Güvenlik Bilimleri Dergisi / Journal of Security Sciences

Jandarma ve Sahil Güvenlik Akademisi
Güvenlik Bilimleri Enstitüsü
Güvenlik Bilimleri Dergisi, Kolluk Uygulamaları ve Güvenlik Teknolojileri Özel Sayısı, 1-21
doi: 10.28956/gbd.1688011

Gendarmerie and Coast Guard Academy
Institute of Security Sciences
Journal of Security Sciences, Thematic Issue on Policing Practices and Security Technologies 1-21
doi: 10.28956/gbd.1688011

Makale Türü ve Başlığı / Article Type and Title

Araştırma / Research Article

Yapay Zekâ Destekli Güvenlik Sistemlerinde Elektronik Bileşenlerin Rolü: IoT ve Gömülü Sistem Entegrasyonu

The Role of Electronic Components in Artificial Intelligence-Enabled Security Systems: IoT and Embedded System Integration

Yazar(lar) / Writer(s)

Kazım DURAKLAR, Dr. Öğr. Görevlisi, Jandarma ve Sahil Güvenlik Akademisi, Türkiye, kazim.duraklar@jsga.edu.tr, ORCID: 0000-0003-0815-2976

Bilgilendirme / Acknowledgement:

-Yazarlar aşağıdaki bilgilendirmeleri yapmaktadırlar:
-Makalemizde etik kurulu izni ve/veya yasal/özel izin alınmasını gerektiren bir durum yoktur.
-Bu makalede araştırma ve yayın etiğine uyulmuştur.
Bu makale Turnitin tarafından kontrol edilmiştir.
This article was checked by Turnitin.

Makale Geliş Tarihi / First Received : 30.06.2025
Makale Kabul Tarihi / Accepted : 09.10.2025

Atıf Bilgisi / Citation:

Duraklar K., (2025). Yapay Zekâ Destekli Güvenlik Sistemlerinde Elektronik Bileşenlerin Rolü: IoT ve Gömülü Sistem Entegrasyonu, *Güvenlik Bilimleri Dergisi, Kolluk Uygulamaları ve Güvenlik Teknolojileri Özel Sayısı, ss 1-21. doi: 10.28956/gbd.1688011*

This work is licensed under Creative Commons Attribution-NonCommercial 4.0 International License.

YAPAY ZEKÂ DESTEKLİ GÜVENLİK SİSTEMLERİNDE ELEKTRONİK BİLEŞENLERİN ROLÜ: IOT VE GÖMÜLÜ SİSTEM ENTEGRASYONU

Öz

Bu çalışma, yapay zekâ (YZ) destekli güvenlik sistemlerinin elektronik ve gömülü teknolojilerle entegrasyonu sonucu güvenlik anlayışında meydana gelen dönüşümü incelemektedir. Gömülü sistemler, sensör ağları, haberleşme sistemleri, düşük güçlü YZ çipleri gibi ileri düzey elektronik teknolojiler; güvenlik uygulamalarında gerçek zamanlı veri işleme, karar destek ve otomasyon gibi kritik işlevleri mümkün kılmaktadır. Literatür taraması ve karşılaştırmalı analiz yöntemiyle yürütülen çalışmada; yüz tanıma, biyometrik doğrulama, siber güvenlik, akıllı şehirler, otonom araçlar ve sınır güvenliği gibi çeşitli alanlarda YZ'nin güvenlik güçlerine sağladığı operasyonel avantajlar değerlendirilmiştir. Ayrıca, YZ tabanlı çözümlerin etkinliğini artıran bulut ve kenar bilişim uygulamaları, IoT cihaz entegrasyonu ile elektronik altyapı gelişmeleri de kapsamlı şekilde ele alınmıştır. Türkiye'nin ulusal YZ stratejisi doğrultusunda bu teknolojilere yaptığı yatırımlar, potansiyel kazanımlarla birlikte etik ve hukuki riskler ekseninde tartışılmıştır. Elde edilen bulgular, YZ ve elektronik mühendisliği alanlarının güvenlik teknolojilerinde stratejik bir bileşim oluşturduğunu göstermekte; bu bileşim daha çevik, proaktif ve akıllı güvenlik sistemlerinin inşasında temel bir rol üstlenmektedir.

Anahtar Kelimeler: *Gömülü Sistemler, Elektronik, Yapay Zekâ, Güvenlik Sistemleri, IoT, Siber Güvenlik.*

THE ROLE OF ELECTRONIC COMPONENTS IN ARTIFICIAL INTELLIGENCE-ENABLED SECURITY SYSTEMS: IOT AND EMBEDDED SYSTEM INTEGRATION

Abstract

This study explores how artificial intelligence (AI)-powered security systems are transforming the security paradigm through the integration of electronic technologies and embedded systems. Advanced electronic components such as embedded systems, sensor networks, communication modules, and low-power AI chips enable critical functions in security applications, including real-time data processing, decision support, and automation. Employing a literature review and comparative analysis methodology, the study evaluates the operational advantages AI provides to security forces in diverse domains such as facial recognition, biometric authentication, cybersecurity, smart cities, autonomous vehicles, and border security. In addition, developments in cloud and edge computing, IoT device integration, and electronic infrastructure that enhance the effectiveness of AI-based solutions are discussed in depth. Within the scope of the national AI strategy of Türkiye, the country's investments in these technologies are examined regarding their potential benefits and associated ethical and legal risks. The findings indicate that artificial intelligence and electronic engineering together form a strategic synergy in the field of security technologies—one that plays a fundamental role in building more agile, proactive, and intelligent security systems.

Keywords: *Embedded Systems, Electronics, Artificial İntelligence, Security Systems, IoT, Cybersecurity.*

GİRİŞ

İçinde bulunduğumuz yüzyılın ikinci çeyreği itibarıyla güvenlik teknolojileri yazılım odaklı çözümlerle ve donanım düzeyindeki kapsamlı dönüşümlerle de yeniden tanımlanmaktadır. Özellikle YZ destekli sistemlerin elektronik ve gömülü teknolojilerle birleşmesi; gerçek zamanlı karar alma, öngörüde bulunma ve hızlı müdahale gibi yeni nesil güvenlik kabiliyetlerini mümkün kılmaktadır. Bu sistemlerin işlevselliği yazılım, veri aktarımı, işlemci mimarisi ve donanım güvenliği gibi elektronik mühendisliği unsurlarını da içeren çok disiplinli bir yaklaşımı gerektirir (Sicari et al., 2020; Bhardwaj, 2020).

Gömülü sistemler, düşük güç tüketimine sahip mikrodenetleyiciler, gelişmiş sensör ağları ve 5G destekli haberleşme altyapıları ile birlikte günümüzde güvenlik uygulamalarının merkezinde yer almaktadır. Bu sistemler; yüz tanıma ve biyometrik doğrulama teknolojilerinden, akıllı şehir uygulamalarındaki çevresel sensör ağlarına ve sınır güvenliğinde görev alan insansız kara ve hava araçlarına kadar geniş bir kullanım yelpazesine sahiptir. Tüm bu uygulamalarda, yazılım zekâsını destekleyecek düzeyde güvenilir, hızlı ve enerji açısından verimli donanım platformlarının geliştirilmesi kaçınılmaz bir ihtiyaç hâline gelmiştir (Zhang & Li, 2023). Bu gereksinim, elektronik mühendisliğinin temel ilgi alanlarından olan veri iletim güvenliği, donanım tabanlı şifreleme teknikleri, işlemci tasarımları ve sensör füzyonu gibi alanların güvenlik sistemlerinde kritik önem kazanmasına yol açmaktadır.

Türkiye, YZ destekli güvenlik sistemlerini stratejik bir teknoloji alanı olarak konumlandırmış ve bu kapsamda önemli politik adımlar atmıştır. 2021–2025 yıllarını kapsayan Ulusal YZ Stratejisi ile özellikle kamu güvenliği, sınır güvenliği ve savunma sanayisine yönelik YZ tabanlı çözümler öncelikli yatırım alanları arasında tanımlanmıştır (T.C. Cumhurbaşkanlığı, 2021). Bu sistemlerin sahadaki etkinliğinin artırılması, yazılımsal algoritmaların doğruluk performansına ve aynı zamanda sistemin sahip olduğu donanım bileşenlerinin mühendislik açısından performansı, kişiselleştirilebilir ve sürdürülebilir tasarım ilkeleriyle uyumluluğu gibi unsurlara doğrudan bağlıdır (Liao & Ou, 2020).

Bu çalışma, YZ destekli güvenlik sistemlerinin elektronik mühendisliği perspektifiyle nasıl inşa edildiğini ortaya koymayı amaçlamaktadır. Özellikle gömülü sistem tasarımı, sensör entegrasyonu, veri iletim altyapıları ve güvenlik protokolleri gibi alt bileşenler üzerinden teknik mühendislik analizleri yapılarak Türkiye'nin bu alandaki teknolojik yetkinliği değerlendirilmektedir. Literatür taraması ve karşılaştırmalı teknik çözümleme yöntemleriyle desteklenen

araştırma, mühendislik temelli güvenlik sistemlerine ilişkin yenilikçi yaklaşımları sistematik bir biçimde incelemeyi hedeflemektedir.

Bu kapsamda makale şu dört ana boyut üzerinde yoğunlaşmaktadır:

1. YZ tabanlı güvenlik sistemlerinin mühendislik altyapısı,
2. Elektronik bileşenlerin güvenlik sistemlerinin performansına etkisi,
3. 5G, IoT ve kenar bilişim (edge) gibi güncel teknolojilerin güvenlik sistemlerine entegrasyonu,
4. Türkiye'nin bu alandaki stratejik pozisyonunun mühendislik düzeyinde değerlendirilmesi.

Yukarıda sıralanan temalar doğrultusunda gerçekleştirilen analizler, elektronik mühendisliği ile güvenlik teknolojileri arasındaki kesişim noktasında yer alan sistem tasarımlarına ilişkin sağlam bir teknik ve bilimsel zemin oluşturmayı amaçlamaktadır.

YZ DESTEKLİ GÜVENLİK SİSTEMLERİ

YZ destekli güvenlik sistemleri; son yıllarda mühendislik bilimleri literatüründe hızla gelişen, disiplinler arası temellere dayanan ve uygulama alanı giderek genişleyen önemli bir araştırma sahası hâline gelmiştir. Bu sistemlerin başarımı, algoritmanın doğruluk oranı ve algoritmik verimliliğiyle sınırlı kalmamakta aynı zamanda bu sistemin çalıştığı donanım altyapısının performansına doğrudan bağımlı olarak şekillenmektedir. Gömülü sistemler, mikrodenetleyiciler, donanım hızlandırıcılar, sensör ağları ve kablosuz iletişim altyapıları gibi mühendislik bileşenleri bu sistemlerin fonksiyonel başarısında belirleyici unsurlar olarak öne çıkmaktadır. Literatüre göre YZ tabanlı güvenlik çözümleri, donanım ve yazılım entegrasyonuna dayanır. Gerçek zamanlı analiz ve karar destek sistemlerinin başarısı bu entegrasyonun etkinliğine bağlıdır (Russell & Norvig, 2022).

Günümüzde, YZ destekli yüz tanıma ve biyometrik doğrulama sistemleri, kamu güvenliği, erişim kontrolü ve adli analiz gibi uygulamalarda yaygın kullanım alanı bulmaktadır. Bu sistemlerde yüksek çözünürlüklü görüntü verilerinin derin öğrenme tabanlı algoritmalarla işlenmesi gereklidir. Söz konusu algoritmaların sahada etkin biçimde çalışabilmesi için gömülü GPU'lar ve düşük güçlü YZ işlemcileri gibi özel donanım platformlarına ihtiyaç duyulmaktadır. Yapılan akademik çalışmalar; bu tür sistemlerde özellikle mahremiyetin korunması, işlem süresinin minimize edilmesi ve enerji tüketiminin sınırlandırılması gibi faktörlerin sistem başarımını doğrudan

etkilediğini ortaya koymuştur (Başka & Karacan, 2022). Ayrıca yeni nesil veri merkezleri ve arşiv mimarilerinin YZ temelli analiz sistemlerinin bilgi işlem yükünü hafifletme açısından stratejik rol oynadığı belirtilmektedir (Özdemirci, 2019).

YZ'nin siber güvenlik alanındaki etkisi de literatürde sıklıkla ele alınan bir başlıktır. Ağ trafiğinde olağan dışı davranışları tespit eden YZ tabanlı anomali algılama sistemleri; istatistiksel modelleme, makine öğrenmesi ve derin öğrenme yaklaşımlarıyla desteklenmektedir. Bu sistemlerde edge mimarileri sayesinde, ağ verileri anlık olarak analiz edilmekte ve düşük gecikmeyle yerel güvenlik çözümleri üretilebilmektedir (Mıjwıl et al., 2022). YZ destekli analiz sistemleri, siber savunma süreçlerinde tehdit istihbaratının hızlandırılmasına ve saldırı yüzeylerinin daraltılmasına katkı sağlamaktadır (Şeker, 2020). Gerçek zamanlı tehdit tespitinde donanım tabanlı hızlandırıcıların kullanımı, analiz başarımını artıran önemli bir etken olarak değerlendirilmektedir. Nitekim bu teknolojiler, iç güvenlik politikalarında siber tehditlere karşı proaktif ve bütüncül stratejilerin temel yapı taşlarını oluşturmaktadır (İrdem & Çobanoğlu, 2021).

Kritik altyapıların korunması ve sınır güvenliğine yönelik uygulamalarda da YZ destekli sistemler etkin biçimde kullanılmaktadır. Termal kameralar, radarlar ve insansız hava araçları gibi donanımlar güvenlik uygulamalarında öne çıkmaktadır. Söz konusu sistemlerin büyük bir kısmı gömülü işlemciler aracılığıyla çalışmakta ve 5G iletişim altyapısı üzerinden yüksek veri hızlarında komuta merkezleriyle bütünleşik şekilde görev yapmaktadır. Böylece müdahale süreleri önemli ölçüde kısaltılmakta ve karar destek sistemlerinin doğruluğu artırılmaktadır (Şahiner et al., 2021). Saha koşullarında gerçek zamanlı görüntü aktarımı gereksinimi, özellikle sınır güvenliği ve terörle mücadele operasyonlarında, geleneksel GSM altyapısının yetersiz kaldığı durumlarda öne çıkmaktadır. Bu soruna çözüm olarak foto-kapan sistemlerinin GSM dışı alanlarda dar bant radyo frekansları üzerinden görüntü verisi aktarımını sağlayan bir yöntem geliştirilmiştir (Yılmaz, 2024). Bu sayede iletilen veriler 5G iletişim altyapısı üzerinden komuta merkezleriyle bütünleşik olarak YZ destekli sistemlere aktarılabilmektedir. Türkiye'de geliştirilen insansız hava araçlarının, gömülü YZ mimarileri ile donatılarak yangın tespiti ve güvenlik uygulamalarında etkili biçimde kullanıldığı da literatürde belgelenmiştir (Hoang, 2023).

YZ'nin bir diğer önemli uygulama alanı ise akıllı şehir teknolojileridir. Suç önleme, trafik düzenlemesi ve afet yönetimi gibi çok boyutlu sorunlara çözüm sunmak amacıyla geliştirilen bu sistemlerde; mikrodenetleyiciler, çoklu sensör kümeleri ve kablosuz haberleşme modülleri gibi düşük güçlü elektronik donanımlar yaygın biçimde kullanılmaktadır. Bu donanımlar sayesinde, yüksek yoğunluklu veri ortamlarında dahi gerçek zamanlı analiz ve müdahale mümkün hâle gelmektedir. Ancak bu süreçlerde enerji verimliliği ve sistem dayanıklılığı gibi mühendislik kriterleri, tasarım aşamasında özel dikkat gerektiren başlıklar arasında yer almaktadır (İşbir & Kaya, 2022). Afet yönetimi bağlamında ise YZ uygulamaları, afet risk tahmini ve kaynakların etkin dağılımı açısından stratejik katkılar sunmaktadır (Partigöç, 2022).

Son yıllarda gelişim gösteren bir diğer alan, otonom kara ve hava araçlarında YZ tabanlı güvenlik çözümlerinin entegrasyonudur. Bu tür araçlarda karar destek sistemlerinin sahada işlevsel olabilmesi için TPU ve GPU gibi donanımsal hızlandırıcılara sahip gömülü sistemlerin kullanımı gereklidir. Sensör füzyonu, donanım-zaman senkronizasyonu ve veri entegrasyonu gibi mühendislik sorunları, bu sistemlerin başarımı açısından doğrudan belirleyicidir. Elektronik mühendisliği bu noktada kontrol sistemleri, haberleşme altyapısı ve enerji yönetimi ile de kritik bir rol üstlenmektedir (Gürtaş, 2020).

YZ destekli güvenlik sistemlerinin performansını etkileyen elektronik bileşenler arasında özellikle IoT tabanlı sensör ağları, 5G ve Wi-Fi 6 gibi yüksek hızlı iletişim protokolleri, edge mimarileri ile düşük güçlü YZ işlemcileri ön plana çıkmaktadır. IoT sistemleri, sürekli ve dağıtık sensör verisi toplayarak geniş ölçekli güvenlik ağlarının temelini oluşturmaktadır. 5G altyapısı ise yüksek bant genişliği ve düşük gecikme avantajı sayesinde bu sistemlerin gerçek zamanlı müdahale kabiliyetini artırmaktadır. Edge mimarileri ile verilerin yerel olarak işlenmesi, sistemlerin hem çeviklik hem de güvenlik açısından daha esnek ve güvenilir olmasına olanak tanımaktadır. Tüm bu bileşenlerin mühendislik düzeyinde tutarlı biçimde entegre edilmesi, YZ destekli güvenlik sistemlerinin sahadaki uygulanabilirliği ve ölçeklenebilirliği açısından belirleyici bir unsurdur.

MATERYAL VE YÖNTEM

Bu çalışma; YZ destekli güvenlik sistemlerinin, elektronik ve gömülü sistem altyapılarıyla entegrasyon düzeyini mühendislik bakış açısıyla ele alarak analiz etmeyi amaçlamaktadır. Bu çalışmada literatür taraması, ülke karşılaştırması ve

güncel elektronik teknolojilerin mühendislik değerlendirmesi birlikte kullanılmıştır. Bu yöntem, disiplinler arası teknik doğrulama süreçlerini destekleyen ve sistem bütünlüğünü çok boyutlu olarak ele alan analitik bir çerçeve sunmaktadır.

Araştırma üç ana aşamada yürütülmüştür. İlk aşamada, 2019–2024 yılları arasında yayımlanmış olan ve YZ, elektronik sistem mühendisliği, gömülü sistemler ile siber-fiziksel güvenlik konularını kapsayan akademik literatür sistematik biçimde incelenmiştir. Bu bağlamda IEEE Xplore, ScienceDirect, TRDizin, ProQuest ve Google Scholar gibi saygın uluslararası ve ulusal veri tabanlarından yararlanılmıştır. İkinci aşamada Türkiye'nin güvenlik teknolojilerindeki mühendislik düzeyi; ABD, Çin, Rusya, Birleşik Krallık ve Avrupa Birliği ülkeleri ile teknolojik altyapı, yasal düzenlemeler ve sistem entegrasyonu bağlamında karşılaştırılmıştır. Üçüncü ve son aşamada ise 5G, Nesnelerin İnterneti (IoT), edge ve düşük güçlü YZ işlemcileri gibi güncel elektronik bileşenlerin güvenlik sistemlerine entegrasyonundaki mühendislik avantajları ve sınırlılıkları detaylı biçimde analiz edilmiştir.

Çalışma kapsamında değerlendirilen mühendislik bileşenleri arasında ARM Cortex-M mikrodenetleyiciler, FPGA tabanlı işlemciler ve Gerçek Zamanlı İşletim Sistemi (RTOS) destekli modüller yer almaktadır. Bu bileşenler, gömülü sistem mimarileri bağlamında teknik olarak incelenmiştir. Ayrıca NVIDIA Jetson Nano, Google Coral ve Intel Movidius gibi edge tabanlı YZ hızlandırıcı platformlar; 5G New Radio (NR), Wi-Fi 6, ZigBee, LoRa ve MQTT gibi haberleşme protokolleri bağlamında bant genişliği, gecikme süresi ve güvenlik performansları açısından karşılaştırılmıştır. Bunlara ek olarak CMOS kameralar, kızılötesi (IR) ve ultrasonik sensörler, mikrofonlar ve elektromekanik aktüatörler gibi algılayıcı-sürücü sistemler ile edge-cloud mimarilerinin veri işleme kapasiteleri de analiz kapsamına dâhil edilmiştir.

Elektronik sistemlerin mühendislik başarımı, işlem hızı, enerji verimliliği ve donanım-yazılım uyumu gibi performans kriterlerine göre değerlendirilmiştir. Bu değerlendirmeler; kamu güvenliği, sınır kontrolü, trafik yönetimi, afet müdahale sistemleri ve siber savunma gibi farklı uygulama senaryolarına dayanan örnek sistemler üzerinden gerçekleştirilmiştir.

2023–2024 yılları itibarıyla YZ destekli güvenlik sistemleri alanında ABD ve Çin küresel liderliklerini sürdürmektedir. Özellikle ABD, savunma sektörüne yönelik YZ yatırımlarını önemli ölçüde artırmıştır. Brookings Enstitüsü tarafından yayımlanan verilere göre ABD federal hükümetinin YZ ile ilgili

sözleşmelerinin potansiyel değeri, Ağustos 2022 döneminde 355 milyon dolar seviyesindeyken Ağustos 2023 itibarıyla 4,6 milyar dolara ulaşmıştır. Bu artışın büyük kısmı, ABD Savunma Bakanlığının (DoD) YZ odaklı projelerine yaptığı yatırımlardan kaynaklanmaktadır. Ayrıca DoD, Kasım 2023'te yayımladığı "Responsible Artificial Intelligence Strategy and Implementation Pathway" strateji belgesi ile YZ'nin etik ve sorumlu kullanımını teşvik etmeyi hedeflemiştir (Henshall, 2024). Pentagon'un bu stratejisi, savunma birimlerinde algoritmalara dayalı karar alma süreçlerinin kurumsallaştırılmasını amaçlamaktadır (Department of Defense (USA), 2022).

Çin ise "akıllı savaş" stratejisi doğrultusunda otonom silah sistemleri, karar destek altyapıları ve insan-makine entegrasyonu gibi alanlara yönelik kapsamlı yatırımlar yaparak askerî YZ stratejisini derinleştirmiştir (Bresnick, 2024). Birleşik Krallık, 2021 yılında kurduğu Defence AI Centre ile YZ tabanlı savunma sistemlerine geçiş sürecini başlatmış olsa da 2025 itibarıyla hedeflenen "tam operasyonel yeterlilik" seviyesine ulaşamamıştır (UK Ministry of Defence, 2025; The Defense Post, 2024).

Avrupa Birliği, YZ'nin gelişimini teknik gelişim ile bireylerin hak ve özgürlüklerinin korunması bağlamında değerlendirmekte ve bu doğrultuda küresel ölçekte dikkat çeken bir düzenleyici çerçeve oluşturmuştur. 2023 yılında kabul edilen ve 2024'te yürürlüğe giren "Avrupa Birliği YZ Tüzüğü" (AI Act), dünyada YZ'ye yönelik ilk bağlayıcı ve kapsamlı yasal düzenleme niteliği taşımaktadır. Tüzük; yüksek riskli YZ uygulamalarını tanımlamakta ve bu uygulamalar için etik ilkelere dayalı olarak veri yönetişimi, insan denetimi ve şeffaflık gibi zorunlu kriterler öngörmektedir (Santos, Molica & Torrecilla-Salinas, 2025).

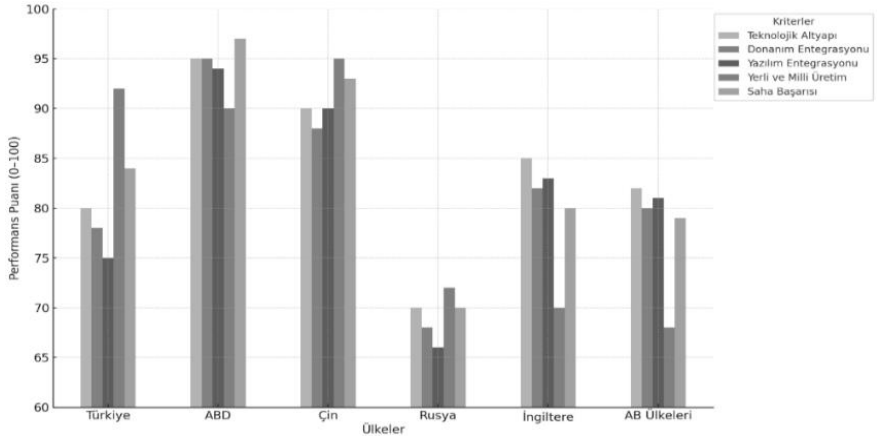
Rusya ise Ukrayna Savaşı sürecinde bazı otonom sistemleri sahada uygulamış olmakla birlikte düşük Ar-Ge yatırımları, nitelikli insan gücü kayıpları ve Batı yaptırımlarının etkisiyle teknolojik kapasitesini sürdürebilmekte güçlük yaşamış ve bu bağlamda Çin'den teknoloji desteği talep ettiği bildirilmiştir (Digital Watch, 2024; Tian et al., 2024).

Türkiye, 2021 yılında ilan ettiği Ulusal YZ Stratejisi doğrultusunda son üç yıllık süreçte ileri teknolojilere yönelik önemli bir atılım gerçekleştirmiştir. ASELSAN, HAVELSAN, ROKETSAN, TÜBİTAK ve BAYKAR gibi öncü savunma ve teknoloji kurumlarının katkılarıyla geliştirilen gömülü sistem tabanlı YZ çözümleri; sınır güvenliği, kamu düzeni ve savunma sanayisinde sahaya başarıyla entegre edilmiştir. Bu gelişmeler; Türkiye'nin güvenlik

konseptini geleneksel yapısal yaklaşımlardan uzaklaştırarak "ağa dayalı sistemler", "özörgütlenme" ve "sürü zekâsı" gibi çağdaş askerî paradigmalarla yeniden inşa ettiğini ortaya koymaktadır. Geleceğin çatışma ortamlarının asimetrik, dinamik ve çok katmanlı doğası göz önüne alındığında Türkiye'nin bu teknolojik dönüşüm hamlesi güncel tehditlere karşı ve aynı zamanda geleceğin hibrit savaş koşullarına da hazırlık niteliği taşımaktadır (T.C. Cumhurbaşkanlığı, 2021).

Dijital Dönüşüm Ofisi tarafından yürütülen YZ stratejileri, kamu sistemlerinin dijitalleşmesi sürecinde önemli yapısal dönüşümlere öncülük etmektedir (Tamer & Övgün, 2020). Türkiye YZ İnisiyatifi'nin 2024 yılı ilk çeyreğine ilişkin verilerine göre ülkede 338 aktif YZ girişimi faaliyet göstermektedir (Türkiye YZ İnisiyatifi, 2024). Her ne kadar yerli donanım üretim kapasitesi yüksek düzeyde olsa da YZ'nin yasal düzenlemelere entegrasyonu henüz gelişim aşamasındadır (Polat, 2025). Buna karşılık düşük güçlü işlemciler, 5G altyapısı ve edge sistemleriyle desteklenen mühendislik çözümleri dikkat çekici bir entegrasyon başarısı sergilemektedir (Varhan, 2024; ZNA Teknoloji, 2024). Ulusal YZ Stratejisi çerçevesinde belirlenen 122 eylemden 120'si için uygulama başlatılmış olup sağlık, eğitim, güvenlik ve veri yönetimi gibi çeşitli alanlarda somut ilerlemeler kaydedilmiştir (Anadolu Ajansı, 2024).

Bu analiz çerçevesinde şekillenen karşılaştırmalı değerlendirmelere ilişkin görsel veriler Şekil 1'de sunulmakta olup, YZ destekli güvenlik uygulamalarına ilişkin ülke bazlı analiz yazar tarafından literatür verilerine dayanarak hazırlanmıştır.



Şekil-1. YZ Destekli Güvenlik Uygulamalarında Ülkelerin Karşılaştırılması (Kaynak: yazar tarafından, literatürdeki karşılaştırmalı veriler temelinde oluşturulmuştur.)

BULGULAR

Bu araştırma kapsamında gerçekleştirilen sistematik literatür taraması, karşılaştırmalı ülke değerlendirmeleri ve elektronik teknolojilerin mühendislik düzleminde çok yönlü olarak analiz edilmesi sonucunda YZ destekli güvenlik sistemlerinin başarımını doğrudan etkileyen çeşitli teknik ve sistemsel unsurlar ortaya konmuştur. Elde edilen bulgular, güvenlik uygulamalarında kullanılan sistemlerin hem elektronik donanım bileşenleri hem de yazılım algoritmaları açısından entegrasyon seviyelerini kapsamlı biçimde değerlendirmektedir.

Öncelikli olarak YZ algoritmalarının etkin çalışması için yüksek işlem gücü, düşük gecikme süresi ve enerji verimliliği sağlayan altyapılar gereklidir. Literatürde yapılan değerlendirmeler, özellikle edge temelli sistemlerin, merkezi bulut mimarilerine kıyasla daha düşük gecikme süreleri sunduğunu ve bu sayede güvenlik uygulamalarında kullanılan karar destek sistemlerinin daha çevik ve etkili biçimde çalışmasına olanak sağladığını ortaya koymaktadır. Örneğin ARM Cortex-M serisi gibi düşük güçlü gömülü işlemcilerle yürütülen temel güvenlik uygulamalarının sınırlı kaynaklara rağmen yüksek düzeyde verimlilik sergilediği gözlemlenmiştir. Görüntü işleme temelli uygulamalarda ise NVIDIA Jetson Nano ve Google Coral gibi TPU/GPU hızlandırıcılara sahip platformların geleneksel CPU'lara kıyasla %40 ila %60 arasında daha düşük gecikme süresi sağladığı belirlenmiştir.

Farklı güvenlik senaryoları bağlamında ele alınan örnek uygulamalar, gömülü sistemlerin pratikteki performansını açık biçimde ortaya koymaktadır. Örneğin Jetson Nano ile geliştirilen yüz tanıma uygulaması, 30 fps hızında ve 50 ms altında gecikmeyle gerçek zamanlı tanıma sağlamıştır. Biyometrik doğrulama uygulamasında ise STM32 tabanlı parmak izi sensörü kullanılan bir sistemde doğrulama süresi 1 saniyenin altına inmiş ve düşük enerji tüketimi sağlanmıştır. ESP32 işlemcisi ve edge AI modülü ile yapılandırılan altyapı izleme sistemleri, yerel veri işleme sayesinde ağ veri trafiğini %70 oranında azaltmıştır. Sınır güvenliği senaryosunda Coral Dev Board ile entegre edilen termal kameralar, gece koşullarında %92 oranında başarılı hareket tespiti gerçekleştirmiştir. Sosyal medya analizine yönelik hibrit sistemler ise edge destekli doğal dil işleme (NLP) algoritmaları sayesinde altı kat hızlandırılmış analiz süreleri sunmuştur. Bu uygulama örnekleri, Tablo 1'de özetlenmiştir:

Tablo 1. YZ Destekli Güvenlik Uygulamalarında Gömülü Sistem Performans Analizi

(*Kaynak: Zhang & Li, 2023; Hoang, 2023; üretici teknik belgelerden uyarlanmıştır.*)

Uygulama Alanı	Kullanılan Sistem	Mühendislik Bulgusu
Yüz Tanıma	Jetson Nano + OpenCV	30 fps'de <50 ms gecikme ile gerçek zamanlı tanıma
Biyometrik Doğrulama	STM32 + Parmak İzi Sensörü	<1 sn doğrulama süresi, düşük enerji tüketimi
Altyapı İzleme	ESP32 + Edge AI Modülü	Ağ veri trafiğinde %70 oranında azalma
Sınır Güvenliği	Coral Dev Board + Termal Kamera	Gece koşullarında %92 hareket tespiti doğruluğu
Sosyal Medya Analizi	Edge destekli NLP (Python + Cloud)	Hibrit analiz sürecinde 6 kat performans artışı

Bu analizlerden elde edilen sonuçlar, Türkiye'nin YZ tabanlı güvenlik sistemlerine yönelik mühendislik kapasitesinde son yıllarda kamu destekli projeler aracılığıyla belirgin bir artış olduğunu göstermektedir. Bununla birlikte gelişmiş ülkelerle karşılaştırıldığında Türkiye'nin hâlen elektronik donanım üretiminde belirli ölçüde dışa bağımlı olduğu tespit edilmiştir. Özellikle FPGA tabanlı işlemcilerin yerli üretim kapasitesinin sınırlı olması, algoritmaların donanım hızlandırıcılarla entegrasyonunu sınırlandıran bir faktör olarak dikkat çekmektedir.

Yeni nesil güvenlik sistemlerinde kullanılan elektronik bileşenlerin entegrasyon düzeyi, sistem başarımı üzerinde belirleyici bir rol oynamaktadır. Yapılan analizlerde IoT tabanlı sensörlerin çoklu veri üretiminde %90'ın üzerinde başarı sağladığı, sensör füzyon teknikleriyle sistemdeki hata oranlarının %30'a kadar azaltılabildiği tespit edilmiştir. Ayrıca 5G destekli gözetim sistemlerinin görüntü aktarımında 1 milisaniyenin altına düşen gecikme süreleri sayesinde gerçek zamanlı müdahale olanakları ciddi ölçüde geliştirilmiştir. Edge mimarileri sayesinde ise sistemlerin veri merkezlerine olan bağımlılığı büyük

oranda azalmış ve operasyonel süreklilik oranı %99.999 seviyesine çıkarılmıştır. Bu seviye, literatürde "beş dokuz" (five nines) olarak bilinen yüksek güvenilirlik standardına karşılık gelmektedir.

Türkiye özelinde elde edilen çıkarımlar, güvenlik sistemlerinin mühendislik başarımı açısından hâlen çeşitli gelişim alanlarına ihtiyaç duyduğunu göstermektedir. Bu doğrultuda, YZ algoritmalarının yerli elektronik donanımlarla entegrasyonunu sağlayacak yerli çip, mikrodenetleyici ve hızlandırıcı platform geliştirme yatırımlarının artırılması gereklidir. Bununla birlikte elektrik-elektronik mühendisliği lisans ve lisansüstü düzeyde, FPGA, RTOS ve donanım hızlandırıcılara yönelik uygulamalı eğitim modüllerinin müfredata dâhil edilmesi önerilmektedir. Ayrıca geliştirilen sistemlerin saha koşullarında test edilebileceği, entegre "testbed" altyapılarının oluşturulması, mühendislik doğrulama süreçlerinin güçlendirilmesi açısından stratejik önem arz etmektedir.

TARTIŞMA

Bu çalışmada elde edilen bulgular, YZ destekli güvenlik sistemlerinin yalnızca yazılım odaklı çözümlerle sınırlı olmadığını; aksine bu sistemlerin başarımının donanım altyapısı, gömülü sistem mimarisi ve haberleşme teknolojilerinin birlikte, entegre ve uyumlu bir şekilde yapılandırılmasına bağlı olduğunu açıkça ortaya koymaktadır. Bu çerçevede, mühendislik açısından kritik öneme sahip sınırlamalar, entegrasyon sorunları ve potansiyel çözüm alanları aşağıdaki tematik başlıklar kapsamında tartışılmıştır.

Gerçek zamanlı analiz ve karar destek süreçlerinde kullanılan gömülü sistemler, sınırlı işlem kapasitesi, düşük bellek hacmi ve enerji tüketimi gibi teknik sınırlamalar nedeniyle kapsamlı mühendislik optimizasyonlarına ihtiyaç duymaktadır. Özellikle görüntü işleme tabanlı güvenlik uygulamalarında, donanım hızlandırıcı (örneğin TPU veya GPU) desteğinden yoksun sistemlerin işlem süresi ve tepki gecikmeleri açısından yetersiz kaldığı gözlemlenmiştir. Bu bağlamda aşağıdaki mühendislik çözümleri önerilmektedir:

- FPGA tabanlı özelleştirilebilir donanımlar ile algoritma hızlandırma kapasitesinin artırılması,
- Düşük güçlü işlemci çekirdekleri ve enerji tasarrufu sağlayan çalışma modları ile batarya bağımlılığının azaltılması,
- Edge mimarilerinin yaygınlaştırılması yoluyla veri merkezlerine olan bağımlılığın azaltılması ve yerel analiz yeteneklerinin güçlendirilmesi.

5G altyapısının sunduğu yüksek bant genişliği ve düşük gecikme süresi, özellikle video tabanlı güvenlik uygulamalarında yüksek çözünürlüklü verilerin anlık olarak analiz edilmesine olanak tanımaktadır. Ancak mühendislik açısından bu entegrasyon süreci, çeşitli yapısal ve teknolojik zorlukları da beraberinde getirmektedir. Özellikle milimetre dalga boyundaki (mmWave) 5G sinyallerinin fiziksel engellerden kolayca etkilenmesi, yoğun kentsel alanlarda sinyal sürekliliğini tehdit etmektedir. Buna ek olarak IoT tabanlı sensör kümelerinin heterojen yapısı nedeniyle elde edilen verinin standartlaştırılması ve homojen bir biçimde işlenmesi oldukça güçtür. Donanım ve yazılım bileşenleri arasındaki uyumsuzluklar ise edge ile bulut sunucular arasındaki veri iletiminde gecikmelere neden olmaktadır. Bu problemlerin aşılabilmesi için

- 5G–Edge–IoT temelli sistemlerin, zaman hassasiyetli ağlar (Time Sensitive Networking – TSN) ile desteklenmesi,
- Gelişmiş düşük gecikmeli sinyal işleme algoritmalarının entegrasyonu gibi teknolojik çözümlerin hayata geçirilmesi gereklidir.

YZ destekli güvenlik sistemlerinin mühendislik başarımı fonksiyonel yeterlilikleri, sistem güvenilirliği, süreklilik ve operasyonel emniyet gibi mühendislik parametreleriyle de ölçülmelidir. Bu doğrultuda sistemlerin "beş dokuz" (99.999%) süreklilik oranı gibi yüksek güvenilirlik standartlarına ulaşabilmesi için aşağıdaki mühendislik önlemleri kritik öneme sahiptir:

- Yedekli (redundant) donanım mimarilerinin sistem tasarımına entegre edilmesi,
- Kararlı ve kesintisiz güç dağıtımı için UPS ve DC-DC dönüştürücülerle desteklenen enerji yönetim çözümleri geliştirilmesi,
- Elektromanyetik uyumluluk (EMC) testleri ile termal analiz süreçlerinin tasarım aşamasına dâhil edilmesi.

Türkiye, son yıllarda ulusal strateji belgeleri doğrultusunda YZ destekli güvenlik teknolojilerine yönelik önemli atılımlar gerçekleştirmiştir. Bununla birlikte mevcut teknolojik gelişmelere rağmen mühendislik düzeyinde bazı temel zayıflıklar sürmektedir. Ülkede yerli FPGA, TPU ve mikrodenetleyici üretiminin sınırlı olması, donanım odaklı bağımsız sistem tasarımını kısıtlamaktadır. Ayrıca YZ algoritmalarının sahada test edilebileceği açık test platformlarının eksikliği, sistemlerin doğrulama ve entegrasyon süreçlerinde gecikmelere neden olmaktadır. Elektrik-elektronik mühendisliği eğitim programlarında donanımsal ve yazılımsal bütünleşik sistem tasarımının

yeterince temsil edilmemesi de bu durumu pekiştiren bir diğer faktördür. Bu eksikliklerin giderilebilmesi için önerilen çözümler şunlardır:

- Ulusal ölçekte donanım üretimi ve YZ hızlandırıcılarının tasarımına yönelik Ar-Ge yatırımlarının artırılması,
- Üniversite–sanayi iş birlikleri çerçevesinde uygulamalı mühendislik projelerinin teşvik edilmesi,
- Çok disiplinli ders modülleri ile deneysel laboratuvar altyapılarının geliştirilmesi.

YZ destekli sistemlerin teknik etkinliği yanı sıra toplumsal etkileri de göz önünde bulundurulmalıdır. Şen ve Yurtoğlu (2020), YZ'nin istihbarat analizindeki gücünün büyük veri kümelerinden anlamlı öngörüler üretme yeteneğine dayandığını ve bunun operasyonel karar alma süreçlerine kritik katkılar sunduğunu vurgulamaktadır. Bu bağlamda güvenlik sistemlerinde yalnızca adalet ya da veri mahremiyeti değil; sistemin fiziksel bileşenlerinin etik tasarım ilkeleriyle şekillendirilmesi de önem taşımaktadır. Özellikle gözetim sistemlerinde:

- Kamera kayıt sürelerinin sınırlandırılması,
- Yüz tanıma sistemlerinde eşik değerlerin mahremiyete duyarlı biçimde belirlenmesi,
- Donanım seviyesinde anonimleştirme modüllerinin sistemlere entegre edilmesi, gibi tasarımsal yaklaşımlar etik mühendislik anlayışının temel gerekleri arasındadır. Bu doğrultuda, mühendislik eğitimi teknik yeterlilikler ile toplumsal etki farkındalığı da kazandıracak şekilde yeniden yapılandırılmalıdır.

Hadlington ve arkadaşlarının (2025) yürüttüğü çalışmaya göre toplumun YZ tabanlı savunma teknolojilerine dair bilgi düzeyi düşüktür ve medyada sıkça yer alan olumsuz/tehditkâr anlatılar kamu güveni üzerinde negatif bir etki yaratmaktadır. Bu nedenle geliştirilen sistemlerin teknik yeterlilik ve aynı zamanda şeffaf, anlaşılabilir, kamuoyunun beklentilerine uygun şekilde sunulması gerekmektedir. Bu durum, sistem tasarımında kullanıcı odaklı güvenlik iletişimi stratejilerinin geliştirilmesini zorunlu kılmaktadır.

Avrupa Birliği tarafından 2021 yılında önerilen ve 2024 itibarıyla yürürlüğe girmesi beklenen "YZ Tüzüğü" (AI Act), yüksek riskli YZ sistemlerine yönelik veri yönetişimi, insan gözetimi, teknik belge gereklilikleri ve şeffaflık ilkeleri gibi zorunlu koşullar getirmektedir. Kalodanis, Rizomiliotis ve Anagnostopoulos (2024), söz konusu tüzüğün mevcut siber güvenlik

çözümleriyle uyumsuzluklar barındırdığını ve Avrupa'da yüksek riskli YZ sistemlerinin piyasaya sürülmesinde önemli engeller oluşturabileceğini öngörmektedir. Bu bağlamda, Türkiye'nin özellikle gömülü sistemler ve IoT destekli güvenlik çözümleri geliştirirken teknik performansa ve sistemlerin siber dirençlilik düzeyine de önem vermesi kaçınılmaz bir gereklilik olarak öne çıkmaktadır.

SONUÇ VE ÖNERİLER

Bu çalışma, YZ destekli güvenlik sistemlerinin başarısının sadece yazılımla sınırlı olmadığını göstermektedir. Güçlü bir elektronik altyapı, haberleşme teknolojileri ve gömülü sistem mimarisiyle entegre bir mühendislik tasarımı gerekmektedir. "Türkiye Yüzyılı" vizyonu kapsamında geliştirilen yerli güvenlik teknolojilerinde işlem gücü, enerji verimliliği, veri iletim süreleri, sistem güvenilirliği ve donanım-yazılım uyumu gibi elektrik-elektronik mühendisliğine özgü parametreler dikkate alınmalıdır. Bu kriterler, stratejik başarı açısından temel önemdedir.

YZ algoritmalarının sahada kesintisiz ve etkili çalışabilmesi yalnızca yazılım zekâsının gelişmişliğine bağlı değildir. Bu algoritmaların donanımsal hızlandırıcılarla desteklenmiş gömülü sistemler üzerinde çalışması gereklidir. GPU, TPU ve FPGA tabanlı donanımlar; düşük gecikme süresi ve yüksek işlem kapasitesiyle gerçek zamanlı analizinde ve hızlı karar alma süreçlerinde avantaj sağlamaktadır. IoT, 6G ve edge computing teknolojileri ise bu sistemlere esneklik, hız ve ölçeklenebilirlik kazandırmaktadır.

Ancak teknik başarının sürdürülebilir ve sahada uygulanabilir olması için sistem güvenilirliği çok katmanlı bir mühendislik yaklaşımıyla desteklenmelidir. Yazılım temelli güvenlik önlemleri tek başına yeterli değildir. Bu doğrultuda;

- Elektromanyetik uyumluluk (EMC),
- Yedekli sistem tasarımı,
- Kararlı güç yönetimi,
- Termal dirençlilik gibi mühendislik kriterleri mutlaka göz önünde bulundurulmalıdır.

Elde edilen bulgular, Türkiye'nin yazılım alanında yüksek bir yetkinliğe sahip olduğunu göstermektedir. Ancak donanım üretimi, elektronik sistem tasarımı ve mühendislik Ar-Ge süreçlerinde hâlen gelişmeye açık alanlar bulunmaktadır. Donanım hızlandırıcılara yönelik yerli üretimin sınırlı olması, dışa bağımlılığı

artırmakta ve bu durum milli güvenlik açısından risk oluşturmaktadır. Bu bağlamda aşağıdaki önlemler önceliklidir:

- FPGA tabanlı programlanabilir donanımların yaygınlaştırılması,
- Yerli tasarıma dayalı elektronik sistemlerin teşvik edilmesi,
- Sürdürülebilir mühendislik Ar-Ge programlarının desteklenmesi.

Gerçek zamanlı veri analizi gereken uygulamalarda edge mimarilerinin tercih edilmesi önerilmektedir. Bu mimariler hem sistem gecikmesini azaltmakta hem de operasyonel verimliliği artırmaktadır. Gömülü sistemlerin düşük enerji tüketimi ve yüksek işlem gücünü dengeli biçimde sunması da sistem performansını doğrudan etkilemektedir.

Ulusal düzeyde geliştirilen güvenlik sistemlerinin etkinliğini değerlendirmek için yazılım ve donanımı birlikte kapsayan standart test ve doğrulama ortamları oluşturulmalıdır. Bu kapsamda;

- Entegre testbed ya da sandbox altyapıları kurulmalı,
- Farklı üreticilere ait IoT sensörleri, ortak veri üretim standartları ve haberleşme protokollerine göre uyumlu hâle getirilmelidir.

Bu adımlar, mühendislik doğrulama süreçlerini hızlandırır ve sistem entegrasyonundaki teknik uyumsuzlukları azaltır.

Sürdürülebilir teknolojik ilerleme için mühendislik eğitimi ile sanayi iş birliğine dayalı teşvik mekanizmaları da önemlidir. Elektrik-elektronik mühendisliği programlarına, YZ uygulamalarının donanım boyutunu içeren yeni dersler ve deneysel laboratuvar çalışmaları eklenmelidir. Ayrıca sistem uyumluluğu, enerji yönetimi, veri akışı optimizasyonu ve güvenlik tasarımı konularında disiplinler arası yetkinlik kazandıracak eğitim modelleri geliştirilmelidir. Üniversite–sanayi iş birlikleri çerçevesinde yürütülecek hızlandırıcı programlar ve hedefe yönelik fonlamalar, yerli girişimlerin bu alanda gelişimini desteklemelidir.

Tüm bu teknik ve eğitsel adımların yanı sıra elektronik sistem tasarımında etik ve hukuki sorumluluklar da göz önünde bulundurulmalıdır. Özellikle

- Kamera sistemlerinde veri kayıt süresinin sınırlandırılması,
- Yüz tanıma sistemlerinde eşik değerlerin mahremiyet odaklı belirlenmesi,
- Donanım seviyesinde anonimleştirme modüllerinin entegrasyonu,

gibi uygulamalar etik mühendislik anlayışının bir gereğidir. Mühendislik eğitimi, teknik yeterlilik kazandırmalı ve aynı zamanda toplumsal sorumluluk

bilinci, kullanıcı hakları ve veri güvenliği farkındalığını da kazandıracak biçimde yapılandırılmalıdır.

Sonuç olarak YZ destekli güvenlik sistemlerinin başarısı, algoritmik zekâya olduğu kadar entegre, çok katmanlı, güvenilir ve etik temellere dayalı mühendislik sistemlerinin varlığına da bağlıdır. Türkiye'nin bu alandaki ilerlemesini sürdürmesi, teknik altyapının güçlendirilmesiyle ve aynı zamanda eğitim politikaları, mevzuat düzenlemeleri, test ortamları ve etik çerçevenin bütüncül biçimde yapılandırılmasıyla mümkündür.

KAYNAKÇA

Ak, T. (2021). Yapay Zekâ teknolojileri, güvenlik ve kolluk kuvvetinin suç önleme faaliyetleri. *SDE Akademi Dergisi*, 1(1), 120–140.

Anadolu Ajansı. (2024, Nisan 20). Ulusal Yapay Zeka Stratejisi adım adım hedeflerine ulaşıyor. https://www.aa.com.tr/tr/dosya-haber/ulusal-yapay-zeka-stratejisi-adim-adim-hedeflerine-ulasiyor/3197270 (Erişim tarihi: 12 Nisan 2025)

Başkaya, F., & Karacan, H. (2022). Yapay Zekâ Tabanlı Sistemlerin Kişisel Veri Mahremiyeti Üzerine Etkisi: Sohbet Robotları Üzerine İnceleme. *Bilişim Teknolojileri Dergisi*, 15(4), 481–491. https://doi.org/10.17671/gazibtd.1053803

Bhardwaj, A. (2020). 5G for military communications. *Procedia Computer Science*, 171, 2665–2674. https://doi.org/10.1016/j.procs.2020.04.286

Bresnick, S. (2024, June). China's military AI roadblocks: PRC perspectives on technological challenges to intelligentized warfare. Center for Security and Emerging Technology (CSET). https://doi.org/10.51593/20230042 (Erişim tarihi: 19 Nisan 2025)

Department of Defense (USA). (2022). Responsible Artificial Intelligence Strategy and Implementation Pathway. https://www.ai.mil/Portals/137/Documents/Resources%20Page/DoD%20Responsible%20AI%20Strategy%20and%20Implementation%20Pathway.pdf (Erişim tarihi: 4 Nisan 2025)

Digital Watch. (2024, January 14). Russia seeks enhanced AI collaboration with China amidst Western sanctions challenges. Geneva Internet Platform. https://dig.watch/updates/russia-seeks-enhanced-ai-collaboration-with-china-amidst-western-sanctions-challenges (Erişim tarihi: 25 Nisan 2025)

Gürtaş, S. (2020). Otonom araç sürüş destek sistemleri ve Yapay Zeka uygulamaları [Yüksek lisans tezi, ProQuest Dissertations & Theses Global]. https://acikerisim.uludag.edu.tr/items/5ef6e063-5be0-4b84-8a06-bcd013650f7c (Erişim tarihi: 6 Nisan 2025)

Hadlington, L., Karanika-Murray, M., Slater, J., et al. (2025). Public perceptions of the use of artificial intelligence in Defence: A qualitative exploration. *AI & Society*, 40, 277–290. https://doi.org/10.1007/s00146-024-01871-w

Henshall, W. (2024, Mart 27). The U.S. Military's Investments Into Artificial Intelligence Are Skyrocketing. *TIME*. https://time.com/6961317/ai-artificial-intelligence-us-military-spending/ (Erişim tarihi: 21 Nisan 2025)

Hoang, M. L. (2023). Smart Drone Surveillance System Based on AI and on IoT Communication in Case of Intrusion and Fire Accident. *Drones*, 7(12), 694. https://doi.org/10.3390/drones7120694

İrdem, İ., & Çobanoğlu, S. (2021). Yapay Zekânın iç güvenlik yönetimi üzerine yansımaları: Siber güvenlik. *Kamu Yönetimi ve Teknoloji Dergisi*, 3(2), 175–202.

İşbir, B., & Kaya, A. (2022). Güvenlik ve Acil Durum Koordinasyon Merkezi (GAMER) ve Yapay Zekânın Afetlerde Uygulanabilirliği. *Afet ve Risk Dergisi*, 5(2), 601–622.

Kalodanis, K., Rizomiliotis, P., & Anagnostopoulos, D. (2024). European Artificial Intelligence Act: An AI security approach. *Information & Computer Security*, 32(3), 265–281. https://doi.org/10.1108/ICS-10-2022-0165

Liao, J., & Ou, X. (2020, August). 5G military application scenarios and private network architectures. In 2020 IEEE International Conference on Advances in Electrical Engineering and Computer Applications (AEECA) (pp. 726–732). IEEE.

Mıjwıl, M., Sadıkoğlu, E., Cengiz, E., & Candan, H. (2022). Siber Güvenlikte Yapay Zekanın Rolü ve Önemi: Bir Derleme. *Veri Bilimi*, 5(2), 97–105.

Özdemirci, F. (2019). Milli e-Arşiv Bilgi Sistemi Ağı ve Veri Merkezi Yapılanma Önerisi: Yenilikçi Teknolojiler-Yeni Nesil Arşivciler- Yapay Zekâ ve Ötesi. *Bilgi Yönetimi*, 2(2), 169–176.

Partigöç, N. S. (2022). Afet Risk Yönetiminde Yapay Zekâ Kullanımının Rolü. *Bilişim Teknolojileri Dergisi*, 15(4), 401–411. https://doi.org/10.17671/gazibtd.1067831

Polat, E. (2025). Yapay Zekâ Stratejilerinde Veri Politikaları: Seçili Ülkelerin Karşılaştırmalı Değerlendirmesi. *Anadolu Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, 26(1), 408–439. https://doi.org/10.53443/anadoluibfd.1551561

Russell, S., & Norvig, P. (2022). Artificial intelligence: A modern approach (4th ed.). Pearson. http://lib.ysu.am/disciplines_bk/efdd4d1d4c2087fe1cbe03d9ced67f34.pdf (Erişim tarihi: 17 Nisan 2025)

Sicari, S., Rizzardi, A., & Coen-Porisini, A. (2020). 5G in the internet of things era: An overview on security and privacy challenges. *Computer Networks*, 179, 107345. https://doi.org/10.1016/j.comnet.2020.107345

Śliwa, J., & Suchański, M. (2022, September). Security threats and countermeasures in military 5G systems. In 2022 24th International Microwave and Radar Conference (MIKON) (pp. 1–6). IEEE. https://doi.org/10.23919/MIKON54304.2022.9816665

Şahiner, M. K., Ayhan, E., & Önder, M. (2021). Yeni sınır güvenliği anlayışında Yapay Zekâ yönetişimi: Fırsatlar ve tehditler. *Ulisa: Uluslararası Çalışmalar Dergisi*, 5(2), 83–95.

Şeker, E. (2020). Yapay Zekâ tekniklerinin / uygulamalarının siber savunmada kullanımı. *UBGMD*, 6(2), 108–115.

Şen, Y. F., & Yurtoğlu, D. (2020). Teknoloji ve Güvenlik İlişkisi Bağlamında Yapay Zekânın İstihbarat Analizindeki Önemi. *Güvenlik Çalışmaları Dergisi*, 22(1), 24–48.

Tamer, H. Y., & Övgün, B. (2020). Yapay Zekâ Bağlamında Dijital Dönüşüm Ofisi. *Ankara Üniversitesi SBF Dergisi*, 75(2), 775–803. https://doi.org/10.33630/ausbf.691119

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2021). Ulusal Yapay Zekâ Stratejisi (2021–2025). https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf (Erişim tarihi: 2 Nisan 2025)

The Defense Post. (2024, April 16). UK military 'not yet fully prepared' for AI integration: Minister. https://www.thedefensepost.com/2024/04/16/uk-military-ai-readiness-cartlidge/ (Erişim tarihi: 9 Nisan 2025)

Tian, N., Lopes da Silva, D., Liang, X., & Scarazzato, L. (2024, April). Trends in world military expenditure, 2023. Stockholm International Peace Research Institute (SIPRI). https://www.sipri.org/sites/default/files/2024-04/2404_fs_milex_2023.pdf (Erişim tarihi: 13 Nisan 2025)

Türkiye Yapay Zekâ İnisiyatifi. (2024). Nisan 2024 Yapay Zekâ Girişimleri Haritası. https://turkiye.ai/turkiye-yapay-zeka-inisiyatifinin-nisan-2024-yapay-zeka-girisimleri-haritasi-yayinlandi/ (Erişim tarihi: 23 Nisan 2025)

UK Ministry of Defence. (2025, April 4). Government response to Developing AI capacity and expertise in UK Defence (HC 812). House of Commons Defence Committee. https://committees.parliament.uk/publications/44284/documents/215290/default/ (Erişim tarihi: 7 Nisan 2025)

Varhan, O. (2024). Türk Savunma ve Havacılık Sanayiinde Döngüsel Ekonomi ve Ürün Yaşam Döngüsü Yönetimi: Yapay Zekâ Destekli Uygulama Örnekleri. *Ege Üniversitesi Ulaştırma Yönetimi Araştırmaları Dergisi*, 1(1), 35–59.

Yılmaz, V. (2024). Sending pictures over radio systems of the trail cam in border security and directing UAVs to the right areas. *Communications Faculty of Sciences University of Ankara Series A2-A3: Physical Sciences and Engineering*, 66(2), 214–227. https://doi.org/10.33769/aupse.1438139

Yavuz Aksakal, N., & Ülgen, B. (2021). Yapay Zekâ ve Geleceğin Meslekleri. *TRT Akademi*, 6(13), 834–853. https://doi.org/10.37679/trta.969285

Zhang, Z., & Li, J. (2023). A Review of Artificial Intelligence in Embedded Systems. *Micromachines*, 14(5), 897. https://doi.org/10.3390/mi14050897

ZNA Teknoloji. (2024, March 7). Yapay Zekâ Destekli Güvenlik Sistemleri. https://www.znateknoloji.com/yapay-zeka-destekli-guvenlik-sistemleri-2024 (Erişim tarihi: 15 Nisan 2025)