağlayarak hizmet veremez duruma gelmelerine neden olmaktadır. Bu saldırılar, genellikle binlerce cihazın aynı anda hedef sisteme sahte trafik göndermesiyle gerçekleştirilmektedir. Büyük ölçekli DDoS saldırıları, finans kuruluşları, devlet sistemleri ve e-ticaret platformları gibi kritik hizmet sağlayıcılarını hedef alarak iş sürekliliğini bozabilmektedir (Efe, 2021a).

Gelişmiş kalıcı tehditler (APT), uzun vadeli ve hedef odaklı saldırılar olarak bilinmektedir. Bu tür saldırılar, genellikle devletler veya büyük organizasyonlar tarafından gerçekleştirilmekte ve belirli bir kurum veya hükümetin bilgi sistemlerine sızarak uzun süre fark edilmeden bilgi toplamak veya sistemleri manipüle etmek amacı taşımaktadır. Bu çerçevede Jada ve Mayayiiise (2024) çalışmasında yapay zekanın organizasyonel siber güvenlik üzerindeki etkisi bir sistematik literatür taraması ile ele alınmıştır. Çalışma, AI'nin siber güvenlikteki rolünü ve bu teknolojinin organizasyonlarda nasıl bir güvenlik sağlayabileceğini araştırmaktadır. APT saldırıları,

genellikle çok aşamalı bir süreç izlemekte ve saldırganlar, hedef sisteme sızmak için sıfır gün açıkları, kimlik avı yöntemleri veya kötü amaçlı yazılımlar gibi teknikleri kullanmaktadır. İç tehditler, kurum içindeki çalışanlar veya yetkili kullanıcılar tarafından gerçekleştirilen siber saldırılar olarak tanımlanmaktadır. Bu tür tehditler, kasıtlı veya kasıtsız hatalar sonucu ortaya çıkabilmektedir (Das ve Sandhane, 2021; Efe, 2021a). Kötü niyetli çalışanlar, kurumsal verileri çalmak veya sistemleri sabote etmek amacıyla hareket edebilirken, dikkatsiz veya eğitimsiz kullanıcılar da güvenlik açıklarına neden olabilmektedir. İç tehditler, genellikle organizasyonlar için en büyük güvenlik risklerinden biri olarak kabul edilmekte ve bu tür tehditleri önlemek için güçlü kimlik doğrulama, erişim kontrolleri ve çalışan eğitim programları uygulanmaktadır (Efe, 2021b).

2.1.3. Geleneksel Siber Savunma Yöntemleri

Geleneksel siber savunma yöntemleri, dijital sistemlerin ve ağların yetkisiz erişime, kötü amaçlı yazılımlara, veri ihlallerine ve diğer siber tehditlere karşı korunmasını sağlamak amacıyla geliştirilen güvenlik önlemlerinden oluşmaktadır. Bu yöntemler, uzun yıllar boyunca bilgi teknolojileri güvenliğinin temel taşlarını oluşturmuş olup, günümüzde de birçok sistemde aktif olarak kullanılmakta ama siber tehditlerin karmaşıklığının ve çeşitliliğinin artmasıyla birlikte geleneksel yöntemlerin yetersiz kaldığı durumlar ortaya çıkmakta ve daha gelişmiş güvenlik çözümlerine duyulan ihtiyaç giderek artmaktadır (Eltayeb, 2024). Bu kapsamda Kale (2024) çalışmasında AI odaklı siber güvenlik tehditleri ve bu tehditlerin organizasyonel sonuçları tartışılmaktadır. Çalışma, AI'nin siber güvenlik tehditleri ile başa çıkma yeteneklerinin organizasyonel güvenlik üzerindeki etkilerini incelemektedir. Geleneksel siber savunma yaklaşımlarının temelinde, belirli bir tehdit modeli üzerinden geliştirilen ve önceden bilinen tehditleri tespit etmeye odaklanan güvenlik mekanizmaları yer almaktadır. Bunlar arasında güvenlik duvarları, antivirüs yazılımları, izinsiz giriş tespit ve önleme sistemleri (IDS/IPS), kimlik doğrulama ve erişim kontrol mekanizmaları gibi temel güvenlik araçları bulunmaktadır. Ayrıca Naik vd., (2022) çalışmasında yapay zeka tekniklerinin siber güvenlik alanındaki etkileri ve bu teknolojilerin güvenlik artırma üzerindeki katkıları ele alınmıştır. Çalışma,

AI'nin siber tehditlere karşı savunma stratejilerine nasıl dahil edilebileceğini kapsamlı bir şekilde incelemektedir.

Bu sistemler, belirli güvenlik politikaları çerçevesinde çalışmakta ve belirlenen tehdit vektörlerine karşı koruma sağlamaktadır. Güvenlik duvarları, geleneksel siber savunma sistemlerinin en temel bileşenlerinden biri olarak kabul edilmektedir. Ağ trafiğini denetleyerek yetkisiz erişimi engellemekte ve belirli kurallar çerçevesinde veri alışverişini filtrelemektedir. Paket filtreleme, durum denetimli filtreleme ve uygulama katmanı filtreleme gibi farklı türleri bulunan güvenlik duvarları, kötü amaçlı trafiği tespit ederek ağın güvenliğini sağlamakta fakat modern saldırı teknikleri giderek daha sofistike hale geldiğinden, geleneksel güvenlik duvarları bazen yeterli koruma sağlayamamakta ve saldırganlar, güvenlik duvarlarını aşmak için çeşitli yöntemler geliştirmektedir (Efe, 2021b; Eltayeb, 2024).

Antivirüs yazılımları, geleneksel siber güvenlik stratejilerinin en yaygın kullanılan unsurlarından biri olarak sistemleri kötü amaçlı yazılımlara karşı korumaktadır. Antivirüs programları, zararlı dosyaları imza tabanlı tarama yöntemleriyle tespit ederek silmekte veya karantinaya almaktadır. İmza tabanlı tarama yöntemleri, yalnızca bilinen tehditlere karşı etkili olabilmekte ancak bilinmeyen veya yeni ortaya çıkan tehditleri tespit etmede yetersiz kalmaktadır (Fayet, 2023). IDS sistemleri, yalnızca saldırıları tespit etmekle kalmakta ve kullanıcıları uyarırken IPS sistemleri aktif olarak müdahale ederek tehditleri engellemektedir. Tüm bunlarla beraber Palani vd., (2024) çalışmasında yapay zeka ve generatif AI'nın siber güvenlik alanındaki dönüşüm üzerindeki etkileri tartışılmaktadır. Çalışma, AI ve generatif AI'nın siber güvenlikteki rolünü, bu teknolojilerin tehdit tespiti ve savunma stratejilerindeki katkılarını incelemektedir.

Bu sistemler, genellikle imza tabanlı veya anomali tabanlı tespit mekanizmaları kullanmakta ama imza tabanlı yöntemler, bilinmeyen tehditlere karşı etkisiz kalmakta, anomali tabanlı yöntemler ise yanlış pozitif oranlarının yüksekliği nedeniyle güvenlik ekiplerine ek yük getirmektedir. Bu çerçevede kimlik doğrulama ve erişim kontrol mekanizmaları, kullanıcıların yetkilendirilmiş erişime sahip olmalarını sağlamak amacıyla geliştirilmiş geleneksel güvenlik önlemleri arasında yer almaktadır

(Folorunso vd., 2024). Parola tabanlı doğrulama, çok faktörlü kimlik doğrulama (MFA) ve biyometrik doğrulama gibi yöntemler, yetkisiz erişimi önlemekte ve sistemlerin güvenliğini artırmaktadır. Geleneksel siber savunma yöntemleri, belirli ölçüde güvenlik sağlamakla birlikte, modern tehditlerin artan sofistikasyonu karşısında bazı zorluklarla karşılaşmaktadır. Bu konu bağlamında Nami vd., (2024) çalışmasında yapay zekanın ulusal savunma stratejileri olarak kullanımı üzerine odaklanılmıştır. Çalışma, AI'nin askeri güvenlikteki uygulamaları ve bu teknolojilerin ulusal savunma stratejilerine olan etkilerini tartışmaktadır.

2.2. Yapay Zeka ve Siber Güvenlik

Yapay zeka, siber güvenlik alanında giderek daha önemli bir rol oynamakta ve geleneksel güvenlik yaklaşımlarının yetersiz kaldığı noktada yeni nesil çözümler sunmaktadır. Günümüz siber tehditleri giderek daha karmaşık hale gelmekte, saldırganlar gelişmiş yöntemler kullanarak güvenlik önlemlerini aşmaya çalışmaktadır. Bu bağlamda yapay zeka tabanlı sistemler, büyük veri analizi, anomali tespiti, tehdit tahmini ve otomatik saldırı müdahalesi gibi alanlarda siber savunmaya önemli katkılar sağlamaktadır (Fayet, 2023; Folorunso vd., 2024). Yapay zeka, hem savunma mekanizmalarının daha etkin hale gelmesini sağlamakta hem de saldırganların yeni teknikler geliştirmesiyle ortaya çıkan tehditlere karşı daha hızlı adaptasyon imkanı sunmaktadır. Bu süreç bağlamında Gilbert ve Gilbert (2024) çalışmasında yapay zekanın siber güvenlik savunma mekanizmaları üzerindeki etkisi ve gelecekteki eğilimler tartışılmaktadır. Çalışma, AI'nin siber güvenlikteki rolünü, savunma stratejilerini nasıl dönüştürdüğünü ve bu alandaki yeni zorlukları ele almaktadır.

Siber güvenlikte yapay zeka kullanımı, özellikle büyük hacimli verilerin analiz edilmesi ve anlamlandırılması noktasında büyük bir avantaj sağlamaktadır. Geleneksel güvenlik sistemleri, belirli saldırı imzalarına dayanarak tehditleri tespit etmekte ve genellikle bilinen tehditlere karşı etkili olmaktadır. Yapay zeka, bu noktada dinamik tehdit algılama mekanizmaları ile bilinmeyen tehditleri tanımlayabilmekte ve saldırılara karşı daha hızlı ve etkili bir savunma süreci oluşturabilmektedir (Gilbert ve Gilbert, 2024). Bu çerçevede makine öğrenimi ve derin öğrenme gibi yapay zeka teknikleri, siber güvenlik sistemlerinde giderek yaygınlaşmakta ve güvenlik operasyon

merkezlerinin iş yükünü azaltmaktadır. Makine öğrenimi algoritmaları, sistemlerde anormal davranışları tespit edebilmekte ve belirli bir saldırı modeline dayanmadan tehditleri tanımlayabilmektedir. Bu sayede imza tabanlı tehdit tespit yöntemlerinin sınırlılıkları aşılmakta ve bilinmeyen saldırılara karşı daha etkin bir savunma mekanizması geliştirilmektedir. Derin öğrenme algoritmaları ise büyük veri kümelerini analiz ederek tehdit modellerini çıkarabilmekte ve saldırganların kullandığı yöntemleri tahmin ederek güvenlik sistemlerinin kendini sürekli olarak güncellemesini sağlamaktadır (Govea vd., 2024). Yapay zeka destekli siber güvenlik sistemleri, tehdit istihbaratı ve anomali tespiti konularında da önemli yenilikler sunmaktadır. Tehdit istihbaratı, saldırıların gerçekleşmeden önce öngörülmesi ve olası risklerin belirlenmesi için büyük önem taşımaktadır. Bu çerçevede Efe (2021a) çalışmasında yapay zeka odaklı siber risk ve güvenlik yönetimi ele alınmıştır. Çalışma, AI'nın siber güvenlik yönetimi için sunduğu risk azaltma yöntemleri ve stratejiler hakkında bilgi sağlamaktadır. Yapay zeka, küresel tehdit verilerini analiz ederek saldırganların kullandığı teknikleri tespit edebilmekte ve güvenlik sistemlerini bu tehditlere karşı otomatik olarak güncelleyebilmektedir. Anomali tespiti ise sistemlerin olağandışı davranışlarını analiz ederek potansiyel saldırıları erken aşamada tespit etmeye yardımcı olmaktadır. Bu yöntem, özellikle geleneksel güvenlik önlemlerini aşabilen sofistike saldırılara karşı etkili bir savunma katmanı oluşturmaktadır. Bu süreçle ilişkili olarak Obi vd., (2024) çalışmasında modern siber tehditler ve gelişmiş savunma stratejileri üzerine kapsamlı bir inceleme yapılmıştır. Çalışma, AI kullanarak siber güvenlik tehditlerinin nasıl önlenebileceği ve savunma stratejilerinin nasıl geliştirilmesi gerektiği üzerine yoğunlaşmaktadır.

Siber güvenlikte yapay zeka kullanımının bir diğer önemli boyutu ise otomatik saldırı yanıt sistemleridir. Geleneksel güvenlik sistemleri, saldırıları tespit ettikten sonra genellikle insan müdahalesine ihtiyaç duymakta ve bu süreç zaman kaybına yol açmaktadır. Yapay zeka tabanlı otomatik yanıt sistemleri, saldırı anında devreye girerek tehditleri izole edebilmekte, kötü amaçlı yazılımları temizleyebilmekte ve sistemlerin saldırılardan etkilenmesini minimize edebilmektedir (Gilbert ve Gilbert, 2024; Govea vd., 2024). Bu tür sistemler, özellikle büyük ölçekli ağlarda ve kurumsal güvenlik operasyon merkezlerinde saldırılara hızlı yanıt verilmesini sağlayarak siber

güvenlik süreçlerini daha etkili ve verimli hale getirmektedir. Öncelikle yapay zeka algoritmalarının eğitilmesi için büyük miktarda veri gerekmekte ve bu verilerin kalitesi, sistemlerin başarısını doğrudan etkilemektedir.

Yanılıcı veya eksik verilerle eğitilen yapay zeka sistemleri, yanlış pozitif ve yanlış negatif sonuçlar üretebilmekte ve güvenlik ekiplerini yanıltabilmektedir. Bunun yanı sıra saldırganlar da yapay zeka teknolojilerini kullanarak güvenlik sistemlerini atlatmaya yönelik yeni yöntemler geliştirmekte ve yapay zeka destekli tehditler ortaya çıkmaktadır (Ikemefuna ve Orekha, 2024). Ayrıca Sanclemente (2023) çalışmasında dijital araçlar ve yapay zekanın ulusal güvenlik, siber güvenlik ve AI yanlışlıkları üzerindeki etkileri ele alınmıştır. Çalışma, AI'nin ulusal güvenlik stratejilerine ve siber savunmaya katkılarını analiz etmekte, AI ve teknoloji odaklı politikaların nasıl şekillendirildiğini incelemektedir.

Yapay zeka ve siber güvenlik ilişkisinde dikkate alınması gereken bir diğer önemli konu ise etik ve hukuki boyutlardır. Yapay zeka tabanlı güvenlik sistemleri, büyük miktarda kullanıcı verisini analiz etmekte ve bu durum, veri gizliliği ve kişisel mahremiyet konularında endişelere yol açmaktadır. Ayrıca yapay zeka algoritmalarının karar alma süreçlerinin şeffaf olmaması, güvenlik sistemlerinin nasıl çalıştığı konusunda belirsizlik yaratabilmekte ve bu durum hukuki açıdan yeni düzenlemelere duyulan ihtiyacı ortaya çıkarmaktadır (Jada ve Mayayiise, 2024). Yapay zeka destekli siber güvenlik sistemlerinin etik ve hukuki çerçevede nasıl kullanılacağı, gelecekte bu teknolojilerin yaygınlaşmasını ve güvenlik politikalarının şekillenmesini doğrudan etkilemektedir. Tüm bunlarla beraber Bonfanti (2020) çalışmasında yapay zeka ve siber güvenliğin geleceği tartışılmaktadır. Çalışma, yapay zekanın siber güvenlik alanında sunduğu fırsatlar ve karşılaştığı belirsizlikleri inceleyerek bu teknolojinin gelecekteki potansiyel kullanım alanlarına dair önemli bilgiler sunmaktadır. Büyük veri analitiği, makine öğrenimi, derin öğrenme ve otomatik tehdit yanıt mekanizmaları gibi teknolojiler, siber tehditlere karşı daha güçlü bir savunma sağlamak ve saldırıların önceden tespit edilerek engellenmesini mümkün kılmakta fakat bu teknolojilerin etkin bir şekilde kullanılabilmesi için veri kalitesinin artırılması, saldırganların yapay zekaya karşı geliştirdiği yöntemlere karşı

önlemler alınması ve etik ile hukuki düzenlemelerin oluşturulması büyük önem taşımaktadır (Ikemefuna ve Orekha, 2024; Jada ve Mayayiise, 2024).

2.2.1. Yapay Zekanın Tanımı ve Gelişim Süreci

Yapay zeka, insan zekasını taklit eden, öğrenme, problem çözme, muhakeme yapma, karar verme ve dil işleme gibi bilişsel yetenekleri algoritmalar ve veri tabanlı modeller aracılığıyla gerçekleştiren bir bilim dalı olarak tanımlanmaktadır (Kale, 2024). Yapay zeka, makinelerin çevresindeki verileri analiz ederek karar verebilmesini ve çeşitli görevleri yerine getirebilmesini sağlayan gelişmiş bir teknoloji alanı olarak dikkat çekmektedir. Temelinde matematik, istatistik, bilgisayar bilimi ve sinirbilim gibi disiplinlerden beslenen yapay zeka, makine öğrenimi, derin öğrenme, doğal dil işleme ve karar destek sistemleri gibi farklı alt dallardan oluşmaktadır. İlk dönem yapay zeka çalışmaları, kural tabanlı sistemler ve sembolik hesaplama yöntemlerine odaklanmış, makinelerin mantıksal çıkarımlarda bulunabilmesi için belirli kurallar çerçevesinde programlanması gerektiği düşünülmüştür (Lysenko vd., 2024).

1980’li yıllarda, yapay zeka alanında uzman sistemler geliştirilmiş ve belirli görevleri yerine getirmek için kurallara dayalı karar mekanizmaları oluşturulmuştur. 1990’lı yıllara gelindiğinde, istatistiksel öğrenme yöntemlerinin gelişmesiyle birlikte makine öğrenimi algoritmaları ön plana çıkmış ve yapay zeka sistemlerinin daha geniş bir kullanım alanına yayılmasını sağlamıştır. Makine öğrenimi, sistemlerin deneyimlerden öğrenerek kendi performanslarını geliştirmesine olanak tanımakta ve istatistiksel analizler yardımıyla veri setlerindeki desenleri tanımlayarak tahminleme yapmasını sağlamaktadır (Kale, 2024; Lysenko vd., 2024). Bu yaklaşım, yapay zeka sistemlerinin daha esnek ve adaptif olmasını mümkün kılmakta, insan müdahalesine daha az ihtiyaç duyar hale gelmesini sağlamaktadır. 2000’li yıllardan itibaren büyük veri teknolojileri ve yüksek işlem gücüne sahip donanımların gelişmesiyle birlikte yapay zeka, daha karmaşık problemleri çözebilecek kapasiteye ulaşmıştır. Yapay zekanın gelişim süreci, siber güvenlik alanında da köklü değişimlere neden olmaktadır. Geleneksel güvenlik yaklaşımları, tehditleri belirli kurallara göre tespit ederken yapay zeka tabanlı sistemler, bilinmeyen tehditleri öngörerek proaktif bir güvenlik anlayışı benimsemektedir (Maathuis ve Cools, 2025). Özellikle büyük ölçekli siber saldırıların önceden tahmin edilmesi, anomali tespiti ve otomatik güvenlik yanıtları gibi konularda

yapay zeka teknolojileri önemli katkılar sunmaktadır. Günümüzde yapay zeka, siber güvenlik alanında gerçek zamanlı tehdit analizi yapabilen, öğrenerek gelişebilen ve sürekli olarak kendini güncelleyebilen sistemlerin oluşturulmasına olanak tanımaktadır. Veri madenciliği, doğal dil işleme ve derin öğrenme algoritmaları, güvenlik açıklarını belirlemek ve saldırılara karşı etkili çözümler sunmak amacıyla kullanılmaktadır (Mijwil vd., 2022).

2.2.2. Yapay Zeka Türleri ve Uygulama Alanları

Yapay zeka, farklı yetenek seviyelerine ve uygulama alanlarına göre sınıflandırılmakta ve çeşitli sektörlerde yenilikçi çözümler sunmaktadır. Yapay zeka türleri, temel olarak zayıf yapay zeka ve güçlü yapay zeka olmak üzere iki ana kategoride ele alınmaktadır. Zayıf yapay zeka, belirli bir görevi yerine getirmek için tasarlanmış sistemleri ifade etmekte olup günümüzde en yaygın kullanılan yapay zeka türünü oluşturmaktadır. Güçlü yapay zeka ise insan zekasına eşdeğer bilişsel yeteneklere sahip olmayı hedefleyen sistemleri kapsamakta ve günümüzde henüz tam anlamıyla geliştirilememiştir (Maathuis ve Cools, 2025; Mijwil vd., 2022). Zayıf yapay zeka, belirli bir amaca yönelik olarak tasarlanmış, dar kapsamlı bir problem çözme yeteneğine sahip sistemleri içermektedir. Örneğin yüz tanıma sistemleri, konuşma tanıma teknolojileri, öneri motorları ve otonom sürüş sistemleri gibi uygulamalar, zayıf yapay zeka kapsamında değerlendirilmektedir. Tüm bunlarla beraber Sayyaparaju (2024) çalışmasında AI'nin siber savunmaya entegrasyonu, otonom tehdit tespiti ve önleme stratejilerinin nasıl birleştirilebileceği ele alınmıştır. Çalışma, yapay zekanın siber güvenlikte otonom sistemlere nasıl entegre olabileceği ve bunun güvenlik süreçlerine nasıl katkı sağladığı üzerine yoğunlaşmaktadır.

Güçlü yapay zeka, insan benzeri bilişsel yeteneklere sahip olması hedeflenen yapay zeka sistemlerini ifade etmektedir. Bu tür yapay zeka, problem çözme, muhakeme yapma, duygusal anlayış geliştirme ve öğrenme yeteneklerine sahip olmasıyla insan zekasına benzer bir işleyiş göstermeyi amaçlamaktadır (Naik vd., 2022). Yapay zekanın uygulama alanları oldukça geniş bir yelpazeye yayılmakta ve farklı sektörlerde yenilikçi çözümler sunmaktadır. Siber güvenlik, sağlık, finans, eğitim, ulaşım, üretim ve savunma sanayii gibi birçok alanda yapay zeka teknolojileri aktif olarak kullanılmaktadır. Siber güvenlik alanında yapay zeka, tehdit algılama,

anomali tespiti ve otomatik saldırı önleme mekanizmaları gibi çeşitli görevlerde kritik bir rol oynamaktadır. Büyük veri analizi ve makine öğrenimi algoritmaları, siber tehditleri önceden tahmin edebilmekte ve sistemleri güvenlik açıklarına karşı koruyabilmektedir (Nami vd., 2024).

Yapay zeka tabanlı sistemler, zararlı yazılımları tespit etmek, şüpheli ağ aktivitelerini analiz etmek ve tehdit istihbaratı üretmek amacıyla yaygın bir şekilde kullanılmaktadır. Sağlık sektöründe yapay zeka, hastalık teşhisi, tıbbi görüntü analizi, kişiselleştirilmiş tedavi planları ve ilaç geliştirme süreçlerinde etkin bir şekilde yer almaktadır. Derin öğrenme algoritmaları, tıbbi görüntüleme cihazlarından elde edilen verileri analiz ederek kanser gibi hastalıkların erken teşhis edilmesini sağlamaktadır (Naik vd., 2022; Nami vd., 2024). Ayrıca doğal dil işleme teknikleri, tıbbi kayıtların analiz edilmesi ve sağlık verilerinin anlamlandırılması için kullanılmaktadır. Finans sektöründe yapay zeka, dolandırıcılık tespiti, algoritmik ticaret, müşteri hizmetleri otomasyonu ve risk analizi gibi çeşitli alanlarda kullanılmaktadır. Ayrıca Lysenko vd., (2024) çalışmasında yapay zekanın siber güvenlikteki rolü ve tehditlerin korunması ve tespiti için otomasyonun önemi ele alınmıştır. Çalışma, AI'nın siber güvenlik tehditlerinin önceden tespit edilmesi ve güvenlik önlemlerinin otomatikleştirilmesi üzerindeki potansiyelini tartışmaktadır. Bu kapsamda Radanliev (2024) çalışmasında siber diplomasi bağlamında yapay zeka, IoT, blok zincirleri ve kuantum bilişim teknolojilerinin siber güvenlik üzerindeki riskleri ve fırsatları tanımlanmıştır. Çalışma, bu teknolojilerin siber güvenlik politikalarına etkilerini, aynı zamanda siber diplomasi alanında yeni fırsatlar yaratabileceklerini tartışmaktadır.

Makine öğrenimi tabanlı sistemler, kullanıcı harcama alışkanlıklarını analiz ederek dolandırıcılık faaliyetlerini tespit edebilmekte ve finansal işlemleri güvence altına alabilmektedir. Bunun yanı sıra finansal piyasalarda yapay zeka tabanlı algoritmalar, büyük veri setlerini analiz ederek yatırım kararlarını optimize edebilmektedir. Eğitim alanında yapay zeka, kişiselleştirilmiş öğrenme deneyimleri sunmak, öğrenci performansını analiz etmek ve eğitim materyallerini otomatik olarak uyarlamak için kullanılmaktadır (Obi vd., 2024). Yapay zeka destekli akıllı öğretim sistemleri, öğrenciye özel öğrenme yolları belirleyerek eğitimin daha verimli ve etkili olmasını sağlamaktadır. Ayrıca doğal dil işleme teknolojileri, dil öğrenme

uygulamalarında otomatik çeviri ve konuşma tanıma gibi işlevler sunmaktadır. Ulaşım sektöründe yapay zeka, otonom araçlar, trafik yönetimi sistemleri ve akıllı lojistik çözümleri geliştirmek için kullanılmaktadır (Öz, 2023).

Genel olarak üretim sektöründe yapay zeka, akıllı robotlar, üretim hatlarının otomasyonu ve tahmine dayalı bakım sistemleri gibi uygulamalarda yer almaktadır. Endüstri 4.0 kapsamında yapay zeka destekli üretim sistemleri, verimliliği artırmak ve üretim süreçlerini optimize etmek amacıyla kullanılmaktadır. Ayrıca Efe (2021b) çalışmasında yapay zeka ve Endüstri 4.0 arasındaki ilişki siber güvenlik perspektifinden analiz edilmiştir. Çalışma, Endüstri 4.0'ın getirdiği yeniliklerin siber güvenlik alanında nasıl yeni zorluklar ortaya çıkardığını ve bu sorunlarla başa çıkma yöntemlerini tartışmaktadır. Robotik sistemler, insan iş gücünü destekleyerek tekrarlayan ve tehlikeli işlerde daha güvenli ve hassas bir üretim süreci sunmaktadır. Zayıf yapay zeka günümüzde birçok alanda aktif olarak kullanılmakta, ancak güçlü yapay zeka kavramı henüz teorik bir aşamada bulunmaktadır. Siber güvenlikten sağlığa, finanstan eğitime kadar geniş bir yelpazede yapay zeka teknolojileri, sistemleri daha akıllı, hızlı ve verimli hale getirmekte ve insan hayatına önemli katkılar sağlamaktadır.

2.2.3. Siber Güvenlikte Yapay Zeka Kullanımı

Yapay zeka, siber güvenlik alanında giderek daha önemli bir araç haline gelmekte ve geleneksel güvenlik yöntemlerinin karşılaştığı sınırlamaları aşmaya yardımcı olmaktadır. Günümüzde siber saldırılar, yalnızca imza tabanlı güvenlik sistemleriyle engellenemeyecek kadar karmaşık ve sofistike bir hal almaktadır. Bu nedenle yapay zeka destekli sistemler, tehditlerin daha hızlı tespit edilmesi, analiz edilmesi ve engellenmesi için kullanılmaktadır (Obi vd., 2024; Öz, 2023). Tüm bunlarla beraber Eltayeb (2024) çalışmasında siber tehdit istihbaratının, gelecekteki siber saldırıları önceden tahmin etme ve engelleme üzerindeki rolü incelenmiştir. Çalışma, yapay zekanın siber tehditleri analiz etme ve güvenlik önlemleri almak için nasıl kullanılabileceğini ele almaktadır.

Yapay zeka, büyük veri analitiği, anomali tespiti, tehdit istihbaratı ve otomatik saldırı müdahalesi gibi alanlarda siber güvenlik süreçlerine entegre edilerek savunma

mekanizmalarını güçlendirmektedir. Geleneksel siber güvenlik yaklaşımları, çoğunlukla bilinen tehditleri tespit etmeye yönelik olarak çalışmakta ve yeni saldırı türlerine karşı yetersiz kalabilmektedir. Yapay zeka destekli güvenlik sistemleri, makine öğrenimi ve derin öğrenme algoritmaları sayesinde sürekli olarak yeni tehditleri öğrenebilmekte ve saldırı paternlerini analiz ederek bilinmeyen tehditlere karşı daha etkili bir savunma sağlamaktadır (Özdemir, 2024). Siber güvenlikte yapay zeka kullanımının en önemli alanlarından biri anomali tespit sistemleri olmaktadır. Yapay zeka tabanlı anomali tespit sistemleri, ağ trafiğini, kullanıcı davranışlarını ve sistem loglarını analiz ederek olağandışı aktiviteleri belirleyebilmekte ve tehditleri gerçek zamanlı olarak tespit edebilmektedir. Geleneksel güvenlik sistemleri, genellikle belirli bir tehdit modeline dayandığı için bilinmeyen saldırıları tespit etmekte zorlanmaktadır. Yapay zeka, tehdit istihbaratı oluşturma süreçlerinde de etkin bir şekilde kullanılmaktadır. Güvenlik sistemleri, küresel tehdit verilerini analiz ederek yeni ortaya çıkan saldırı tekniklerini belirleyebilmekte ve güvenlik ekiplerine önceden uyarılarda bulunabilmektedir (Özkurt, 2020). Yapay zeka destekli tehdit istihbaratı sistemleri, büyük veri analitiği kullanarak dünya genelindeki siber tehditleri takip etmekte ve saldırganların yöntemlerini tahmin ederek güvenlik önlemlerinin önceden alınmasını sağlamaktadır. Bunun yanı sıra otomatik saldırı müdahale sistemleri, yapay zeka tabanlı siber güvenlik çözümlerinin önemli bir bileşeni haline gelmektedir. Geleneksel güvenlik sistemleri, saldırıları tespit ettikten sonra genellikle insan müdahalesine ihtiyaç duymakta ve bu durum, özellikle büyük ölçekli saldırılar karşısında zaman kaybına neden olabilmektedir (Özdemir, 2024; Özkurt, 2020).

Yapay zeka destekli otomatik müdahale sistemleri, tehditleri tespit ettiği anda otomatik olarak aksiyon alabilmekte, kötü amaçlı yazılımları izole edebilmekte ve ağ trafiğini kontrol altına alarak saldırıların etkisini en aza indirebilmektedir. Siber güvenlikte yapay zeka kullanımının bir diğer önemli alanı ise kimlik doğrulama ve erişim kontrol sistemleri olmaktadır. Geleneksel parola tabanlı kimlik doğrulama yöntemleri, sosyal mühendislik saldırılarına ve kimlik avı tekniklerine karşı zayıf kalabilmektedir (Palani vd., 2024). Yapay zeka destekli biyometrik kimlik doğrulama sistemleri, kullanıcıların yüz tanıma, ses analizi ve davranışsal biyometri gibi özelliklerini analiz ederek daha güvenli bir kimlik doğrulama süreci sunmaktadır. Bu

sistemler, kullanıcıların sistem üzerindeki hareketlerini analiz ederek anomali tespit edebilmekte ve yetkisiz erişimleri önleyebilmektedir. Yapay zeka, siber tehdit simülasyonları ve güvenlik testleri gibi alanlarda da büyük bir katkı sağlamaktadır (Palani vd., 2024). Güvenlik ekipleri, yapay zeka destekli saldırı simülasyonları oluşturarak sistemlerinin savunma yeteneklerini test edebilmekte ve zayıf noktaları belirleyerek gerekli güvenlik önlemlerini alabilmektedir. Bu simülasyonlar, gerçek saldırı ortamlarını taklit ederek organizasyonların siber güvenlik kapasitelerini artırmalarına yardımcı olmaktadır. Örneğin adversarial saldırılar, yapay zeka tabanlı güvenlik sistemlerini manipüle etmek için özel olarak tasarlanmış saldırılar olarak öne çıkmaktadır. Saldırganlar, yapay zeka modellerinin yanlış kararlar vermesine neden olacak şekilde sistemleri kandırabilmekte ve güvenlik açıklarını istismar edebilmektedir (Palani vd., 2024; Radanliev, 2024).

Yapay zeka destekli siber güvenlik sistemlerinin etik ve hukuki boyutları da dikkatle ele alınması gereken konular arasında yer almaktadır. Bu sistemler, büyük miktarda kullanıcı verisini analiz etmekte ve bu durum, veri gizliliği ve kişisel mahremiyet konularında endişelere yol açmaktadır. Ayrıca yapay zeka algoritmalarının karar alma süreçlerinin şeffaf olmaması, güvenlik sistemlerinin nasıl çalıştığı konusunda belirsizlik yaratabilmekte ve bu durum hukuki açıdan yeni düzenlemelere duyulan ihtiyacı ortaya çıkarmaktadır (Roshanaei vd., 2024). Tüm bunlarla beraber Fayet (2023) çalışmasında Fransa'nın yapay zeka entegrasyonu ve nükleer komuta ve kontrol, kuvvet yapıları ve karar alma süreçleri üzerindeki etkisi ele alınmıştır. Çalışma, AI'nın askeri güvenlik alanındaki karar süreçlerini nasıl dönüştürebileceği üzerine odaklanmaktadır. Büyük veri analitiği, anomali tespiti, tehdit istihbaratı ve otomatik saldırı müdahale mekanizmaları gibi teknolojiler, siber tehditlere karşı daha güçlü bir savunma oluşturmakta ama yapay zeka destekli sistemlerin etkin bir şekilde çalışabilmesi için veri kalitesinin artırılması, saldırıların yapay zekaya karşı geliştirdiği yöntemlere karşı önlemler alınması ve etik ile hukuki düzenlemelerin oluşturulması büyük önem taşımaktadır (Salem vd., 2024).

2.3. Siber Savunmada Yapay Zeka Entegrasyonu

Yapay zeka, siber savunma sistemlerine entegre edilerek güvenlik önlemlerinin daha etkili, hızlı ve otomatik hale gelmesini sağlamaktadır. Geleneksel siber güvenlik yöntemleri, genellikle reaktif bir yapıya sahip olmakta ve tehditlerin belirlenmesi için imza tabanlı sistemler ya da manuel müdahaleler gerektirmektedir (Roshanaei vd.,, 2024; Salem vd.,, 2024). Yapay zeka tabanlı sistemler, tehditleri önceden tahmin edebilmekte, büyük veri analitiği yaparak güvenlik açıklarını belirleyebilmekte ve saldırılara otomatik olarak yanıt verebilmektedir. Siber savunmada yapay zeka entegrasyonu, özellikle büyük hacimli verilerin analiz edilmesi ve anlamlandırılması noktasında büyük bir avantaj sağlamaktadır. Bu süreçle ilişkili olarak Alowaidi vd.,, (2023) çalışmasında yapay zekanın siber-fiziksel sistemlerde siber güvenliğe entegrasyonu ele alınmıştır. Çalışma, yapay zekanın kritik altyapılarda nasıl bir güvenlik çözümü sunduğunu ve bu alandaki yenilikçi yaklaşımlarını incelemektedir.

Günümüzde siber saldırılar giderek daha sofistike hale gelmekte ve saldırganlar sürekli olarak yeni yöntemler geliştirmektedir. Yapay zeka destekli siber güvenlik sistemleri, geleneksel güvenlik mekanizmalarının aksine yalnızca bilinen tehditleri değil, bilinmeyen ve yeni ortaya çıkan saldırıları da tespit edebilmektedir. Bu süreç, yapay zekanın makine öğrenimi, derin öğrenme ve doğal dil işleme gibi teknikleri kullanarak sistemleri sürekli olarak güncellemesi ve tehdit algılama yeteneğini geliştirmesi ile mümkün olmaktadır (Sanclemente, 2023). Siber savunmada yapay zeka entegrasyonunun en önemli katkılarından biri, otomatik tehdit algılama ve yanıt mekanizmaları oluşturmaktadır. Geleneksel güvenlik sistemleri, tehditleri belirli kurallar çerçevesinde tanımlamakta ve manuel incelemeye ihtiyaç duymaktadır. Bu sayede, saldırıların etkisi minimize edilmekte ve tehditlerin yayılması önlenmektedir. Yapay zeka, siber tehdit istihbaratı süreçlerinde de büyük bir rol oynamaktadır (Sayyaparaju, 2024). Yapay zeka tabanlı sistemler, dünya genelindeki siber tehdit verilerini gerçek zamanlı olarak analiz edebilmekte ve saldırganların yöntemlerini öngörerek savunma mekanizmalarını geliştirebilmektedir. Bu süreç, büyük veri analitiği teknikleri kullanılarak gerçekleştirilmekte ve güvenlik açıkları tespit edilerek erken müdahale imkanı sunmaktadır (Sanclemente, 2023; Sayyaparaju, 2024).

Siber savunmada yapay zeka entegrasyonunun bir diğer önemli boyutu, anomalilere karşı gelişmiş algılama sistemlerinin oluşturulması olmaktadır. Yapay zeka tabanlı sistemler, kullanıcı davranışlarını analiz ederek olağandışı aktiviteleri belirleyebilmekte ve şüpheli işlemleri anında rapor edebilmektedir (Sulaiman vd., 2024). Örneğin bir kullanıcının olağan dışı bir saat diliminde veya coğrafi konumda sisteme giriş yapması durumunda yapay zeka destekli sistemler, bunu anormal bir aktivite olarak algılayarak kimlik doğrulama sürecini devreye sokabilmektedir. Bu tür önlemler, sosyal mühendislik saldırılarını, hesap ele geçirme girişimlerini ve veri ihlallerini engellemede büyük bir rol oynamaktadır. Bunun yanı sıra yapay zeka tabanlı sistemler, otomatik saldırı simülasyonları ve güvenlik testleri gerçekleştirme konusunda da büyük bir avantaj sunmaktadır. Güvenlik uzmanları, yapay zeka destekli saldırı simülasyonları oluşturarak sistemlerin güvenlik açıklarını test edebilmekte ve güvenlik önlemlerini buna göre şekillendirebilmektedir. Bu tür simülasyonlar, gerçek saldırı senaryolarını taklit ederek organizasyonların savunma kapasitelerini artırmalarına yardımcı olmaktadır (Sultan ve Sultan, 2024).

Yapay zeka entegrasyonu, kimlik doğrulama ve erişim kontrol mekanizmalarının güçlendirilmesi açısından da büyük bir önem taşımaktadır. Bu kapsamda Öz (2023) çalışmasında soğuk savaştan akıllı savaşa geçiş sürecinde yapay zeka teknolojilerinin rolü incelenmiştir. Çin ve ABD örnekleri üzerinden yapılan analiz, bu ülkelerin AI teknolojilerini savunma stratejilerine nasıl entegre ettiğini ve bu entegrasyonun siber güvenlik üzerindeki etkilerini tartışmaktadır. Geleneksel parola tabanlı güvenlik sistemleri, günümüzde kimlik avı saldırılarına karşı savunmasız kalabilmekte ve sosyal mühendislik teknikleri kullanılarak kolayca aşılabilmektedir. Yapay zeka destekli biyometrik doğrulama sistemleri, yüz tanıma, ses analizi ve davranışsal biyometri gibi özellikleri kullanarak daha güvenli kimlik doğrulama süreçleri sunmaktadır (Sulaiman vd., 2024; Sultan ve Sultan, 2024). Ayrıca yapay zeka tabanlı sistemler, kullanıcı davranışlarını analiz ederek kimlik doğrulama süreçlerini dinamik hale getirmekte ve yetkisiz erişim girişimlerine karşı daha güçlü bir savunma sağlamaktadır. Öncelikle yapay zeka sistemlerinin eğitilmesi için büyük miktarda veri gerekmekte ve bu verilerin doğruluğu, sistemlerin güvenilirliğini doğrudan etkilemektedir. Yanıltıcı veya eksik verilerle eğitilen yapay zeka sistemleri,

yanlış pozitif ve yanlış negatif tespitler üretebilmekte ve güvenlik ekiplerinin yanlış yönlendirilmesine neden olabilmektedir (Tao vd., 2021). Özellikle adversarial saldırılar, yapay zeka modellerini manipüle etmek için özel olarak tasarlanmış olup güvenlik sistemlerinin yanlış kararlar vermesine neden olabilmektedir. Örneğin bir saldırgan, yapay zeka modelini yanıltmak için belirli giriş verilerini değiştirerek sistemin tehdidi algılamamasını sağlayabilmektedir. Bu tür saldırılar, yapay zeka tabanlı güvenlik sistemlerinin sürekli olarak güncellenmesini ve daha dayanıklı hale getirilmesini zorunlu kılmaktadır (Temara, 2024).

Genel olarak son olarak siber savunmada yapay zeka entegrasyonunun etik ve hukuki boyutları da dikkate alınması gereken önemli konular arasında yer almaktadır. Yapay zeka tabanlı güvenlik sistemleri, büyük miktarda kullanıcı verisini analiz etmekte ve bu durum, kişisel mahremiyet ve veri gizliliği açısından bazı riskler yaratmaktadır (Tao vd., 2021; Temara, 2024). Ayrıca yapay zeka algoritmalarının karar alma süreçlerinin şeffaf olmaması, güvenlik sistemlerinin nasıl çalıştığı konusunda belirsizlik yaratabilmekte ve bu durum, hukuki düzenlemelere duyulan ihtiyacı artırmaktadır. Büyük veri analitiği, anomali tespiti, tehdit istihbaratı ve otomatik saldırı yanıt mekanizmaları gibi teknolojiler, siber tehditlere karşı daha güçlü bir savunma oluşturmaktadır (Ukhanova, 2022).

2.3.1. Yapay Zeka Destekli Tehdit Tespit Sistemleri

Yapay zeka destekli tehdit tespit sistemleri, geleneksel güvenlik mekanizmalarının sınırlılıklarını aşarak siber saldırıları daha hızlı ve doğru bir şekilde tespit etmeyi amaçlamaktadır. Günümüzde siber saldırılar, giderek daha karmaşık hale gelmekte ve saldırganlar, mevcut güvenlik sistemlerini aşmak için gelişmiş yöntemler kullanmaktadır (Zeng, 2022). Geleneksel tehdit tespit sistemleri, çoğunlukla imza tabanlı çalışmakta ve yalnızca önceden tanımlanmış tehditleri algılayabilmekte fakat yapay zeka tabanlı tehdit tespit sistemleri, makine öğrenimi, derin öğrenme ve büyük veri analitiği tekniklerini kullanarak bilinmeyen tehditleri de tespit edebilmekte ve sistemlerin saldırılara karşı daha dirençli hale gelmesini sağlamaktadır. Yapay zeka destekli tehdit tespit sistemleri, büyük veri analizi yaparak olağandışı aktiviteleri belirlemekte ve ağ trafiği, kullanıcı davranışları ile sistem logları üzerinde anomali tespiti gerçekleştirmektedir. Geleneksel güvenlik çözümleri, genellikle belirli bir

tehdit modeline dayanmakta ve statik kurallar üzerinden çalışmakta fakat saldırganlar, yeni nesil tehditler geliştirdikçe bu sistemlerin etkinliği azalmaktadır (Ukhanova, 2022; Zeng, 2022). Yapay zeka, sürekli olarak öğrenme yeteneğine sahip olduğu için tehditlerin evrimini analiz edebilmekte ve yeni saldırı yöntemlerine karşı daha hızlı tepki verebilmektedir. Ayrıca Aldhamer (2024) çalışmasında yapay zekanın siber güvenlik üzerindeki gelecekteki etkileri tartışılmaktadır. Çalışma, yapay zeka teknolojilerinin evrimi ve gelecekte siber güvenlik uygulamalarıyla nasıl bütünleşebileceği hakkında kapsamlı bir analiz sunmaktadır.

Tehdit tespit süreçlerinde en sık kullanılan yapay zeka tekniklerinden biri makine öğrenimi algoritmaları olmaktadır. Makine öğrenimi, sistemlerde geçmişte gerçekleşmiş saldırı örneklerini analiz ederek belirli örüntüleri tanımlamakta ve yeni tehditleri tespit etmek için bu bilgilerden yararlanmaktadır (Zhang vd., 2021). Özellikle gözetimli öğrenme teknikleri, zararlı ve zararsız aktiviteleri sınıflandırarak güvenlik sistemlerinin daha hassas hale gelmesini sağlamaktadır. Bunun yanı sıra, gözetimsiz öğrenme yöntemleri, herhangi bir önceden etiketlenmiş veriye ihtiyaç duymadan sistemlerdeki olağandışı aktiviteleri belirleyerek bilinmeyen tehditleri ortaya çıkarmaktadır. Derin öğrenme algoritmaları, yapay sinir ağları kullanarak tehditlerin daha detaylı bir şekilde analiz edilmesine olanak tanımaktadır. Derin öğrenme modelleri, çok katmanlı yapıları sayesinde büyük ölçekli veriler üzerinde karmaşık ilişkileri öğrenebilmekte ve saldırı paternlerini tespit edebilmektedir (Abdulhussein, 2024).

Yapay zeka destekli tehdit tespit sistemleri, anomali tespiti yaparak bilinmeyen tehditlere karşı proaktif bir güvenlik yaklaşımı benimsemektedir. Anomali tespit sistemleri, normal kullanıcı davranışlarını ve ağ trafiğini analiz ederek olağandışı aktiviteleri belirleyebilmekte ve sistem yöneticilerini potansiyel tehditler konusunda uyarabilmektedir. Örneğin bir kullanıcının alışılmışın dışında bir saat diliminde veya farklı bir IP adresinden giriş yapması durumunda yapay zeka tabanlı anomali tespit sistemleri, bu aktiviteyi şüpheli olarak işaretleyerek güvenlik önlemlerinin devreye girmesini sağlamaktadır (Aldasoro vd., 2024). Bunun yanı sıra doğal dil işleme (NLP) teknikleri, siber tehdit istihbaratında önemli bir rol oynamaktadır. Bu durum bağlamında Özdemir (2024) çalışmasında yapay zeka ve makine öğrenmesinin siber

tehdit istihbaratındaki rolü ele alınmıştır. Çalışma, AI ve ML teknolojilerinin siber tehditlerin tespit ve analizinde nasıl kullanılabileceğini inceleyerek, bu teknolojilerin siber güvenlikteki gelecekteki potansiyeline dair önemli bulgular sunmaktadır. Tüm bunlarla beraber Mijwil vd., (2022) çalışmasında yapay zekanın siber güvenlikteki rolü ve önemi üzerine bir derleme sunulmuştur. Çalışma, yapay zekanın siber güvenlikteki uygulamalarını, bu teknolojinin tehditleri nasıl tespit ettiğini ve siber güvenlikteki rolünü kapsamlı bir şekilde incelemektedir.

Yapay zeka destekli tehdit tespit sistemleri, internet üzerindeki tehdit raporlarını, sosyal medya içeriklerini ve siber güvenlikle ilgili diğer kaynakları analiz ederek yeni tehditleri belirleyebilmekte ve saldırganların kullandığı yöntemler hakkında bilgi toplayabilmektedir. Doğal dil işleme teknolojileri, siber tehditlerin erken aşamada tespit edilmesine yardımcı olmakta ve güvenlik ekiplerine daha hızlı müdahale etme imkanı sunmaktadır (Abdulhussein, 2024; Aldasoro vd., 2024). Yapay zeka destekli tehdit tespit sistemleri, zararlı yazılım tespiti konusunda da büyük bir ilerleme sağlamaktadır. Geleneksel antivirüs yazılımları, genellikle imza tabanlı tarama yaparak bilinen kötü amaçlı yazılımları belirlemekte ama yapay zeka tabanlı zararlı yazılım tespit sistemleri, kötü amaçlı yazılımların davranışlarını analiz ederek bunları daha yüksek doğrulukla belirleyebilmekte ve yeni ortaya çıkan tehditlere karşı daha etkin bir koruma sağlamaktadır (Aldhamer, 2024). Bununla birlikte yapay zeka destekli tehdit tespit sistemlerinin bazı sınırlamaları da bulunmaktadır. Bu çerçevede yanıltıcı veya eksik verilerle eğitilen yapay zeka modelleri, yanlış pozitif veya yanlış negatif sonuçlar üretebilmekte ve güvenlik ekiplerinin hatalı kararlar almasına neden olabilmektedir. Makine öğrenimi, derin öğrenme, anomali tespiti ve doğal dil işleme gibi teknikler sayesinde tehditlerin erken aşamada belirlenmesi ve saldırılara karşı daha hızlı yanıt verilmesi mümkün hale gelmektedir (Alowaidi vd., 2023).

2.3.2. Otomasyon ve Anomali Tespiti

Yapay zeka tabanlı siber güvenlik sistemleri, tehditleri tespit etmek ve saldırılara hızlı yanıt verebilmek için otomasyon ve anomali tespiti mekanizmalarını kullanmaktadır. Geleneksel siber güvenlik yöntemleri genellikle insan müdahalesine dayalı olmakta ve tehditlere karşı reaktif bir yaklaşım benimsemekte fakat saldırganlar giderek daha sofistike teknikler geliştirmekte ve güvenlik sistemlerini aşmak için yeni

yöntemler kullanmaktadır. Bu bağlamda yapay zeka destekli otomasyon ve anomali tespit sistemleri, siber tehditleri proaktif bir şekilde ele alarak daha hızlı, ölçeklenebilir ve etkili bir savunma mekanizması oluşturmaktadır. Otomasyon, siber güvenlik süreçlerinde insan müdahalesine duyulan ihtiyacı azaltarak olaylara daha hızlı tepki verilmesini sağlamaktadır (Aldhamer, 2024; Alowaidi vd., 2023). Geleneksel güvenlik ekipleri, tehditleri manuel olarak tespit etmekte ve analiz etmekte ancak bu süreç büyük miktarda zaman ve insan kaynağı gerektirmektedir. Yapay zeka tabanlı otomatik sistemler, ağ trafiğini sürekli izleyerek anormal aktiviteleri belirleyebilmekte ve şüpheli olayları otomatik olarak işleyerek saldırılara karşı anında önlemler alabilmektedir. Bu sayede saldırılar gerçekleşmeden önce tespit edilmekte ve tehditlerin etkisi minimize edilmektedir (Araya ve King, 2022).

Anomali tespiti, otomasyonun en önemli bileşenlerinden biri olarak öne çıkmaktadır. Geleneksel tehdit tespit sistemleri, belirli kurallar çerçevesinde çalışmakta ve yalnızca önceden tanımlanmış saldırı türlerini algılayabilmekte ama saldırganlar sürekli olarak yeni teknikler geliştirdiğinden, geleneksel sistemler bilinmeyen tehditlere karşı yetersiz kalmaktadır. Yapay zeka tabanlı anomali tespit sistemleri, normal ağ trafiği ve kullanıcı davranışlarını analiz ederek olağandışı aktiviteleri tespit edebilmekte ve bilinmeyen tehditlere karşı daha güçlü bir savunma oluşturmaktadır (Arroyo-Figueroa, 2023). Anomali tespiti sistemleri, makine öğrenimi ve derin öğrenme tekniklerinden yararlanarak tehditleri tanımlamakta ve bu tehditlere karşı uygun önlemleri önceden alabilmektedir. Denetimli öğrenme teknikleri, önceden sınıflandırılmış veri setlerinden öğrenerek bilinen saldırı paternlerini tanımlamakta ve benzer saldırıları tespit etmektedir. Denetimsiz öğrenme teknikleri ise herhangi bir etiketlenmiş veri setine ihtiyaç duymadan veri içindeki örüntüleri ve anomalileri belirleyerek bilinmeyen tehditleri algılamaktadır. Bu teknikler sayesinde siber güvenlik sistemleri sürekli olarak öğrenmekte ve tehditlere karşı daha esnek ve dinamik bir yaklaşım benimsemektedir (Araya ve King, 2022; Arroyo-Figueroa, 2023). Bunlarla beraber Ukhanova (2022) çalışmasında Japonya'nın siber güvenlik ve siber savunma stratejileri ele alınmıştır. Çalışma, Japonya'nın siber güvenlikteki yaklaşımlarını, siber tehditler karşısında nasıl savunma stratejileri geliştirdiğini incelemektedir.

Otomasyon ve anomali tespiti, özellikle büyük ölçekli kurumsal ağlar ve bulut sistemleri için kritik bir öneme sahip olmaktadır. Büyük veri analitiği teknikleri kullanılarak milyonlarca veri noktası anlık olarak analiz edilmekte ve güvenlik açıkları belirlenmektedir. Geleneksel yöntemlerle bu kadar büyük hacimli veriyi analiz etmek mümkün olmamakta ve manuel güvenlik incelemeleri saldırıları önlemede yetersiz kalmaktadır. Yapay zeka destekli otomasyon sistemleri, sürekli olarak veri akışını izleyerek anormal durumları tespit edebilmekte ve güvenlik ekiplerine gerçek zamanlı uyarılar göndermektedir. Anomali tespiti sistemleri, kullanıcı ve varlık davranış analizi ile desteklenerek daha kapsamlı bir tehdit tespit mekanizması oluşturmaktadır (Bhardwaj, 2023). Örneğin bir çalışanın aniden büyük miktarda veri indirmesi, normalde kullanmadığı sistemlere erişim sağlaması veya alışılmamışın dışında bir IP adresinden giriş yapması, yapay zeka tabanlı sistemler tarafından tehdit olarak algılanabilmekte ve güvenlik ekiplerine bildirilmektedir.

APT saldırıları, genellikle belirli bir kuruluş veya devlet kurumunu hedef almakta ve uzun süre fark edilmeden sistemlere sızmaktadır. Geleneksel güvenlik sistemleri, bu tür saldırıları genellikle geç tespit etmekte ve saldırganların uzun süre boyunca sistemlere erişimini engelleyememekte fakat yapay zeka tabanlı anomali tespit sistemleri, saldırganların sistemlere sızma ve veri sızdırma girişimlerini erken aşamada belirleyerek müdahale süresini kısaltmaktadır. Otomasyon ve anomali tespit sistemleri, otomatik yanıt mekanizmaları ile desteklenerek tehditlere karşı daha hızlı aksiyon alınmasını sağlamaktadır. Geleneksel sistemlerde, bir tehdit tespit edildiğinde genellikle manuel müdahale gerekmekte ve bu durum saldırıların yayılmasına neden olabilmektedir (Binhammad vd., 2024). Örneğin zararlı bir yazılım tespit edildiğinde yapay zeka tabanlı sistemler, etkilenen cihazı otomatik olarak karantinaya almakta ve ağ üzerindeki bağlantısını keserek saldırının yayılmasını önlemektedir. Öncelikle yapay zeka tabanlı güvenlik sistemlerinin başarısı, kullanılan veri setlerinin kalitesine bağlı olmaktadır. Eksik veya yanıltıcı verilerle eğitilen sistemler, yanlış pozitif veya yanlış negatif tespitler yapabilmekte ve güvenlik ekiplerinin hatalı müdahalelerde bulunmasına neden olabilmektedir. Ayrıca saldırganlar da yapay zeka sistemlerine karşı yeni nesil saldırılar geliştirerek anomali tespit sistemlerini yanıltmaya çalışmaktadır (Bhardwaj, 2023; Binhammad vd., 2024).

2.3.3. Makine Öğrenimi ile Saldırı Önleme

Makine öğrenimi, siber güvenlikte saldırı önleme mekanizmalarını daha akıllı, hızlı ve etkili hale getirmekte ve tehditlere karşı proaktif savunma stratejilerinin geliştirilmesine katkı sağlamaktadır. Geleneksel siber güvenlik sistemleri, büyük ölçüde imza tabanlı tehdit tespiti ve kural tabanlı filtreleme yöntemlerine dayanmakta olup, önceden bilinen saldırı türlerine karşı etkili olmaktadır. Makine öğrenimi tabanlı saldırı önleme sistemleri, geçmiş saldırı verilerini analiz ederek yeni tehditleri tahmin edebilmekte ve saldırılar gerçekleşmeden önce önleyici tedbirler alabilmektedir (Bonfanti, 2020). Makine öğrenimi, verilerden örüntüler çıkarmak ve bu örüntüler aracılığıyla sistemleri eğitmek için istatistiksel ve matematiksel algoritmalar kullanmaktadır. Siber güvenlik alanında, saldırıların tespit edilmesi ve önlenmesi için büyük miktarda verinin analiz edilmesi gerekmekte olup makine öğrenimi teknikleri bu süreci otomatikleştirerek tehdit algılama ve saldırı önleme süreçlerini hızlandırmaktadır. Özellikle büyük veri analitiği ve gerçek zamanlı tehdit istihbaratı ile desteklenen makine öğrenimi sistemleri, anormal davranışları tespit edebilmekte ve saldırıları henüz başlangıç aşamasında engelleyebilmektedir (Bonfanti ve Kohler, 2020). Tüm bunlarla ilişkili olarak Sulaiman et al. (2024) çalışmasında epidemik siber güvenlik tehditlerine yönelik savunma stratejileri, makine öğrenimi yöntemleri kullanılarak modellenmiştir. Çalışma, AI tabanlı yaklaşımların epidemik tehditlere karşı nasıl etkili bir şekilde uygulanabileceği üzerine yeni bir bakış açısı sunmaktadır.

Geleneksel antivirüs yazılımları, genellikle imza tabanlı tarama tekniklerine dayanmakta ve yalnızca önceden bilinen kötü amaçlı yazılımları tespit edebilmektedir. Makine öğrenimi algoritmaları, zararlı yazılımların davranışsal analizini yaparak bunları tespit edebilmekte ve bilinmeyen kötü amaçlı yazılımlara karşı daha güçlü bir koruma sağlamaktadır. Örneğin bir fidye yazılımı, kullanıcı dosyalarını şifrelemeye başlamadan önce sistem içindeki hareketleri analiz edilerek erken aşamada tespit edilebilmekte ve sistem yöneticileri uyarılmaktadır. Makine öğrenimi destekli saldırı önleme sistemleri, dağıtık ağlarda tehdit istihbaratı oluşturma konusunda da önemli bir avantaj sağlamaktadır (Center for Security Studies, 2019). Geleneksel güvenlik sistemleri genellikle tek bir noktada tehditleri analiz ederken, makine öğrenimi tabanlı sistemler, bulut bilişim ve büyük veri analitiği ile desteklenerek küresel tehditleri

izleyebilmekte ve saldırganların kullandığı yeni teknikleri daha geniş bir perspektiften değerlendirebilmektedir (Bonfanti, 2022; Center for Security Studies, 2019).

Yanılıcı, eksik veya hatalı verilerle eğitilen sistemler, yanlış pozitif ve yanlış negatif sonuçlar üretebilmekte ve güvenlik ekiplerinin hatalı müdahalelerde bulunmasına neden olabilmektedir. Ayrıca saldırganlar da makine öğrenimi algoritmalarını manipüle etmek için yeni teknikler geliştirmekte ve adversarial saldırılar yoluyla güvenlik sistemlerini yanıltmaya çalışmaktadır. Örneğin saldırganlar, makine öğrenimi tabanlı bir güvenlik sistemine belirli veri manipülasyonları uygulayarak yanlış kararlar vermesini sağlayabilmekte ve sistemin tehditleri algılamasını engelleyebilmektedir (Chouraik vd., 2024). Makine öğrenimi tabanlı saldırı önleme sistemlerinin etkinliği, otomatik yanıt mekanizmaları ile desteklendiğinde daha da artmaktadır. Geleneksel güvenlik sistemleri, saldırıları tespit ettikten sonra genellikle manuel müdahale gerektirmektedir. Örneğin bir DDoS saldırısı tespit edildiğinde, yapay zeka tabanlı sistemler, saldırının kaynağını otomatik olarak engelleyerek hizmetin kesintiye uğramasını önleyebilmektedir (Çalışkan, 2024). Anomali tespiti, zararlı yazılım analizi, ağ trafiği izleme ve otomatik tehdit yanıtı gibi alanlarda makine öğrenimi algoritmaları, geleneksel yöntemlere kıyasla daha yüksek doğruluk oranları sağlamakta fakat bu sistemlerin başarılı olabilmesi için veri kalitesinin artırılması, saldırganların yapay zekaya karşı geliştirdiği yeni taktiklerin sürekli olarak analiz edilmesi ve güvenlik sistemlerinin sürekli güncellenmesi gerekmektedir (Chouraik vd., 2024; Çalışkan, 2024).

2.4. Siber Savunma Stratejilerinde Yapay Zeka Örnekleri

Yapay zeka, siber güvenlik alanında giderek daha fazla benimsenmekte ve saldırılara karşı gelişmiş savunma mekanizmaları oluşturmak için kullanılmaktadır. Günümüzde birçok devlet kurumu, özel şirket ve uluslararası organizasyon, yapay zeka destekli siber güvenlik çözümlerini benimseyerek sistemlerini daha güvenli hale getirmektedir. Yapay zeka, tehdit algılama, anomali tespiti, tehdit istihbaratı ve otomatik saldırı önleme gibi alanlarda büyük ilerlemeler sağlamaktadır. Çeşitli sektörlerde ve kurumlarda uygulanan başarılı yapay zeka destekli siber savunma stratejileri, siber tehditlere karşı daha etkili bir mücadele yürütülmesini mümkün kılmaktadır (Das ve Sandhane, 2021). Yapay zeka destekli siber savunma sistemleri,

özellikle büyük veri analitiği, makine öğrenimi ve derin öğrenme algoritmaları ile desteklenmekte ve tehditleri daha hızlı tespit edebilmektedir. Örneğin finans sektöründe faaliyet gösteren büyük şirketler, dolandırıcılık girişimlerini engellemek amacıyla yapay zeka tabanlı anomali tespit sistemleri kullanmaktadır (Efe, 2021a). Bankalar, müşteri işlemlerini analiz ederek olağandışı aktiviteleri belirleyebilmekte ve dolandırıcılık girişimlerini daha saldırı gerçekleşmeden tespit edebilmektedir. Bununla beraber Aldasoro vd., (2024) çalışmasında merkez bankacılığında yapay zeka ve siber güvenliğin rolü ele alınmıştır. Çalışma, yapay zekanın merkezi bankaların siber güvenlik stratejilerine nasıl entegre edilebileceği ve bu teknolojilerin finansal güvenlikteki etkileri üzerine odaklanmaktadır.

Devlet kurumları ve ulusal güvenlik ajansları da yapay zeka destekli siber savunma stratejilerini benimsemekte ve ulusal güvenliği tehdit eden siber saldırılara karşı önlemler almaktadır. Özellikle ABD Ulusal Güvenlik Ajansı (NSA) ve İngiltere'deki GCHQ gibi istihbarat kurumları, yapay zeka destekli siber tehdit istihbaratı sistemlerini kullanarak siber saldırıları erken aşamada tespit edebilmekte ve saldırganların kullandığı teknikleri analiz edebilmektedir. Bu tür sistemler, dünya çapında gerçekleşen siber saldırıları gerçek zamanlı olarak izleyerek saldırganların hareketlerini tahmin etmekte ve ulusal güvenliği tehdit eden siber operasyonları önlemeye yardımcı olmaktadır (Das ve Sandhane, 2021; Efe, 2021a). Siber güvenlikte yapay zeka kullanımının başarılı örneklerinden biri de Google'ın Chronicle projesi olmaktadır. Google'ın yapay zeka tabanlı güvenlik şirketi Chronicle, büyük veri analitiği ve makine öğrenimi tekniklerini kullanarak tehditleri daha hızlı tespit etmeyi ve saldırılara karşı otomatik savunma mekanizmaları geliştirmeyi hedeflemektedir. Chronicle, farklı kaynaklardan elde edilen siber tehdit verilerini analiz ederek saldırıların erken aşamada belirlenmesini sağlamak ve güvenlik ekiplerine kapsamlı tehdit raporları sunmaktadır (Efe, 2021b).

Yapay zeka destekli siber güvenlik çözümlerinin bir diğer başarılı örneği Darktrace adlı şirket tarafından geliştirilen siber tehdit tespit sistemleri olmaktadır. Darktrace, yapay sinir ağlarını kullanarak ağ trafiğini analiz etmekte ve olağandışı aktiviteleri belirleyerek potansiyel tehditleri önlemektedir. Şirketin geliştirdiği "Enterprise Immune System" adlı yapay zeka destekli güvenlik platformu, biyolojik

başıklık sistemine benzer bir mantıkla çalışmakta ve siber tehditleri tespit ederek sistemleri otomatik olarak koruma altına almaktadır. Bu sistem, herhangi bir saldırı girişimini anında tespit ederek güvenlik ekiplerine gerçek zamanlı uyarılar göndermektedir (Efe, 2021b). Yapay zeka, uluslararası organizasyonlar tarafından da siber güvenlik stratejilerinin güçlendirilmesi amacıyla kullanılmaktadır. Örneğin Avrupa Birliği'nin yapay zeka destekli siber güvenlik projeleri, Avrupa'daki devlet kurumlarının ve özel şirketlerin siber tehditlere karşı daha dirençli hale gelmesini sağlamaktadır. Avrupa Siber Güvenlik Ajansı (ENISA), yapay zeka tabanlı tehdit istihbaratı ve siber saldırı simülasyonları geliştirerek Avrupa genelinde güvenlik standartlarını artırmayı hedeflemektedir. Bu sistemler, Avrupa'daki devlet kurumlarının siber saldırılara karşı hazırlıklı olmasını sağlamak ve kritik altyapıların korunmasına yardımcı olmaktadır (Efe, 2021b; Eltayeb, 2024).

Yapay zeka destekli siber savunma stratejileri, askeri ve savunma sanayii alanında da büyük bir öneme sahip olmaktadır. ABD Savunma Bakanlığı'na bağlı Savunma İleri Araştırma Projeleri Ajansı (DARPA), yapay zeka tabanlı tehdit tespit sistemleri geliştirmekte ve bu sistemleri askeri ağların güvenliğini sağlamak için kullanmaktadır. Tüm bunlarla beraber Maathuis ve Cools (2025) çalışmasında askeri siber güvenlikte yapay zekanın rolü incelenmiştir. Çalışma, askeri alanda siber güvenliğin güçlendirilmesinde AI kullanımının nasıl bir etki yarattığını ve bu teknolojilerin savaş stratejilerine olan katkılarını araştırmaktadır. Yapay zeka destekli saldırı simülasyonları ve siber savaş senaryoları, askeri sistemlerin siber saldırılara karşı korunmasına yardımcı olmaktadır (Fayet, 2023). Özellikle kritik askeri altyapıların güvenliğini sağlamak amacıyla geliştirilen bu sistemler, düşman devletler veya hacker grupları tarafından gerçekleştirilebilecek siber saldırılara karşı hızlı ve otomatik yanıt mekanizmaları sunmaktadır. Bu çerçevede Govea vd., (2024) çalışmasında siber güvenliğin kritik enerji altyapısına dönüştürülmesinde yapay zekanın etkisi incelenmiştir. Çalışma, AI'nin enerji sektöründeki siber güvenlik önlemlerine nasıl entegre edilebileceğini ve bu teknolojinin sektördeki etkilerini araştırmaktadır.

Yapay zeka tabanlı siber güvenlik çözümlerinin başarılı bir diğer örneği ise IBM'in Watson for Cyber Security platformu olmaktadır. IBM Watson, doğal dil

işleme ve makine öğrenimi tekniklerini kullanarak tehdit istihbaratı sağlamakta ve güvenlik ekiplerinin tehditleri daha hızlı analiz etmesine yardımcı olmaktadır. Watson, dünya genelinde yayımlanan siber güvenlik raporlarını, araştırma makalelerini ve tehdit istihbarat verilerini analiz ederek güvenlik uzmanlarına detaylı bilgiler sunmakta ve saldırılara karşı alınabilecek önlemleri önermektedir (Folorunso vd., 2024). Genel olarak özel şirketler de yapay zeka destekli siber güvenlik çözümlerini benimseyerek müşteri verilerini ve kurumsal ağlarını koruma altına almaktadır. Örneğin büyük teknoloji şirketleri, çalışanlarının sistemlerine erişim sağlarken yapay zeka destekli kimlik doğrulama ve erişim kontrol sistemlerini kullanmaktadır. Yapay zeka, kullanıcı davranışlarını analiz ederek anormal aktiviteleri belirlemekte ve yetkisiz erişimleri engelleyerek veri güvenliğini sağlamaktadır (Fayet, 2023; Folorunso vd., 2024). Devlet kurumlarından özel şirketlere, finans sektöründen askeri sistemlere kadar birçok alanda yapay zeka destekli güvenlik çözümleri, siber tehditlerin önlenmesine ve saldırılara karşı daha etkili savunma mekanizmalarının oluşturulmasına katkı sağlamaktadır. Yapay zeka, gelecekte siber güvenliğin en kritik bileşenlerinden biri olmaya devam edecek ve siber tehditlere karşı daha proaktif ve akıllı çözümler sunmaya devam edecektir (Gilbert ve Gilbert, 2024).

2.4.1. Dünyada Siber Güvenlik

Dijitalleşmenin hızla yayılmasıyla birlikte siber güvenlik, uluslararası düzeyde en önemli güvenlik konularından biri haline gelmektedir. Devletler, özel şirketler ve bireyler, giderek daha fazla dijital sistemlere bağımlı hale gelmekte ve bu durum, siber tehditlerin kapsamını genişletmektedir. Siber saldırılar, yalnızca bireysel veya kurumsal güvenliği değil, aynı zamanda ulusal güvenliği ve küresel ekonomik istikrarı da tehdit etmektedir. Bu nedenle dünya genelinde ülkeler, siber güvenlik stratejilerini güçlendirmekte ve siber tehditlere karşı uluslararası iş birlikleri geliştirmektedir (Govea vd., 2024). Siber güvenlik alanında gelişmiş ülkeler, ulusal güvenlik stratejilerine siber savunma mekanizmalarını entegre etmekte ve siber saldırılara karşı kapsamlı önlemler almaktadır. Bu kapsamda Sultan ve Sultan (2024) çalışmasında yapay zekanın siber güvenlikteki rolü, sistematik bir yaklaşım ile ele alınmıştır. Çalışma, AI'nin siber tehditlere karşı nasıl bir savunma mekanizması sunduğunu ve bu teknolojinin güvenlik stratejileri üzerindeki etkilerini tartışmaktadır. ABD, özellikle

devlet destekli siber saldırılara karşı koymak için yapay zeka tabanlı siber savunma sistemlerini devreye sokmakta ve kritik altyapıların korunmasına yönelik düzenlemeler geliştirmektedir (Gilbert ve Gilbert, 2024; Govea vd., 2024). Ayrıca Pentagon ve Savunma Bakanlığı, yapay zeka destekli siber savaş stratejilerini kullanarak ülkenin siber tehditlere karşı daha dirençli olmasını sağlamaktadır. Bu bağlamda Center for Security Studies (CSS) (2019) çalışmasında farklı ülkelerin ulusal siber güvenlik stratejileri karşılaştırılmış ve İsviçre'nin karşılaştığı zorluklar ele alınmıştır. Çalışma, farklı ülke stratejilerinin siber güvenlikte nasıl şekillendiğini ve bunun uygulama süreçlerini detaylandırmaktadır.

Avrupa Birliği (AB) de siber güvenlik alanında önemli adımlar atmaktadır. Avrupa Siber Güvenlik Ajansı (ENISA), AB ülkeleri arasında koordinasyonu sağlamakta ve siber tehditlere karşı ortak çözümler geliştirmektedir. AB'nin "Genel Veri Koruma Yönetmeliği (GDPR)" gibi düzenlemeleri, kişisel verilerin korunmasını sağlamakta ve siber güvenlik standartlarını yükseltmektedir. Çin, siber güvenlik alanında dünya genelinde en güçlü altyapılardan birine sahip olmaktadır. Çin hükümeti, devlet destekli siber güvenlik projeleri geliştirerek kritik altyapıları koruma altına almakta ve ulusal güvenlik stratejilerini siber tehditlere karşı uyarlamaktadır (Ikemefuna ve Orekha, 2024). Aynı zamanda Çin'in ulusal güvenlik politikaları kapsamında geliştirdiği siber savunma sistemleri, yapay zeka destekli tehdit tespit sistemlerini içermekte ve saldırılara karşı otomatik yanıt mekanizmaları sağlamaktadır. Çin, büyük veri analitiği ve yapay zeka kullanarak siber güvenlik önlemlerini artırmakta ve devlet destekli siber saldırılara karşı aktif savunma politikaları benimsemektedir (Jada ve Mayayiise, 2024).

Rusya, siber güvenliği ulusal güvenlik stratejisinin önemli bir parçası olarak görmekte ve bu alanda devlet destekli çalışmalar yürütmektedir. Rusya, özellikle siber tehdit istihbaratı toplama, saldırıları tespit etme ve güvenlik açıklarını kapatma konusunda ileri düzey sistemler geliştirmektedir. Rus hükümeti, ulusal altyapıları siber saldırılardan korumak için güçlü güvenlik duvarları ve tehdit tespit sistemleri kullanmaktadır. Ayrıca Rusya'nın siber güvenlik politikaları, yapay zeka ve makine öğrenimi teknikleriyle desteklenen saldırı tespit ve savunma mekanizmalarını içermektedir. Bu çerçevede Ikemefuna ve Orekha (2024) çalışmasında öngörücü siber

savunma üzerine odaklanılmıştır. Çalışma, yapay zeka ve makine öğrenimi kullanarak siber tehditleri tahmin etme ve bu tehditlere karşı proaktif önlemler almayı amaçlayan yeni yaklaşımları incelemektedir.

İsrail, siber güvenlik alanında en gelişmiş ülkelerden biri olarak öne çıkmaktadır. İsrail hükümeti, siber güvenlik sektörüne büyük yatırımlar yapmakta ve siber tehditlere karşı güçlü bir savunma altyapısı oluşturmaktadır. İsrail, ulusal güvenlik politikaları kapsamında siber tehditleri tespit eden ve önleyen gelişmiş yapay zeka tabanlı sistemler geliştirmektedir. Uluslararası düzeyde siber güvenlik stratejileri, ülkeler arası iş birlikleri ve ortak güvenlik politikalarıyla güçlendirilmektedir (Ikemefuna ve Orekha, 2024; Jada ve Mayayiise, 2024). NATO, siber güvenliği kolektif savunmanın bir parçası olarak görmekte ve üye ülkeler arasında siber tehditlere karşı iş birliği yapılmasını teşvik etmektedir. NATO'nun siber savunma girişimleri, üye ülkelerin siber tehditlerle mücadelede daha güçlü politikalar geliştirmesine yardımcı olmakta ve siber savaş senaryolarına karşı hazırlıklı olmayı sağlamaktadır (Kale, 2024). Birleşmiş Milletler (BM), küresel siber güvenlik politikalarının oluşturulmasına katkı sağlamakta ve dünya genelinde siber tehditlerle mücadele edilmesine yönelik uluslararası iş birliklerini teşvik etmektedir. BM, siber güvenlik alanında standartların belirlenmesi ve ülkeler arasında bilgi paylaşımının artırılması için çalışmalar yürütmektedir. Özel sektör ve büyük teknoloji şirketleri de siber güvenliğin güçlendirilmesine katkı sağlamaktadır. Google,

Microsoft, IBM ve Amazon gibi teknoloji devleri, yapay zeka destekli siber güvenlik çözümleri geliştirerek siber tehditlere karşı daha akıllı ve etkili savunma mekanizmaları oluşturmaktadır (Lysenko vd., 2024). Bu şirketler, bulut tabanlı güvenlik sistemleri, tehdit istihbaratı platformları ve otomatik saldırı önleme sistemleri geliştirerek küresel siber güvenlik standartlarını yükseltmektedir. Tüm bunlarla beraber dünyada siber güvenlik stratejileri giderek daha fazla önem kazanmakta ve ülkeler, siber tehditlere karşı daha güçlü savunma mekanizmaları geliştirmektedir. Yapay zeka, büyük veri analitiği ve makine öğrenimi teknikleri, siber güvenlik alanında devrim niteliğinde yenilikler sunmakta ve tehditlere karşı daha etkili çözümler sağlamakta ama siber güvenlik politikalarının sürekli olarak güncellenmesi, uluslararası iş birliklerinin artırılması ve siber tehditlere karşı daha kapsamlı

düzenlemelerin yapılması gerekmektedir (Kale, 2024; Lysenko vd., 2024). Ayrıca Chouraik, El-founir ve Taibi (2024) çalışmasında yapay zekanın siber güvenlikteki etkisi ve bu teknolojinin tehdit yönetimi alanındaki paradigmayı nasıl değiştirdiği incelenmiştir. Çalışma, AI'nın siber güvenlikte nasıl yeni bir yaklaşım sunduğunu ve tehditlerin önceden tespit edilmesini nasıl mümkün kıldığını tartışmaktadır. Bu kapsamda Zhang vd., (2021) çalışmasında yapay zekanın siber güvenlikteki ilerlemeleri, karşılaşılan zorluklar ve fırsatlar incelenmiştir. Çalışma, AI'nın siber tehditlerle mücadelede nasıl bir devrim yaratabileceğini ve bu teknolojinin güvenlik alanındaki potansiyelini araştırmaktadır.

2.4.2. Türkiye'de Siber Güvenlik

Türkiye, dijitalleşmenin hız kazanmasıyla birlikte siber güvenlik alanına giderek daha fazla önem vermekte ve ulusal güvenlik stratejilerinde siber tehditlere karşı kapsamlı politikalar geliştirmektedir. Kamu kurumları, özel sektör ve akademik çalışmalar, Türkiye'nin siber güvenlik altyapısını güçlendirmek amacıyla çeşitli projeler yürütmektedir. Siber tehditlerin küresel ölçekte artması ve kritik altyapıların hedef alınması, Türkiye'nin de bu alanda güçlü bir savunma mekanizması oluşturmasını zorunlu kılmaktadır (Maathuis ve Cools, 2025). Bu nedenle Türkiye'de siber güvenlik alanında hem teknik hem de hukuki düzenlemeler yapılmakta ve uluslararası iş birlikleri güçlendirilmektedir. Ayrıca Çalışkan (2024) çalışmasında yapay zeka ile güçlendirilmiş siber saldırıların uluslararası ilişkiler üzerindeki etkileri incelenmiştir. Çalışma, AI tabanlı siber tehditlerin uluslararası ilişkilerde nasıl yeni dinamikler yarattığını ve bu tehditlere karşı alınacak önlemleri araştırmaktadır. Türkiye, siber güvenlik stratejilerini geliştirmek için Ulusal Siber Güvenlik Stratejisi ve Eylem Planı gibi politikalar benimsemekte ve devletin dijital varlıklarını korumak için çeşitli önlemler almaktadır. Bilgi Teknolojileri ve İletişim Kurumu (BTK) bünyesinde faaliyet gösteren Ulusal Siber Olaylara Müdahale Merkezi (USOM), Türkiye'de siber saldırılara karşı hızlı ve etkin müdahaleler gerçekleştirmek amacıyla kurulmuş olup ulusal siber güvenlik stratejilerinin uygulanmasında kritik bir rol oynamaktadır. USOM, tehdit istihbaratı toplamakta, siber olayları analiz etmekte ve kamu ile özel sektör kuruluşlarına güvenlik konularında rehberlik etmektedir.

Türkiye’de siber güvenlik politikalarının önemli bir ayağını kritik altyapıların korunması oluşturmaktadır. Enerji santralleri, finans kurumları, iletişim sistemleri, sağlık sektörü ve ulaştırma ağları gibi kritik altyapılar, siber saldırılara karşı korunmakta ve bu alanlarda güvenlik önlemleri artırılmaktadır (Mijwil vd., 2022). Özellikle enerji ve finans sektöründe yer alan kuruluşlar, siber saldırılara karşı daha güçlü güvenlik sistemleri oluşturmakta ve yapay zeka destekli tehdit tespit mekanizmalarını devreye sokmaktadır. Türkiye’de yapay zeka tabanlı siber güvenlik çözümleri de giderek daha fazla benimsenmektedir. Büyük veri analitiği, makine öğrenimi ve derin öğrenme teknikleri kullanılarak tehditlerin önceden tespit edilmesi ve saldırılara karşı otomatik yanıt mekanizmalarının geliştirilmesi için çeşitli projeler yürütülmektedir (Maathuis ve Cools, 2025; Mijwil vd., 2022). Bu bağlamda Türkiye, siber güvenlik alanında yerli ve milli çözümler geliştirme hedefi doğrultusunda çeşitli projeler yürütmektedir. TÜBİTAK, ASELSAN, HAVELSAN ve Roketsan gibi savunma sanayii kuruluşları, yapay zeka destekli siber güvenlik sistemleri geliştirmekte ve Türkiye’nin dijital güvenliğini artırmak için yerli teknolojiler üretmektedir. HAVELSAN’ın geliştirdiği Siber Güvenlik Operasyon Merkezi (SOC), tehditlerin izlenmesi, anomali tespiti ve saldırılara hızlı müdahale edilmesi için yapay zeka ve büyük veri teknolojilerinden faydalanmaktadır. Türkiye’de siber güvenlik alanında yapılan çalışmalar, sadece kamu ve özel sektörle sınırlı kalmamakta, aynı zamanda akademik alanda da önemli gelişmeler yaşanmaktadır. Üniversitelerde siber güvenlik merkezleri kurulmakta ve bu alanda uzman yetiştirilmesi için yüksek lisans ve doktora programları açılmaktadır (Naik vd., 2022).

Türkiye’nin siber güvenlik alanındaki bir diğer önemli politikası uluslararası iş birlikleri ve NATO ile ortak çalışmalar olmaktadır. Türkiye, NATO Siber Savunma Mükemmeliyet Merkezi’nin faaliyetlerine katılmakta ve NATO müttefikleriyle siber tehdit istihbaratı paylaşımı yapmaktadır (Nami vd., 2024). Ayrıca Avrupa Birliği ve diğer uluslararası kuruluşlarla ortak projeler yürütülmekte ve küresel siber güvenlik standartlarına uyum sağlanmaktadır. Bu süreçle ilişkili olarak Folorunso vd., (2024) çalışmasında yapay zekanın siber güvenlik ve güvenlik uyumu üzerindeki etkisi incelenmiştir. Çalışma, yapay zekanın güvenlik uyumu süreçlerini nasıl güçlendirdiğini ve bu teknolojinin siber tehditlere karşı nasıl bir savunma sunduğunu

tartışmaktadır. Bununla birlikte Türkiye’de siber güvenlik alanında hala çeşitli zorluklar ve geliştirilmesi gereken alanlar bulunmaktadır. Siber suçların artması, kritik altyapılara yönelik saldırıların çoğalması ve sosyal mühendislik saldırılarının daha yaygın hale gelmesi, güvenlik önlemlerinin sürekli olarak güncellenmesini zorunlu kılmaktadır. Özellikle fidye yazılımı saldırıları, kimlik avı saldırıları ve devlet destekli siber casusluk faaliyetleri, Türkiye’nin siber güvenlik gündeminde önemli bir yer tutmaktadır (Naik vd., 2022; Nami vd., 2024).

Türkiye, Siber Güvenlik Yasası ve diğer yasal düzenlemelerle siber tehditlere karşı hukuki altyapıyı güçlendirmekte ve kişisel verilerin korunmasını sağlamak amacıyla çeşitli önlemler almaktadır. Kişisel Verileri Koruma Kurumu (KVKK), bireylerin dijital güvenliğini artırmak için denetimler yapmakta ve veri ihlallerine karşı yaptırımlar uygulamaktadır (Obi vd., 2024; Öz, 2023). Bu kapsamda Zeng (2022) çalışmasında yapay zekanın siber güvenlikteki tehditleri nasıl güçlendirebileceği ve bu tehditlere karşı alınacak stratejik önlemler tartışılmaktadır. Çalışma, AI tabanlı siber saldırılara karşı hangi stratejilerin uygulanabileceğine dair öneriler sunmaktadır. Ayrıca siber güvenlik alanında farkındalık artırıcı kampanyalar düzenlenmekte ve bireylerin dijital tehditlere karşı bilinçlendirilmesi sağlanmaktadır.

3. YÖNTEM

3.1. Araştırma Deseni

Bu araştırmada nicel araştırma yöntemi çerçevesinde betimsel ve ilişkisel tarama modelleri bir arada kullanılmıştır. Betimsel tarama modeli, belirli bir konuda var olan durumu tanımlamayı ve mevcut durumu oluşturan değişkenleri analiz ederek betimleyici sonuçlar elde etmeyi amaçlamıştır. İlişkisel tarama boyutu ise betimlenen değişkenler arasındaki ilişkilerin derecesini ve yönünü belirlemeye odaklanmıştır. Araştırma deseni, siber güvenlik alanındaki farkındalık, yapay zeka tabanlı güvenlik çözümlerine yönelik tutumlar ve kurumsal güvenlik politikalarına uyum gibi değişkenleri kapsamlı bir şekilde incelemeyi mümkün kılmıştır. Araştırma deseninin bütüncül yapısı, hem betimleyici istatistiklerle mevcut tabloyu ortaya koymayı hem de değişkenler arasındaki etkileşimleri analiz etmeyi sağlamıştır. Nicel yöntemlerin tercih edilmesinde, siber güvenlik ve yapay zeka gibi teknoloji odaklı alanlarda veri analizinin ölçülebilir ve istatistiksel olarak yorumlanabilir sonuçlar sunması etkili olmuştur. Betimsel ve ilişkisel tarama modellerinin birlikte uygulanması, araştırmada geniş kapsamlı bir bakış açısı sağlamakla birlikte, araştırmacının farklı değişkenler arasındaki ilişkileri daha derinlemesine incelemesine olanak tanımıştır.

3.2. Evren ve Örneklem

Araştırmanın evrenini, Türkiye’de faaliyet gösteren teknoloji şirketleri ve farklı sektörlerdeki şirketlerin bilişim veya teknoloji departmanlarında görev yapan uzmanlar oluşturmuştur. Bu evren, siber güvenlik alanında karar verici, uygulayıcı veya politika belirleyici konumda bulunan profesyonellerden meydana gelmiştir. Evrenin büyüklüğü kesin olarak bilinmediğinden, bilinmeyen evren durumunda kullanılan örneklem hesaplama yöntemleri uygulanarak yaklaşık bir alt limit belirlenmiştir. Yapılan hesaplamalarda, %95 güven düzeyi ve %10 örneklem hatası temel alınarak en az 96 katılımcıya ulaşılması gerektiği tespit edilmiştir. Örneklem sayısının öngörülemeyen veri kayıplarına (eksik doldurulmuş anketler, geçersiz cevaplar gibi) karşı daha fazla tutulması amacıyla 120 katılımcı hedefi belirlenmiştir. Katılımcılar, evrende yer alan teknoloji sektöründeki uzmanlar ve farklı sektörlerdeki şirketlerin bilişim departmanlarında çalışan kişiler arasından basit tesadüfi örnekleme

yöntemiyle seçilmiştir. Bu yaklaşım, her bir katılımcının seçilme olasılığını eşit tutarak verilerin temsil gücünü arttırmayı amaçlamıştır.

3.3. Veri Toplama Süreci

Veri toplama süreci, 01.03.2025 tarihinde başlayıp 01.09.2025 tarihinde sona erecek şekilde planlanmıştır. Süreç başlamadan önce, katılımcılara araştırmanın amacı, kapsamı ve gizlilik ilkeleri hakkında bilgi verilmiş ve gönüllü katılım esasına dayalı olarak onamları alınmıştır. Araştırmanın evrenini oluşturan uzmanlar ve bilişim departmanı çalışanları ile çevrimiçi platformlar aracılığıyla veya yüz yüze görüşmelerle iletişime geçilmiştir. Anket formu, çevrimiçi uygulama (örneğin Google Forms) veya basılı form olarak katılımcılara sunulmuştur. Katılımcıların araştırmaya katılımını kolaylaştırmak amacıyla, araştırmanın önemini vurgulayan kısa bir bilgilendirme metni paylaşılmış ve veri toplama araçlarının kapsamı hakkında özet bilgiler verilmiştir. Süreç boyunca, katılımcıların sorularını yanıtlamak ve anket doldurma konusunda yaşanabilecek teknik veya içerik kaynaklı sorunları gidermek için çevrimiçi destek sağlanmıştır. Toplanan veriler düzenli olarak kontrol edilmiş, eksik veya tutarsız veriler tespit edildiğinde katılımcılardan bilgi teyidi istenmiştir.

3.4. Veri Toplama Araçları

Bu araştırmada, nicel verileri elde etmek amacıyla araştırmacı tarafından geliştirilen ve güncel literatürdeki geçerli ölçeklerden yararlanılarak yapılandırılan bir anket formu kullanılmıştır. Anket formu, demografik bilgiler, siber güvenlik farkındalığı, yapay zeka tabanlı güvenlik çözümlerine yönelik tutumlar ve kurumsal güvenlik politikalarına uyum olmak üzere çeşitli bölümlerden oluşmuştur. Her bir bölümün alt başlıkları, literatürde sıkça karşılaşılan siber tehdit türleri, güvenlik önlemleri ve yapay zeka uygulamalarından yola çıkarak belirlenmiştir. Ankette, beşli Likert ölçeği kullanılmıştır. Katılımcılar, 1 (Kesinlikle Katılmıyorum) ile 5 (Kesinlikle Katılıyorum) arasında derecelendirerek kendi algı, tutum ve farkındalık düzeylerini ifade etmişlerdir. Ölçek maddeleri hazırlanırken, hem kurumların siber güvenlik politikalarına dair çalışan uyumunu hem de bireysel farkındalığı ölçmeye yönelik ifadeler oluşturulmuştur. Bu ifadelerin geliştirilmesinde, mevcut geçerli ve güvenilir ölçekler, uluslararası raporlar ve akademik çalışmalar gözden geçirilmiştir. Anketin ön

uygulaması, küçük bir katılımcı grubuna yapılarak anlaşılabilirlik, tutarlılık ve süre bakımından değerlendirilmiş ve elde edilen geri bildirimler doğrultusunda gerekli düzeltmeler yapılmıştır.

3.5. Veri Analizi

Toplanan veriler, istatistiksel analiz yazılımları kullanılarak değerlendirilmiştir. İlk aşamada, anket formunda yer alan maddelere verilen yanıtların eksiksiz ve tutarlı olup olmadığı kontrol edilmiş ve geçersiz formlar analiz dışı bırakılmıştır. Ardından, verilerin tanımlayıcı istatistikleri (frekans, yüzde, ortalama, standart sapma) incelenerek temel dağılımlar belirlenmiştir. Ölçeklerin yapı geçerliliğini ortaya koymak amacıyla açımlayıcı faktör analizi uygulanmış ve faktör yük değerlerine göre maddelerin uygunluğu değerlendirilmiştir. Faktör analizi sonucunda, ölçeklerin alt boyutlarının belirlenmesi sağlanmış ve bu boyutlar arasındaki iç tutarlılık Cronbach's Alpha katsayısıyla hesaplanmıştır. Daha sonra, verilerin normal dağılıma uygunluğu çarpıklık ve basıklık değerleri yardımıyla incelenmiştir. Normal dağılıma uygunluk tespit edildiği durumlarda, ölçek puanları ile demografik değişkenler arasındaki ilişkileri ortaya koymak ve farklılıkları test etmek amacıyla parametrik testler (t testi ve ANOVA) uygulanmıştır. Gruplar arası farklılıklar anlamlı çıktığında, hangi gruplar arasında farklılık olduğunu belirlemek üzere Post-Hoc analizler yürütülmüştür.

4. BULGULAR

GEÇERLİK VE GÜVENİRLİK ANALİZİ

Açımlayıcı Faktör Analizi

Araştırmada kullanılan ölçeklerin yapı geçerliğini tespit etmek için açımlayıcı faktör analizi yapılmıştır. Ölçeğin faktör analizine uygun olup olmadığını anlamak amacıyla KMO ve Bartlett testi yapılmıştır. KMO katsayısı örneklemin büyüklüğünü test etmek için hesaplanırken normal dağılım koşulu Bartlett testiyle incelenmektedir. Bu kapsamda KMO testi ölçüm sonucunun .50 ve daha üstü, Bartlett küresellik testi sonucunun da istatistiksel olarak anlamlı olması gerekmektedir (Jeong, 2004: 70). Faktör analizi işleminde ölçek maddelerinin faktörlere atanması ya da ölçekten çıkarılması işlemlerinde faktör yükü değerlerine bakılmıştır.

Güvenirlilik Analizi

Cronbach's alfa katsayısı ölçeğin güvenirlik düzeyini vermektedir. Katsayı 0 ile 1 arasında değişmektedir. Alfa (α) katsayısına bağlı olarak ölçeğin güvenilirliği şu şekilde yorumlanmaktadır (Nunnally, 1967, 248).

- $.00 \leq \alpha < .40$ ise ölçek güvenilir değildir,^{[1][2]}
- $.40 \leq \alpha < .60$ ise ölçeğin güvenirliği düşük,^{[1][2]}
- $.60 \leq \alpha < .80$ ise ölçek oldukça güvenilir,^{[1][2]}
- $.80 \leq \alpha < 1.00$ ise ölçek yüksek derecede güvenilir bir ölçektir.

Tablo 1: Siber Güvenlik Farkındalığı ve Davranışları

	n	Minimum	Maximum	ort	ss
1.Siber güvenlik tehditleri hakkında yeterli bilgiye sahibim.	132	1	5	3,54	1,181
2.Çalıştığım kurumda veya kişisel kullanım için siber güvenlik eğitimleri alıyorum.	132	1	5	2,95	0,745
3.Güçlü şifreler oluşturur ve düzenli olarak değiştiririm.	132	1	5	4,01	1,122
4.Yazılım güncellemelerini düzenli olarak yaparım.	132	1	5	3,97	1,139
5.Phishing (oltalama) saldırılarını tanıyabilir ve tespit edebilirim.	132	1	5	3,70	1,215
6.Kendi cihazlarımda güvenlik duvarı ve antivirüs yazılımı kullanırım.	132	1	5	3,74	1,183

7.Sosyal mühendislik saldırılarına karşı dikkatliyim.	132	1	5	3,87	1,135
8.Çevrimiçi bağlantılarımda veri güvenliği konusunda dikkatli davranırım.	132	1	5	4,03	1,112
9.Yapay zeka destekli güvenlik araçlarını kullanmayı faydalı buluyorum.	132	1	5	3,83	1,099
10.Yapay zeka destekli sistemlerin siber tehditlere karşı farkındalığı artıracağını düşünüyorum.	132	1	5	3,86	1,085

Bu çalışmada, “Siber Güvenlik Farkındalığı ve Davranışları” ölçeğine ait maddelerin tanımlayıcı istatistikleri değerlendirilmiş; her bir maddenin ortalama ($\bar{X}$) ve standart sapma (SS) değerleri incelenmiştir. Bu analiz, katılımcıların siber güvenlik farkındalık düzeylerini ve ilgili davranış eğilimlerini yansıtmak amacıyla yapılmıştır. Tanımlayıcı istatistikler doğrultusunda, en yüksek ortalama değer “Çevrimiçi bağlantılarımda veri güvenliği konusunda dikkatli davranırım” ($\bar{X} = 4,03$, SS = 1,112) maddesinde olduğu görülmektedir. Bu bulgu, katılımcıların çevrimiçi veri güvenliği konusunda genel olarak dikkatli davrandıklarını göstermektedir. Bunu takiben, “Güçlü şifreler oluşturur ve düzenli olarak değiştiririm” ($\bar{X} = 4,01$, SS = 1,122) ve “Yazılım güncellemelerini düzenli olarak yaparım” ($\bar{X} = 3,97$, SS = 1,139) ifadeleri yüksek ortalama değerleriyle öne çıkmaktadır. Bu sonuçlar, bireylerin temel güvenlik uygulamalarını büyük ölçüde benimsediğini ortaya koymaktadır.

“Yapay zeka destekli sistemlerin siber tehditlere karşı farkındalığı artıracağını düşünüyorum” ($\bar{X} = 3,86$, SS = 1,085) ve “Sosyal mühendislik saldırılarına karşı dikkatliyim” ($\bar{X} = 3,87$, SS = 1,135) maddeleri de yüksek ortalamalarla katılımcıların ileri düzey siber güvenlik yaklaşımlarına dair olumlu görüşlerini yansıtmaktadır.

Buna karşın, en düşük ortalama “Çalıştığım kurumda veya kişisel kullanım için siber güvenlik eğitimleri alıyorum” ($\bar{X} = 2,95$, SS = 0,745) maddesinde gözlemlenmiştir. Bu durum, katılımcıların siber güvenlik eğitimi alma düzeylerinin görece düşük olduğunu ve kurumsal/kişisel düzeyde bu konuda daha fazla eğitim ihtiyacı olduğunu göstermektedir.

Katılımcıların bireysel siber güvenlik önlemlerine yönelik davranışlarının genellikle olumlu olduğunu, ancak kurumsal düzeyde siber güvenlik eğitimi alma oranlarının görece düşük kaldığını ortaya koymaktadır. Ayrıca, standart sapma

değerlerinin 1'in üzerinde olması, bazı maddelerde katılımcı yanıtlarında çeşitlilik olduğunu göstermektedir.

Tablo 2: Verinin Faktör Analizine Uygunluğu

KMO		0,884
	X ²	1203,682
Bartlett Testi	sd	45
	p	0,000

Veri setinin faktör analizine uygunluğu Kaiser-Meyer-Olkin (KMO) örneklem yeterlilik ölçütü ve Bartlett Küresellik Testi ile değerlendirilmiştir. KMO değeri 0,884 olarak hesaplanmıştır ve bu değer, örneklemin faktör analizine son derece uygun olduğunu göstermektedir. Bartlett Küresellik Testi sonucunda hesaplanan Ki-Kare değeri 1203,682 olup, bu değer 45 serbestlik derecesiyle anlamlı bulunmuştur ($p < 0,001$). Bu sonuçlar, değişkenler arasında yeterli düzeyde korelasyon olduğunu ve veri setinin faktör analizi uygulamak için uygun olduğunu ortaya koymaktadır.

Tablo 3: Siber Güvenlik Farkındalığı ve Davranışları Ölçeğine Ait Açıklayıcı Faktör Analizi ve Güvenilirlik Sonuçları

	Siber Güvenlik Farkındalığı ve Davranışları	Açıklanan Varyans Oranı	Cronbach's Alpha
3.Güçlü şifreler oluşturur ve düzenli olarak değiştiririm.	0,914		
8.Çevrimiçi bağlantılarımda veri güvenliği konusunda dikkatli davranırım.	0,902		
4.Yazılım güncellemelerini düzenli olarak yaparım.	0,890		
7.Sosyal mühendislik saldırılarına karşı dikkatliyim.	0,876		
5.Phishing (oltalama) saldırılarını tanıyabilir ve tespit edebilirim.	0,829	72,746	0,952
6.Kendi cihazlarımda güvenlik duvarı ve antivirüs yazılımı kullanırım.	0,828		
10.Yapay zeka destekli sistemlerin siber tehditlere karşı farkındalığı artıracağını düşünüyorum.	0,825		
9.Yapay zeka destekli güvenlik araçlarını kullanmayı faydalı buluyorum.	0,820		
1.Siber güvenlik tehditleri hakkında yeterli bilgiye sahibim.	0,784		

Açıklayıcı faktör analizi sonucunda, “Siber Güvenlik Farkındalığı ve Davranışları” ölçeğinin tek faktörlü bir yapı sergilediği belirlenmiştir. Faktör yükleri incelendiğinde, tüm maddelerin yüklerinin oldukça yüksek olduğu ve ölçeğin ölçtüğü

yapıya güçlü katkı sağladığı görülmektedir. En yüksek faktör yükü “Güçlü şifreler oluşturur ve düzenli olarak değiştiririm.” maddesinde (0,914) yer almakta, bunu “Çevrimiçi bağlantılarımda veri güvenliği konusunda dikkatli davranırım.” (0,902), “Yazılım güncellemelerini düzenli olarak yaparım.” (0,890) ve “Sosyal mühendislik saldırılarına karşı dikkatliyim.” (0,876) gibi maddeler izlemektedir. En düşük faktör yükü ise “Siber güvenlik tehditleri hakkında yeterli bilgiye sahibim.” maddesinde olup, 0,784 olarak hesaplanmıştır. Tüm maddelerin faktör yüklerinin 0,70’in üzerinde olması, ölçeğin yapı geçerliliğinin güçlü olduğunu göstermektedir.

Analiz sonucunda elde edilen bu tek faktörlü yapı, toplam varyansın %72,746’sını açıklamaktadır. Bu oran, sosyal bilimler araştırmalarında tek faktörlü yapılar için oldukça yeterli bir açıklama gücüne işaret etmektedir. Ölçeğin iç tutarlılığını değerlendirmek amacıyla yapılan güvenilirlik analizinde, Cronbach’s Alpha katsayısı 0,952 olarak bulunmuştur. Bu yüksek değer, ölçeğin son derece güvenilir ve iç tutarlılığı güçlü bir ölçme aracı olduğunu ortaya koymaktadır. Faktör yükü 0,30’un altında kalan “2.Çalıştığım kurumda veya kişisel kullanım için siber güvenlik eğitimleri alıyorum.” maddesi analiz dışında bırakılmıştır.

Tablo 4: Risk Algısı ve Yapay Zeka Destekli Güvenlik Önlemleri

	n	Minimum	Maximum	ort	ss
11.Siber güvenlik tehditleri, günlük işlerimi ve mesleğimi etkileyebilir.	132	1	5	3,99	1,149
12.Yapay zeka tabanlı güvenlik çözümleri tehditleri önceden tespit edebilir.	132	1	5	3,78	1,107
13.Yapay zeka destekli güvenlik sistemleri saldırılara daha hızlı yanıt verir.	132	1	5	3,82	1,090
14.Yapay zeka destekli güvenlik sistemlerinin yanlış pozitif (false positive) tehdit algılaması sorun yaratabilir.	132	1	5	3,72	1,135
15.Yapay zeka, saldırıların kaynağını daha hızlı belirleyebilir.	132	1	5	3,77	1,143
16.Yapay zekanın siber saldırıları önceden tahmin edebilme kabiliyetine güveniyorum.	132	1	5	3,51	1,156
17.Yapay zeka, insan faktörünü azaltarak siber güvenliği daha etkili hale getirebilir.	132	1	5	3,60	1,145
18.Yapay zeka destekli güvenlik çözümleri veri gizliliği açısından risk taşıyabilir.	132	1	5	3,60	1,158
19.Yapay zeka tabanlı güvenlik çözümlerinin uzun vadede kurumsal güvenlik maliyetlerini azaltacağını düşünüyorum.	132	1	5	3,78	1,141
20.Yapay zeka destekli güvenlik sistemlerinin bireysel kullanıcılar için uygun olduğunu düşünüyorum.	132	1	5	3,58	1,166

Bu çalışmada, “Risk Algısı ve Yapay Zeka Destekli Güvenlik Önlemleri” ölçeğine ait maddelerin tanımlayıcı istatistikleri değerlendirilmiş; her bir maddenin ortalama ($\bar{X}$) ve standart sapma (SS) değerleri incelenmiştir. Bu analiz, katılımcıların yapay zeka tabanlı siber güvenlik çözümlerine yönelik algılarını ve güvenlik risklerine dair farkındalık düzeylerini ortaya koymak amacıyla yapılmıştır.

Tanımlayıcı istatistikler doğrultusunda, en yüksek ortalama değer “Siber güvenlik tehditleri, günlük işlerimi ve mesleğimi etkileyebilir” ($\bar{X} = 3,99$, SS = 1,149) maddesinde olduğu görülmektedir. Bu bulgu, katılımcıların siber güvenlik tehditlerini bireysel ve mesleki yaşam açısından önemli bir risk unsuru olarak gördüklerini göstermektedir. Bunu takiben, “Yapay zeka destekli güvenlik sistemleri saldırılara daha hızlı yanıt verir” ($\bar{X} = 3,82$, SS = 1,090) ve “Yapay zeka tabanlı güvenlik çözümleri tehditleri önceden tespit edebilir” ($\bar{X} = 3,78$, SS = 1,107) maddeleri yüksek ortalamalarıyla dikkat çekmektedir. Bu sonuçlar, katılımcıların yapay zekanın proaktif tehdit yönetiminde etkili olabileceğine dair olumlu görüşlere sahip olduklarını ortaya koymaktadır.

“Yapay zeka tabanlı güvenlik çözümlerinin uzun vadede kurumsal güvenlik maliyetlerini azaltacağını düşünüyorum” ($\bar{X} = 3,78$, SS = 1,141) ve “Yapay zeka, saldırıların kaynağını daha hızlı belirleyebilir” ($\bar{X} = 3,77$, SS = 1,143) ifadeleri de benzer şekilde yüksek ortalama değerleriyle öne çıkmaktadır. Bu durum, katılımcıların yapay zekanın hem ekonomik katkı sağlayacağına hem de analiz süreçlerini hızlandıracağına inandıklarını göstermektedir.

En düşük ortalama değer ise “Yapay zekanın siber saldırıları önceden tahmin edebilme kabiliyetine güveniyorum” ($\bar{X} = 3,51$, SS = 1,156) maddesinde gözlemlenmiştir. Bu durum, katılımcıların bu teknolojiye duyduğu güvenin diğer maddelere kıyasla görece daha sınırlı olduğunu işaret etmektedir. Ayrıca, “Yapay zeka destekli güvenlik çözümleri veri gizliliği açısından risk taşıyabilir” ($\bar{X} = 3,60$, SS = 1,158) maddesi, bu sistemlerin olası olumsuz yönlerine dair farkındalık bulunduğunu göstermektedir.

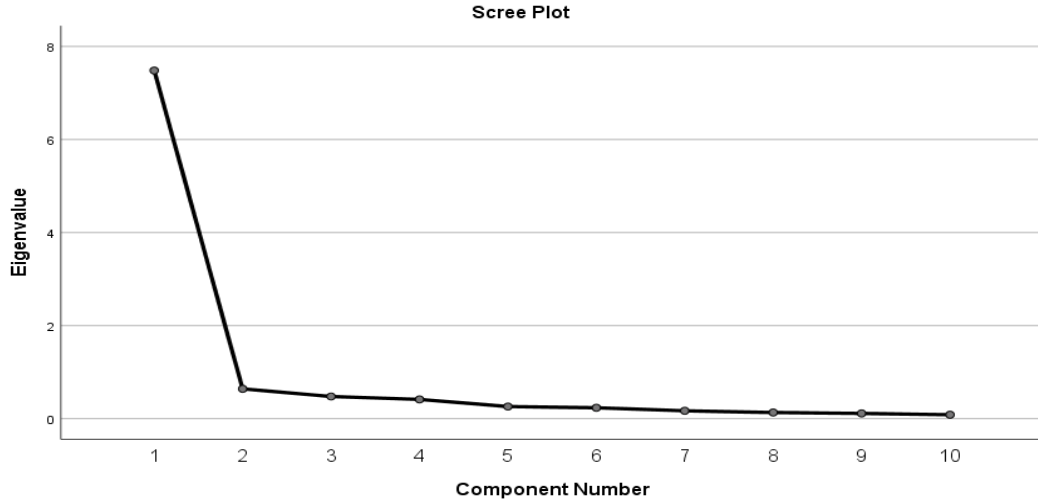
Katılımcıların yapay zeka destekli güvenlik çözümlerini genel olarak olumlu değerlendirdiğini, ancak veri gizliliği ve öngörü kapasitesi konularında daha temkinli

yaklaştıklarını ortaya koymaktadır. Ayrıca, tüm maddelerde standart sapma değerlerinin 1'in üzerinde olması, yanıtların yüksek düzeyde değişkenlik gösterdiğini ve bireyler arasında görüş ayrılıklarının bulunduğunu göstermektedir.

Tablo 5: Verinin Faktör Analizine Uygunluğu

KMO		0,928
Bartlett Testi	X ²	1438,540
	sd	45
	p	0,000

Veri setinin faktör analizine uygunluğu Kaiser-Meyer-Olkin (KMO) örneklem yeterlilik ölçütü ve Bartlett Küresellik Testi ile değerlendirilmiştir. KMO değeri 0,928 olarak hesaplanmıştır ve bu değer, örneklem büyüklüğünün faktör analizine son derece uygun olduğunu göstermektedir. Bartlett Küresellik Testi sonucunda hesaplanan Ki-Kare (χ^2) değeri 1438,540 olup, 45 serbestlik derecesi ile anlamlı bulunmuştur ($p < 0,001$). Bu sonuçlar, değişkenler arasında yeterli düzeyde korelasyon bulunduğunu ve veri setinin faktör analizi için uygun olduğunu açıkça ortaya koymaktadır.



Şekil 1: Risk Algısı ve Yapay Zeka Destekli Güvenlik Önlemleri Ölçeğine Ait Açımlayıcı Faktör Analizi Grafiği

Tablo 6: Risk Algısı ve Yapay Zeka Destekli Güvenlik Önlemleri Ölçeğine Ait Açımlayıcı Faktör Analizi ve Güvenirlik Sonuçları

	Risk Algısı ve Yapay Zeka Destekli Güvenlik Önlemleri	Açıklanan Varyans Oranı	Cronbach's Alpha
13.Yapay zeka destekli güvenlik sistemleri saldırılara daha hızlı yanıt verir.	0,926	74,825	0,962

12.Yapay zeka tabanlı güvenlik çözümleri tehditleri önceden tespit edebilir.	0,920
15.Yapay zeka, saldırıların kaynağını daha hızlı belirleyebilir.	0,911
19.Yapay zeka tabanlı güvenlik çözümlerinin uzun vadede kurumsal güvenlik maliyetlerini azaltacağını düşünüyorum.	0,905
17.Yapay zeka, insan faktörünü azaltarak siber güvenliği daha etkili hale getirebilir.	0,905
16.Yapay zekanın siber saldırıları önceden tahmin edebilme kabiliyetine güveniyorum.	0,869
14.Yapay zeka destekli güvenlik sistemlerinin yanlış pozitif (false positive) tehdit algılaması sorun yaratabilir.	0,822
18.Yapay zeka destekli güvenlik çözümleri veri gizliliği açısından risk taşıyabilir.	0,806
11.Siber güvenlik tehditleri, günlük işlerimi ve mesleğimi etkileyebilir.	0,799
20.Yapay zeka destekli güvenlik sistemlerinin bireysel kullanıcılar için uygun olduğunu düşünüyorum.	0,769

Açımlayıcı faktör analizi sonucunda, “Risk Algısı ve Yapay Zeka Destekli Güvenlik Önlemleri” ölçeğinin tek faktörlü bir yapı sergilediği belirlenmiştir. Faktör yükleri incelendiğinde, tüm maddelerin yüklerinin oldukça yüksek olduğu ve ölçeğin ölçtüğü yapıya güçlü katkı sağladığı görülmektedir. En yüksek faktör yükü, “Yapay zeka destekli güvenlik sistemleri saldırılara daha hızlı yanıt verir.” maddesinde (0,926) yer almakta; bunu “Yapay zeka tabanlı güvenlik çözümleri tehditleri önceden tespit edebilir.” (0,920), “Yapay zeka, saldırıların kaynağını daha hızlı belirleyebilir.” (0,911) ve “Yapay zeka tabanlı güvenlik çözümlerinin uzun vadede kurumsal güvenlik maliyetlerini azaltacağını düşünüyorum.” (0,905) gibi maddeler izlemektedir. En düşük faktör yükü ise “Yapay zeka destekli güvenlik sistemlerinin bireysel kullanıcılar için uygun olduğunu düşünüyorum.” maddesinde olup, 0,769 olarak hesaplanmıştır. Tüm maddelerin faktör yüklerinin 0,70’in üzerinde olması, ölçeğin yapı geçerliliğinin oldukça güçlü olduğunu göstermektedir.

Analiz sonucunda elde edilen bu tek faktörlü yapı, toplam varyansın %74,825’ini açıklamaktadır. Bu oran, sosyal bilimlerde kullanılan ölçekler açısından yüksek bir açıklayıcılık düzeyine işaret etmektedir. Ölçeğin iç tutarlılığı Cronbach’s Alpha katsayısı ile 0,962 olarak hesaplanmıştır. Bu değer, ölçeğin son

derece güvenilir olduğunu ve maddeler arasında çok güçlü bir iç tutarlılık bulunduğunu ortaya koymaktadır.

Tablo 7: Kurumsal ve Bireysel Siber Güvenlik Politikaları

	n	Minimum	Maximum	ort	ss
21.Çalıştığım kurumda bilgi güvenliği politikalarına yönelik eğitimler düzenlenmektedir.	132	1	5	3,55	1,344
22.Çalıştığım kurum, siber güvenlik politikalarına uymam konusunda beni teşvik etmektedir.	132	1	5	3,56	1,292
23.Yapay zeka destekli güvenlik çözümlerinin kurumsal güvenliğe katkısı büyüktür.	132	1	5	3,73	1,118
24.Çalıştığım kurumda yapay zeka destekli güvenlik sistemleri aktif olarak kullanılmaktadır.	132	1	5	2,95	0,628
25.Yapay zeka destekli güvenlik araçları veri sızıntılarını önlemede etkilidir.	132	1	5	3,59	1,098
26.Kurumlarda yapay zeka tabanlı güvenlik çözümlerinin entegrasyonu zaman alabilir.	132	1	5	3,76	1,147
27.Kurumların siber güvenlik politikaları yeterince günceldir.	132	1	5	2,95	1,181
28.Yapay zeka destekli güvenlik çözümleri çalışanların siber güvenlik uyumunu artırır.	132	1	5	3,63	1,022
29.Çalıştığım kurumda çalışanların siber güvenlik farkındalığı yeterlidir.	132	1	5	3,13	1,213
30.Yapay zeka, kurumsal siber güvenlik tehditlerine karşı en etkili çözüm olarak görülmelidir.	132	1	5	3,24	1,153

Bu çalışmada, “Kurumsal ve Bireysel Siber Güvenlik Politikaları” ölçeğine ait maddelerin tanımlayıcı istatistikleri değerlendirilmiş; her bir maddenin ortalama ($\bar{X}$) ve standart sapma (SS) değerleri incelenmiştir. Bu analiz, katılımcıların kurumlarında uygulanan siber güvenlik politikalarına ve yapay zeka destekli güvenlik sistemlerine yönelik algılarını ortaya koymak amacıyla yapılmıştır.

Tanımlayıcı istatistikler doğrultusunda, en yüksek ortalama değer “Yapay zeka tabanlı güvenlik çözümlerinin entegrasyonu zaman alabilir” ($\bar{X} = 3,76$, SS = 1,147) maddesinde olduğu görülmektedir. Bu durum, katılımcıların yapay zeka tabanlı güvenlik sistemlerinin kurumsal entegrasyon sürecinin zaman gerektirdiğine dair farkındalıklarının yüksek olduğunu göstermektedir. Bunu takiben, “Yapay zeka destekli güvenlik çözümlerinin kurumsal güvenliğe katkısı büyüktür” ($\bar{X} = 3,73$, SS = 1,118) ve “Yapay zeka destekli güvenlik çözümleri çalışanların siber güvenlik uyumunu artırır” ($\bar{X} = 3,63$, SS = 1,022) ifadeleri yüksek ortalamalarıyla dikkat çekmektedir. Bu bulgular, yapay zekanın güvenlik farkındalığını artırıcı etkisine olan inancı yansıtmaktadır.

Benzer şekilde, “Yapay zeka destekli güvenlik araçları veri sızıntılarını önlemede etkilidir” ($\bar{X} = 3,59$, $SS = 1,098$) ve “Çalıştığım kurum, siber güvenlik politikalarına uymam konusunda beni teşvik etmektedir” ($\bar{X} = 3,56$, $SS = 1,292$) maddeleri de katılımcıların hem kurumsal yönlendirmeleri hem de teknolojik çözümleri olumlu değerlendirdiklerini ortaya koymaktadır. Buna karşın, en düşük ortalamalar “Çalıştığım kurumda yapay zeka destekli güvenlik sistemleri aktif olarak kullanılmaktadır” ($\bar{X} = 2,95$, $SS = 0,628$) ve “Kurumların siber güvenlik politikaları yeterince günceldir” ($\bar{X} = 2,95$, $SS = 1,181$) maddelerinde gözlemlenmiştir. Bu durum, kurumların yapay zeka entegrasyonunda ve güvenlik politikalarının güncelliğinde eksiklikler olduğuna dair katılımcıların kararsız veya olumsuz değerlendirmelerde bulunduğunu göstermektedir.

“Çalıştığım kurumda çalışanların siber güvenlik farkındalığı yeterlidir” ($\bar{X} = 3,13$, $SS = 1,213$) ve “Yapay zeka destekli güvenlik sistemlerinin bireysel kullanıcılar için uygun olduğunu düşünüyorum” ($\bar{X} = 3,24$, $SS = 1,153$) ifadeleri ise katılımcıların bu konularda daha temkinli ve farklı görüşlere sahip olduklarını göstermektedir. Katılımcıların yapay zeka destekli güvenlik çözümlerine genel olarak olumlu yaklaştığını, ancak kurumsal kullanım düzeyi, güncellik ve uygulama yaygınlığı konularında bazı tereddütlere sahip olduklarını ortaya koymaktadır. Ayrıca, birçok maddenin standart sapma değerinin 1’in üzerinde olması, katılımcı görüşlerinde belirgin bir çeşitlilik olduğunu göstermektedir.

Tablo 8: Verinin Faktör Analizine Uygunluğu

KMO		0,862
	x2	1006,956
Bartlett's testi	sd	45
	p	0,000

Veri setinin faktör analizine uygunluğu Kaiser-Meyer-Olkin (KMO) örneklem yeterlilik ölçütü ve Bartlett Küresellik Testi ile değerlendirilmiştir. Yapılan analiz sonucunda KMO değeri 0,862 olarak hesaplanmış olup, bu değer örneklemin faktör analizine oldukça uygun olduğunu göstermektedir. Bartlett Küresellik Testi sonucunda elde edilen Ki-Kare (χ^2) değeri 1006,956, 45 serbestlik derecesi ile istatistiksel olarak anlamlı bulunmuştur ($p < 0,001$). Bu sonuçlar, değişkenler arasında yeterli düzeyde

korelasyon bulunduğunu ve veri setinin faktör analizine uygun olduğunu açıkça ortaya koymaktadır.

Tablo 9: Kurumsal ve Bireysel Siber Güvenlik Politikaları Ölçeğine Ait Açıklayıcı Faktör Analizi ve Güvenirlik Sonuçları

	Yapay Zeka Destekli Kurumsal Güvenlik Algısı Alt Boyutu	Açıklanan Varyans Oranı	Cronbach's Alpha
28.Yapay zeka destekli güvenlik çözümleri çalışanların siber güvenlik uyumunu artırır.	0,906		
23.Yapay zeka destekli güvenlik çözümlerinin kurumsal güvenliğe katkısı büyüktür.	0,898		
25.Yapay zeka destekli güvenlik araçları veri sızıntılarını önlemede etkilidir.	0,877	51,264	0,911
26.Kurumlarda yapay zeka tabanlı güvenlik çözümlerinin entegrasyonu zaman alabilir.	0,768		
30.Yapay zeka, kurumsal siber güvenlik tehditlerine karşı en etkili çözüm olarak görülmelidir.	0,741		
24.Çalıştığım kurumda yapay zeka destekli güvenlik sistemleri aktif olarak kullanılmaktadır.	0,840		
22.Çalıştığım kurum, siber güvenlik politikalarına uymam konusunda beni teşvik etmektedir.	0,725	22,887	0,769
21.Çalıştığım kurumda bilgi güvenliği politikalarına yönelik eğitimler düzenlenmektedir.	0,672		

Açıklayıcı faktör analizi sonucunda, “Kurumsal ve Bireysel Siber Güvenlik Politikaları” ölçeğinin iki faktörlü bir yapı sergilediği belirlenmiştir. Faktör yükleri incelendiğinde, maddelerin anlamlı biçimde iki alt boyut altında toplandığı görülmektedir.

Birinci faktör, “Yapay Zeka Destekli Kurumsal Güvenlik Algısı” olarak adlandırılmıştır. Bu faktörde yer alan maddeler, yapay zeka tabanlı sistemlerin kurumsal güvenliğe katkılarını ve güvenlik süreçlerindeki etkinliklerini yansıtmaktadır. En yüksek faktör yükü “Yapay zeka destekli güvenlik çözümleri çalışanların siber güvenlik uyumunu artırır” (0,906) maddesinde yer almakta; bunu “Yapay zeka destekli güvenlik çözümlerinin kurumsal güvenliğe katkısı büyüktür” (0,898) ve “Yapay zeka destekli güvenlik araçları veri sızıntılarını önlemede etkilidir”

(0,877) maddeleri takip etmektedir. Bu alt boyut, toplam varyansın %51,264'ünü açıklamakta ve güvenilirlik düzeyi Cronbach's Alpha = 0,911 ile oldukça yüksek bir iç tutarlılık sergilemektedir.

İkinci faktör ise “Kurumsal Uyum ve Eğitim Destekli Güvenlik Politikaları” olarak adlandırılmıştır. Bu boyutta, kurumların çalışanlarını siber güvenlik konusunda eğitime, teşvik etme ve kurumsal sistemlerde yapay zeka kullanımı gibi konular yer almaktadır. En yüksek faktör yükü “Çalıştığım kurumda yapay zeka destekli güvenlik sistemleri aktif olarak kullanılmaktadır” (0,840) maddesinde gözlemlenmiştir. Bunu “Çalıştığım kurum, siber güvenlik politikalarına uymam konusunda beni teşvik etmektedir” (0,725) ve “Çalıştığım kurumda bilgi güvenliği politikalarına yönelik eğitimler düzenlenmektedir” (0,672) maddeleri takip etmektedir. Bu faktör, toplam varyansın %22,887'sini açıklamakta olup, iç tutarlılığı Cronbach's Alpha = 0,769 olarak hesaplanmıştır.

Faktör yükü 0,30'un altında kalan “27. Kurumların siber güvenlik politikaları yeterince günceldir.” ve “29. Çalıştığım kurumda çalışanların siber güvenlik farkındalığı yeterlidir.” maddeleri analiz dışında bırakılmıştır.

Tablo 10: Siber Zorbalık ve Dijital Güvenlik

	n	Minimum	Maximum	ort	ss
31.Yapay zeka, siber zorbalık içeriklerini tespit etmede başarılıdır.	132	1	5	3,60	1,097
32.Sosyal medya platformları yapay zeka destekli güvenlik sistemleri ile daha güvenli hale getirilebilir.	132	1	5	3,74	1,046
33.Yapay zeka destekli içerik filtreleme sistemleri etkili bir siber zorbalık önleme yöntemidir.	132	1	5	3,64	1,106
34.Yapay zeka destekli güvenlik çözümleri kişisel mahremiyeti ihlal edebilir.	132	1	5	3,61	1,060
35.Çevrimiçi platformlarda yapay zeka tarafından otomatik içerik denetimi yapılmalıdır.	132	1	5	3,76	1,092
36.Yapay zeka, dijital ortamda kötü amaçlı içerikleri engellemede başarılıdır.	132	1	5	3,69	1,042
37.Çevrimiçi taciz ve zorbalık, yapay zeka sistemleri sayesinde azaltılabilir.	132	1	5	3,81	1,064
38.Siber zorbalık yapan kişileri tespit etmek için yapay zeka destekli sistemler kullanışlıdır.	132	1	5	3,86	1,071
39.Yapay zeka tabanlı algoritmalar çevrimiçi tehditleri daha iyi analiz eder.	132	1	5	3,70	1,070
40.Yapay zeka destekli siber güvenlik çözümleri, çocukların çevrimiçi güvenliğini artırabilir.	132	1	5	3,83	1,066

Bu çalışmada, “Siber Zorbalık ve Dijital Güvenlik” ölçeğine ait maddelerin tanımlayıcı istatistikleri değerlendirilmiş; her bir maddenin ortalama ($\bar{X}$) ve standart sapma (SS) değerleri incelenmiştir. Bu analiz, katılımcıların yapay zeka destekli sistemlerin dijital güvenlik süreçlerinde ve siber zorbalıkla mücadeledeki rolüne ilişkin algılarını ortaya koymak amacıyla gerçekleştirilmiştir.

Tanımlayıcı istatistikler doğrultusunda, en yüksek ortalama değer “Siber zorbalık yapan kişileri tespit etmek için yapay zeka destekli sistemler kullanışlıdır” ($\bar{X} = 3,86$, $SS = 1,071$) maddesinde olduğu görülmektedir. Bu bulgu, katılımcıların yapay zeka sistemlerinin siber zorbalık yapan bireyleri tanımlamada etkili araçlar olduğuna inandıklarını göstermektedir. Bunu takiben, “Yapay zeka destekli siber güvenlik çözümleri, çocukların çevrimiçi güvenliğini artırabilir” ($\bar{X} = 3,83$, $SS = 1,066$) ve “Çevrimiçi taciz ve zorbalık, yapay zeka sistemleri sayesinde azaltılabilir” ($\bar{X} = 3,81$, $SS = 1,064$) maddeleri yüksek ortalamalarıyla dikkat çekmektedir. Bu bulgular, yapay zekanın çevrimiçi tehditlerle mücadelede koruyucu bir işlev üstlendiğine yönelik yaygın bir görüş olduğunu ortaya koymaktadır.

Benzer şekilde, “Çevrimiçi platformlarda yapay zeka tarafından otomatik içerik denetimi yapılmalıdır” ($\bar{X} = 3,76$, $SS = 1,092$) ve “Sosyal medya platformları yapay zeka destekli güvenlik sistemleri ile daha güvenli hale getirilebilir” ($\bar{X} = 3,74$, $SS = 1,046$) ifadeleri de, katılımcıların yapay zeka destekli içerik denetim sistemlerine olumlu yaklaştığını göstermektedir.

Diğer yandan, görece daha düşük ortalama değerler “Yapay zeka, siber zorbalık içeriklerini tespit etmede başarılıdır” ($\bar{X} = 3,60$, $SS = 1,097$) ve “Yapay zeka destekli güvenlik çözümleri kişisel mahremiyeti ihlal edebilir” ($\bar{X} = 3,61$, $SS = 1,060$) maddelerinde gözlemlenmiştir. Bu durum, bazı katılımcıların yapay zekanın mahremiyet ihlali riski taşıyabileceğine veya içerik tespiti konusunda sınırlı başarıya sahip olabileceğine dair temkinli bir tutum sergilediğini göstermektedir.

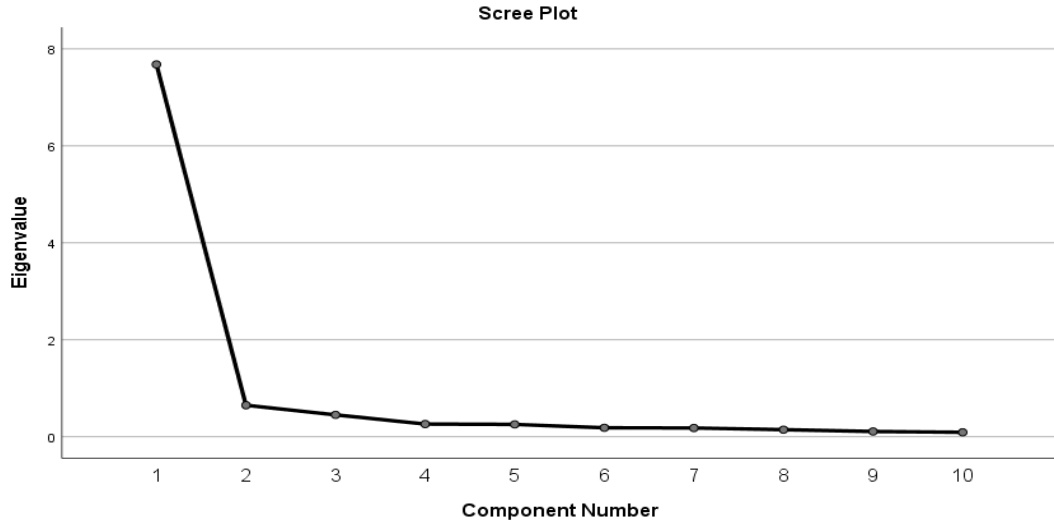
Katılımcıların yapay zeka destekli güvenlik çözümlerini dijital güvenliğin artırılması ve siber zorbalığın önlenmesi açısından genel olarak olumlu değerlendirdiklerini ortaya koymaktadır. Bununla birlikte, kişisel mahremiyet ve içerik analiz kapasitesi gibi konularda bazı çekincelerin bulunduğu görülmektedir.

Ayrıca, tüm maddelerde standart sapma değerlerinin 1'in üzerinde olması, yanıtların çeşitlilik gösterdiğini ve katılımcılar arasında bu konuda farklı düşünce yapılarına sahip bireylerin yer aldığını göstermektedir.

Tablo 11: Verinin Faktör Analizine Uygunluğu

KMO		0,948
Bartlett's Testi	x2	1505,886
	sd	45
	p	0,000

Veri setinin faktör analizine uygunluğu Kaiser-Meyer-Olkin (KMO) örneklem yeterlilik ölçütü ve Bartlett Küresellik Testi ile değerlendirilmiştir. KMO değeri 0,948 olarak hesaplanmıştır ve bu değer, örneklem büyüklüğünün faktör analizine mükemmel derecede uygun olduğunu göstermektedir. Bartlett Küresellik Testi sonucunda hesaplanan Ki-Kare (χ^2) değeri 1505,886, 45 serbestlik derecesi ile anlamlı bulunmuştur ($p < 0,001$). Bu sonuçlar, değişkenler arasında yeterli düzeyde korelasyon bulunduğunu ve veri setinin faktör analizi için son derece uygun olduğunu ortaya koymaktadır.



Şekil 2: Siber Zorbalık ve Dijital Güvenlik Ölçeğine Ait Açımlayıcı Faktör Analizi Grafiği

Tablo 12: Siber Zorbalık ve Dijital Güvenlik Ölçeğine Ait Açımlayıcı Faktör Analizi ve Güvenirlik Sonuçları

	Faktör Yüğü 1	Açıklanan Varyans Oranı	Cronbach's Alpha
--	---------------	-------------------------	------------------

39.Yapay zeka tabanlı algoritmalar çevrimiçi tehditleri daha iyi analiz eder.	0,918		
37.Çevrimiçi taciz ve zorbalık, yapay zeka sistemleri sayesinde azaltılabilir.	0,914		
38.Siber zorbalık yapan kişileri tespit etmek için yapay zeka destekli sistemler kullanışlıdır.	0,909		
33.Yapay zeka destekli içerik filtreleme sistemleri etkili bir siber zorbalık önleme yöntemidir.	0,903		
40.Yapay zeka destekli siber güvenlik çözümleri, çocukların çevrimiçi güvenliğini artırabilir.	0,900		
32.Sosyal medya platformları yapay zeka destekli güvenlik sistemleri ile daha güvenli hale getirilebilir.	0,894	76,786	0,966
36.Yapay zeka, dijital ortamda kötü amaçlı içerikleri engellemede başarılıdır.	0,884		
35.Çevrimiçi platformlarda yapay zeka tarafından otomatik içerik denetimi yapılmalıdır.	0,873		
31.Yapay zeka, siber zorbalık içeriklerini tespit etmede başarılıdır.	0,870		
34.Yapay zeka destekli güvenlik çözümleri kişisel mahremiyeti ihlal edebilir.	0,671		

Açımlayıcı faktör analizi sonucunda, “Siber Zorbalık ve Dijital Güvenlik” ölçeğinin tek faktörlü bir yapı sergilediği belirlenmiştir. Faktör yükleri incelendiğinde, tüm maddelerin yüksek yük değerlerine sahip olduğu ve ölçeğin ölçmek istediği yapıyı güçlü bir şekilde temsil ettiği görülmektedir. En yüksek faktör yükü “Yapay zeka tabanlı algoritmalar çevrimiçi tehditleri daha iyi analiz eder” maddesinde (0,918) yer almakta; bunu “Çevrimiçi taciz ve zorbalık, yapay zeka sistemleri sayesinde azaltılabilir” (0,914) ve “Siber zorbalık yapan kişileri tespit etmek için yapay zeka destekli sistemler kullanışlıdır” (0,909) maddeleri takip etmektedir. En düşük faktör yükü ise “Yapay zeka destekli güvenlik çözümleri kişisel mahremiyeti ihlal edebilir” maddesinde (0,671) gözlemlenmiştir. Bu değer de kabul edilebilir düzeyde olup, söz konusu maddenin yapı ile ilişkisini sürdürdüğünü göstermektedir.

Tek faktörlü bu yapı, toplam varyansın %76,786’sını açıklamaktadır. Bu oran, sosyal bilimlerde kullanılan ölçekler için oldukça yüksek ve yeterlidir. Ölçeğin iç tutarlılığını değerlendirmek amacıyla yapılan güvenilirlik analizinde Cronbach’s Alpha katsayısı 0,966 olarak hesaplanmıştır. Bu değer, ölçeğin iç tutarlılığının son derece yüksek olduğunu ve maddeler arasında güçlü bir uyum bulunduğunu göstermektedir.

Tablo 13: Siber Güvenlik Tehdit Farkındalığı

	n	Minimum	Maximum	ort	ss
41.Günümüzde siber saldırganların en çok kimlik bilgilerini ele geçirmeye yönelik saldırılar gerçekleştirdiğini düşünüyorum.	132	1	5	3,93	1,100
42.Yapay zeka tabanlı tehdit algılama sistemlerinin siber saldırılara karşı daha etkili olduğunu düşünüyorum.	132	1	5	3,70	1,039
43.Siber saldırganlar, sahte web siteleri ve oltalama teknikleri ile kurumsal hesaplara erişim sağlama konusunda daha başarılı hale gelmiştir.	132	1	5	3,95	1,003
44.Çalıştığım kurumda çok faktörlü kimlik doğrulamanın (MFA) siber saldırılara karşı etkin bir önlem olduğuna inanıyorum.	132	1	5	3,79	1,166
45.Günümüzde fidye yazılımı saldırılarının şirketler için en büyük tehditlerden biri olduğunu düşünüyorum.	132	1	5	3,81	1,092
46.Siber saldırganlar, kimlik avı saldırılarında yapay zeka tabanlı teknikleri daha fazla kullanmaya başlamıştır.	132	1	5	3,67	1,130
47.Sosyal mühendislik saldırılarının genellikle çalışan hatalarından kaynaklandığını düşünüyorum.	132	1	5	3,73	1,132
48.Siber güvenlik olaylarıyla başa çıkmak için proaktif güvenlik önlemlerinin alınması gerektiğine inanıyorum.	132	1	5	3,95	1,029
49.İşletmelerin saldırılara karşı güvenlik açıklarını belirlemek için düzenli güvenlik testleri yapması gerektiğini düşünüyorum.	132	1	5	4,08	1,119
50.Yapay zeka destekli tehdit avcılığı (threat hunting) yöntemlerinin geleneksel güvenlik çözümlerine kıyasla daha hızlı tespit sağladığını düşünüyorum.	132	1	5	3,79	1,070

Bu çalışmada, “Siber Güvenlik Tehdit Farkındalığı” ölçeğine ait maddelerin tanımlayıcı istatistikleri değerlendirilmiş; her bir maddenin ortalama ($\bar{X}$) ve standart sapma (SS) değerleri incelenmiştir. Bu analiz, katılımcıların güncel siber saldırı türleri, tehdit algısı ve yapay zeka destekli savunma sistemlerine ilişkin farkındalık düzeylerini ortaya koymak amacıyla yapılmıştır.

Tanımlayıcı istatistikler doğrultusunda, en yüksek ortalama değer “İşletmelerin saldırılara karşı güvenlik açıklarını belirlemek için düzenli güvenlik testleri yapması gerektiğini düşünüyorum” ($\bar{X} = 4,08$, $SS = 1,119$) maddesinde olduğu görülmektedir. Bu bulgu, katılımcıların siber güvenlikte proaktif denetim ve test süreçlerinin önemine dair güçlü bir farkındalığa sahip olduklarını göstermektedir. Bunu takiben, “Siber saldırganlar, sahte web siteleri ve oltalama teknikleri ile kurumsal hesaplara erişim sağlama konusunda daha başarılı hale gelmiştir” ($\bar{X} = 3,95$, $SS = 1,003$) ve “Siber güvenlik olaylarıyla başa çıkmak için proaktif güvenlik önlemlerinin alınması gerektiğine inanıyorum” ($\bar{X} = 3,95$, $SS = 1,029$) ifadeleri de

yüksek ortalamalarıyla dikkat çekmektedir. Bu sonuçlar, kullanıcıların hem tehditlerin gelişen niteliğine hem de savunma gerekliliklerine yönelik bilinç düzeylerinin yüksek olduğunu ortaya koymaktadır.

Benzer şekilde, “Günümüzde siber saldırganların en çok kimlik bilgilerini ele geçirmeye yönelik saldırılar gerçekleştirdiğini düşünüyorum” ($\bar{X} = 3,93$, $SS = 1,100$) ve “Günümüzde fidye yazılımı saldırılarının şirketler için en büyük tehditlerden biri olduğunu düşünüyorum” ($\bar{X} = 3,81$, $SS = 1,092$) ifadeleri de katılımcıların güncel tehdit unsurlarına yönelik farkındalıklarının oldukça güçlü olduğunu göstermektedir. Görece daha düşük ortalama değere sahip olan ifadelerden biri, “Siber saldırganlar, kimlik avı saldırılarında yapay zeka tabanlı teknikleri daha fazla kullanmaya başlamıştır” ($\bar{X} = 3,67$, $SS = 1,130$) olup, bu maddeye verilen yanıtların da çoğunlukla olumlu olduğu ancak diğer maddelere kıyasla biraz daha farklılaştığı görülmektedir. Bu duruma benzer şekilde, “Yapay zeka tabanlı tehdit algılama sistemlerinin siber saldırılara karşı daha etkili olduğunu düşünüyorum” ($\bar{X} = 3,70$, $SS = 1,039$) maddesi de yapay zeka destekli önlemler konusunda temkinli bir iyimserliğe işaret etmektedir.

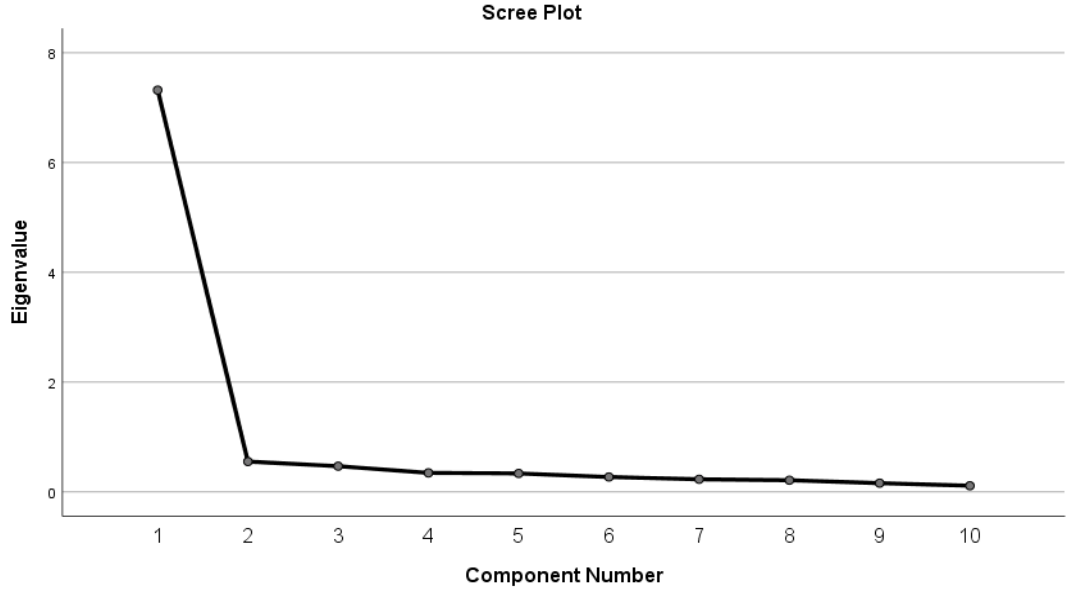
Katılımcıların genel olarak siber saldırı türlerine, savunma önlemlerine ve tehdit farkındalığına ilişkin yüksek düzeyde bir bilince sahip olduklarını göstermektedir. Ayrıca, standart sapma değerlerinin tüm maddelerde 1’in üzerinde olması, bireyler arasında konuya dair algı düzeylerinin çeşitlilik gösterdiğine işaret etmektedir.

Tablo 14: Verinin Faktör Analizine Uygunluğu

KMO		0,943
Bartlett's Testi	X2	1254,565
	sd	45
	p	0,000

Veri setinin faktör analizine uygunluğu, Kaiser-Meyer-Olkin (KMO) örneklem yeterlilik ölçütü ve Bartlett Küresellik Testi ile değerlendirilmiştir. KMO değeri 0,943 olarak hesaplanmıştır ve bu değer, örneklemin faktör analizine son derece uygun olduğunu göstermektedir. Bartlett Küresellik Testi sonucunda elde edilen Ki-Kare (χ^2) değeri 1254,565, 45 serbestlik derecesi ile anlamlı bulunmuştur ($p < 0,001$). Bu

sonuçlar, değişkenler arasında yeterli düzeyde korelasyon bulunduğunu ve veri setinin faktör analizi için uygun olduğunu açıkça ortaya koymaktadır.



Şekil 3: Siber Güvenlik Tehdit Farkındalığı Ölçeğine Ait Açımlayıcı Faktör Analizi Grafiği

Tablo 15: Siber Güvenlik Tehdit Farkındalığı Ölçeğine Ait Açımlayıcı Faktör Analizi ve Güvenirlik Sonuçları

	Faktör Yüğü 1	Açıklanan Varyans Oranı	Cronbach's Alpha
49.İşletmelerin saldırılara karşı güvenlik açıklarını belirlemek için düzenli güvenlik testleri yapması gerektiğini düşünüyorum.	0,909	73,191	0,958
48.Siber güvenlik olaylarıyla başa çıkmak için proaktif güvenlik önlemlerinin alınması gerektiğine inanıyorum.	0,902		
43.Siber saldırganlar, sahte web siteleri ve oltalama teknikleri ile kurumsal hesaplara erişim sağlama konusunda daha başarılı hale gelmiştir.	0,888		
50.Yapay zeka destekli tehdit avcılığı (threat hunting) yöntemlerinin geleneksel güvenlik çözümlerine kıyasla daha hızlı tespit sağladığını düşünüyorum.	0,859		
41.Günümüzde siber saldırganların en çok kimlik bilgilerini ele geçirmeye yönelik saldırılar gerçekleştirdiğini düşünüyorum.	0,854		
45.Günümüzde fidye yazılımı saldırılarının şirketler için en büyük tehditlerden biri olduğunu düşünüyorum.	0,853		
42.Yapay zeka tabanlı tehdit algılama sistemlerinin siber saldırılara karşı daha etkili olduğunu düşünüyorum.	0,838		

46.Siber saldırganlar, kimlik avı saldırılarında yapay zeka tabanlı teknikleri daha fazla kullanmaya başlamıştır.	0,829		
47.Sosyal mühendislik saldırılarının genellikle çalışan hatalarından kaynaklandığını düşünüyorum.	0,817		
44.Çalıştığım kurumda çok faktörlü kimlik doğrulamanın (MFA) siber saldırılara karşı etkin bir önlem olduğuna inanıyorum.	0,798		

Açımlayıcı faktör analizi sonucunda, “Siber Güvenlik Tehdit Farkındalığı” ölçeğinin tek faktörlü bir yapı sergilediği belirlenmiştir. Faktör yükleri incelendiğinde, tüm maddelerin anlamlı biçimde aynı faktör altında toplandığı ve ölçeğin yüksek yapısal bütünlük gösterdiği görülmektedir. Faktörde yer alan maddeler; siber saldırı türlerine yönelik bilgi düzeyini, proaktif güvenlik önlemleri konusundaki farkındalığı ve yapay zeka destekli çözümlere duyulan güveni kapsamaktadır. En yüksek faktör yükü “İşletmelerin saldırılara karşı güvenlik açıklarını belirlemek için düzenli güvenlik testleri yapması gerektiğini düşünüyorum” (0,909) maddesinde yer almakta; bunu “Siber güvenlik olaylarıyla başa çıkmak için proaktif güvenlik önlemlerinin alınması gerektiğine inanıyorum” (0,902) ve “Siber saldırganlar, sahte web siteleri ve ortalama teknikleri ile kurumsal hesaplara erişim sağlama konusunda daha başarılı hale gelmiştir” (0,888) maddeleri takip etmektedir. En düşük faktör yükü ise “Çalıştığım kurumda çok faktörlü kimlik doğrulamanın (MFA) siber saldırılara karşı etkin bir önlem olduğuna inanıyorum” maddesinde (0,798) yer almaktadır.

Bu faktör yapısı, toplam varyansın %73,191’ini açıklamaktadır ve bu oran, sosyal bilimler alanında tek faktörlü yapılarda oldukça yeterli bir açıklama düzeyini ifade etmektedir. Ölçeğin iç tutarlılığı Cronbach’s Alpha = 0,958 olarak hesaplanmış olup, bu değer ölçeğin son derece güvenilir ve istikrarlı bir ölçüm aracı olduğunu göstermektedir.

Tablo 16: Yapay Zeka ile Desteklenen Güvenlik Çözümleri

	n	Minimum	Maximum	ort	ss
51.Yapay zeka destekli güvenlik çözümleri, siber tehditleri insanlardan daha hızlı tespit edebilir.	132	1	5	3,86	1,133
52.Çalıştığım kurum, yapay zeka tabanlı güvenlik araçlarını kullanmaktadır.	132	1	5	3,34	1,289
53.Yapay zeka destekli güvenlik çözümleri sayesinde tehdit algılama ve yanıt süresi kısalmaktadır.	132	1	5	3,80	1,080

54.Yapay zeka destekli analiz araçları sayesinde güvenlik olaylarının kök neden analizi daha hızlı yapılabilir.	132	1	5	3,81	1,057
55.Kurumların tehdit istihbaratı için yapay zeka destekli sistemler kullanmasını önemli buluyorum.	132	1	5	3,83	1,092
56.Yapay zeka destekli güvenlik sistemleri saldırganların tekniklerini sürekli olarak öğrenebilir ve kendini geliştirebilir.	132	1	5	3,86	1,047
57.Şirketlerdeki güvenlik analistlerinin iş yükünü azaltmak için yapay zeka destekli çözümler kullanılmalıdır.	132	1	5	3,89	1,100
58.Geleneksel güvenlik çözümleri, yeni nesil yapay zeka destekli çözümlerle entegre edilmelidir.	132	1	5	3,87	1,094

Bu çalışmada, “Yapay Zeka ile Desteklenen Güvenlik Çözümleri” ölçeğine ait maddelerin tanımlayıcı istatistikleri değerlendirilmiş; her bir maddenin ortalama ($\bar{X}$) ve standart sapma (SS) değerleri incelenmiştir. Bu analiz, katılımcıların yapay zeka tabanlı güvenlik sistemlerine yönelik algılarını, bu sistemlerin etkinliğini ve kurumsal kullanıma ilişkin görüşlerini ortaya koymak amacıyla yapılmıştır.

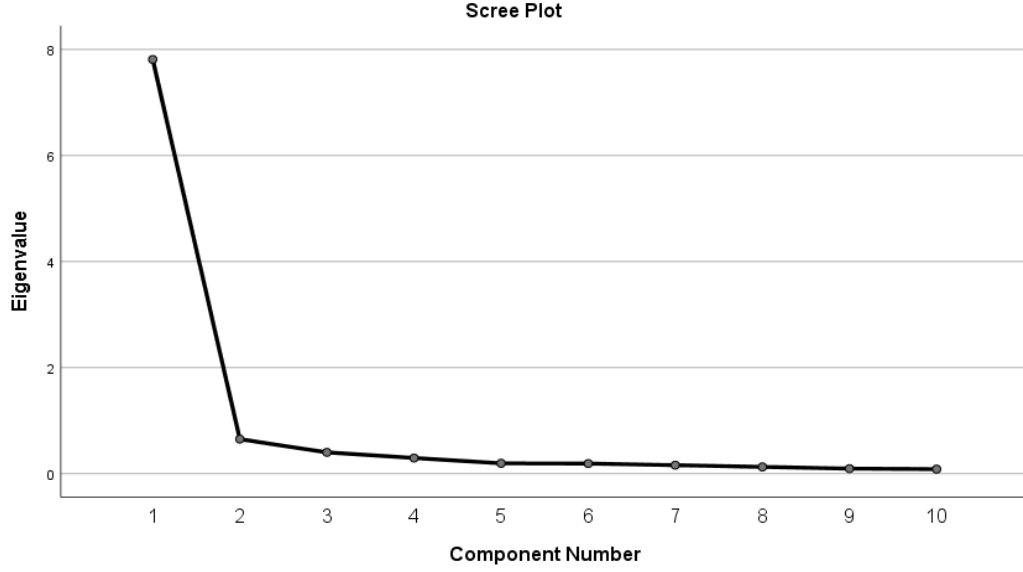
Tanımlayıcı istatistikler doğrultusunda, en yüksek ortalama değer “Şirketlerdeki güvenlik analistlerinin iş yükünü azaltmak için yapay zeka destekli çözümler kullanılmalıdır” ($\bar{X} = 3,89$, SS = 1,100) maddesinde olduğu görülmektedir. Bu bulgu, yapay zeka uygulamalarının insan kaynağı üzerindeki yükü hafifletme potansiyeline yönelik güçlü bir inanç olduğunu göstermektedir. Bunu takiben, “Geleneksel güvenlik çözümleri, yeni nesil yapay zeka destekli çözümlerle entegre edilmelidir” ($\bar{X} = 3,87$, SS = 1,094) ve “Yapay zeka destekli güvenlik çözümleri, siber tehditleri insanlardan daha hızlı tespit edebilir” ($\bar{X} = 3,86$, SS = 1,133) ifadeleri yüksek ortalamalarıyla dikkat çekmektedir. Bu sonuçlar, katılımcıların yapay zekanın hız, verimlilik ve entegrasyon gücüne olan inancını ortaya koymaktadır. Ayrıca, “Yapay zeka destekli güvenlik sistemleri saldırganların tekniklerini sürekli olarak öğrenebilir ve kendini geliştirebilir” ($\bar{X} = 3,86$, SS = 1,047) ve “Yapay zeka destekli analiz araçları sayesinde güvenlik olaylarının kök neden analizi daha hızlı yapılabilir” ($\bar{X} = 3,81$, SS = 1,057) ifadeleri de teknolojiye dair beklentilerin ileri düzeyde olduğunu göstermektedir. Katılımcılar bu sistemlerin yalnızca tespit değil, aynı zamanda analiz, öğrenme ve gelişim boyutlarında da avantaj sağladığını düşünmektedir.

En düşük ortalama değerin “Çalıştığım kurum, yapay zeka tabanlı güvenlik araçlarını kullanmaktadır” ($\bar{X} = 3,34$, $SS = 1,289$) maddesinde yer aldığı görülmektedir. Bu durum, kurumsal uygulamada bu tür teknolojilerin yaygın kullanımının hala sınırlı olabileceğine işaret etmektedir. Diğer tüm ifadeler daha yüksek ortalamalarla değerlendirilmiş olup, bu fark algı ile mevcut uygulama düzeyi arasında bir boşluk olduğunu göstermektedir. Katılımcıların yapay zeka ile desteklenen güvenlik çözümlerine ilişkin oldukça olumlu bir tutuma sahip olduklarını, bu teknolojilerin hem operasyonel hem de stratejik katkılarına inandıklarını ortaya koymaktadır. Tüm maddelerde standart sapma değerlerinin 1’in üzerinde olması, bireyler arasında görüş farklılıklarının bulunduğunu göstermektedir.

Tablo 17: Verinin Faktör Analizine Uygunluğu

KMO		0,949
Bartlett's Testi	X2	1595,905
	sd	45
	p	0,000

Veri setinin faktör analizine uygunluğu, Kaiser-Meyer-Olkin (KMO) örneklem yeterlilik ölçütü ve Bartlett Küresellik Testi ile değerlendirilmiştir. KMO değeri 0,949 olarak hesaplanmıştır ve bu değer, örneklem büyüklüğünün faktör analizine mükemmel derecede uygun olduğunu göstermektedir. Bartlett Küresellik Testi sonucunda elde edilen Ki-Kare (χ^2) değeri 1595,905, 45 serbestlik derecesi ile istatistiksel olarak anlamlı bulunmuştur ($p < 0,001$). Bu sonuçlar, değişkenler arasında yeterli düzeyde korelasyon olduğunu ve veri setinin faktör analizi için son derece uygun olduğunu açıkça ortaya koymaktadır.



Şekil 4: Yapay Zeka ile Desteklenen Güvenlik Çözümleri Ölçeğine Ait Açımlayıcı Faktör Analizi Grafiği

Tablo 18: Yapay Zeka ile Desteklenen Güvenlik Çözümleri Ölçeğine Ait Açımlayıcı Faktör Analizi ve Güvenirlilik Sonuçları

	Faktör Yüğü 1	Açıklanan Varyans Oranı	Cronbach's Alpha
55.Kurumların tehdit istihbaratı için yapay zeka destekli sistemler kullanmasını önemli buluyorum.	0,944	78,113	0,966
54.Yapay zeka destekli analiz araçları sayesinde güvenlik olaylarının kök neden analizi daha hızlı yapılabilir.	0,922		
53.Yapay zeka destekli güvenlik çözümleri sayesinde tehdit algılama ve yanıt süresi kısalmaktadır.	0,921		
58.Geleneksel güvenlik çözümleri, yeni nesil yapay zeka destekli çözümlerle entegre edilmelidir.	0,920		
56.Yapay zeka destekli güvenlik sistemleri saldırganların tekniklerini sürekli olarak öğrenebilir ve kendini geliştirebilir.	0,910		
51.Yapay zeka destekli güvenlik çözümleri, siber tehditleri insanlardan daha hızlı tespit edebilir.	0,898		
57.Şirketlerdeki güvenlik analistlerinin iş yükünü azaltmak için yapay zeka destekli çözümler kullanılmalıdır.	0,882		
59.Yapay zeka destekli güvenlik çözümleri, yanlış pozitif (false positive) oranını azaltmada etkilidir.	0,876		

60.Yapay zeka, kimlik avı (phishing) saldırılarını tespit etmede insanlardan daha başarılıdır.	0,858		
52.Çalıştığım kurum, yapay zeka tabanlı güvenlik araçlarını kullanmaktadır.	0,679		

Açımlayıcı faktör analizi sonucunda, “Yapay Zeka ile Desteklenen Güvenlik Çözümleri” ölçeğinin tek faktörlü bir yapı sergilediği belirlenmiştir. Faktör yükleri incelendiğinde, tüm maddelerin bu faktör altında yüksek yük değerlerine sahip olduğu ve ölçeğin ölçmekte olduğu kavrama güçlü katkılar sunduğu görülmektedir.

En yüksek faktör yükü, “Kurumların tehdit istihbaratı için yapay zeka destekli sistemler kullanmasını önemli buluyorum” maddesinde olup 0,944 olarak hesaplanmıştır. Bunu, “Yapay zeka destekli analiz araçları sayesinde güvenlik olaylarının kök neden analizi daha hızlı yapılabilir” (0,922), “Yapay zeka destekli güvenlik çözümleri sayesinde tehdit algılama ve yanıt süresi kısalmaktadır” (0,921), ve “Geleneksel güvenlik çözümleri, yeni nesil yapay zeka destekli çözümlerle entegre edilmelidir” (0,920) maddeleri takip etmektedir. Bu ifadeler, katılımcıların yapay zekanın hem analitik hız hem de entegrasyon kapasitesi açısından güvenlik sistemlerinde önemli avantajlar sağladığına inandıklarını göstermektedir.

Diğer yüksek faktör yüklerine sahip maddeler arasında “Yapay zeka destekli güvenlik sistemleri saldırganların tekniklerini sürekli olarak öğrenebilir ve kendini geliştirebilir” (0,910), “Yapay zeka destekli güvenlik çözümleri, siber tehditleri insanlardan daha hızlı tespit edebilir” (0,898), ve “Şirketlerdeki güvenlik analistlerinin iş yükünü azaltmak için yapay zeka destekli çözümler kullanılmalıdır” (0,882) ifadeleri yer almaktadır. Bu maddeler, katılımcıların yapay zekanın hem reaktif hem de öğrenen bir güvenlik bileşeni olarak değerlendirildiğini ortaya koymaktadır.

Faktör yükü bakımından en düşük değer, “Çalıştığım kurum, yapay zeka tabanlı güvenlik araçlarını kullanmaktadır” maddesinde görülmüş olup, 0,679 olarak hesaplanmıştır. Bu değer teknik olarak kabul edilebilir sınırın üzerinde yer almakta, ancak diğer maddelere kıyasla daha sınırlı bir katkı sunduğunu göstermektedir.

Analiz sonucunda elde edilen tek faktörlü yapı, toplam varyansın %78,113’ünü açıklamaktadır. Bu oran, sosyal bilimlerde oldukça yüksek kabul edilmekte olup

ölçeğin yapısal geçerliliğinin güçlü olduğunu göstermektedir. Ayrıca, ölçeğin iç tutarlılığını değerlendirmek amacıyla yapılan analizde Cronbach's Alpha katsayısı 0,966 olarak hesaplanmıştır. Bu değer, ölçeğin son derece güvenilir olduğunu ve maddeler arasında yüksek düzeyde iç tutarlılık bulunduğunu ortaya koymaktadır.

Tablo 19: Siber Güvenlik Stratejileri ve Politikalar

	n	Minimum	Maximum	ort	ss
61.Çalıştığım kurumda düzenli olarak siber güvenlik farkındalık eğitimleri verilmektedir.	132	1	5	3,36	1,309
62.Çalışanların siber güvenlik politikalarına uyum sağlaması için düzenli denetimler yapılmaktadır.	132	1	5	3,46	1,250
63.Bir siber güvenlik olayının yaşanması halinde nasıl hareket etmem gerektiğini biliyorum.	132	1	5	3,68	1,161
64.Çalıştığım kurum, güvenlik olaylarını simüle eden tatbikatlar yapmaktadır.	132	1	5	3,23	1,283
65.Yapay zeka destekli güvenlik çözümlerinin şirket politikalarına entegre edilmesi gerektiğine inanıyorum.	132	1	5	3,87	1,022
66.Kurumum, çalışanlarına güçlü parola politikaları uygulamaktadır.	132	1	5	3,77	1,183
67.Siber tehditleri yönetmek için yapay zeka destekli risk değerlendirme sistemleri kullanılmalıdır.	132	1	5	3,81	1,127
68.Siber saldırılara karşı düzenli güvenlik analizleri yapılması gereklidir.	132	1	5	3,96	1,073
69.Siber güvenlik politikaları, şirketlerin itibarını doğrudan etkilemektedir.	132	1	5	3,94	1,138
70.Siber güvenlik politikalarının belirlenmesinde yapay zeka araçlarının kullanılması stratejik bir avantaj sağlar.	132	1	5	3,87	1,080

Bu çalışmada, “Siber Güvenlik Stratejileri ve Politikalar” ölçeğine ait maddelerin tanımlayıcı istatistikleri değerlendirilmiş; her bir maddenin ortalama ($\bar{X}$) ve standart sapma (SS) değerleri analiz edilmiştir. Bu değerlendirme, katılımcıların kurumlarında uygulanan siber güvenlik stratejilerine, yapay zeka destekli çözümlere ve politika uygulamalarına yönelik algılarını ortaya koymak amacıyla yapılmıştır. Tanımlayıcı istatistikler doğrultusunda, en yüksek ortalama değer “Siber saldırılara karşı düzenli güvenlik analizleri yapılması gereklidir” ($\bar{X} = 3,96$, $SS = 1,073$) maddesinde olduğu görülmektedir. Bu bulgu, katılımcıların siber güvenliğinin sürdürülebilirliğini sağlamak için sistematik analizlerin önemine yüksek düzeyde inandıklarını göstermektedir. Bunu takiben, “Siber güvenlik politikaları, şirketlerin itibarını doğrudan etkilemektedir” ($\bar{X} = 3,94$, $SS = 1,138$) ve “Siber güvenlik politikalarının belirlenmesinde yapay zeka araçlarının kullanılması stratejik bir avantaj sağlar” ($\bar{X} = 3,87$, $SS = 1,080$) ifadeleri yüksek ortalamalarıyla dikkat çekmektedir. Bu

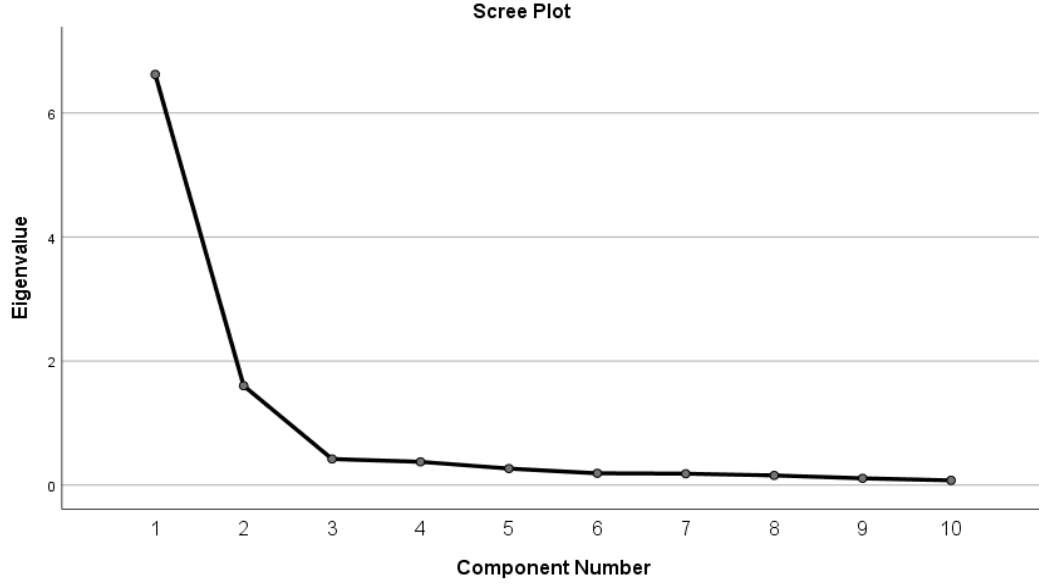
sonuçlar, yapay zekanın politika süreçlerine entegrasyonunun stratejik olarak değerlendirildiğini ortaya koymaktadır.

Benzer şekilde, “Yapay zeka destekli güvenlik çözümlerinin şirket politikalarına entegre edilmesi gerektiğine inanıyorum” ($\bar{X} = 3,87$, $SS = 1,022$) ve “Siber tehditleri yönetmek için yapay zeka destekli risk değerlendirme sistemleri kullanılmalıdır” ($\bar{X} = 3,81$, $SS = 1,127$) ifadeleri de katılımcıların yapay zeka tabanlı çözümleri yalnızca teknik değil, aynı zamanda kurumsal strateji düzeyinde de değerli bulduklarını göstermektedir. Görece daha düşük ortalama değerler, doğrudan kurumsal uygulamaları sorgulayan ifadelerle aittir. Örneğin, “Çalıştığım kurum, güvenlik olaylarını simüle eden tatbikatlar yapmaktadır” ($\bar{X} = 3,23$, $SS = 1,283$) ve “Çalıştığım kurumda düzenli olarak siber güvenlik farkındalık eğitimleri verilmektedir” ($\bar{X} = 3,36$, $SS = 1,309$) gibi maddeler, kurumsal uygulamaların yeterliliği konusunda katılımcıların daha temkinli ya da farklı görüşler sergilediğini ortaya koymaktadır. Katılımcıların siber güvenlik stratejileri ve politikalarının önemine ilişkin güçlü bir farkındalığa sahip olduklarını ve yapay zeka tabanlı çözümlerin bu stratejilere entegre edilmesini desteklediklerini göstermektedir. Bununla birlikte, kurum içi uygulamalara yönelik algıların daha çeşitli olduğu ve bazı alanlarda iyileştirme gereksinimi hissedildiği görülmektedir. Ayrıca, tüm maddelerde standart sapma değerlerinin 1’in üzerinde olması, görüşlerin çeşitlilik gösterdiğini ortaya koymaktadır.

Tablo 20: Verinin Faktör Analizine Uygunluğu

KMO		0,893
Bartlett's Testi	x2	1371,204
	sd	45
	p	0,000

Veri setinin faktör analizine uygunluğu, Kaiser-Meyer-Olkin (KMO) örneklem yeterlilik ölçütü ve Bartlett Küresellik Testi ile değerlendirilmiştir. KMO değeri 0,893 olarak hesaplanmış olup, bu değer örneklem büyüklüğünün faktör analizine oldukça uygun olduğunu göstermektedir. Bartlett Küresellik Testi sonucunda elde edilen Ki-Kare (χ^2) değeri 1371,204, 45 serbestlik derecesi ile anlamlı bulunmuştur ($p < 0,001$). Bu sonuçlar, değişkenler arasında yeterli düzeyde korelasyon olduğunu ve veri setinin faktör analizine uygun olduğunu ortaya koymaktadır.



Şekil 5: Siber Güvenlik Stratejileri ve Politikalar Ölçeğine Ait Açıklayıcı Faktör Analizi Grafiği

Tablo 21: Siber Güvenlik Stratejileri ve Politikalar Ölçeğine Ait Açıklayıcı Faktör Analizi ve Güvenirlik Sonuçları

	Yapay Zeka Tabanlı Stratejik Siber Güvenlik Politikaları Alt boyutu	Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları Alt Boyutu	Açıklanan Varyans Oranı	Cronbach's Alpha
70.Siber güvenlik politikalarının belirlenmesinde yapay zeka araçlarının kullanılması stratejik bir avantaj sağlar.	0,894			
69.Siber güvenlik politikaları, şirketlerin itibarını doğrudan etkilemektedir.	0,887			
65.Yapay zeka destekli güvenlik çözümlerinin şirket politikalarına entegre edilmesi gerektiğine inanıyorum.	0,884		46,060	0,920
68.Siber saldırılara karşı düzenli güvenlik analizleri yapılması gereklidir.	0,873			
67.Siber tehditleri yönetmek için yapay zeka destekli risk değerlendirme sistemleri kullanılmalıdır.	0,873			
62.Çalışanların siber güvenlik politikalarına uyum sağlaması için düzenli denetimler yapılmaktadır.		0,890	36,164	0,956

61.Çalıştığım kurumda düzenli olarak siber güvenlik farkındalık eğitimleri verilmektedir.		0,889		
64.Çalıştığım kurum, güvenlik olaylarını simüle eden tatbikatlar yapmaktadır.		0,859		
63.Bir siber güvenlik olayının yaşanması halinde nasıl hareket etmem gerektiğini biliyorum.		0,705		
66.Kurumum, çalışanlarına güçlü parola politikaları uygulamaktadır.		0,661		

Açımlayıcı faktör analizi sonucunda, “Siber Güvenlik Stratejileri ve Politikalar” ölçeğinin iki alt boyutlu bir yapı sergilediği belirlenmiştir. Faktör yükleri incelendiğinde, maddelerin anlamlı şekilde iki ayrı tematik yapıda toplandığı ve her iki alt boyutun da yüksek iç tutarlılık değerlerine sahip olduğu görülmektedir.

Birinci alt boyut, “Yapay Zeka Tabanlı Stratejik Siber Güvenlik Politikaları” olarak adlandırılmıştır. Bu boyutta yer alan maddeler, yapay zeka destekli sistemlerin kurumsal politika yapım süreçlerine entegrasyonu ve siber tehditlerin stratejik düzeyde yönetilmesine odaklanmaktadır. En yüksek faktör yükü, “Siber güvenlik politikalarının belirlenmesinde yapay zeka araçlarının kullanılması stratejik bir avantaj sağlar” maddesinde (0,894) yer almakta; bunu “Siber güvenlik politikaları, şirketlerin itibarını doğrudan etkilemektedir” (0,887) ve “Yapay zeka destekli güvenlik çözümlerinin şirket politikalarına entegre edilmesi gerektiğine inanıyorum” (0,884) gibi ifadeler takip etmektedir. Bu alt boyut, toplam varyansın %46,060’ını açıklamakta ve iç tutarlılığı Cronbach’s Alpha = 0,920 olarak hesaplanmıştır. Bu değer, ölçeğin ilk alt boyutunun yüksek derecede güvenilir olduğunu göstermektedir.

İkinci alt boyut, “Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları” olarak isimlendirilmiştir. Bu boyut, kurumsal ölçekteki eğitim, denetim ve uygulama süreçlerine ilişkin değerlendirmeleri kapsamaktadır. En yüksek faktör yükü “Çalışanların siber güvenlik politikalarına uyum sağlaması için düzenli denetimler yapılmaktadır” (0,890) ve “Çalıştığım kurumda düzenli olarak siber güvenlik farkındalık eğitimleri verilmektedir” (0,889) maddelerinde görülmekte; bunu “Güvenlik olaylarını simüle eden tatbikatlar yapılmaktadır” (0,859) ve “Bir siber güvenlik olayının yaşanması halinde nasıl hareket etmem gerektiğini biliyorum” (0,705) maddeleri izlemektedir. Bu alt boyut, toplam varyansın %36,164’ünü

açıklamakta olup iç tutarlılığı Cronbach's Alpha = 0,956 olarak hesaplanmıştır. Bu da ikinci alt boyutun oldukça yüksek düzeyde güvenilir olduğunu göstermektedir.

Tablo 22: Siber Güvenlik Tehditleri ve Savunma Mekanizmaları

	n	Minimum	Maximum	ort	ss
71.Fidye yazılımlarına karşı kurumların yedekleme stratejileri oluşturması gerekmektedir.	132	1	5	4,12	1,119
72.Yapay zeka destekli tehdit avcılığı (threat hunting) saldırıları önlemede etkili bir stratejidir.	132	1	5	3,81	1,049
73.Siber güvenlik sistemlerinin otomatik saldırı simülasyonları yapması gereklidir.	132	1	5	4,02	1,022
74.Yapay zeka tabanlı saldırı tespit sistemleri, gelişmiş tehditleri tespit etmede başarılıdır.	132	1	5	3,72	0,999
75.Kimlik avı saldırıları kurumlar için en büyük güvenlik tehditlerinden biridir.	132	1	5	4,02	1,045
76.Siber saldırılar sonrası veri kurtarma stratejileri oluşturulmalıdır.	132	1	5	4,10	1,069
77.Kimlik tabanlı saldırılar, şirketlerin en zayıf güvenlik noktalarından biridir.	132	1	5	3,96	1,037
78.Siber saldırganlar, kimlik avı saldırılarında giderek daha sofistike hale gelmektedir.	132	1	5	4,00	1,019
79.Yapay zeka destekli güvenlik çözümlerinin saldırılara karşı daha iyi bir koruma sağladığını düşünüyorum.	132	1	5	3,87	0,992
80.Kurumların siber saldırılarla mücadele etmek için tehdit istihbaratı ekipleri oluşturması gereklidir.	132	1	5	4,03	1,084

Bu çalışmada, “Siber Güvenlik Tehditleri ve Savunma Mekanizmaları” ölçeğine ait maddelerin tanımlayıcı istatistikleri değerlendirilmiş; her bir maddenin ortalama ($\bar{X}$) ve standart sapma (SS) değerleri incelenmiştir. Bu analiz, katılımcıların siber tehditlere ilişkin farkındalık düzeylerini ve savunma stratejilerine yönelik tutumlarını belirlemeye yönelik olarak gerçekleştirilmiştir.

Tanımlayıcı istatistikler doğrultusunda, en yüksek ortalama değer “Fidye yazılımlarına karşı kurumların yedekleme stratejileri oluşturması gerekmektedir” ($\bar{X} = 4,12$, $SS = 1,119$) maddesinde olduğu görülmektedir. Bu bulgu, katılımcıların veri yedekleme sistemlerinin siber saldırılar karşısındaki önemine dair güçlü bir farkındalığa sahip olduklarını göstermektedir. Bunu takiben, “Siber saldırılar sonrası veri kurtarma stratejileri oluşturulmalıdır” ($\bar{X} = 4,10$, $SS = 1,069$) ve “Kurumların siber saldırılarla mücadele etmek için tehdit istihbaratı ekipleri oluşturması gereklidir” ($\bar{X} = 4,03$, $SS = 1,084$) ifadeleri, saldırı sonrası hazırlık süreçlerine ilişkin bilinç düzeyinin de oldukça yüksek olduğunu ortaya koymaktadır.

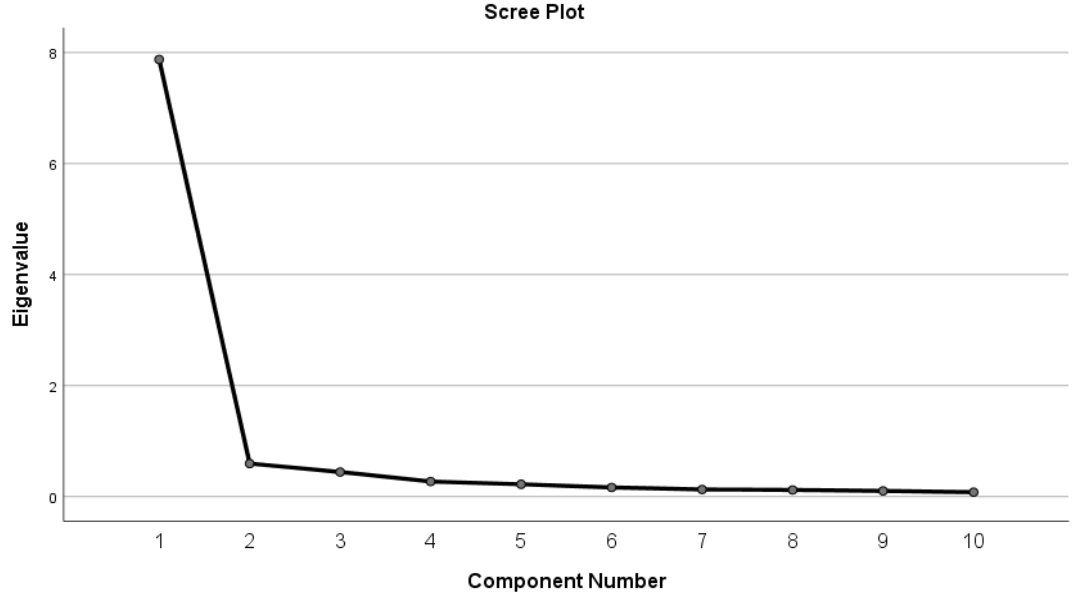
Benzer şekilde, “Siber güvenlik sistemlerinin otomatik saldırı simülasyonları yapması gereklidir” ($\bar{X} = 4,02$, $SS = 1,022$) ve “Kimlik avı saldırıları kurumlar için en büyük güvenlik tehditlerinden biridir” ($\bar{X} = 4,02$, $SS = 1,045$) maddeleri de yüksek ortalama değerleriyle öne çıkmaktadır. Bu sonuçlar, kurumların sadece reaktif değil aynı zamanda proaktif güvenlik önlemleri alma gerekliliğine yönelik güçlü bir algı geliştirdiklerini göstermektedir. Diğer yandan, görece daha düşük ortalamalar “Yapay zeka tabanlı saldırı tespit sistemleri, gelişmiş tehditleri tespit etmede başarılıdır” ($\bar{X} = 3,72$, $SS = 0,999$) ve “Yapay zeka destekli tehdit avcılığı (threat hunting) saldırıları önlemede etkili bir stratejidir” ($\bar{X} = 3,81$, $SS = 1,049$) maddelerinde yer almıştır. Bu durum, katılımcıların yapay zekaya dayalı savunma teknolojilerine olumlu yaklaşımlar sergilemekle birlikte, bu sistemlerin başarı düzeyine dair daha temkinli bir değerlendirme yaptıklarını göstermektedir.

Katılımcıların siber tehditlere karşı savunma mekanizmaları geliştirme konusunda oldukça bilinçli olduklarını; özellikle veri yedekleme, tehdit istihbaratı ve saldırı sonrası müdahale gibi alanlarda güçlü tutumlar sergilediklerini ortaya koymaktadır. Ayrıca, tüm maddelerde standart sapma değerlerinin 1’e yakın veya üzerinde olması, görüş çeşitliliğini ve katılımcılar arasında konuya dair farkındalık düzeylerinin farklılık gösterdiğini yansıtmaktadır.

Tablo 23: Verinin Faktör Analizine Uygunluğu

KMO		0,935
	X2	1632,424
Bartlett's Testi	sd	45
	p	0,000

Veri setinin faktör analizine uygunluğu, Kaiser-Meyer-Olkin (KMO) örneklem yeterlilik ölçütü ve Bartlett Küresellik Testi ile değerlendirilmiştir. Yapılan analiz sonucunda KMO değeri 0,935 olarak hesaplanmış olup, bu değer örneklem büyüklüğünün faktör analizine son derece uygun olduğunu göstermektedir. Bartlett Küresellik Testi sonucunda elde edilen Ki-Kare (χ^2) değeri 1632,424, 45 serbestlik derecesi ile anlamlı bulunmuştur ($p < 0,001$). Bu sonuçlar, değişkenler arasında yeterli düzeyde korelasyon olduğunu ve veri setinin faktör analizi için oldukça elverişli olduğunu ortaya koymaktadır.



Şekil 6: Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeğine Ait Açıklayıcı Faktör Analizi Grafiği

Tablo 24: Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeğine Ait Açıklayıcı Faktör Analizi ve Güvenirlik Sonuçları

	Geleneksel ve Stratejik Tehdit Farkındalığı Alt Boyutu	Yapay Zeka Destekli Savunma Sistemleri Alt Boyutu	Açıklanan Varyans Oranı	Cronbach's Alpha
76.Siber saldırılar sonrası veri kurtarma stratejileri oluşturulmalıdır.	0,859	0,381	50,493	0,962
75.Kimlik avı saldırıları kurumlar için en büyük güvenlik tehditlerinden biridir.	0,836	0,394		
71.Fidye yazılımlarına karşı kurumların yedekleme stratejileri oluşturması gerekmektedir.	0,807	0,451		
78.Siber saldırganlar, kimlik avı saldırılarında giderek daha sofistike hale gelmektedir.	0,799	0,433		
73.Siber güvenlik sistemlerinin otomatik saldırı simülasyonları yapması gereklidir.	0,783	0,457		
77.Kimlik tabanlı saldırılar, şirketlerin en zayıf güvenlik noktalarından biridir.	0,760	0,491	35,721	0,942
74.Yapay zeka tabanlı saldırı tespit sistemleri, gelişmiş tehditleri tespit etmede başarılıdır.	0,409	0,876		
79.Yapay zeka destekli güvenlik çözümlerinin saldırılara karşı daha iyi bir koruma sağladığını düşünüyorum.	0,410	0,842		

72.Yapay zeka destekli tehdit avcılığı (threat hunting) saldırıları önlemede etkili bir stratejidir.	0,541	0,774		
--	-------	-------	--	--

Açımlayıcı faktör analizi sonucunda, “Siber Güvenlik Tehditleri ve Savunma Mekanizmaları” ölçeğinin iki alt boyutlu bir yapı sergilediği belirlenmiştir. Faktör yükleri incelendiğinde, maddelerin anlamlı biçimde iki faktörde toplandığı ve her iki boyutun da yüksek düzeyde iç tutarlılığa sahip olduğu görülmektedir.

Birinci alt boyut, “Geleneksel ve Stratejik Tehdit Farkındalığı” olarak adlandırılmıştır. Bu boyut, fidye yazılımları, kimlik avı saldırıları, saldırı sonrası kurtarma stratejileri ve güvenlik tatbikatları gibi konularda tehdit algısını ve stratejik hazırlığı kapsamaktadır. En yüksek faktör yükü, “Siber saldırılar sonrası veri kurtarma stratejileri oluşturulmalıdır” (0,859) maddesinde yer almakta; bunu “Kimlik avı saldırıları kurumlar için en büyük güvenlik tehditlerinden biridir” (0,836) ve “Fidye yazılımlarına karşı kurumların yedekleme stratejileri oluşturması gerekmektedir” (0,807) maddeleri takip etmektedir. Bu alt boyut, toplam varyansın %50,493’ünü açıklamakta olup, iç tutarlılığı Cronbach’s Alpha = 0,962 olarak hesaplanmıştır. Bu değer, yüksek bir iç tutarlılık düzeyine işaret etmektedir.

İkinci alt boyut, “Yapay Zeka Destekli Savunma Sistemleri” olarak adlandırılmıştır. Bu boyut, yapay zeka tabanlı saldırı tespit sistemleri, tehdit avcılığı ve savunma çözümlerine yönelik değerlendirmeleri içermektedir. Bu faktörde en yüksek faktör yükü “Yapay zeka tabanlı saldırı tespit sistemleri, gelişmiş tehditleri tespit etmede başarılıdır” (0,876) maddesinde yer alırken, “Yapay zeka destekli güvenlik çözümlerinin saldırılara karşı daha iyi bir koruma sağladığını düşünüyorum” (0,842) ve “Yapay zeka destekli tehdit avcılığı (threat hunting) saldırıları önlemede etkili bir stratejidir” (0,774) maddeleri de bu boyutu anlamlı şekilde temsil etmektedir. Bu alt boyut, %35,721 oranında varyans açıklamakta ve Cronbach’s Alpha = 0,942 değeriyle oldukça yüksek bir güvenilirlik göstermektedir.

Faktör yükü düşük kalan ve yapısal bütünlüğe katkı sağlamadığı belirlenen “80. Kurumların siber saldırılarla mücadele etmek için tehdit istihbaratı ekipleri oluşturması gereklidir.” maddesi analiz dışında bırakılmıştır. Sonuç olarak, elde edilen bulgular, “Siber Güvenlik Tehditleri ve Savunma Mekanizmaları” ölçeğinin iki

boyutlu, geçerli ve güvenilir bir yapı sunduğunu göstermektedir. Ölçek; hem klasik tehdit algılarına hem de yapay zeka destekli savunma mekanizmalarına ilişkin tutumları ölçmede etkili bir değerlendirme aracıdır.

Değişkenler arasındaki ilişki düzeylerini incelemek amacıyla **Spearman korelasyon analizi** uygulanmıştır. Bu analizde, ölçekler ve alt boyutlar arasındaki ilişkiler **korelasyon katsayısı (r)** ve **anlamlılık düzeyi (p)** ile değerlendirilmiştir. Tüm ilişki katsayıları pozitif yönde ve anlamlı bulunmuş olup, analiz sonuçları bireylerin siber güvenlik ve yapay zeka destekli sistemler hakkındaki tutumlarının birbirini tamamladığını göstermektedir.

Tablo 25: Katılımcıların Demografik Özelliklerine Ait Dağılımlar

	n	%
Cinsiyetiniz:		
Kadın	44	33,3
Erkek	86	65,2
Belirtmek istemiyorum	2	1,5
Yaş Aralığınız:		
18-24	20	15,2
25-34	70	53,0
35-44	18	13,6
45 ve üzeri	24	18,2
Eğitim Seviyeniz:		
Lise	8	6,1
Lisans	79	59,8
Yüksek Lisans	25	18,9
Doktora	20	15,2
Mesleğiniz:		
Akademisyen	23	17,4
BT Uzmanı	53	40,2
Sistem Yöneticisi	9	6,8
SIEM Uzmanı	0	0,0
Diğer	47	35,6
Siber güvenlik alanında herhangi bir eğitim aldınız mı?		
Evet	77	58,3
Hayır	55	41,7

Bu çalışmada yer alan katılımcıların demografik özellikleri incelendiğinde, cinsiyet dağılımının çoğunlukla erkeklerden oluştuğu görülmektedir. Katılımcıların %65,2'si erkek (n = 86), %33,3'ü kadın (n = 44) ve %1,5'i (n = 2) cinsiyetini belirtmek istemediğini ifade etmiştir. Bu durum, araştırmanın örnekleminde erkeklerin daha yüksek oranda temsil edildiğini göstermektedir. Yaş dağılımı incelendiğinde, katılımcıların büyük bir kısmının 25–34 yaş aralığında yer aldığı tespit edilmiştir

(%53,0; n = 70). Bunu %18,2 ile 45 yaş ve üzeri (n = 24), %15,2 ile 18–24 yaş (n = 20) ve %13,6 ile 35–44 yaş (n = 18) grupları takip etmektedir. Bu bulgu, örneklemin büyük ölçüde genç ve orta yaş yetişkinlerden oluştuğunu göstermektedir.

Eğitim düzeyi açısından değerlendirildiğinde, katılımcıların çoğunluğunun lisans mezunu olduğu belirlenmiştir (%59,8; n = 79). Bunu %18,9 ile yüksek lisans (n = 25), %15,2 ile doktora (n = 20) ve %6,1 ile lise mezunları (n = 8) takip etmektedir. Bu sonuçlar, araştırma grubunun büyük oranda yükseköğretim düzeyinde eğitime sahip bireylerden oluştuğunu ortaya koymaktadır. Mesleki dağılıma bakıldığında, en yüksek oran %40,2 ile BT uzmanlarına (n = 53) aittir. Akademisyenler %17,4 (n = 23) oranında temsil edilirken, sistem yöneticilerinin oranı %6,8 (n = 9), SIEM uzmanı ise örnekleme yer almamıştır (n = 0). “Diğer” meslek grubu %35,6 (n = 47) oranıyla ikinci büyük grubu oluşturmaktadır. Bu bulgu, katılımcıların önemli bir kısmının bilgi teknolojileri sektöründe çalıştığını göstermektedir.

Son olarak, siber güvenlik alanında eğitim alma durumuna bakıldığında, katılımcıların %58,3’ü (n = 77) bu alanda eğitim aldığını, %41,7’si (n = 55) ise almadığını belirtmiştir. Bu durum, örneklemin büyük bir kısmının siber güvenlik konusunda bilgi sahibi olduğunu, ancak eğitim almayanların da önemli bir orana sahip olduğunu göstermektedir.

Tablo 26: Ölçek ve Alt Boyutlara Ait Tanımlayıcı İstatistikler (n = 132)

	n	Minimum	Maximum	ort	ss
Siber Güvenlik Farkındalığı ve Davranışları Ölçeği	132	9	45	34,55	8,75
Risk Algısı ve Yapay Zeka Destekli Güvenlik Önlemleri Ölçeği	132	10	50	37,14	9,83
Yapay Zeka Destekli Kurumsal Güvenlik Algısı alt boyutu	132	5	25	17,95	4,76
Kurumsal Uyum ve Eğitim Destekli Güvenlik Politikaları alt boyutu	132	3	15	10,07	2,82
Kurumsal ve Bireysel Siber Güvenlik Politikaları Ölçeği	132	8	38	28,02	6,84
Siber Zorbalık ve Dijital Güvenlik Ölçeği	132	10	50	37,23	9,36
Siber Güvenlik Tehdit Farkındalığı Ölçeği	132	10	50	38,41	9,29
Yapay Zeka ile Desteklenen Güvenlik Çözümleri Ölçeği	132	10	50	37,69	9,73
Yapay Zeka Tabanlı Stratejik Siber Güvenlik Politikaları alt boyutu	132	5	25	19,45	5,02
Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları alt boyutu	132	5	25	17,52	5,39
Siber Güvenlik Stratejileri ve Politikalar Ölçeği	132	10	50	36,97	9,39
Geleneksel ve Stratejik Tehdit Farkındalığı alt boyutu	132	6	30	24,23	5,79

Yapay Zeka Destekli Savunma Sistemleri alt boyutu	132	3	15	11,40	2,88
Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeği	132	9	45	35,63	8,35

Bu çalışmada kullanılan ölçek ve alt boyutlara ilişkin tanımlayıcı istatistikler değerlendirilmiştir. Her bir ölçek için minimum, maksimum, ortalama ($\bar{X}$) ve standart sapma (SS) değerleri hesaplanmıştır. Aşağıda her ölçüte ilişkin bulgular ayrıntılı şekilde sunulmaktadır:

- **Siber Güvenlik Farkındalığı ve Davranışları Ölçeği:** Katılımcıların bu ölçekteki puanları 9 ile 45 arasında değişmekte olup, ortalama değer 34,55 ve standart sapma 8,75 olarak hesaplanmıştır. Bu bulgu, bireylerin temel güvenlik davranışları ve dijital ortamlarda güvenli hareket etme farkındalıklarının orta-yüksek düzeyde olduğunu göstermektedir.
- **Risk Algısı ve Yapay Zeka Destekli Güvenlik Önlemleri Ölçeği:** Bu ölçekte puanlar 10 ile 50 arasında değişmekte olup, ortalama 37,14 ve standart sapma 9,83'tür. Katılımcıların yapay zeka destekli güvenlik önlemleri hakkındaki risk algılarının olumlu yönde olduğu ve farkındalık düzeylerinin yüksek olduğu görülmektedir.
- **Yapay Zeka Destekli Kurumsal Güvenlik Algısı Alt Boyutu:** Puanlar 5 ile 25 arasında değişmiş; ortalama 17,95, standart sapma ise 4,76 olarak hesaplanmıştır. Bu durum, katılımcıların kurumsal güvenlik bağlamında yapay zeka teknolojilerini genel olarak olumlu değerlendirdiğini ortaya koymaktadır. Kurumsal Uyum ve Eğitim Destekli Güvenlik Politikaları Alt Boyutu: Puan aralığı 3 ile 15 arasında olup, ortalama 10,07 ve standart sapma 2,82'dir. Bu sonuç, kurumsal düzeyde siber güvenlik uyumu ve eğitim uygulamalarına dair algının orta düzeyde olduğunu göstermektedir. Kurumsal ve Bireysel Siber Güvenlik Politikaları Ölçeği: Katılımcıların bu ölçekteki puanları 8 ile 38 arasında değişmekte olup, ortalama 28,02, standart sapma ise 6,84 olarak belirlenmiştir. Bu bulgu, bireysel ve kurumsal güvenlik politikalarına ilişkin farkındalık düzeyinin yüksek olduğunu göstermektedir.
- **Siber Zorbalık ve Dijital Güvenlik Ölçeği:** Puanlar 10 ile 50 arasında değişmekte; ortalama 37,23, standart sapma ise 9,36'dır. Bu sonuç,

katılımcıların dijital ortamda siber zorbalık risklerine karşı duyarlılıklarının yüksek düzeyde olduğunu göstermektedir.

- **Siber Güvenlik Tehdit Farkındalığı Ölçeği:** Bu ölçekteki puanlar 10 ile 50 arasında değişmekte; ortalama 38,41, standart sapma 9,29'dur. Katılımcıların güncel siber tehditlere ilişkin farkındalık düzeylerinin yüksek olduğu anlaşılmaktadır.
- **Yapay Zeka ile Desteklenen Güvenlik Çözümleri Ölçeği:** Puanlar 10 ile 50 arasında değişmiş; ortalama 37,69, standart sapma 9,73 olarak bulunmuştur. Bu durum, yapay zeka destekli güvenlik çözümlerine yönelik olumlu tutumların güçlü olduğunu göstermektedir.
- **Yapay Zeka Tabanlı Stratejik Siber Güvenlik Politikaları Alt Boyutu:** Katılımcıların puanları 5 ile 25 arasında değişmiş; ortalama 19,45, standart sapma 5,02'dir. Bu değer, stratejik düzeyde yapay zeka ile entegre siber güvenlik politikalarına yönelik yüksek bir farkındalığı işaret etmektedir. Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları Alt Boyutu: Puanlar 5 ile 25 arasında değişmiş; ortalama 17,52, standart sapma 5,39 olarak hesaplanmıştır. Bu bulgu, kurumların güvenlik farkındalığı ve uygulamaları açısından olumlu bir algıya sahip olduğunu göstermektedir. Siber Güvenlik Stratejileri ve Politikalar Ölçeği: Puanlar 10 ile 50 arasında değişmekte; ortalama 36,97, standart sapma 9,39 olarak hesaplanmıştır. Katılımcıların siber güvenliğe dair kurumsal stratejilere yönelik farkındalık ve değerlendirmelerinin yüksek olduğu anlaşılmaktadır.
- **Geleneksel ve Stratejik Tehdit Farkındalığı Alt Boyutu:** Bu alt boyutta puanlar 6 ile 30 arasında değişmiş; ortalama 24,23, standart sapma 5,79'dur. Bu bulgu, katılımcıların hem geleneksel hem de gelişmiş tehdit türlerine karşı farkındalıklarının güçlü olduğunu göstermektedir. Yapay Zeka Destekli Savunma Sistemleri Alt Boyutu: Puanlar 3 ile 15 arasında değişmekte olup, ortalama 11,40, standart sapma 2,88 olarak belirlenmiştir. Bu durum, yapay zeka destekli savunma sistemlerine yönelik olumlu ancak daha temkinli bir tutum sergilendiğini göstermektedir. Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeği: Katılımcıların bu ölçekteki puanları 9 ile 45 arasında

değişmiş; ortalama 35,63, standart sapma ise 8,35 olarak bulunmuştur. Bu bulgu, siber tehditlere karşı bireylerin savunma stratejileri geliştirme konusunda farkındalıklarının yüksek olduğunu göstermektedir.

Tablo 27: Cinsiyete Göre Ölçek ve Alt Boyutların Karşılaştırılması (Mann-Whitney U Testi Sonuçları)

	Kadın (n=44)			Erkek (n=86)			u	p
	ort	ss	Median	ort	ss	Median		
Siber Güvenlik Farkındalığı ve Davranışları Ölçeği	32,93	9,12	36,00	35,66	8,09	36,00	1563,500	0,105
Risk Algısı ve Yapay Zeka Destekli Güvenlik Önlemleri Ölçeği	35,43	10,15	39,50	38,19	9,13	40,00	1620,000	0,179
Yapay Zeka Destekli Kurumsal Güvenlik Algısı alt boyutu	17,75	4,67	19,00	18,19	4,67	19,00	1760,500	0,515
Kurumsal Uyum ve Eğitim Destekli Güvenlik Politikaları alt boyutu	9,77	2,95	11,00	10,28	2,67	11,00	1713,500	0,372
Kurumsal ve Bireysel Siber Güvenlik Politikaları Ölçeği	27,52	6,86	29,50	28,47	6,57	30,00	1717,000	0,387
Siber Zorbalık ve Dijital Güvenlik Ölçeği	36,73	9,41	39,00	37,69	8,94	40,00	1747,500	0,475
Siber Güvenlik Tehdit Farkındalığı Ölçeği	38,39	9,56	40,50	38,97	8,55	40,00	1861,500	0,880
Yapay Zeka ile Desteklenen Güvenlik Çözümleri Ölçeği	36,64	9,28	39,00	38,41	9,52	40,00	1591,500	0,137
Yapay Zeka Tabanlı Stratejik Siber Güvenlik Politikaları alt boyutu	19,16	4,89	20,00	19,71	4,88	20,00	1732,500	0,422
Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları alt boyutu	16,98	5,17	19,00	17,85	5,34	20,00	1685,000	0,304
Siber Güvenlik Stratejileri ve Politikalar Ölçeği	36,14	9,09	39,00	37,56	9,11	40,00	1674,000	0,281
Geleneksel ve Stratejik Tehdit Farkındalığı alt boyutu	24,09	5,22	24,50	24,44	5,79	25,00	1708,000	0,361
Yapay Zeka Destekli Savunma Sistemleri alt boyutu	11,43	2,70	12,00	11,44	2,85	12,00	1886,500	0,978
Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeği	35,52	7,71	36,00	35,88	8,24	36,50	1762,000	0,518

*p<0,05; Mann-Whitney U testi

Katılımcıların cinsiyetine göre ölçek ve alt boyut puanlarında anlamlı bir fark olup olmadığı Mann-Whitney U testi ile analiz edilmiştir. Analiz sonuçlarına göre tüm değişkenlerde $p > 0,05$ olduğu için kadın ve erkek katılımcılar arasında istatistiksel olarak anlamlı bir farklılık bulunmamaktadır

Tablo 28: Yaş Gruplarına Göre Ölçek ve Alt Boyutların Karşılaştırılması (Kruskal-Wallis Testi Sonuçları)

	Yaş Aralığınız:													
	18-24(n=20)			25-34 (n=70)			35-44 (n=18)			45 ve üzeri (n=24)				
	ort	ss	Median	ort	ss	Median	ort	ss	Median	ort	ss	Median	X2	P
Siber Güvenlik Farkındalığı ve Davranışları Ölçeği	33,70	8,07	36,00	34,39	9,64	36,00	34,94	9,00	35,50	35,46	6,44	36,50	0,327	0,955
Risk Algısı ve Yapay Zeka Destekli Güvenlik Önlemleri Ölçeği	34,95	10,49	40,00	37,19	10,65	40,00	38,28	8,94	39,00	38,00	7,31	39,00	1,028	0,794
Yapay Zeka Destekli Kurumsal Güvenlik Algısı alt boyutu	16,40	5,28	18,50	18,14	5,24	20,00	17,83	4,09	19,00	18,79	2,92	19,00	3,701	0,296
Kurumsal Uyum ve Eğitim Destekli Güvenlik Politikaları alt boyutu	8,80	2,84	9,00	10,53	2,56	11,00	9,94	3,37	11,00	9,88	2,89	10,50	7,528	0,057
Kurumsal ve Bireysel Siber Güvenlik Politikaları Ölçeği	25,20	7,21	27,00	28,67	7,36	31,00	27,78	6,62	28,00	28,67	4,48	29,00	6,111	0,106
Siber Zorbalık ve Dijital Güvenlik Ölçeği	33,90	9,08	37,00	37,71	10,30	40,00	36,61	8,47	38,50	39,08	6,78	39,00	5,111	0,164
Siber Güvenlik Tehdit Farkındalığı Ölçeği	36,60	11,56	41,00	38,81	9,25	40,00	35,89	10,37	39,50	40,63	5,63	42,00	1,971	0,578
Yapay Zeka ile Desteklenen Güvenlik Çözümleri Ölçeği	36,30	10,48	40,00	37,94	10,87	40,00	36,83	9,21	39,00	38,75	5,28	38,00	2,653	0,448
Yapay Zeka Tabanlı Stratejik Siber Güvenlik Politikaları alt boyutu	18,25	5,13	20,00	19,76	5,20	20,00	18,44	5,20	20,00	20,33	4,18	20,00	4,105	0,250
Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları alt boyutu	15,85	5,66	16,50	18,64	5,27	20,00	17,33	5,67	17,00	15,75	4,75	16,00	8,443	0,038*
Siber Güvenlik Stratejileri ve Politikalar Ölçeği	34,10	9,31	35,00	38,40	9,66	40,00	35,78	10,43	36,50	36,08	7,42	36,50	6,981	0,073
Geleneksel ve Stratejik Tehdit Farkındalığı alt boyutu	23,75	5,17	24,00	24,31	5,98	25,00	23,06	6,33	25,00	25,25	5,42	27,50	3,122	0,373
Yapay Zeka Destekli Savunma Sistemleri alt boyutu	11,35	2,85	12,00	11,36	2,99	12,00	11,06	3,11	12,00	11,83	2,48	12,00	0,551	0,908
Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeği	35,10	7,83	36,00	35,67	8,56	36,00	34,11	9,30	36,50	37,08	7,64	40,00	2,160	0,540

*p<0,05 ; Kruskal-Wallis Testi

Katılımcıların yaş gruplarına göre ölçek ve alt boyut puanları Kruskal-Wallis testi ile karşılaştırılmıştır. Analiz sonucunda, yalnızca bir alt boyutta yaş grupları arasında anlamlı bir farklılık tespit edilmiştir ($p < 0,05$). Diğer tüm değişkenlerde istatistiksel olarak anlamlı fark bulunmamıştır ($p > 0,05$). Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları alt boyutu açısından yaş grupları arasında anlamlı farklılık tespit edilmiştir ($X^2 = 8,443$; $p = 0,038$). En yüksek ortalama 25-34 yaş grubuna aittir ($\bar{X} = 18,64 \pm 5,27$), bunu 35-44 yaş grubu ($\bar{X} = 17,33 \pm 5,67$) ve 45 yaş ve üzeri grup ($\bar{X} = 15,75 \pm 4,75$) izlemektedir. En düşük ortalama ise 18-24 yaş grubundadır ($\bar{X} = 15,85 \pm 5,66$). Bu sonuç, genç yaş grubundaki bireylerin kurumsal güvenlik uygulamalarına yönelik farkındalığının daha düşük olabileceğini göstermektedir.

Katılımcıların eğitim düzeyine göre ölçek ve alt boyut puanları Kruskal-Wallis testi ile karşılaştırılmıştır. Yapılan analiz sonucunda sadece bir ölçekte eğitim düzeyine göre anlamlı fark bulunmuştur ($p < 0,05$). Diğer tüm ölçek ve alt boyutlarda eğitim düzeyi açısından anlamlı bir fark tespit edilmemiştir ($p > 0,05$). Siber Güvenlik Farkındalığı ve Davranışları Ölçeği açısından eğitim düzeyine göre anlamlı fark tespit edilmiştir ($X^2 = 17,417$; $p = 0,001$). En düşük ortalama lise mezunlarında görülmüştür ($\bar{X} = 24,13 \pm 10,30$), en yüksek ortalamalar ise yüksek lisans ($\bar{X} = 37,96 \pm 7,31$) ve lisans ($\bar{X} = 34,71 \pm 8,63$) düzeyindedir. Bu bulgu, eğitim düzeyi arttıkça bireylerin siber güvenlik farkındalığı ve güvenli davranış geliştirme eğilimlerinin yükseldiğini göstermektedir.

Tablo 29: Eğitim Düzeyine Göre Ölçek ve Alt Boyutların Karşılaştırılması (Kruskal-Wallis Testi Sonuçları)

	Eğitim Seviyeniz:													
	Lise (n=8)			Lisans (n=79)			Yüksek Lisans (n=25)			Doktora (n=20)			X2	P
	ort	ss	Median	ort	ss	Median	ort	ss	Median	ort	ss	Median		
Siber Güvenlik Farkındalığı ve Davranışları Ölçeği	24,13	10,30	27,00	34,71	8,63	36,00	37,96	7,31	38,00	33,85	7,29	34,00	17,417	0,001*
Risk Algısı ve Yapay Zeka Destekli Güvenlik Önlemleri Ölçeği	28,75	15,24	32,50	37,54	9,69	40,00	39,12	8,58	41,00	36,45	8,10	37,00	6,432	0,092
Yapay Zeka Destekli Kurumsal Güvenlik Algısı alt boyutu	16,38	5,97	16,50	18,15	5,08	19,00	18,36	4,13	19,00	17,30	3,71	18,00	3,796	0,284
Kurumsal Uyum ve Eğitim Destekli Güvenlik Politikaları alt boyutu	9,63	2,72	10,50	10,13	2,79	11,00	10,56	3,22	11,00	9,40	2,46	10,00	4,631	0,201
Kurumsal ve Bireysel Siber Güvenlik Politikaları Ölçeği	26,00	8,14	27,50	28,28	7,20	30,00	28,92	6,36	30,00	26,70	5,46	27,00	5,045	0,169
Siber Zorbalık ve Dijital Güvenlik Ölçeği	37,50	13,56	38,00	37,42	9,83	40,00	37,60	7,53	39,00	35,95	8,15	38,50	1,537	0,674
Siber Güvenlik Tehdit Farkındalığı Ölçeği	39,88	13,80	44,00	38,37	10,01	40,00	40,44	3,88	40,00	35,45	8,88	39,00	5,962	0,113
Yapay Zeka ile Desteklenen Güvenlik Çözümleri Ölçeği	35,00	13,18	37,00	38,27	10,29	40,00	37,60	8,19	39,00	36,60	8,00	38,50	3,942	0,268
Yapay Zeka Tabanlı Stratejik Siber Güvenlik Politikaları alt boyutu	16,63	7,85	18,00	19,87	5,16	20,00	19,48	3,97	20,00	18,90	4,18	20,00	3,470	0,325
Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları alt boyutu	15,50	7,03	13,50	18,03	5,46	20,00	18,20	5,26	20,00	15,45	4,12	15,00	6,616	0,085
Siber Güvenlik Stratejileri ve Politikalar Ölçeği	32,13	14,48	31,50	37,90	9,57	40,00	37,68	7,88	41,00	34,35	7,46	35,00	6,582	0,086
Geleneksel ve Stratejik Tehdit Farkındalığı alt boyutu	21,38	9,23	25,50	24,44	5,61	24,00	25,52	4,62	27,00	22,90	5,99	25,00	2,669	0,446
Yapay Zeka Destekli Savunma Sistemleri alt boyutu	10,88	4,19	12,50	11,52	3,06	12,00	11,68	1,77	12,00	10,80	2,76	11,50	2,506	0,474
Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeği	32,25	13,39	38,50	35,96	8,29	36,00	37,20	6,17	40,00	33,70	8,48	36,00	2,504	0,475

*p<0,05 ; Kruskal-Wallis Testi

Tablo 30: Mesleğe Göre Ölçek ve Alt Boyutların Karşılaştırılması (Kruskal-Wallis Testi Sonuçları)

	Mesleğiniz:													
	Akademisyen (n=23)			BT Uzmanı (n=53)			Sistem Yöneticisi (n=9)			Diğer (n=47)			X2	P
	ort	ss	Median	ort	ss	Median	ort	ss	Median	ort	ss	Median		
Siber Güvenlik Farkındalığı ve Davranışları Ölçeği	34,09	7,00	34,00	35,55	8,11	36,00	35,11	8,34	34,00	33,55	10,28	36,00	2,305	0,512
Risk Algısı ve Yapay Zeka Destekli Güvenlik Önlemleri Ölçeği	36,39	7,08	38,00	38,23	10,27	40,00	39,44	4,85	39,00	35,85	11,10	40,00	4,491	0,213
Yapay Zeka Destekli Kurumsal Güvenlik Algısı alt boyutu	17,57	3,01	18,00	18,49	4,96	19,00	17,44	4,82	18,00	17,64	5,28	19,00	2,834	0,418
Kurumsal Uyum ve Eğitim Destekli Güvenlik Politikaları alt boyutu	9,52	2,19	10,00	10,77	2,55	11,00	10,56	2,13	11,00	9,45	3,32	11,00	7,768	0,051
Kurumsal ve Bireysel Siber Güvenlik Politikaları Ölçeği	27,09	4,54	27,00	29,26	6,90	31,00	28,00	6,24	29,00	27,09	7,73	30,00	5,975	0,113
Siber Zorbalık ve Dijital Güvenlik Ölçeği	36,43	7,24	39,00	38,34	10,24	40,00	36,78	5,80	37,00	36,47	9,90	40,00	4,289	0,232
Siber Güvenlik Tehdit Farkındalığı Ölçeği	38,48	4,66	40,00	38,17	10,21	40,00	42,89	5,11	43,00	37,79	10,42	40,00	3,839	0,279
Yapay Zeka ile Desteklenen Güvenlik Çözümleri Ölçeği	38,35	4,95	39,00	38,55	10,45	40,00	35,89	11,71	37,00	36,74	10,41	40,00	2,487	0,478
Yapay Zeka Tabanlı Stratejik Siber Güvenlik Politikaları alt boyutu	19,00	3,40	20,00	19,98	5,24	20,00	18,22	5,14	20,00	19,32	5,47	20,00	4,388	0,222
Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları alt boyutu	15,78	3,19	15,00	19,04	5,06	20,00	18,11	5,01	20,00	16,53	6,27	20,00	10,031	0,018*
Siber Güvenlik Stratejileri ve Politikalar Ölçeği	34,78	5,27	35,00	39,02	9,64	40,00	36,33	9,77	39,00	35,85	10,38	40,00	10,917	0,012*
Geleneksel ve Stratejik Tehdit Farkındalığı alt boyutu	23,65	5,33	25,00	25,19	5,51	26,00	24,22	5,70	26,00	23,43	6,32	24,00	3,852	0,278
Yapay Zeka Destekli Savunma Sistemleri alt boyutu	11,09	2,04	12,00	11,70	3,09	12,00	11,11	2,57	12,00	11,28	3,08	12,00	3,632	0,304
Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeği	34,74	7,04	36,00	36,89	8,12	37,00	35,33	7,94	36,00	34,70	9,28	36,00	2,951	0,399

*p<0,05 ; Kruskal-Wallis Test

Katılımcıların meslek gruplarına göre ölçek ve alt boyut puanlarında farklılık olup olmadığı Kruskal-Wallis testi ile analiz edilmiştir. Analiz sonucunda iki değişkende meslek grupları arasında anlamlı farklılık tespit edilmiştir ($p < 0,05$). Diğer tüm değişkenlerde istatistiksel olarak anlamlı fark bulunmamıştır ($p > 0,05$). Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları alt boyutu açısından meslek grupları arasında anlamlı farklılık tespit edilmiştir ($X^2 = 10,031$; $p = 0,018$). En yüksek ortalama BT uzmanlarında gözlemlenmiştir ($\bar{X} = 19,04 \pm 5,06$), bunu sistem yöneticileri ($\bar{X} = 18,11 \pm 5,01$) takip etmektedir. En düşük ortalama ise akademisyen grubuna aittir ($\bar{X} = 15,78 \pm 3,19$). Bu bulgu, BT sektöründe çalışan bireylerin kurumsal güvenlik uygulamalarına yönelik daha yüksek farkındalığa sahip olduğunu göstermektedir. Siber Güvenlik Stratejileri ve Politikalar Ölçeği açısından da anlamlı bir fark bulunmuştur ($X^2 = 10,917$; $p = 0,012$). En yüksek ortalama BT uzmanlarında bulunmuştur ($\bar{X} = 39,02 \pm 9,64$), bunu sistem yöneticileri ($\bar{X} = 36,33 \pm 9,77$) ve diğer meslek grupları ($\bar{X} = 35,85 \pm 10,38$) izlemiştir. Akademisyen grubunda ortalama değerler daha düşük olması ($\bar{X} = 34,78 \pm 5,27$) dikkat çekmektedir. Bu sonuç, BT uzmanlarının siber güvenlik stratejilerine ilişkin algı düzeylerinin diğer meslek gruplarına kıyasla daha yüksek olduğunu ortaya koymaktadır.

Bu çalışmada, katılımcıların siber güvenlik eğitimi alıp almama durumlarına göre ölçek ve alt boyut puanlarında anlamlı farklılık olup olmadığı Mann-Whitney U testi ile analiz edilmiştir. Analiz sonucunda aşağıdaki değişkenlerde anlamlı farklılıklar tespit edilmiştir ($p < 0,05$): Siber Güvenlik Farkındalığı ve Davranışları Ölçeği puanları, siber güvenlik eğitimi alan bireylerde ($\bar{X} = 36,27 \pm 8,66$) eğitim almayanlara göre ($\bar{X} = 32,15 \pm 8,37$) anlamlı derecede daha yüksektir ($U = 1180,000$; $p = 0,000$). Bu bulgu, eğitim alan bireylerin güvenli dijital davranışlar konusunda daha bilinçli olduğunu göstermektedir.

Risk Algısı ve Yapay Zeka Destekli Güvenlik Önlemleri Ölçeği puanları, eğitim alanlarda ($\bar{X} = 38,17 \pm 9,99$) daha yüksektir. Eğitim almayan grubun ortalaması $35,71 \pm 9,50$ olup, fark istatistiksel olarak anlamlıdır ($U = 1645,000$; $p = 0,029$). Bu sonuç, eğitilmiş bireylerin siber tehditlere yönelik risk algılarını güçlendirdiğini göstermektedir. Yapay Zeka Destekli Kurumsal Güvenlik Algısı alt boyutu, eğitim alanlarda ($\bar{X} = 18,48 \pm 4,88$) anlamlı biçimde daha yüksektir. Eğitim almayanlarda bu

değer $17,22 \pm 4,53$ 'tür ($U = 1669,000$; $p = 0,037$). Bu durum, yapay zeka tabanlı güvenlik sistemlerine yönelik olumlu algının eğitimle birlikte geliştiğini göstermektedir.

Tablo 31: Siber Güvenlik Eğitimi Alıp Almama Durumuna Göre Ölçek ve Alt Boyutların Karşılaştırılması

	Siber güvenlik alanında eğitim aldım (n=77)			Siber güvenlik alanında eğitim almadım (n=55)			U	P
	ort	ss	Median	ort	ss	Median		
Siber Güvenlik Farkındalığı ve Davranışları Ölçeği	36,27	8,66	37,00	32,15	8,37	33,00	1180,000	0,000*
Risk Algısı ve Yapay Zeka Destekli Güvenlik Önlemleri Ölçeği	38,17	9,99	40,00	35,71	9,50	38,00	1645,000	0,029*
Yapay Zeka Destekli Kurumsal Güvenlik Algısı alt boyutu	18,48	4,88	20,00	17,22	4,53	19,00	1669,000	0,037*
Kurumsal Uyum ve Eğitim Destekli Güvenlik Politikaları alt boyutu	10,55	2,67	11,00	9,40	2,91	10,00	1609,000	0,017*
Kurumsal ve Bireysel Siber Güvenlik Politikaları Ölçeği	29,03	6,92	31,00	26,62	6,53	27,00	1531,000	0,007*
Siber Zorbalık ve Dijital Güvenlik Ölçeği	37,57	9,68	40,00	36,76	8,97	39,00	1890,000	0,291
Siber Güvenlik Tehdit Farkındalığı Ölçeği	38,97	9,67	41,00	37,62	8,75	40,00	1776,000	0,114
Yapay Zeka ile Desteklenen Güvenlik Çözümleri Ölçeği	38,35	10,40	40,00	36,76	8,73	38,00	1655,500	0,032*
Yapay Zeka Tabanlı Stratejik Siber Güvenlik Politikaları alt boyutu	19,62	5,23	20,00	19,22	4,75	20,00	1885,000	0,273
Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları alt boyutu	18,26	5,37	20,00	16,47	5,29	17,00	1664,000	0,035*
Siber Güvenlik Stratejileri ve Politikalar Ölçeği	37,88	9,71	40,00	35,69	8,86	38,00	1659,500	0,034*
Geleneksel ve Stratejik Tehdit Farkındalığı alt boyutu	24,64	5,99	25,00	23,65	5,50	24,00	1768,500	0,104
Yapay Zeka Destekli Savunma Sistemleri alt boyutu	11,61	3,08	12,00	11,11	2,57	12,00	1789,500	0,118
Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeği	36,25	8,69	37,00	34,76	7,84	36,00	1723,500	0,066

* $p < 0,05$; Mann-Whitney U testi

Kurumsal Uyum ve Eğitim Destekli Güvenlik Politikaları alt boyutu açısından da anlamlı fark saptanmıştır ($U = 1609,000$; $p = 0,017$). Eğitim alan bireylerin puanı $10,55 \pm 2,67$ iken, eğitim almayanlarda bu değer $9,40 \pm 2,91$ 'dir. Bu sonuç, güvenlik politikalarına uyumun eğitimle desteklendiğini ortaya koymaktadır. Kurumsal ve Bireysel Siber Güvenlik Politikaları Ölçeği puanları, eğitim alan grupta ($\bar{X} = 29,03 \pm 6,92$) anlamlı şekilde daha yüksektir. Eğitim almayan grubun ortalaması $26,62 \pm 6,53$ 'tür ($U = 1531,000$; $p = 0,007$). Bu, bireylerin hem kurumsal hem kişisel düzeyde güvenlik politikalarına karşı daha duyarlı olduğunu göstermektedir.

Yapay Zeka ile Desteklenen Güvenlik Çözümleri Ölçeği açısından da anlamlı fark mevcuttur ($U = 1655,500$; $p = 0,032$). Eğitim alan bireylerin ortalaması $38,35 \pm 10,40$ iken, eğitim almayanlarda bu değer $36,76 \pm 8,73$ 'tür. Bu bulgu, yapay zeka destekli güvenlik teknolojilerine duyulan güvenin eğitimle arttığını göstermektedir. Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları alt boyutu da eğitim alan bireylerde daha yüksek bulunmuştur ($\bar{X} = 18,26 \pm 5,37$) ve fark istatistiksel olarak anlamlıdır ($U = 1664,000$; $p = 0,035$). Eğitim almayanlarda ortalama puan $16,47 \pm 5,29$ 'dur. Siber Güvenlik Stratejileri ve Politikalar Ölçeği puanları, eğitim alan bireylerde ($\bar{X} = 37,88 \pm 9,71$) eğitim almayanlara ($\bar{X} = 35,69 \pm 8,86$) kıyasla anlamlı derecede yüksektir ($U = 1659,500$; $p = 0,034$). Bu fark, eğitimin güvenlik stratejilerine dair bilgi düzeyini artırdığını göstermektedir.

Yapılan korelasyon analizine göre, Siber Güvenlik Farkındalığı ve Davranışları Ölçeği ile çalışmada yer alan tüm ölçekler ve alt boyutlar arasında istatistiksel olarak anlamlı ($p < 0,001$) ve pozitif yönde orta kuvvetli ilişkiler olduğu belirlenmiştir. Bu ölçek ile Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeği ($r = 0,575$), Geleneksel ve Stratejik Tehdit Farkındalığı alt boyutu ($r = 0,565$), Siber Güvenlik Stratejileri ve Politikalar Ölçeği ($r = 0,561$), Yapay Zeka ile Desteklenen Güvenlik Çözümleri Ölçeği ($r = 0,537$), Risk Algısı ve Yapay Zeka Destekli Güvenlik Önlemleri Ölçeği ($r = 0,533$), Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları alt boyutu ($r = 0,531$), Kurumsal ve Bireysel Siber Güvenlik Politikaları Ölçeği ($r = 0,527$), Yapay Zeka Destekli Savunma Sistemleri alt boyutu ($r = 0,518$), Yapay Zeka Tabanlı Stratejik Siber Güvenlik Politikaları alt boyutu ($r = 0,476$), Kurumsal Uyum ve Eğitim Destekli Güvenlik Politikaları alt boyutu ($r = 0,475$), Yapay Zeka Destekli

Kurumsal Güvenlik Algısı alt boyutu ($r = 0,451$), Siber Güvenlik Tehdit Farkındalığı Ölçeği ($r = 0,451$) ve Siber Zorbalık ve Dijital Güvenlik Ölçeği ($r = 0,420$) arasında pozitif ve orta kuvvetli ilişkiler bulunmaktadır. Bu sonuçlar, bireylerin siber güvenlik farkındalık düzeyleri arttıkça, hem bireysel hem de kurumsal düzeyde yapay zeka destekli güvenlik uygulamalarına, risk algılamalarına ve stratejik önlemlere yönelik tutumlarının da belirgin biçimde yükseldiğini göstermektedir. Dolayısıyla farkındalık, güvenlik stratejileri ile bütünsel olarak uyumlu gelişmektedir

Risk Algısı ve Yapay Zeka Destekli Güvenlik Önlemleri Ölçeği ile diğer tüm ölçek ve alt boyutlar arasında yapılan korelasyon analizinde, tüm ilişkiler pozitif yönlü ve istatistiksel olarak anlamlıdır ($p < 0,001$). Bu ölçek ile Yapay Zeka Destekli Kurumsal Güvenlik Algısı alt boyutu ($r = 0,705$), Kurumsal ve Bireysel Siber Güvenlik Politikaları Ölçeği ($r = 0,667$), Siber Zorbalık ve Dijital Güvenlik Ölçeği ($r = 0,629$) ve Yapay Zeka Destekli Savunma Sistemleri alt boyutu ($r = 0,606$) arasında pozitif ve kuvvetli ilişkiler bulunmaktadır. Diğer tüm değişkenlerle ise pozitif ve orta kuvvetli ilişkiler gözlemlenmiştir. Bu kapsamda; Yapay Zeka ile Desteklenen Güvenlik Çözümleri Ölçeği ($r = 0,572$), Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeği ($r = 0,563$), Siber Güvenlik Stratejileri ve Politikalar Ölçeği ($r = 0,528$), Yapay Zeka Tabanlı Stratejik Siber Güvenlik Politikaları alt boyutu ($r = 0,516$), Geleneksel ve Stratejik Tehdit Farkındalığı alt boyutu ($r = 0,485$), Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları alt boyutu ($r = 0,444$), Kurumsal Uyum ve Eğitim Destekli Güvenlik Politikaları alt boyutu ($r = 0,439$) ve Siber Güvenlik Tehdit Farkındalığı Ölçeği ($r = 0,425$) ile orta kuvvetli pozitif ilişkiler elde edilmiştir. Bu sonuçlar, bireylerin risk algısı yükseldikçe hem yapay zeka destekli savunma sistemlerine hem de kurumsal siber güvenlik politikalarına yönelik tutumlarının olumlu yönde geliştiğini göstermektedir. Özellikle yapay zeka temelli güvenlik algıları ve bireysel farkındalıkla birlikte bu güvenlik politikalarının etkili biçimde içselleştirildiği anlaşılmaktadır.

Tablo 32: Ölçek ve Alt Boyutlar Arasındaki Korelasyonlar (Spearman Korelasyon Katsayıları)

		Siber Güvenlik Farkındalığı ve Davranışları Ölçeği	Risk Algısı ve Yapay Zeka Destekli Güvenlik Önlemleri Ölçeği	Yapay Zeka Destekli Kurumsal Güvenlik Algısı alt boyutu	Kurumsal Uyum ve Eğitim Destekli Güvenlik Politikaları alt boyutu	Kurumsal ve Bireysel Siber Güvenlik Politikaları Ölçeği	Siber Zorbalık ve Dijital Güvenlik Ölçeği	Siber Güvenlik Tehdit Farkındalığı Ölçeği	Yapay Zeka ile Desteklenen Güvenlik Çözümleri Ölçeği	Yapay Zeka Tabanlı Stratejik Siber Güvenlik Politikaları alt boyutu	Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları alt boyutu	Siber Güvenlik Stratejileri ve Politikalar Ölçeği	Geleneksel ve Stratejik Tehdit Farkındalığı alt boyutu	Yapay Zeka Destekli Savunma Sistemleri alt boyutu	Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeği
Siber Güvenlik Farkındalığı ve Davranışları Ölçeği	r	1,000													
	p														
Risk Algısı ve Yapay Zeka Destekli Güvenlik Önlemleri Ölçeği	r	,533**	1,000												
	p	0,000													
Yapay Zeka Destekli Kurumsal Güvenlik Algısı alt boyutu	r	,451**	,705**	1,000											
	p	0,000	0,000												
Kurumsal Uyum ve Eğitim Destekli Güvenlik Politikaları alt boyutu	r	,475**	,439**	,525**	1,000										
	p	0,000	0,000	0,000											
Kurumsal ve Bireysel Siber Güvenlik Politikaları Ölçeği	r	,527**	,667**	,894**	,825**	1,000									
	p	0,000	0,000	0,000	0,000										
Siber Zorbalık ve Dijital Güvenlik Ölçeği	r	,420**	,629**	,624**	,338**	,557**	1,000								
	p	0,000	0,000	0,000	0,000	0,000									
Siber Güvenlik Tehdit Farkındalığı Ölçeği	r	,451**	,425**	,443**	,466**	,496**	,526**	1,000							
	p	0,000	0,000	0,000	0,000	0,000	0,000								
Yapay Zeka ile Desteklenen Güvenlik Çözümleri Ölçeği	r	,537**	,572**	,587**	,434**	,587**	,599**	,591**	1,000						
	p	0,000	0,000	0,000	0,000	0,000	0,000	0,000							
Yapay Zeka Tabanlı Stratejik Siber Güvenlik Politikaları alt boyutu	r	,476**	,516**	,537**	,354**	,509**	,650**	,460**	,655**	1,000					
	p	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000						
	r	,531**	,444**	,456**	,694**	,641**	,454**	,435**	,544**	,515**	1,000				

Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları alt boyutu	p	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	
Siber Güvenlik Stratejileri ve Politikalar Ölçeği	r	,561**	,528**	,554**	,645**	,676**	,596**	,478**	,653**	,762**	,921**	1,000			
	p	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	
Geleneksel ve Stratejik Tehdit Farkındalığı alt boyutu	r	,565**	,485**	,470**	,418**	,475**	,580**	,585**	,617**	,759**	,529**	,663**	1,000		
	p	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	
Yapay Zeka Destekli Savunma Sistemleri alt boyutu	r	,518**	,606**	,643**	,325**	,567**	,672**	,525**	,708**	,724**	,478**	,621**	,701**	1,000	
	p	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	
Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeği	r	,575**	,563**	,551**	,386**	,524**	,666**	,593**	,707**	,819**	,503**	,681**	,949**	,850**	1,000
	p	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000	0,000

Yapay Zeka Destekli Kurumsal Güvenlik Algısı alt boyutu ile diğer ölçek ve alt boyutlar arasında yapılan korelasyon analizine göre, tüm ilişkiler pozitif yönlü ve istatistiksel olarak anlamlı bulunmuştur ($p < 0,001$). Bu alt boyut ile Kurumsal ve Bireysel Siber Güvenlik Politikaları Ölçeği ($r = 0,894$) arasında pozitif yönlü çok kuvvetli, Yapay Zeka Destekli Savunma Sistemleri alt boyutu ($r = 0,643$) ve Siber Zorbalık ve Dijital Güvenlik Ölçeği ($r = 0,624$) ile ise pozitif yönlü kuvvetli ilişkiler bulunmaktadır. Diğer değişkenler ile pozitif ve orta kuvvetli düzeyde ilişkiler gözlemlenmiştir. Bu bağlamda; Kurumsal Uyum ve Eğitim Destekli Güvenlik Politikaları alt boyutu ($r = 0,525$), Yapay Zeka ile Desteklenen Güvenlik Çözümleri Ölçeği ($r = 0,587$), Yapay Zeka Tabanlı Stratejik Siber Güvenlik Politikaları alt boyutu ($r = 0,537$), Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları alt boyutu ($r = 0,456$), Siber Güvenlik Stratejileri ve Politikalar Ölçeği ($r = 0,554$), Geleneksel ve Stratejik Tehdit Farkındalığı alt boyutu ($r = 0,470$) ve Siber Güvenlik Tehdit Farkındalığı Ölçeği ($r = 0,443$) ile olan ilişkiler orta kuvvetli düzeydedir. Elde edilen bu bulgular, katılımcıların kurumsal güvenlik algıları arttıkça yapay zekaya dayalı sistemleri, stratejik politikaları ve savunma mekanizmalarını daha olumlu değerlendirdiklerini göstermektedir. Özellikle kurumsal güvenlik politikalarının genel yapısıyla olan çok kuvvetli ilişki, bu iki yapının birbiriyle bütünleşik olduğunu ortaya koymaktadır.

Kurumsal Uyum ve Eğitim Destekli Güvenlik Politikaları alt boyutu ile diğer ölçek ve alt boyutlar arasındaki korelasyon analizine göre, tüm ilişkiler pozitif yönlü ve istatistiksel olarak anlamlıdır ($p < 0,001$). Bu alt boyut ile Kurumsal ve Bireysel Siber Güvenlik Politikaları Ölçeği ($r = 0,825$) arasında pozitif ve çok kuvvetli bir ilişki bulunmuştur. Bu durum, kurumsal uyum ve eğitim faaliyetlerinin, genel güvenlik politikalarının algılanışıyla büyük ölçüde örtüştüğünü göstermektedir. Ayrıca, Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları alt boyutu ($r = 0,694$) ve Siber Güvenlik Stratejileri ve Politikalar Ölçeği ($r = 0,645$) ile pozitif ve kuvvetli düzeyde anlamlı ilişkiler saptanmıştır. Bu bulgu, eğitim ve uyum süreçlerinin hem stratejik güvenlik planlaması hem de kurumsal farkındalıkla doğrudan bağlantılı olduğunu göstermektedir. Bununla birlikte, Siber Güvenlik Tehdit Farkındalığı Ölçeği ($r = 0,466$), Yapay Zeka ile Desteklenen Güvenlik Çözümleri Ölçeği ($r = 0,434$),

Geleneksel ve Stratejik Tehdit Farkındalığı alt boyutu ($r = 0,418$), Yapay Zeka Tabanlı Stratejik Siber Güvenlik Politikaları alt boyutu ($r = 0,354$), Siber Zorbalık ve Dijital Güvenlik Ölçeği ($r = 0,338$), Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeği ($r = 0,386$) ve Yapay Zeka Destekli Savunma Sistemleri alt boyutu ($r = 0,325$) ile pozitif ve orta kuvvetli düzeyde ilişkiler bulunmuştur. Bu bulgular, kurumsal uyum ve eğitim politikalarının yalnızca doğrudan kurumsal güvenlikle değil, aynı zamanda yapay zeka destekli sistemler ve tehdit farkındalığı ile de bütüncül bir etkileşim içinde olduğunu göstermektedir. Eğitim ve politika süreçlerinin bu alanlara olumlu katkı sağladığı söylenebilir.

Kurumsal ve Bireysel Siber Güvenlik Politikaları Ölçeği ile diğer ölçek ve alt boyutlar arasında yapılan korelasyon analizine göre tüm ilişkiler pozitif yönlü ve istatistiksel olarak anlamlıdır ($p < 0,001$). En yüksek ilişki, Siber Güvenlik Stratejileri ve Politikalar Ölçeği ($r = 0,676$) ile olup, bu iki değişken arasında pozitif ve kuvvetli bir ilişki olduğu görülmektedir. Bu sonuç, kurumsal ve bireysel güvenlik politikalarının stratejik güvenlik planlamalarıyla doğrudan ve güçlü şekilde bağlantılı olduğunu göstermektedir. Bunu takiben, Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları alt boyutu ($r = 0,641$) ile de pozitif ve kuvvetli bir ilişki belirlenmiştir. Bu bulgu, güvenlik politikalarının yalnızca belirlenmiş stratejilerle değil, aynı zamanda çalışan farkındalığı ve kurumsal uyum uygulamalarıyla da yakından ilişkili olduğunu göstermektedir. Buna ek olarak, Yapay Zeka ile Desteklenen Güvenlik Çözümleri Ölçeği ($r = 0,587$), Yapay Zeka Tabanlı Stratejik Siber Güvenlik Politikaları alt boyutu ($r = 0,509$), Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeği ($r = 0,524$), Yapay Zeka Destekli Savunma Sistemleri alt boyutu ($r = 0,567$), Siber Zorbalık ve Dijital Güvenlik Ölçeği ($r = 0,557$) ve Siber Güvenlik Tehdit Farkındalığı Ölçeği ($r = 0,496$) ile pozitif ve orta kuvvetli ilişkiler gözlemlenmiştir. Ayrıca, Geleneksel ve Stratejik Tehdit Farkındalığı alt boyutu ($r = 0,475$) ile de yine pozitif ve orta kuvvetli bir ilişki bulunmaktadır. Bu bulgular genel olarak, kurumsal ve bireysel düzeyde benimsenen siber güvenlik politikalarının, tehdit farkındalığı, stratejik savunma sistemleri ve yapay zeka temelli güvenlik yaklaşımlarıyla istikrarlı biçimde uyum gösterdiğini ve bu bileşenlerle bütüncül bir yapıda hareket ettiğini ortaya koymaktadır.

Siber Zorbalık ve Dijital Güvenlik Ölçeği ile diğer ölçek ve alt boyutlar arasındaki korelasyon analizine göre tüm ilişkiler pozitif yönlü ve istatistiksel olarak anlamlıdır ($p < 0,001$). En yüksek korelasyon, Yapay Zeka Destekli Savunma Sistemleri alt boyutu ($r = 0,672$) ve Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeği ($r = 0,666$) ile olup, bu değişkenler arasında pozitif ve kuvvetli bir ilişki olduğu görülmektedir. Bu durum, yapay zeka destekli savunma sistemlerinin ve genel tehditlere karşı geliştirilen savunma mekanizmalarının, siber zorbalıkla mücadelede önemli bir yere sahip olduğunu göstermektedir. Benzer şekilde, Yapay Zeka Tabanlı Stratejik Siber Güvenlik Politikaları alt boyutu ($r = 0,650$) ile de pozitif ve kuvvetli bir ilişki saptanmıştır. Bu bulgu, stratejik güvenlik politikalarının siber zorbalıkla mücadelede etkili bir yaklaşım sunduğunu desteklemektedir. Bunun yanı sıra, Yapay Zeka ile Desteklenen Güvenlik Çözümleri Ölçeği ($r = 0,599$), Siber Güvenlik Stratejileri ve Politikalar Ölçeği ($r = 0,596$), Geleneksel ve Stratejik Tehdit Farkındalığı alt boyutu ($r = 0,580$), Siber Güvenlik Tehdit Farkındalığı Ölçeği ($r = 0,526$) ve Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları alt boyutu ($r = 0,454$) ile pozitif ve orta kuvvetli ilişkiler tespit edilmiştir. Bu sonuçlar, siber zorbalıkla mücadelede sadece teknolojik altyapının değil, aynı zamanda tehdit farkındalığı, stratejik yönelimler ve kurumsal farkındalık uygulamalarının da etkili olduğunu göstermektedir.

Siber Güvenlik Tehdit Farkındalığı Ölçeği ile diğer ölçek ve alt boyutlar arasındaki korelasyon analizine göre tüm ilişkiler pozitif yönlü ve istatistiksel olarak anlamlıdır ($p < 0,001$). En yüksek korelasyon değeri, Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeği ($r = 0,593$) ile elde edilmiş olup, bu iki değişken arasında pozitif ve orta kuvvetli bir ilişki olduğu belirlenmiştir. Bu ilişki, bireylerin tehdit farkındalık düzeyi ile siber savunma stratejilerinin algısı arasında anlamlı bir bağlantı olduğunu göstermektedir. Benzer şekilde, Yapay Zeka ile Desteklenen Güvenlik Çözümleri Ölçeği ($r = 0,591$), Geleneksel ve Stratejik Tehdit Farkındalığı alt boyutu ($r = 0,585$) ve Yapay Zeka Destekli Savunma Sistemleri alt boyutu ($r = 0,525$) ile de pozitif ve orta kuvvetli ilişkiler tespit edilmiştir. Bu bulgular, tehdit farkındalığı yüksek bireylerin yapay zeka destekli sistemlere ve genel tehdit analizlerine daha fazla önem verdiğini göstermektedir. Ayrıca, Siber Güvenlik Stratejileri ve Politikalar

Ölçeği ($r = 0,478$), Yapay Zeka Tabanlı Stratejik Siber Güvenlik Politikaları alt boyutu ($r = 0,460$) ve Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları alt boyutu ($r = 0,435$) ile olan ilişkiler de pozitif ve orta kuvvetli düzeydedir. Bu durum, stratejik politika algısı, kurumsal uyum ve tehdit farkındalığı arasında istatistiksel olarak anlamlı bir bağlantı bulunduğunu göstermektedir.

Yapay Zeka ile Desteklenen Güvenlik Çözümleri Ölçeği ile diğer ölçek ve alt boyutlar arasında yapılan korelasyon analizine göre tüm ilişkiler pozitif yönlü ve istatistiksel olarak anlamlıdır ($p < 0,001$). Bu ölçek ile en güçlü ilişki, Yapay Zeka Destekli Savunma Sistemleri alt boyutu ($r = 0,708$) ve Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeği ($r = 0,707$) arasında saptanmış olup, her iki değişkenle pozitif yönde kuvvetli düzeyde ilişki bulunmaktadır. Bu sonuç, yapay zeka tabanlı güvenlik çözümlerinin hem savunma sistemlerinin güçlendirilmesinde hem de siber tehditlere karşı daha etkili savunma mekanizmalarının geliştirilmesinde önemli bir rol oynadığını göstermektedir. Benzer şekilde, Siber Güvenlik Stratejileri ve Politikalar Ölçeği ($r = 0,653$), Yapay Zeka Tabanlı Stratejik Siber Güvenlik Politikaları alt boyutu ($r = 0,655$) ve Geleneksel ve Stratejik Tehdit Farkındalığı alt boyutu ($r = 0,617$) ile de pozitif ve kuvvetli düzeyde ilişkiler mevcuttur. Bu bulgular, katılımcıların yapay zeka çözümlerini, sadece teknolojik araçlar olarak değil, aynı zamanda güvenlik stratejileri ve tehdit algısına dair temel bir bileşen olarak değerlendirdiklerini göstermektedir. Ayrıca, Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları alt boyutu ($r = 0,544$) ile pozitif ve orta kuvvetli bir ilişki bulunmuştur. Bu sonuç, yapay zeka destekli çözümlerin kurumların güvenlik uygulamalarındaki yerini güçlendirdiğini ve çalışan farkındalığını olumlu yönde etkileyebileceğini göstermektedir.

Yapay Zeka Tabanlı Stratejik Siber Güvenlik Politikaları alt boyutu ile diğer değişkenler arasında yapılan korelasyon analizine göre, tüm ilişkiler pozitif yönde ve istatistiksel olarak anlamlıdır ($p < 0,001$). Bu alt boyut ile Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeği ($r = 0,819$) arasında pozitif yönlü çok kuvvetli bir ilişki tespit edilmiştir. Bu bulgu, yapay zeka tabanlı stratejik politikaların, savunma mekanizmalarının etkinliğini artırmada temel bir rol oynadığını göstermektedir. Ayrıca, Siber Güvenlik Stratejileri ve Politikalar Ölçeği ($r = 0,762$), Geleneksel ve

Stratejik Tehdit Farkındalığı alt boyutu ($r = 0,759$) ve Yapay Zeka Destekli Savunma Sistemleri alt boyutu ($r = 0,724$) ile pozitif ve kuvvetli düzeyde ilişkiler gözlemlenmiştir. Bu sonuçlar, yapay zeka destekli stratejilerin tehdit algısı, genel güvenlik stratejileri ve savunma sistemleriyle güçlü bir yapısal bütünlük oluşturduğunu göstermektedir. Son olarak, Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları alt boyutu ($r = 0,515$) ile pozitif ve orta kuvvetli bir ilişki saptanmıştır. Bu bulgu, yapay zeka tabanlı stratejik yaklaşımların kurumsal farkındalık ve güvenlik uyumu ile de uyumlu bir yapı sergilediğini ifade etmektedir. Genel olarak, bu sonuçlar, stratejik düzeyde yapay zeka kullanımının siber güvenliğin birçok boyutuyla anlamlı ve güçlü bir ilişki içinde olduğunu ortaya koymaktadır.

Kurumsal Farkındalık ve Uyum Odaklı Güvenlik Uygulamaları alt boyutu ile yapılan korelasyon analizine göre, bu boyut ile diğer ölçekler arasında pozitif yönlü ve istatistiksel olarak anlamlı ilişkiler tespit edilmiştir ($p < 0,001$). En yüksek korelasyon, Siber Güvenlik Stratejileri ve Politikalar Ölçeği ($r = 0,921$) ile bulunmuş olup bu ilişki pozitif yönde çok kuvvetlidir. Bu bulgu, kurum içi farkındalık ve uyum odaklı güvenlik uygulamalarının, genel siber güvenlik stratejileriyle doğrudan ve güçlü biçimde ilişkili olduğunu göstermektedir.

Bunun yanında, Geleneksel ve Stratejik Tehdit Farkındalığı alt boyutu ($r = 0,529$) ile pozitif yönlü orta kuvvetli, Yapay Zeka Destekli Savunma Sistemleri alt boyutu ($r = 0,478$) ve Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeği ($r = 0,503$) ile de yine pozitif ve orta kuvvetli ilişkiler tespit edilmiştir. Bu sonuçlar, kurumsal güvenlikte farkındalık düzeyinin, tehdit algısı, yapay zeka destekli savunma ve genel güvenlik mekanizmalarıyla koordineli biçimde geliştiğini ortaya koymaktadır. Genel olarak, bu alt boyutun diğer siber güvenlik ölçekleriyle yapısal bütünlük içinde olduğu söylenebilir.

Siber Güvenlik Stratejileri ve Politikalar Ölçeği ile yapılan korelasyon analizine göre, bu ölçek ile diğer bazı değişkenler arasında pozitif yönlü ve istatistiksel olarak anlamlı ilişkiler bulunmuştur ($p < 0,001$). Ölçek ile Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeği ($r = 0,681$) arasında pozitif ve kuvvetli bir ilişki bulunmaktadır. Bu durum, genel güvenlik stratejilerinin ve politikalarının etkili

savunma mekanizmalarıyla doğrudan bağlantılı olduğunu göstermektedir. Ayrıca, Geleneksel ve Stratejik Tehdit Farkındalığı alt boyutu ($r = 0,663$) ve Yapay Zeka Destekli Savunma Sistemleri alt boyutu ($r = 0,621$) ile olan ilişkiler de pozitif ve kuvvetli düzeydedir. Bu sonuçlar, stratejik güvenlik politikalarının yalnızca tehdit algısıyla değil, aynı zamanda ileri düzey teknolojik çözümlerle bütünleşik bir yapıda olduğunu ortaya koymaktadır. Tüm bulgular, siber güvenlik stratejilerinin, hem klasik hem de yapay zeka destekli savunma anlayışlarıyla paralel geliştiğini göstermektedir.

Geleneksel ve Stratejik Tehdit Farkındalığı alt boyutu ile yapılan korelasyon analizinde, iki değişkenle pozitif yönlü ve anlamlı düzeyde kuvvetli ilişkiler tespit edilmiştir ($p < 0,001$). Bu alt boyut ile Siber Güvenlik Tehditleri ve Savunma Mekanizmaları Ölçeği ($r = 0,949$) arasında pozitif çok kuvvetli bir ilişki bulunmaktadır. Bu bulgu, bireylerin ya da kurumların tehdit farkındalığının, savunma mekanizmalarını ne ölçüde geliştirdiğiyle doğrudan bağlantılı olduğunu göstermektedir. Ayrıca, Yapay Zeka Destekli Savunma Sistemleri alt boyutu ($r = 0,701$) ile de pozitif ve kuvvetli bir ilişki bulunmuştur. Bu sonuç, stratejik tehdit farkındalığı düzeyi yüksek olanların aynı zamanda yapay zeka destekli sistemleri daha fazla önemsediklerini ve bu sistemleri etkin savunma araçları olarak gördüklerini ortaya koymaktadır. Genel olarak bu bulgular, tehdit farkındalığı ile hem geleneksel hem de modern savunma yöntemleri arasında güçlü bir bağ olduğunu ortaya koymaktadır.

5. TARTIŞMA

Bu araştırmada öncelikle katılımcıların siber güvenlik farkındalığı ve davranışlarına ilişkin puanlarının orta-yüksek düzeyde seyrettiği görülmekte, özellikle çevrimiçi bağlantılarda veri güvenliğine özen gösterme ve güçlü parola kullanma eğilimleri yüksek ortalamalarla öne çıkmaktadır (Tablo 1). Bu durum, literatürde bireysel koruyucu alışkanlıkların tehdit yüzeyini daralttığına ilişkin bulgularla örtüşmektedir (Efe, 2021a; Abdulhussein, 2024). Bununla birlikte eğitim alımına ilişkin ortalamanın görece düşük kalması, kurum içi kapasite geliştirme programlarının henüz yeterince yaygınlaştırılmadığını düşündürmekte, nitekim benzer eksikliklere Araya ve King (2022) ile Sultan ve Sultan (2024) da işaret etmektedir. Risk algısı ve yapay zeka destekli güvenlik önlemleri ölçeğindeki yüksek puanlar, katılımcıların yapay zekanın proaktif tehdit yönetiminde hız ve maliyet avantajı sağlayacağına dair güçlü bir inanca sahip olduğunu göstermektedir (Tablo 4). Alowaidi vd., (2023) ve Roshanaei vd., (2024) de yapay zeka tabanlı erken uyarı sistemlerinin tehdit öngörüsünü artırdığını belirtmektedir. Bununla birlikte yanlış pozitif riskine ve gizlilik endişesine dair temkinli tutum, Bonfanti (2020) ile Chouraiki vd., (2024) tarafından vurgulanan etik ve doğruluk ikilemlerini teyit etmektedir. Dolayısıyla yapay zeka çözümlerinin benimsenmesi, teknik verimliliğin yanı sıra mahremiyet-şeffaflık dengesinin de kurumsal stratejilere entegre edilmesini gerektirmektedir.

Kurumsal ve bireysel siber güvenlik politikalarına ilişkin bulgular, yapay zeka destekli sistemlerin çalışan uyumunu artıracığına dair olumlu beklentilerin yüksek olduğunu, ancak kurumlarda bu araçların fiilen kullanım düzeyinin sınırlı kaldığını ortaya koymaktadır (Tablo 7). Folorunso vd., (2024) yapay zeka entegrasyonunun teknik değil kültürel direnç kaynaklı gecikmeler yaşayabileceğine dikkat çekmektedir; araştırma bulguları da söz konusu uyum açığını doğrulamaktadır. Kurumsal uyum ve eğitim destekli güvenlik politikaları alt boyutunda 25-34 yaş grubunun en yüksek algıya sahip olması (Tablo 28), dijital yerli kuşağın politika ve eğitim programlarına daha hızlı adapte olabildiğini göstermektedir. Lise mezunlarının farkındalık puanlarının anlamlı biçimde düşük kalması (Tablo 29), eğitim düzeyinin siber hijyen davranışlarını doğrudan etkilediğine dair önceki bulgularla paralel

seyretmektedir (Lysenko vd., 2024). Siber zorbalık ve dijital güvenlik ölçeğindeki yüksek ortalamalar, yapay zeka destekli içerik filtreleme ve tehdit avcılığı yöntemlerine duyulan güvenin güçlü olduğunu göstermektedir (Tablo 10). Bu sonuç, çocukların çevrimiçi güvenliğinin artırılmasında otomatik denetim sistemlerinin kritik rol oynadığını öne süren Binhammad vd., (2024) ve Sanclemente (2023) ile tutarlılık sergilemektedir. Bununla birlikte mahremiyet ihlali endişeleri, algoritmik gözetim eleştirilerini gündeme getirmekte; Gilbert ve Gilbert (2024) ile Chouraik vd., (2024) da bu ikilemi vurgulamaktadır. Dolayısıyla politikalar, koruma-denetim ekseninde insan hakları boyutunu gözeterek tasarlanmalıdır.

Korelasyon analizleri, çalışmadaki tüm ölçek ve alt boyutlar arasında pozitif ve anlamlı ilişkiler bulunduğunu ortaya koymaktadır (Tablo 32). Özellikle yapay zeka ile desteklenen güvenlik çözümleri ölçeği ile yapay zeka destekli savunma sistemleri alt boyutu arasındaki kuvvetli ilişki ($r=0,708$) yapay zeka temelli yaklaşımların savunma mimarisindeki merkeziliğini pekiştirmektedir. Bu bulgu, Naik vd., (2022) ve Zhang vd., (2021) tarafından rapor edilen “öğrenen savunma döngüsü” kavramını desteklemektedir. Diğer taraftan yapay zeka tabanlı stratejik siber güvenlik politikaları ile tehdit ve savunma ölçekleri arasındaki çok kuvvetli korelasyon ($r=0,819$) stratejik politika tasarımı yapay zeka uygulamalarının vazgeçilmezleştiğini göstermektedir; bu eğilim, Maathuis ve Cools (2025) ile Radanliev (2024) tarafından da vurgulanmaktadır. Meslek grupları temelinde yapılan analizde BT uzmanlarının hem kurumsal farkındalık-uyum alt boyutunda hem de siber güvenlik stratejileri ölçeğinde diğer gruplara kıyasla daha yüksek puanlar alması (Tablo 30), sektörel pratik bilgi birikiminin politika bilinciyle paralel geliştiğini göstermektedir. İlgili literatürde BT profesyonellerinin siber olgunluk düzeylerinin akademik personelden istatistiksel olarak yüksek saptandığı çalışmalar bulunmakta (Obi vd., 2024; Efe, 2021b); elde edilen bulgu bu eğilimi doğrulamaktadır. Siber güvenlik eğitimi alan katılımcıların 10 değişkende anlamlı biçimde daha yüksek puan alması (Tablo 31), eğitim müdahalelerinin davranış ve algı boyutlarında somut çıktılar ürettiğini ortaya koymaktadır. Eltayeb (2024) ile Ikemefuna ve Orekha (2024) da benzer şekilde hedefe yönelik eğitimlerin tehdit öngörüsü ve politika uyumunu artırdığını rapor etmektedir.

Siber güvenlik tehdit farkındalığı ölçeğinde en yüksek ortalamanın düzenli güvenlik testlerinin gerekliliğine dair maddeye ait olması (Tablo 13) ve geleneksel-stratejik tehdit farkındalığı alt boyutunun tehdit-savunma ölçeğiyle çok kuvvetli korelasyon göstermesi ($r=0,949$) proaktif denetim mekanizmalarının literatürde atfedilen kritik rolünü pekiştirmektedir (Temara, 2024; Sulaiman vd., 2024). Buna karşılık yapay zeka tabanlı tehdit avcılığına duyulan güvenin görece düşük kalması, veri setinin yapay zekanın öngörü kapasitesine ilişkin temkinli bakış açısını yansıtmakta, Benzer rezervlere Bonfanti ve Kohler (2020) ile Gilbert ve Gilbert (2024) de değinmektedir. Araştırmanın bütünsel bulguları göstermektedir ki bireysel farkındalık, risk algısı, yapay zeka temelli güvenlik uygulamaları ve kurumsal stratejiler karşılıklı olarak birbirini beslemektedir. Yapay zeka destekli çözümler, savunma hızını ve kapsamını artırmakta ancak mahremiyet, etik ve yanlış pozitif sorunları çözülmeden tam entegrasyon mümkün görünmemektedir. Kurumsal düzlemdeki en kritik gereksinimlerden biri, nitelikli eğitim programları ile politika güncellemelerinin eş zamanlı yürütülmesidir. Eğitim düzeyi, mesleki alan ve siber güvenlik eğitimi alımının pek çok ölçekte anlamlı fark yaratması, insan kaynağının kapasite geliştirme sürecinde belirleyici olduğunu ortaya koymaktadır. Dolayısıyla gelecekteki çalışmalar, yapay zeka sistemlerinin etik-teknik dengelerini optimize etmeye, eğitim modüllerini mikro-öğrenme yaklaşımlarıyla desteklemeye ve kurumsal kültürü yapay zeka ile uyumlu şekilde dönüştürmeye odaklanmalıdır.

Genel olarak değişkenler arasındaki korelasyon matrisinde (Tablo 32) yapay zeka destekli savunma sistemleri alt boyutu ile geleneksel-stratejik tehdit farkındalığı alt boyutunun kuvvetli ilişkisi ($r=0,701$) her iki yapı arasında karşılıklı bir etkileşim döngüsünün geliştiğini göstermektedir. Bu döngü, tehdit zekası arttıkça savunma mekanizmalarının “öğrenen” bir karakter kazandığını; savunma mekanizmaları geliştikçe de tehdit farkındalığının daha rafine hale geldiğini ortaya koymaktadır. Naik vd., (2022) tarafından vurgulanan adversarial geri besleme döngüsü, araştırma bulgularında pratik bir karşılık bulmaktadır. Bu durum, siber saldırganların da yapay zeka tabanlı teknikleri giderek daha sofistike hale getirdiği gerçeğiyle birleştiğinde (Tablo 22, madde 78) “yapay zeka-yapay zeka” rekabetini kurumsal stratejilerin

merkezine yerleřtirmektedir (Zhang vd., 2021; Eltayeb, 2024). Çalışmanın demografik analizleri, cinsiyetin ölçek puanları üzerinde anlamlı bir etkisinin bulunmadığını (Tablo 27) ortaya koymaktadır; bu bulgu, siber güvenlik literatüründe cinsiyet temelli farkların giderek kapandığına dair son gözlemlerle paralellik arz etmektedir (Folorunso vd., 2024). Buna karşılık eğitim düzeyinin siber güvenlik farkındalığını anlamlı biçimde etkilediğı (Tablo 29) tespiti, “eğitim-farkındalık” doğrusal ilişkisinin halen güçlü bir değıřken olduğunu göstermektedir. Özellikle yüksek lisans ve doktora düzeyinde anlamlı farkların gözlemlenmesi, uzmanlařmış programların bilgi-beceri aktarımında kritik rol oynadığını desteklemektedir (Mijwil vd., 2022). Aynı şekilde meslek değıřkeninin kurumsal uyum ve strateji algıları üzerindeki belirleyiciliğı (Tablo 30) pratik mesleki deneyimin politika algısına katkı sunduğunu göstermektedir; BT uzmanlarının öne çıkması, Alowaidi vd., (2023) ve Roshanaei vd., (2024) tarafından tanımlanan “alan-içi öğrenme” ile uyum içindedir.

Siber güvenlik eğitimi alan katılımcıların on ayrı ölçekte daha yüksek puan alması (Tablo 31), örgün veya yaygın eğitim programlarının davranışsal çıktılar üzerinde doğrudan etkili olduğunu kanıtlamaktadır. Bu bulgu, Obi vd., (2024) ile Sayyaparaju (2024) tarafından geliştirilen “sürekli eğitim-güvenlik olgunluğu” modelini desteklemektedir. Özellikle yapay zeka destekli kurumsal güvenlik algısında eğitimin belirgin fark yaratması, eğitim içeriklerinin yapay zeka teknolojilerinin kapasite ve sınırlarını içerecek biçimde güncellenmesi gerektiğine işaret etmektedir (Tao vd., 2021; Özdemir, 2024). Ölçeklerin faktör yapılarının yüksek açıklanan varyans oranları ve Cronbach α katsayıları ($\geq 0,911$) ölçeklerin ölçme güvenirliğinin son derece yüksek olduğunu göstermektedir (Tablo 3, 6, 12, 18, 24). Bu sonuç, çalışmada kullanılan maddelerin kuramsal temellerle tutarlı biçimde yapı oluşturduğunu; yapay zeka odaklı savunma, tehdit algısı ve stratejik politika boyutlarının ampirik geçerliliğe sahip olduğunu kanıtlamaktadır. Dolayısıyla araştırma, mevcut ölçeklerin Türkçe bağlamda kullanımı için önemli bir psiko-metrik katkı sunmaktadır; benzer şekilde Efe (2021a) ve Çalışkan (2024) da yerel bağlamda ölçek geçerlik çalışmalarının gerekliliğine vurgu yapmaktadır. Bununla birlikte araştırmanın bazı sınırlılıkları bulunmaktadır. Öncelikle örneklemin Türkiye’de bilgi-teknoloji yoğun bir kitleyi temsil etmesi, bulguların genel nüfusa

genellenebilirliğini kısıtlamaktadır. Nitekim Aldasoro vd., (2024) finansal teknolojiler alanında merkezi bankalar üzerinde yürüttüğü çalışmada sektörler arası bağlamsal farklılıkların sonuçları anlamlı biçimde değiştirebileceğini göstermektedir. Ayrıca çalışmanın kesitsel tasarımı nedensel ilişkileri doğrudan test etmeye olanak tanımamaktadır; Ikemefuna ve Orekha (2024) boylamsal veri ile tehdit algısındaki dinamik değişimlerin daha net izlenebileceğini belirtmektedir. Üçüncü olarak, öz-bildirim temelli ölçeklerin sosyal istenirlik yanlılığı riski taşıdığı bilinmektedir; Bonfanti ve Kohler (2020) bu yanlılığı minimize etmek için davranışsal log verilerinin ölçek verileriyle entegre edilmesini önermektedir. Tüm bunlarla beraber araştırma bulguları, uygulayıcılar için çeşitli çıkarımlar sunmaktadır. Kurumların öncelikle siber güvenlik eğitimlerini modüler yapay zeka simülasyonlarıyla zenginleştirmesi gerekmekte çünkü eğitim alan katılımcılar tehdit algısı ve davranış ölçeklerinde anlamlı biçimde daha yüksek puan almaktadır. İkinci olarak, yapay zeka çözümlerinin yanlış pozitif üretme ve mahremiyet ihlali riskleri, risk-fayda analizleri yapılarak politika belgelerine yansıtılmalıdır; Temara (2024) bu dengeyi sağlamaya dönük çerçeveler önermektedir. Üçüncü olarak, genç çalışan gruplarında kurumsal farkındalık ve uyum puanlarının görece düşük kalması, mentor-temelli programlarla bu açığın kapatılmasını gerekli kılmaktadır; Lysenko vd., (2024) “ters mentorluk” modelini bu bağlamda önererek dijital yerliler ile deneyimli çalışanlar arasında bilgi akışını teşvik etmektedir.

6. SONUÇ VE ÖNERİLER

Sonuç olarak bu araştırma, yapay zeka destekli siber güvenlik uygulamalarına yönelik bireysel farkındalık, kurum-içi politika algısı ve savunma stratejileri arasındaki etkileşimleri kapsamlı biçimde ortaya koymaktadır. Elde edilen bulgulara göre katılımcılar, çevrimiçi veri güvenliği, güçlü parola kullanımı ve yazılım güncellemeleri gibi temel koruyucu davranışları büyük ölçüde benimsediklerini belirtmektedir. Risk algısı ve yapay zeka destekli güvenlik önlemleri ölçeğindeki yüksek puanlar, katılımcıların proaktif tehdit tespiti, maliyet optimizasyonu ve yanıt süresi açısından yapay zekanın önemli avantajlar sunduğuna inandığını ortaya koymaktadır. Bu ikili yaklaşım, yapay zeka çözümlerinin kurumsal politikalarla bütünleşirken şeffaflık, hesap verebilirlik ve veri minimizasyonu ilkeleriyle birlikte ele alınması gereğini vurgulamaktadır.

Faktör analizi sonuçları, incelenen tüm ölçeklerin yüksek yapı geçerliği ve iç tutarlılık sergilediğini doğrulamaktadır. Tek faktörlü ölçeklerde Cronbach's α değerlerinin 0,95'in üzerinde seyretmesi, siber tehdit farkındalığı, yapay zeka temelli savunma sistemlerine güven ve stratejik politika algısı arasında güçlü bir içerik bütünlüğü bulunduğunu göstermektedir. İki faktörlü ölçeklerde ise ilk faktörlerin "yapay zeka odaklı stratejik yönelimler", ikinci faktörlerin "kurumsal uyum ve eğitim" temalarında kümelenmesi, teknolojik entegrasyon ile insan odaklı süreçlerin eş güdümlü ilerlemesinin kritik olduğunu ortaya koymaktadır. Demografik değişkenler incelendiğinde, cinsiyetin siber güvenlik tutum ve davranışları üzerinde anlamlı bir etkisi bulunmamaktadır. Buna karşılık eğitim düzeyi arttıkça siber güvenlik farkındalığı ve yapay zeka tabanlı çözümlere yönelik olumlu tutumların belirgin biçimde yükseldiği görülmektedir. Meslek grupları arasında BT uzmanlarının kurumsal farkındalık ve stratejik politika ölçeklerinde en yüksek puanlara sahip olması, alan-içi deneyimin güvenlik bilinciyle doğrudan ilişkili olduğunu göstermektedir. Ayrıca siber güvenlik eğitimi alan bireylerin hemen tüm ölçeklerde daha yüksek puanlar elde etmesi, eğitim programlarının davranışsal ve bilişsel çıktılar üzerindeki dönüştürücü etkisini doğrulamaktadır. Korelasyon analizi, incelenen tüm ölçek ve alt boyutlar arasında pozitif ve anlamlı ilişkiler bulunduğunu göstermektedir. Özellikle yapay zeka destekli savunma sistemleri alt boyutunun geleneksel-stratejik

tehdit farkındalığı ile ve yapay zeka tabanlı stratejik siber güvenlik politikalarının siber tehditler-savunma ölçeği ile çok kuvvetli ilişkileri, saldırı-savunma döngüsünde yapay zekanın merkezî konuma yerleştiğini kanıtlamaktadır. Bu bütüncül etkileşim ağı, kurumların siber güvenlik olgunluğunu artırmak için teknolojik yatırımları kapsamlı eğitim, risk iletişimi ve güncel politika çerçeveleriyle desteklemesinin zorunlu olduğunu göstermektedir. Bulgular, yapay zeka çözümlerinin sağladığı hız ve öngörü avantajlarının insan faktörü, etik kaygılar ve kurumsal kültürle harmanlanması gerektiğine işaret etmektedir. Gelecekte gerçekleştirilecek boylamsal ve sektörler arası karşılaştırmalı araştırmalar, yapay zeka-temelli savunma stratejilerinin uzun vadeli etkinliğini ve mahremiyet-güvenlik dengesini daha ayrıntılı biçimde değerlendirmektedir.

KAYNAKÇA

- Abdulhussein, M. (2024). The impact of artificial intelligence and machine learning on organizations cybersecurity. *Doctoral dissertation*.
- Aldasoro, I., Doerr, S., Gambacorta, L., Notra, S., Oliviero, T., Whyte, D. (2024). Generative artificial intelligence and cyber security in central banking (BIS Papers No. 145). *Monetary and Economic Department*.
- Aldhamer, M. (2024). The impact of artificial intelligence on the future of cybersecurity. *Multi-Knowledge Electronic Comprehensive Journal for Education and Science Publications (MECSJ)*; 71, 1-10.
- Alowaidi, M., Sharma, S. K., AlEnizi, A., Bhardwaj, S. (2023). Integrating artificial intelligence in cyber security for cyber-physical systems. *Electronic Research Archive*, 31(4); 1876-1896.
- Araya, D., King, M. (2022). The impact of artificial intelligence on military defence and security (CIGI Papers No. 263). *Centre for International Governance Innovation*.
- Arroyo-Figueroa, G. (2023). Artificial intelligence the strategic key of cybersecurity. *International Journal of Combinatorial Optimization Problems and Informatics*, 14(3); 16-23.
- Bhardwaj, M. (2023). AI and cyber security with reference to military/defense. *International Journal of Trend in Research and Development*, 10(4); 3-5.
- Binhammad, M., Alqaydi, S., Othman, A., Abuljadayel, L. H. (2024). The role of AI in cyber security: Safeguarding digital identity. *Journal of Information Security*, 15; 245-278.
- Bonfanti, M. E. (2020). Artificial intelligence and cybersecurity: A promising but uncertain future. *Elcano Royal Institute*, ARI 139/2020.
- Bonfanti, M. E., Kohler, K. (2020). Artificial intelligence for cybersecurity (CSS Analyses in Security Policy No. 265). *ETH Zurich*.
- Bonfanti, M. E. (2022). Artificial intelligence and the offense-defense balance in cyber security. *In CSS Studies in Security and International Relations*.
- Center for Security Studies (CSS), ETH Zurich. (2019). National cybersecurity strategies in comparison – Challenges for Switzerland. *ETH Zurich*.

- Chouraik, C., El-founir, R., Taibi, K. (2024). The impact of AI on cybersecurity: A new paradigm for threat management. *African Journal of Management Engineering and Technology*, 2(2); 92-99.
- Çalışkan, E. M. (2024). The threat of tomorrow: Impacts of artificial intelligence-enhanced cyber-attacks on international relations. *Güvenlik Stratejileri Dergisi*, 12; 109-130.
- Das, R., Sandhane, R. (2021). Artificial intelligence in cyber security. *Journal of Physics: Conference Series*, 1964; 042072.
- Efe, A. (2021a). Yapay zeka odaklı siber risk ve güvenlik yönetimi. *Uluslararası Yönetim Bilişim Sistemleri ve Bilgisayar Bilimleri Dergisi*, 5(2); 144-165.
- Efe, A. (2021b). Yapay zeka ve Endüstri 4.0 ilişkisinin siber güvenlik perspektifinden analizi. *Aydın Adnan Menderes Üniversitesi Sosyal Bilimler Enstitüsü Dergisi*, 8(1); 123-143.
- Eltayeb, O. (2024). Cyber defense using cyber threat intelligence to anticipate and avoid future cyber attacks. *Pakistan Journal of Life and Social Sciences*, 22(2); 1883-1904.
- Fayet, H. (2023). French thinking on AI integration and interaction with nuclear command and control, force structure, and decision-making. *European Leadership Network*.
- Folorunso, A., Adewumi, T., Adewa, A., Okonkwo, R., Olawumi, T. N. (2024). Impact of AI on cybersecurity and security compliance. *Global Journal of Engineering and Technology Advances*, 21(01); 167-184.
- Gilbert, C., Gilbert, M. A. (2024). The impact of AI on cybersecurity defense mechanisms: Future trends and challenges. *Global Scientific Journals*, 12(9); 427.
- Govea, J., Gaibor-Naranjo, W., Villegas-Ch, W. (2024). Transforming cybersecurity into critical energy infrastructure: A study on the effectiveness of artificial intelligence. *Systems*, 12(5); 165.
- Ikemefuna, C. D., Orekha, P. O. (2024). Predictive cyber defense: Harnessing AI and ML for anticipatory threat mitigation. *International Journal of Research Publication and Reviews*, 5(9); 3122-3132.

- Jada, I., Mayayiise, T. O. (2024). The impact of artificial intelligence on organisational cyber security: An outcome of a systematic literature review. *Data and Information Management*, 8(2), 100063.
- Jeong, J. (2004). *Analysis of The Factors And The Roles of Hrd in Organizational Learning Styles As Identified By Key Informants At Selected Corporations in The Republic of Korea*. Yayınlanmamış doktora tezi. Amerika: Texas A&M University. Major Subject: Educational Human Resource Development.
- Kale, A. (2024). AI-driven cybersecurity threats and organizational consequences. *Doctoral dissertation*.
- Lysenko, S., Bobro, N., Korsunova, K., Vasylychshyn, O., Tatarchenko, Y. (2024). The role of artificial intelligence in cybersecurity: Automation of protection and detection of threats. *Economic Affairs*, 69(Special Issue); 43-51.
- Maathuis, C., Cools, K. (2025). The role of AI in military cyber security: Data insights and evaluation methods. *Procedia Computer Science*, 254; 191-200.
- Mijwil, M. M., Sadıkoğlu, E., Cengiz, E., Candan, H. (2022). Siber güvenlikte yapay zekanın rolü ve önemi: Bir derleme. *Veri Bilimi Dergisi*, 5(2); 97-105.
- Naik, B., Mehta, A., Yagnik, H., et al. (2022). The impacts of artificial intelligence techniques in augmentation of cybersecurity: A comprehensive review. *Complex Intelligent Systems*, 8; 1763–1780.
- Nami, J. P. S., Azevedo, G. A. de, Alencar, D. T. F., Kini, K. A. A. (2024). The use of artificial intelligence as a national defense strategy. *Journal of Engineering Research*, 4(6).
- Nunnally, J. C. (1967). *Psychometric Theory*, McGraw-Hill, Inc., 1. Baskı, New York.
- Obi, O. C., Akagha, O. V., Dawodu, S. O., Anyanwu, A., Onwusinkwe, S., Ahmad, I. A. I. (2024). Comprehensive review on cybersecurity: Modern threats and advanced defense strategies. *Computer Science and IT Research Journal*, 5(2); 293-310.
- Öz, O. (2023). Soğuk savaştan akıllı savaşa geçiş sürecinde yapay zeka teknolojilerinin rolü: Çin ve ABD örnekleri. *Yüksek lisans tezi*.
- Özdemir, B. (2024). Siber tehdit istihbaratında yapay zeka ve makine öğrenmesi. *Savunma ve Güvenlik Araştırmaları Dergisi*, 1(1); 75-96.

- Özkurt, C. (2020). Savunma sanayinde dijitalleşmenin kurumsal niteliklere etkisinin yapay zeka yöntemleri ile öngörülmesi: Sakarya ili örneği. *Doktora Tezi*.
- Palani, K. V., Kethar, J., Prasad, S., Torremocha, V. (2024). Impact of AI and generative AI in transforming cybersecurity. *Journal of Student Research*, 13(2).
- Radanliev, P. (2024). Cyber diplomacy: Defining the opportunities for cybersecurity and risks from artificial intelligence, IoT, blockchains, and quantum computing. *Journal of Cyber Security Technology*, 9(1); 28-78.
- Roshanaei, M., Khan, M. R., Sylvester, N. N. (2024). Enhancing cybersecurity through AI and ML: Strategies, challenges, and future directions. *Journal of Information Security*, 15; 320-339.
- Salem, A. H., Azzam, S. M., Emam, O. E., et al. (2024). Advancing cybersecurity: A comprehensive review of AI-driven detection techniques. *Journal of Big Data*, 11; 105.
- Sanclemente, G. L. (2023). Digital tools: Safeguarding national security, cybersecurity, and AI bias. *CEBRI Journal*, 2(7); 1-10.
- Sayyaparaju, K. K. (2024). Integrating AI in cyber defense: A comprehensive approach to autonomous threat detection and mitigation. *Res Militaris*, 14(3); 47.
- Sulaiman, M., Waseem, M., Ali, A. N., Laouini, G., Alshammari, F. S. (2024). Defense strategies for epidemic cyber security threats: Modeling and analysis by using a machine learning approach. *IEEE Access*, 99; 1-1.
- Sultan, M. S., Sultan, M. S. (2024). Leveraging artificial intelligence for enhanced cybersecurity: A systematic approach. *International Journal of Science and Research*, 13(8); 92-100.
- Tao, F., Akhtar, M. S., Jiayuan, Z. (2021). The future of artificial intelligence in cybersecurity: A comprehensive survey. *EAI Endorsed Transactions on Creative Technologies*, 7(7).
- Temara, S. (2024). Harnessing the power of artificial intelligence to enhance next-generation cybersecurity. *World Journal of Advanced Research and Reviews*, 23(02); 797-811.
- Ukhanova, E. (2022). Cybersecurity and cyber defence strategies of Japan. *SHS Web of Conferences*, 134; 00159.

- Zeng, Y. (2022). AI empowers security threats and strategies for cyber attacks. *In 7th International Conference on Intelligent, Interactive Systems and Applications, Procedia Computer Science*, 208; 170-175.
- Zhang, Z., Ning, H., Shi, F., Farhla, F., Xu, Y., Xu, J., Zhang, F., Choo, K.-R. R. (2021). Artificial intelligence in cyber security: Research advances, challenges, and opportunities. *Artificial Intelligence Review*.

