ACADEMIC SOCIAL RESOURCES Journal
Open Access Refereed E-Journal & Refereed & Indexed

RESEARCH ARTICLE
Marketing

Özel Güvenlik Risk Analizinde Yapay Zekâ Kullanımı

The Use of Artificial Intelligence in Private Security Risk Analysis

ÖZET

Bu çalışma, özel güvenlik hizmetleri risk analizinde yapay zekâ (YZ) teknolojilerinin entegrasyonunu derinlemesine incelemektedir. Makine öğrenmesi, derin öğrenme, doğal dil işleme ve görüntü işleme gibi yöntemler kullanılarak, tehdit algılama, erişim kontrolü, tahmine dayalı güvenlik ve siber güvenlik uygulamaları analiz edilmiştir. Vaka örnekleriyle desteklenen bu YZ tabanlı yaklaşımlar, geleneksel analiz yöntemlerine kıyasla daha hızlı, öngörülebilir, proaktif ve veri odaklı sonuçlar sunarak insan hatası potansiyelini azaltmakta ve operasyonel verimliliği artırmaktadır. Makale ayrıca, YZ kullanımının getirdiği etik ve yasal zorlukları (veri gizliliği, algoritmik yanlılık, şeffaflık ve sorumluluk) da ele alarak gelecekteki araştırmalar ve politika önerileri için bir zemin hazırlamaktadır.

Anahtar Kelimeler: Yapay Zekâ, Risk Analizi, Özel Güvenlik

ABSTRACT

This study deeply explores the integration of artificial intelligence (AI) technologies into risk analysis within private security services. Methods such as machine learning, deep learning, natural language processing, and image processing are examined through applications in threat detection, access control, predictive security, and cybersecurity. Supported by case studies, these AI-driven approaches offer faster, more predictable, proactive, and data-driven insights compared to traditional analysis techniques, reducing the potential for human error and enhancing operational efficiency. The article also addresses the ethical and legal challenges (data privacy, algorithmic bias, transparency, and accountability) posed by AI adoption, laying the groundwork for future research and policy recommendations.

Keywords: Artificial Intelligence, Risk Analysis, Private Security

Orkun Konak [1]
C. Gazi Uçkun [2]
Aykut Tosun [3]

How to Cite This Article
Konak, O., Uçkun, C. G. & Tosun, A. (2025). "Özel Güvenlik Risk Analizinde Yapay Zekâ Kullanımı", International Academic Social Resources Journal, (e-ISSN: 2636-7637), Vol:10, Issue:6; pp:520-524. DOI: https://doi.org/10.5281/zenodo.18076516

Arrival: 06 October 2025
Published: 28 December 2025

GİRİŞ

Özel güvenlik sektörü, küresel güvenlik tehditlerinin ve teknolojik gelişmelerin etkisiyle son yıllarda büyük bir dönüşüm geçirmektedir. Kamu güvenliğini tamamlayıcı nitelikteki bu hizmet alanı, kritik altyapıların, özel mülklerin ve toplu yaşam alanlarının korunmasında hayati bir rol üstlenmektedir. Güvenlik ortamının giderek daha dinamik ve karmaşık hale gelmesi (terör olayları, organize suçlar, siber saldırılar gibi), geleneksel risk analizi yaklaşımlarının yetersiz kalmasına neden olmaktadır. Risk analizi, potansiyel tehditlerin tanımlanması, değerlendirilmesi ve önceliklendirilmesi sürecidir (ISO, 2018). Ancak geleneksel yöntemler, büyük veri hacimlerini işleme, hızlı reaksiyon gösterme ve gizli kalmış tehditleri tespit etme konusunda sınırlılıklar barındırmaktadır.

Bu noktada yapay zekâ (YZ) teknolojileri, özel güvenlikte risk analizine yeni bir boyut kazandırmakta ve sektörde bir paradigma değişimi yaratmaktadır. Makine öğrenmesi (ML), derin öğrenme (DL), doğal dil işleme (NLP) ve görüntü işleme gibi YZ dalları, güvenlik tehditlerinin daha hızlı, doğru, öngörülebilir ve proaktif biçimde analiz edilmesini mümkün kılmaktadır (LeCun, Bengio & Hinton, 2015; Coşar, 2023; CoESS, 2024). Bu çalışma, YZ'nin özel güvenlik risk analizine entegrasyonunu, temel teknolojilerini, pratik uygulamalarını ve beraberinde getirdiği etik ve yasal zorlukları kapsamlı bir şekilde incelemeyi amaçlamaktadır.

ÖZEL GÜVENLİKTE RİSK ANALİZİ

KAVRAMSAL ÇERÇEVE VE GELENEKSEL YAKLAŞIMLAR

Risk yönetimi, kurumların hedeflerine ulaşmasını etkileyebilecek belirsizlikleri ele alan, koordineli faaliyetler bütünüdür. ISO 31000 standardı, risk yönetiminin temel ilkelerini belirleyerek bu sürecin yapılandırılmasına katkı sağlar (ISO, 2018). Özel güvenlikte risk analizi, potansiyel güvenlik açıklarını, tehditleri ve bunların olası etkilerini belirlemeyi içerir.

Geleneksel risk analizi yöntemleri genellikle kalitatif (niteliksel) ve kantitatif (niceliksel) yaklaşımları birleştirir:

SWOT Analizi (Strengths, Weaknesses, Opportunities, Threats): Kuruluşun iç güçlü ve zayıf yönleri ile dış fırsat ve tehditlerini değerlendirerek stratejik riskleri belirler.

PEST Analizi (Political, Economic, Social, Technological): Makro çevresel faktörlerin güvenlik riskleri üzerindeki etkilerini inceler (ASIS International, 2010).

[1] Öğr.Gör., Kocaeli Üniversitesi, Hereke Ömer İsmet Uzunyol MYO Mülkiyet Koruma ve Güvenlik Bölümü, Kocaeli, Türkiye
[2] Prof. Dr., Kocaeli Üniversitesi, Hereke Ömer İsmet Uzunyol MYO Mülkiyet Koruma ve Güvenlik Bölümü, Kocaeli, Türkiye
[3] Öğr.Gör., Kocaeli Üniversitesi, Hereke Ömer İsmet Uzunyol MYO Mülkiyet Koruma ve Güvenlik Bölümü, Kocaeli, Türkiye

Risk Matrisleri ve Puanlama: Tehditlerin gerçekleşme olasılığı ile potansiyel etkilerinin çarpılmasıyla risk seviyeleri belirlenir ve önceliklendirilir.

Türkiye'de AISecLab gibi yerli araştırma toplulukları, yapay zekâ destekli risk analiz modelleri geliştirerek bu alandaki akademik ve pratik boşluğu doldurmaktadır (AISecLab, 2024). Sigorta sektörü gibi alanlarda da benzer analizler YZ ile desteklenmeye başlanmıştır (Dünya Gazetesi, 2025).

ZORLUKLAR VE SINIRLILIKLAR

Geleneksel risk analiz yöntemleri belirli bir fayda sağlasa da, hızla değişen ve karmaşıklaşan tehdit ortamında yetersiz kalabilmektedir. Bu sınırlılıklar şunları içerir:

Veri Eksikliği ve Kalitesizliği: Geleneksel analizler genellikle sınırlı veya yapılandırılmamış verilere dayanır, bu da eksik veya yanlış değerlendirmelere yol açabilir.

İnsan Hatası ve Yanlılık (Bias): Analistlerin deneyim ve öznelliği, risk algısında ve değerlendirmesinde tutarsızlıklara veya yanlılıklara neden olabilir. İnsan faktörü, risk kültürünün oluşumu ve uygulanmasında da kritik rol oynar ancak hata payı potansiyeli taşır.

Dinamik Tehdit Ortamı: Tehditler (özellikle siber tehditler, fidye yazılımları, gelişmiş kalıcı tehditler gibi) sürekli evrim geçirdiği için geleneksel yöntemlerle güncel kalmak zordur (ATP Tech, 2023).

Reaktif Yaklaşım: Geleneksel analizler genellikle olaylar meydana geldikten sonra tepki vermeye odaklanır, oysa modern güvenlik proaktif önlemler gerektirir.

Büyük Veri Hacmi: Özellikle video gözetimi, sensör verileri ve olay raporları gibi kaynaklardan gelen devasa veri hacimlerini manuel olarak analiz etmek imkansızdır.

Bu zorluklar, özel güvenlik sektöründe daha hızlı, doğru ve öngörücü analizler yapabilen YZ tabanlı sistemlere olan ihtiyacı artırmıştır.

YAPAY ZEKÂ TEKNOLOJİLERİ

Yapay zekâ, özel güvenlikte risk analizini dönüştüren çeşitli alt alanları ve teknolojileri kapsar:

MAKİNE ÖĞRENMESİ (ML)

Makine öğrenmesi, algoritmaların açıkça programlanmadan verilerden öğrenmesini sağlayan bir YZ dalıdır (Bishop, 2006). Özel güvenlikte ML, olay sınıflandırma, tehdit önceliklendirme, anomali tespiti ve dolandırıcılık tespiti gibi alanlarda kullanılır. Denetimli öğrenme (geçmiş olay verilerinden öğrenme) ve denetimsiz öğrenme (gizli kalıpları keşfetme) algoritmaları (örn. Destek Vektör Makineleri, Karar Ağaçları, Kümeleme) potansiyel güvenlik risklerini otomatik olarak belirleyebilir ve sınıflandırabilir (Coşar, 2023). Örneğin, belirli bir bölgedeki suç oranları veya önceki güvenlik ihlalleri gibi yapılandırılmış veriler üzerinden gelecekteki olayları tahmin etmek için kullanılabilir.

DERİN ÖĞRENME (DL)

Derin öğrenme, insan beyninin çalışma prensibinden esinlenerek çok katmanlı yapay sinir ağları kullanan bir ML alt dalıdır (LeCun, Bengio & Hinton, 2015). Özellikle yapılandırılmamış verilerin (görüntü, ses, video) analizinde üstün başarı gösterir. Evrişimsel Sinir Ağları (CNN), video gözetim sistemlerinde yüz tanıma, nesne tespiti ve şüpheli davranış analizi için kullanılırken, Tekrarlayan Sinir Ağları (RNN) ses kayıtlarındaki anormallikleri veya dil kalıplarını tespit edebilir. ASELSAN'ın biyometrik sistemleri, derin öğrenme ile yüz tanıma ve davranış analizi yaparak güvenlik ihlallerini proaktif olarak önleyebilmektedir (ASELSAN, 2024).

DOĞAL DİL İŞLEME (NLP)

Doğal Dil İşleme, bilgisayarların insan dilini anlamasını, yorumlamasını ve üretmesini sağlayan bir YZ teknolojisidir (Jurafsky & Martin, 2023). Özel güvenlikte NLP, güvenlik raporları, olay kayıtları, sosyal medya verileri ve haber makaleleri gibi metin tabanlı verileri analiz ederek **güvenlik içgörüleri** üretir. Uygulama alanları şunlardır:

Metin Madenciliği: Büyük metin arşivlerinden kritik bilgileri ve tehdit göstergelerini çıkarmak.

Duygu Analizi: Sosyal medya paylaşımlarındaki potansiyel tehdit veya rahatsız edici içerikleri tespit etmek.

Anomali Tespiti: Olağan dışı dil kalıplarını veya anahtar kelimeleri tespit ederek potansiyel güvenlik olaylarını işaretlemek (IBM Security, 2023).

GÖRÜNTÜ İŞLEME

Görüntü işleme, dijital görüntülerin analiz edilmesi ve manipüle edilmesiyle ilgili bir YZ alanıdır (Gonzalez & Woods, 2018). Özel güvenlikte, kameralar aracılığıyla elde edilen video akışlarını gerçek zamanlı olarak analiz etmek için kullanılır. Başlıca uygulamaları:

Yüz Tanıma ve Kimlik Doğrulama: Erişim kontrol noktalarında veya kalabalık alanlarda kişilerin kimliklerini doğrulamak.

Plaka Okuma (LPR): Araç giriş-çıkışlarını yönetmek ve şüpheli araçları tespit etmek.

Nesne Tespiti ve Takibi: Terk edilmiş nesneleri, şüpheli paketleri veya belirli nesnelerin (örn. silahlar) varlığını tespit etmek.

Davranış Analizi: Kişilerin olağan dışı veya şüpheli davranışlarını (koşuşturma, kavga, düşme) otomatik olarak algılamak (www.hikvision.com erişim tarihi: 05.09.2025).

YAPAY ZEKÂ İLE RİSK ANALİZİ UYGULAMALARI

Yapay zekâ teknolojileri, özel güvenlikte risk analizini bir dizi yenilikçi uygulama aracılığıyla **proaktif ve verimli** hale getirmektedir:

TEHDİT ALGILAMA VE ANOMALİ TESPİTİ

YZ destekli sistemler, büyük veri setlerindeki kalıpları ve anomalileri insan gözünün fark edemeyeceği hız ve doğrulukla tespit edebilir. Görüntü işleme ve derin öğrenme algoritmaları, gözetim kameralarındaki video akışlarını analiz ederek şüpheli davranışları (örn. belirli bir alanda uzun süre duran kişiler, kısıtlı bölgelere yaklaşanlar) veya nesneleri (terk edilmiş çanta) gerçek zamanlı olarak algılayabilir. Tokyo metrosunda NEC Corporation tarafından uygulanan AI destekli kameralar, olağandışı davranışları (koşma, merdivenlerde düşme, uzun süre bekleme) tespit ederek güvenlik personelini anında uyarmış ve müdahale süresini önemli ölçüde azaltmıştır. Bu sayede hem güvenlik ihlalleri hem de kaza potansiyeli proaktif olarak yönetilebilmektedir (NEC Corporation, 2022).

ERİŞİM KONTROLÜ VE KİMLİK YÖNETİMİ

Geleneksel erişim kontrol sistemleri genellikle kartlar veya PIN kodlarına dayanırken, YZ destekli sistemler biyometrik verileri (yüz, parmak izi, iris) kullanarak daha güvenli ve verimli çözümler sunar. Derin öğrenme tabanlı yüz tanıma sistemleri, yüksek doğrulukla kimlik doğrulaması yaparak yetkisiz girişleri engeller. ASELSAN'ın geliştirdiği biyometrik sistemler, yapay zekâ destekli yüz tanıma teknolojisiyle yalnızca kimlik doğrulamakla kalmayıp, tanınmayan veya şüpheli kişilerin varlığını da anında tespit ederek güvenlik ihlallerini önlemektedir (ASELSAN, 2024). Bu sistemler, sahtekarlığa (deepfake görüntüleri gibi) karşı da giderek daha dirençli hale gelmektedir.

TAHMİNE DAYALI GÜVENLİK VE KAYNAK OPTİMİZASYONU

Yapay zekâ, geçmiş olay verilerini, suç istatistiklerini, demografik bilgileri, hava durumu verilerini ve hatta sosyal medya eğilimlerini analiz ederek gelecekteki potansiyel güvenlik risklerini tahmin etme yeteneğine sahiptir. Bu "tahmine dayalı polislik" veya "tahmine dayalı güvenlik" yaklaşımları, güvenlik personelinin devriye rotalarını ve kaynak dağılımını optimize etmelerine olanak tanır. IBM Watson, geçmiş olayları ve tehdit istihbaratını analiz ederek güvenlik ekipleri için daha etkin devriye planlaması ve kaynak tahsisi konusunda öneriler sunmuştur (IBM Security, 2023). Bu sayede, riskli bölgelere daha fazla odaklanılarak güvenlik proaktif hale getirilir ve operasyonel verimlilik artırılır. Brantingham, Valasik & Mohler (2018), bu tür sistemlerin potansiyel faydalarını vurgulamakla birlikte, yanlılık risklerine karşı dikkatli olunması gerektiğini belirtmiştir. CoESS, bu tür sistemlerin etik ve yasal uyumunu sağlamanın önemini özellikle vurgulamaktadır (CoESS, 2024).

SİBER GÜVENLİK ENTEGRASYONU

Özel güvenlik artık sadece fiziksel tehditleri değil, siber tehditleri de kapsamaktadır. YZ, siber güvenlikte hem bir savunma aracı hem de bir saldırı aracı olarak çift yönlü bir rol oynar.

Savunma: YZ destekli sistemler, ağ trafiğindeki anomalileri, kötü amaçlı yazılımları (fidye yazılımları, gelişmiş kalıcı tehditler) ve kimlik avı saldırılarını gerçek zamanlı olarak tespit edebilir. Büyük veri analizi ve makine öğrenmesi ile siber saldırıların kalıpları öğrenilir ve henüz bilinmeyen tehditler dahi öngörülebilir. Palantir Technologies gibi firmalar, entegre tehdit algılama platformlarıyla siber ve fiziksel güvenlik verilerini birleştirerek kapsamlı bir risk görünümü sunmaktadır (Palantir Technologies, 2022).

Saldırı: Ne yazık ki, YZ aynı zamanda yapay zekâ destekli siber saldırılar (otomatik fidye yazılımları, akıllı siber casusluk) ve deepfake dolandırıcılıkları gibi yeni nesil tehditlerin de ortaya çıkmasına neden olmuştur (WEF, 2024). Bu durum, özel güvenlikte YZ kullanımıyla birlikte siber güvenlik uzmanlığının da artan önemini gözler önüne sermektedir. UNIDIR (Puscas, 2023) ve Private AI (Gardhouse, 2025) gibi kuruluşlar, YZ'nin uluslararası güvenlik ve veri gizliliği üzerindeki etkilerini analiz ederek bu alandaki risklerin yönetilmesine katkıda bulunmaktadır.

ETİK VE YASAL ÇERÇEVE

Yapay zekâ teknolojilerinin özel güvenlikte yaygınlaşması, beraberinde önemli etik ve yasal tartışmaları getirmektedir. Bu konuların doğru yönetilmesi, YZ sistemlerinin kabul edilebilirliği ve etkinliği açısından kritik öneme sahiptir:

Veri Gizliliği ve Mahremiyet: YZ sistemleri, bireyler hakkında (yüz tanıma, davranış analizi yoluyla) büyük miktarda hassas veri toplar. Bu verilerin depolanması, işlenmesi ve korunması, KVKK (Kişisel Verilerin Korunması Kanunu) ve GDPR (Genel Veri Koruma Tüzüğü) gibi yasal düzenlemelere tam uyum gerektirir. Özel hayatın gizliliğinin ihlal edilmemesi temel bir etik prensiptir.

Algoritmik Yanlılık (Bias): YZ modelleri eğitildikleri veri setlerindeki yanlılıkları öğrenebilir ve bu durum, belirli demografik gruplara karşı ayrımcı sonuçlar doğurabilir (Brantingham, Valasik & Mohler, 2018). Örneğin, bazı yüz tanıma sistemleri belirli etnik gruplarda daha düşük doğruluk oranları gösterebilir. Bu yanlılıkların farkında olmak ve sistemleri adil veri setleriyle eğiterek bu riski minimize etmek büyük önem taşır.

Şeffaflık ve Açıklanabilirlik: YZ modellerinin "kara kutu" doğası, karar verme süreçlerinin insanlar tarafından anlaşılmasını zorlaştırabilir. Güvenlik kararlarının neden alındığının şeffaf bir şekilde açıklanabilmesi, hem hukuki sorumluluk hem de toplumsal güven açısından önemlidir.

Otonom Karar Alma ve Sorumluluk: YZ sistemlerinin giderek daha otonom hale gelmesiyle birlikte, bir güvenlik ihlali veya hatası durumunda hukuki sorumluluğun kime ait olacağı (YZ sistemi sağlayıcısı, kullanıcı kuruluş, operatör) gibi sorular ortaya çıkmaktadır. Bu konuda net yasal çerçevelerin oluşturulması gerekmektedir.

Gözetim Toplumu Endişeleri: Yaygın YZ destekli gözetim sistemleri, "gözetim toplumu" algısını güçlendirebilir ve bireylerin özgürlüklerini kısıtladığı yönünde eleştirilere yol açabilir. Teknolojinin faydaları ile toplumsal kabul arasında bir denge kurulması esastır.

CoESS (2024), "Özel Güvenlikte Yapay Zekânın Etik ve Sorumlu Kullanımına İlişkin Şart" belgesiyle bu etik zorluklara dikkat çekmekte ve sektör için rehberlik sunmaktadır.

SONUÇ VE ÖNERİLER

Yapay zekâ teknolojileri, özel güvenlik sektöründe risk analizini geleneksel yöntemlerin sınırlılıklarını aşarak dönüştürme potansiyeli taşımaktadır. Makine öğrenmesi, derin öğrenme, doğal dil işleme ve görüntü işleme gibi YZ dalları, tehdit algılama, erişim kontrolü, tahmine dayalı güvenlik ve siber güvenlik alanlarında önemli gelişmeler sağlayarak operasyonel verimliliği artırmakta, insan hatası potansiyelini azaltmakta ve güvenlik yaklaşımlarını reaktiften proaktif hale getirmektedir. Gerçek zamanlı analiz, büyük veri işleme kapasitesi ve öngörücü yetenekler, özel güvenlik hizmetlerinin daha stratejik ve etkili olmasını sağlamaktadır.

Ancak, YZ'nin bu alandaki entegrasyonu, veri gizliliği, algoritmik yanlılık, şeffaflık ve sorumluluk gibi önemli etik ve yasal zorlukları da beraberinde getirmektedir. Bu zorlukların üstesinden gelmek ve YZ'nin faydalarından tam olarak yararlanabilmek için aşağıdaki öneriler sunulmaktadır:

Yasal ve Etik Çerçevelerin Geliştirilmesi: YZ uygulamalarına yönelik açık, kapsamlı ve uluslararası düzeyde uyumlu yasal düzenlemelerin ve etik yönergelerin oluşturulması zorunludur. Bu, hem şirketler hem de bireyler için şeffaflık ve güven sağlar.

Veri Kalitesi ve Çeşitliliği: YZ modellerinin doğru ve tarafsız sonuçlar üretebilmesi için yüksek kaliteli, kapsamlı ve çeşitlendirilmiş veri setleriyle eğitilmesi kritik öneme sahiptir. Veri toplama, depolama ve etiketleme süreçlerine yatırım yapılmalıdır.

İnsan-YZ İş Birliği: YZ, insan güvenlik personelinin yerini almak yerine, onların yeteneklerini artıran bir araç olarak konumlandırılmalıdır. İnsanların kritik karar alma, etik değerlendirme ve karmaşık durum yönetimi becerileri, YZ'nin analitik gücüyle birleştirilmelidir.

Eğitim ve Kapasite Geliştirme: Özel güvenlik personelinin YZ teknolojileri konusunda eğitilmesi, bu sistemleri etkin bir şekilde kullanabilmeleri ve potansiyel sorunları anlayabilmeleri için elzemdir. Veri bilimciler ve YZ uzmanları ile güvenlik profesyonelleri arasındaki iş birliği teşvik edilmelidir.

Araştırma ve Geliştirme (Ar-Ge): YZ'nin özel güvenlikteki yeni uygulama alanları, daha güvenli ve dirençli sistemlerin geliştirilmesi ve etik zorlukların çözümü için sürekli Ar-Ge faaliyetlerine yatırım yapılmalıdır. Özellikle deepfake tespiti ve YZ destekli siber saldırılara karşı savunma mekanizmaları üzerinde yoğunlaşılmalıdır.

Yapay zekâ, özel güvenlik sektörünün geleceğini şekillendirecek en önemli teknolojilerden biridir. Bu teknolojinin sunduğu fırsatları en üst düzeye çıkarırken, potansiyel risklerini yönetmek için proaktif ve iş birliğine dayalı

yaklaşımlar benimsenmelidir. Bu sayede, daha güvenli ve akıllı toplumlar inşa etme yolunda önemli adımlar atılabilir.

KAYNAKÇA

AISecLab. (2024). *Yapay Zekâ ile Siber Güvenlik*. https://aiseclab.org

ASELSAN. (2024). *Savunma Teknolojileri Raporu*.

ASIS International. (2010). *General Security Risk Assessment Guidelines*.

ATP Tech. (2023). *Yapay Zekâ ile Siber Güvenlikte Öngörücü Analizlerin Önemi*. https://www.atptech.com

Bishop, C. M. (2006). *Pattern Recognition and Machine Learning*. Springer.

Brantingham, P. J., Valasik, M., & Mohler, G. (2018). Does Predictive Policing Lead to Biased Arrests?. *Journal of Criminal Justice*, *59*, 100–107.

CoESS. (2024). *Charter on Ethical and Responsible Use of AI in Private Security*. https://coess.org

Coşar, M. (2024). Kurumsal Bilgi Güvenliği Yönetiminde Yapay Zekâ Destekli Risk Analizi. Denetişim, (31), 144-155.

Dünya Gazetesi. (2025). *Risk Analizinde Yapay Zekâlı Sistemler Devreye Giriyor*. https://dunya.com

Gardhouse, K. (2025). *AI Safety Report 2025*. Private AI.

Gonzalez, R. C., & Woods, R. E. (2018). *Digital Image Processing*. Pearson.

IBM Security. (2023). *Predictive Threat Intelligence White Paper*.

ISO. (2018). *ISO 31000: Risk Management – Principles and Guidelines*.

Jurafsky, D., & Martin, J. H. (2023). *Speech and Language Processing*. Pearson.

LeCun, Y., Bengio, Y., & Hinton, G. (2015). Deep learning. *Nature*, *521*(7553), 436–444.

NEC Corporation. (2022). *Smart Surveillance Solutions*.

Palantir Technologies. (2022). *Integrated Threat Detection Platform Overview*.

Puscas, I. (2023). *AI and International Security*. UNIDIR.

World Economic Forum. (2024). *Global Risk Report: AI and Cybersecurity*. https://weforum.org

İnternet adresleri

https://hikvision.com. Erişim tarihi: 05.09.2025