International
SOCIAL SCIENCES STUDIES Journal
Open Access Refereed E-Journal & Indexed & Publishing
e-ISSN: 2587-1587

RESEARCH ARTICLE
Political Science and International Relations

Savunma Sanayisinde Yapay Zekâ Tabanlı Sistemlerin Kullanımı: Riskler, Sınırlar ve Güçlendirme Stratejileri

The Use of Artificial Intelligence-Based Systems in the Defense Industry: Risks, Limitations, and Enhancement Strategies

Hazerfen Gültekin [1]

ÖZET

Dijitalleşme sürecinin hızlanmasıyla birlikte savunma sanayii, siber uzayı da içeren çok katmanlı bir güvenlik ekosistemi hâline gelmiştir. Bu dönüşümde yapay zekâ tabanlı sistemlerin tehdit tespiti, karar destek, otonom platform yönetimi ve istihbarat faaliyetleri gibi kritik alanlarda giderek daha yoğun biçimde kullanıldığı görülmektedir. Bununla birlikte, yapay zekâ temelli çözümlerin veri güvenliği, model manipülasyonu ve etik yönetişim gibi risk alanlarını da beraberinde getirdiği anlaşılmaktadır. Bu çalışmanın amacı, savunma sanayiinde kullanılan yapay zekâ tabanlı sistemleri siber güvenlik perspektifinden incelemek; bu sistemlerin sunduğu fırsatları, barındırdığı riskleri ve güçlendirme stratejilerini bütüncül bir çerçeve içinde ortaya koymaktır. Elde edilen bulgular, yapay zekânın savunma sanayiinde tehdit tespit hızını ve karar verme kapasitesini önemli ölçüde artırdığını; ancak model güvenliği, veri bütünlüğü, şeffaflık ve kurumsal yönetişim eksikliklerinin yüksek güvenlik risklerine yol açabildiğini göstermektedir. Türkiye örneği üzerinden yapılan değerlendirmede ise savunma sanayiinin ekonomik ve teknolojik kapasitesinin hızla arttığı, proje portföyünün 1.100'ün üzerine çıktığı ve yerli katkı oranının %80 seviyesine ulaştığı; bu gelişmelerle paralel olarak yapay zekâ tabanlı savunma çözümlerinin ekosistemde stratejik bir bileşen hâline geldiği belirlenmiştir. Sonuç olarak çalışmada, savunma sanayiinde yapay zekâ tabanlı sistemlerin güvenli ve sürdürülebilir biçimde kullanılabilmesi için teknolojik güçlendirme, insan–makine iş birliği, veri yönetişimi ve etik-temelli yönetişim ilkelerini kapsayan entegre bir güvenlik doktrininin gerekliliği vurgulanmaktadır. Bu çerçeve hem mevcut risklerin yönetilmesine hem de savunma alanında sorumlu yapay zekâ kullanımının kurumsallaşmasına katkı sağlama potansiyeli taşımaktadır.

Anahtar Kelimeler: Yapay zekâ, Siber güvenlik, Savunma sanayisi, Otonom sistemler, Türkiye savunma ekosistemi.

ABSTRACT

With the acceleration of digitalization, the defense industry has transformed into a multi-layered security ecosystem that also encompasses cyberspace. In this transformation, artificial intelligence-based systems have been increasingly utilized in critical domains such as threat detection, decision support, autonomous platform management, and intelligence activities. However, it is also understood that AI-driven solutions introduce new risk dimensions, including data security, model manipulation, and ethical governance. The aim of this study is to examine AI-based systems used in the defense industry from a cybersecurity perspective and to present, within a holistic framework, the opportunities offered by these systems, the risks they entail, and the strategies required to strengthen them. The findings indicate that artificial intelligence significantly enhances threat detection speed and decision-making capacity in the defense sector; however, deficiencies in model security, data integrity, transparency, and institutional governance may lead to serious security vulnerabilities. An evaluation based on the case of Türkiye further demonstrates that the economic and technological capacity of the national defense industry has increased rapidly, the project portfolio has exceeded 1,100 programs, and the localization rate has reached %80. Parallel to these developments, AI-based defense solutions have become a strategic component of the defense ecosystem. In conclusion, the study emphasizes the necessity of establishing an integrated security doctrine that incorporates technological reinforcement, human–machine collaboration, data governance, and ethics-based governance principles, in order to ensure the safe and sustainable use of AI-based systems in the defense industry. Such a framework is considered to hold significant potential both for managing existing risks and for institutionalizing responsible AI use in the field of defense.

Keywords: Artificial intelligence, Cybersecurity, Defense industry, Autonomous systems, Turkey's defense ecosystem.

How to Cite This Article
Gültekin, H. (2026). Savunma sanayisinde yapay zekâ tabanlı sistemlerin kullanımı: riskler, sınırlar ve güçlendirme stratejileri. *International Social Sciences Studies Journal*, (e-ISSN:2587-1587) 12(2), 316-325. DOI: https://doi.org/10.5281/zenodo.18818997

Arrival: 19 January 2026
Published: 28 February 2026

GİRİŞ

Dijitalleşme sürecinin hızlanmasıyla birlikte güvenlik alanı, yalnızca kara, hava, deniz ve uzay boyutlarıyla sınırlı olmayan, siber uzayı da içeren çok katmanlı bir yapıya dönüşmüştür. Kritik altyapılar, askeri ağlar, komuta kontrol sistemleri ve savunma sanayii ekosistemi, giderek daha fazla sayıda yazılım bileşeni, sensör ağı ve bağlantılı platform üzerinden işletilmekte; bu durum siber güvenliği ulusal savunmanın ayrılmaz bir parçası hâline

[1] Dr. TÜBİTAK., Ankara, Türkiye ORCID: 0000-0002-2028-2653

getirmektedir (Sen ve diğerleri, 2022). Söz konusu dönüşümde yapay zekâ, yüksek hacimli veriyi işleme, karmaşık örüntüleri tanıma ve gerçek zamanlı karar desteği sağlama kapasitesi sayesinde hem siber savunma hem de savunma sanayiine yönelik uygulamalarda stratejik bir teknoloji olarak öne çıkmaktadır (Achuthan vd., 2024; Şeker, 2020).

Yapay zekânın siber güvenlikte ve savunma sanayiinde kullanımına ilişkin literatür, bu teknolojinin tehdit tespiti, saldırı sınıflandırma, otonom platform yönetimi ve istihbarat, izleme, keşif faaliyetleri gibi alanlarda önemli avantajlar sunduğunu ortaya koymaktadır (Yarali vd., 2023; Alsadie, 2025). Bununla birlikte, yapay zekâya dayalı sistemlerin veri kalitesine olan bağımlılığı, modellerin manipülasyona açık yapısı ve karar süreçlerindeki şeffaflık eksikliği, savunma bağlamında yeni kırılganlık alanlarının oluşmasına yol açmaktadır (Blowersa ve Williams, 2020; Pawlicki vd., 2024). Savunma sanayiinin yüksek riskli ve geri döndürülemez sonuçlara açık niteliği, bu teknolojik kırılganlıkların etik, hukuki ve stratejik boyutlarının da dikkate alınmasını zorunlu kılmaktadır (Martin, 2022; Taddeo vd., 2019).

Türkiye'de savunma sanayii ekosisteminin son yıllarda önemli bir büyüme ivmesi yakaladığı ve bu büyümenin temel itici güçlerinden birinin yapay zekâ tabanlı teknolojilerin geliştirilmesi ve platformlara entegrasyonu olduğu görülmektedir. Türkiye'nin savunma ve havacılık sanayiindeki toplam ciro hacmi 2023 yılı itibarıyla 15,1 milyar ABD dolarına ulaşmış; sektörde faaliyet gösteren firma sayısı 3.500'ün üzerine çıkmıştır. 2024 yılı savunma harcamaları yaklaşık 25 milyar ABD doları düzeyinde gerçekleşirken, savunma ve havacılık ihracatı da 7,2 milyar ABD doları seviyesine ulaşmıştır (Cumhurbaşkanlığı Yatırım ve Finans Ofisi, 2024). Savunma sanayiine ilişkin proje portföyü incelendiğinde, 2002 yılında 62 olan proje sayısının 2020'li yıllarla birlikte hızla yükselerek 2023 yılında 850'ye, 2024 yılı itibarıyla ise 1.100'ün üzerine çıktığı görülmektedir. Benzer biçimde savunma projelerine ilişkin toplam sözleşme tutarının 2002 yılında yaklaşık 5 milyar ABD doları düzeyinden 2023 yılında 96 milyar ABD dolarına ve 2024 yılında 100 milyar ABD dolarının üzerine yükselmesi, sektördeki ekonomik ve teknolojik kapasite artışının bir diğer göstergesi olarak değerlendirilmektedir. Bununla birlikte, savunma sanayiinde yerli katkı oranının 2014 yılında yüzde 35 düzeyinde iken 2024 yılı itibarıyla yüzde 80 seviyesine ulaşmış olması, Türkiye'nin savunma teknolojilerinde dışa bağımlılığını azaltma yönündeki politika ve yatırımlarının somut bir çıktısı olarak öne çıkmaktadır. Bu ekonomik ve kurumsal büyüme ile paralel biçimde, insansız hava araçları, elektronik harp ve karar destek sistemleri gibi alanlarda yapay zekâ tabanlı çözümler yaygınlaşmış; Türkiye Cumhuriyeti Savunma Sanayii Başkanlığı tarafından yayımlanan Geleceğin Yapay Zekâ Teknolojileri Odak Teknoloji Ağı Sonuç Raporu'nda, yapay zekânın tehdit tespiti, rota optimizasyonu, hedef analizleri ve otonom görev icrası gibi kritik işlevlere giderek daha fazla entegre edildiği ortaya konmuştur. Dolayısıyla Türkiye'de savunma sanayiinin teknolojik dönüşümü, yalnızca üretim ve ihracat kapasitesini artırmakla sınırlı kalmamakta; aynı zamanda yapay zekâ tabanlı askerî sistemlerin güvenli, etik ve sürdürülebilir biçimde yönetilmesine yönelik politika ve araştırma gereksinimlerini de güçlendirmektedir (Cumhurbaşkanlığı Savunma Sanayii Başkanlığı, 2025).

Bu çalışmada, savunma sanayiinde kullanılan yapay zekâ tabanlı sistemler, siber güvenlik perspektifinden hareketle ele alınmaktadır. Çalışmanın amacı, öncelikle yapay zekânın siber güvenlik alanındaki genel kullanım çerçevesini ortaya koymak; ardından savunma sanayiinin dijital dönüşümü bağlamında yapay zekâ tabanlı sistemlerin başlıca kullanım alanlarını, bu sistemlerin doğurduğu risk ve sınırlılıkları ve son olarak da teknolojik, kurumsal ve yönetişim odaklı güçlendirme stratejilerini tartışmaktır. Böylece savunma sanayiinde yapay zekâ tabanlı siber güvenlik sistemlerine ilişkin mevcut bilgi birikiminin sentezlenmesi ve gelecekteki araştırmalar ile politika tartışmaları için bütüncül bir kavramsal çerçeve sunulması hedeflenmektedir.

YAPAY ZEKÂNIN SİBER GÜVENLİK ALANINDA KULLANIMI

Yapay zekâ, siber güvenlik alanında giderek artan karmaşık tehdit ortamı karşısında hem savunma hem de saldırı boyutlarını dönüştüren stratejik bir teknoloji hâline gelmiştir. Özellikle büyük hacimli ve dinamik güvenlik verilerinin insan analistlerin kapasitesini aşması, tehdit tespiti ve olay müdahalesi süreçlerinde yapay zekâ tabanlı otomasyon ve öğrenen sistemlerin kullanımını zorunlu kılmaktadır (Achuthan vd., 2024). Makine öğrenmesi ve derin öğrenme yöntemlerinin zararlı yazılım analizi, davranışsal anomali tespiti ve saldırı sınıflandırma gibi alanlarda önemli performans artışları sağladığı; buna karşılık bu sistemlerin veri kalitesine ve modele yönelik saldırılara karşı kırılgan olabildiği ifade edilmektedir (Blowersa ve Williams, 2020). Yapay zekânın bu çift yönlü etkisi, teknolojinin yalnızca teknik bir araç değil, aynı zamanda güvenlik mimarisinin bütününde yeniden düşünülmesi gereken bir unsur olduğunu göstermektedir (Sen vd., 2022).

Siber güvenlik uygulamalarında yapay zekâ yöntemlerinin karar alma süreçlerine entegre edilmesi hem etkinlik hem de hız bakımından önemli kazanımlar doğurmaktadır. Tehdit istihbaratının otomatik işlenmesi, yüksek hacimli ağ trafiğinin gerçek zamanlı analiz edilmesi ve anomali temelli uyarı sistemlerinin geliştirilmesi, bu kazanımlar arasında öne çıkmaktadır (Şeker, 2020). Bununla birlikte, modellerin "kara kutu" niteliği, güvenlik

profesyonellerinin sistem çıktılarının nedenlerini ve sınırlarını anlamasını güçleştirmekte, bu durum güven ve hesap verebilirlik açısından tartışmaları beraberinde getirmektedir. Açıklanabilir yapay zekâ yaklaşımlarının özellikle güvenlik alanında model kararlarının izlenebilirliğini artırarak denetim ve risk yönetimine katkı sağlayabileceği belirtilmektedir (Rjoub vd., 2023). Benzer biçimde, derin öğrenme ve yapay zekâ tabanlı güvenlik çözümlerinde açıklanabilirlik ve şeffaflık düzeyinin yükseltilmesi, yanlış alarm oranlarının kontrol altına alınması ve insan denetiminin güçlendirilmesi bakımından kritik görülmektedir (Pawlicki vd., 2024).

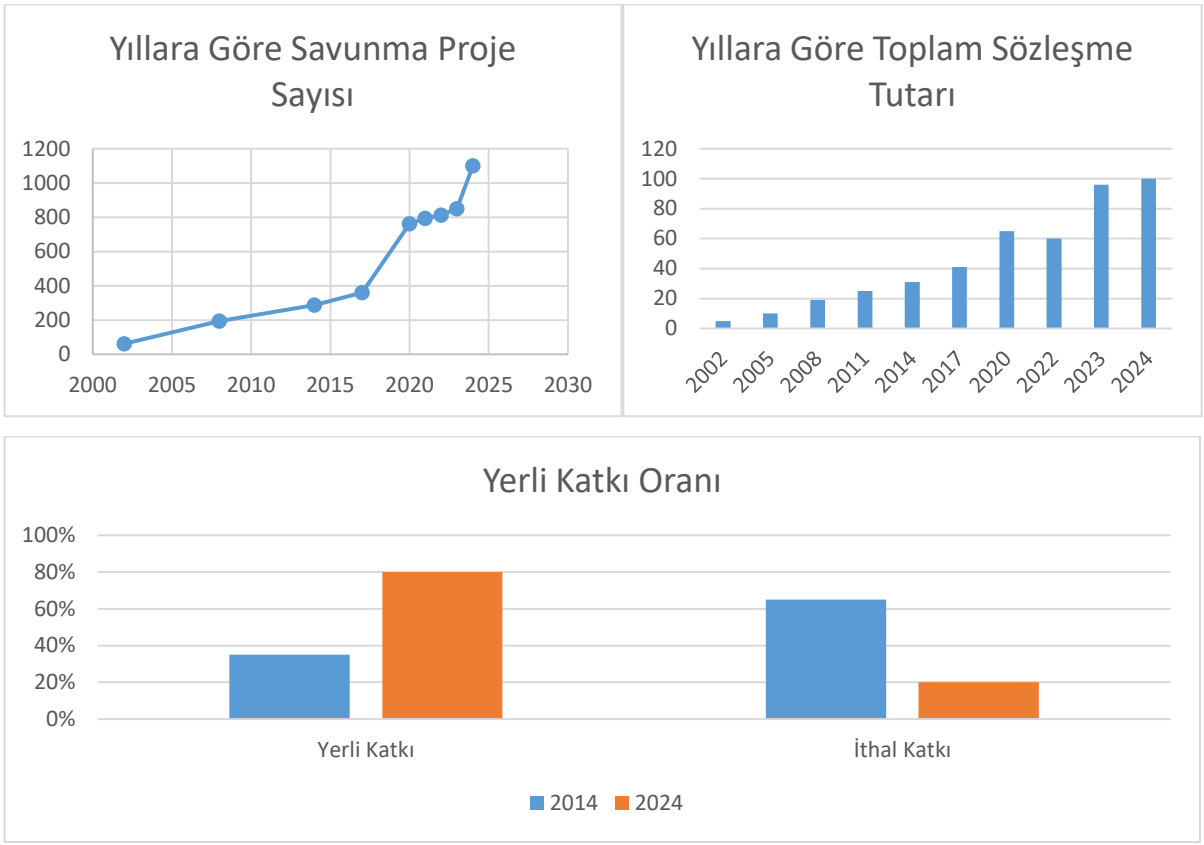
Son olarak, yapay zekânın siber güvenlikteki rolü sadece savunma perspektifi ile sınırlı değildir. Literatürde, yapay zekânın aynı zamanda saldırganlar tarafından da daha sofistike ve hedef odaklı saldırılar geliştirmek amacıyla kullanılabildiği; bu nedenle teknolojinin "çift kullanımlı" bir karakter taşıdığı vurgulanmaktadır (Yarali vd., 2023). Bu durum, yapay zekâ destekli güvenlik sistemlerinin tasarımında yalnızca teknik etkinliğin değil, risklerin öngörülmesi ve yönetilmesinin de zorunlu olduğunu göstermektedir. Dolayısıyla yapay zekâ, siber güvenliğin yerini alan bir mekanizma değil; insan uzmanlığı, yönetişim ve etik ilkelerle birlikte çalıştığında anlamlı ve güvenilir bir bileşen hâline gelen bir destekleyici teknoloji olarak değerlendirilmektedir (Sen vd., 2022).

SAVUNMA SANAYİSİNİN DÖNÜŞÜMÜ

Savunma sanayii, geleneksel olarak yüksek teknoloji yoğunluğu, stratejik bağımlılık riski ve ulusal güvenlik ile doğrudan ilişkili yapısı nedeniyle diğer sektörlerden ayrışan bir konumda yer almaktadır. Günümüzde bu alan, dijitalleşme ve yapay zekâ başta olmak üzere gelişmiş teknolojilerin hızla entegre edildiği bir dönüşüm sürecinden geçmektedir. Ancak bu dönüşüm, yalnızca teknik kapasite artışı ile sınırlı olmayıp aynı zamanda etik, hukuki ve yönetişim boyutlarını da içeren daha geniş kapsamlı bir yeniden yapılanmayı gerekli kılmaktadır (Martin, 2022). Savunma alanında yapay zekâya dayalı karar destek ve otonom sistemlerin yaygınlaşması, teknolojinin etkilerini henüz tam anlamıyla öngöremeden hızlı bir şekilde benimsendiği durumlarda ortaya çıkabilecek geri döndürülemez sonuçlara karşı dikkatli olunmasını zorunlu kılmaktadır. Bu durum literatürde "teknolojik sonuçların öngörülebilirliği ve kontrol edilebilirliği" tartışmaları çerçevesinde ele alınmaktadır (Martin, 2022).

Savunma sanayiinin dijitalleşmesiyle birlikte, siber güvenlik tehditleri askeri kapasitenin ayrılmaz bir parçası hâline gelmiştir. Kritik altyapılara, iletişim ağlarına ve platformlara yönelik saldırıların sayısının ve çeşitliliğinin arttığı; bu saldırıların yalnızca teknik bir zafiyet değil, aynı zamanda ulusal ve uluslararası güvenliğe yönelik stratejik bir tehdit olarak değerlendirildiği ifade edilmektedir (Malatji, 2024). Bu bağlamda yapay zekâ ve makine öğrenmesi temelli çözümler, savunma sektöründe hem operasyonel etkinliği artıran hem de yeni güvenlik risk alanları yaratan çift yönlü bir teknoloji olarak konumlanmaktadır. Dolayısıyla savunma sanayii, yalnızca saldırılara karşı korunması gereken bir alan değil, aynı zamanda teknolojik kapasitenin dönüştürücü etkisini en yoğun biçimde deneyimleyen sektörlerden biri olarak görülmektedir (Sen vd., 2022). Bu çerçevede, yapay zekâya dayalı savunma uygulamalarının yalnızca teknik performans açısından değil, güven ve etik sorumluluk perspektifinden de ele alınması gerektiği vurgulanmaktadır. Yapay zekâ sistemlerine duyulan güvenin koşulsuz ve sınırsız bir kabule dönüşmesi, insan denetiminin zayıflamasına ve beklenmeyen sonuçlara yol açabilecek risklerin artmasına neden olabilmektedir. Bu nedenle güven kavramının, sistemlerin gerçekten güvenilir ve denetlenebilir olmasını önceleyen bir anlayışla yeniden çerçevelenmesi gerektiği savunulmaktadır (Taddeo vd., 2019). Savunma sanayii açısından bu yaklaşım, teknoloji kullanımının sadece etkinlik odaklı değil, aynı zamanda etik ve stratejik denge gözetilerek planlanması gerektiğini göstermektedir.

Türkiye'de savunma ve havacılık sanayii, son on yılda kaydettiği hızlı büyüme ile dikkat çeken stratejik sektörlerden biri hâline gelmiştir. Savunma sanayii iş hacmi yaklaşık üç kat artarak 2023 yılında 15,1 milyar ABD dolarına ulaşmış; sektörün ekosistemi ise 3.500'ün üzerinde firmanın faaliyet gösterdiği geniş bir yapıya dönüşmüştür. Aynı dönemde savunma ve havacılık projelerinde yürütülen çalışmaların etkisiyle Türkiye'nin toplam savunma harcamasının 2024 yılı itibarıyla 25 milyar ABD dolarına ulaştığı belirtilmektedir. İhracat performansındaki artış da bu büyümenin önemli göstergelerinden biridir. Nitekim savunma ve havacılık sektörünün ihracat değeri 2024 yılında 7,2 milyar ABD dolarına yükselerek Türkiye'yi küresel savunma tedarik zincirinin önemli aktörlerinden biri konumuna taşımıştır (Cumhurbaşkanlığı Yatırım ve Finans Ofisi, 2024).



Şekil 1. Türkiye'de Savunma Sanayii Proje Sayısı, Toplam Sözleşme Tutarı ve Yerli Katkı Oranı
Kaynak: Cumhurbaşkanlığı Yatırım ve Finans Ofisi (2025). *Defense & aerospace industry in Türkiye;* https://www.invest.gov.tr/view?path=_tr_library_publications_lists_investpublications_savunma-havacilik-sektoru-raporu.pdf&view=flipbook&page=1 adresinden 31.12.2025 tarihinde erişildi.

Şekil 1'deki grafik seti, Türkiye'nin savunma sanayiinde son yirmi yılda yaşanan yapısal dönüşümü niceliksel olarak ortaya koymaktadır. Yıllara göre savunma projesi sayısındaki artış incelendiğinde, 2002 yılında 62 olan proje portföyünün 2024 yılı itibarıyla 1.100'ün üzerine çıktığı ve böylece proje çeşitliliği ile kurumsal kapasitenin belirgin biçimde genişlediği görülmektedir. Buna paralel olarak toplam sözleşme tutarının da aynı dönemde kademeli bir artış göstererek 100 milyar ABD dolarını aşması, savunma sanayiinin ekonomik ölçeğinin stratejik bir büyüklüğe ulaştığını göstermektedir. Üçüncü grafikte yer alan yerlilik oranı ise bu niceliksel büyümeye eşlik eden niteliksel dönüşümü yansıtmaktadır. Nitekim 2014 yılında yüzde 35 düzeyinde olan yerli katkının 2024 yılına gelindiğinde yüzde 80 seviyesine yükselmesi hem teknoloji geliştirme kapasitesinin güçlendiğine hem de dışa bağımlılığın azaldığına işaret etmektedir. Birlikte değerlendirildiğinde bu göstergeler, Türkiye'nin savunma sanayii ekosisteminin yalnızca hacim olarak büyümediğini, aynı zamanda yerli üretim ve teknolojik yeterlilik temelli bir olgunlaşma sürecine girdiğini göstermektedir.

Bu veriler, Türkiye'nin savunma sanayii alanında teknolojik kapasitesini ve küresel pazardaki varlığını güçlendirdiğini; sektördeki kurumsal ve üretim altyapısının ise giderek daha olgun ve rekabetçi bir yapıya kavuştuğunu göstermektedir. Türkiye'nin savunma sanayii ekosisteminde yaşanan bu büyüme ve teknolojik olgunlaşma süreci, yapay zekâ tabanlı askerî sistemlerin geliştirilmesi ve operasyonel kapasiteye entegre edilmesiyle somut bir görünüm kazanmıştır. Bu çerçevede aşağıda, Türkiye'de savunma sanayiinde kullanılan seçili yapay zekâ tabanlı sistemler örnekleyici nitelikte sunulmaktadır.

Tablo 1. Türkiye'de savunma sanayiinde yapay zekâ tabanlı seçili sistemler

Sistem Adı	Geliştirici	Sistem Tipi	Yapay Zekâ Özellikleri
İHA Elektronik Destek Podu	TÜBİTAK BİLGEM	İHA Podu	Tehdit radarlarının tespiti ve konumlandırılması için yapay zekâ destekli algoritmalar
İHA Elektronik Harp Podu	TÜBİTAK BİLGEM	İHA Podu	Çoklu tehdidi aynı anda tespit ve karıştırma için yapay zekâ destekli algoritmalar
MILKED-3A3	ASELSAN	Mobil ED Sistemi	Düşman iletişimlerinin tespiti, analizi, konuşma ve konuşmacı tanıma
ANTIDOT Serisi Podlar	ASELSAN	İHA Podu	Tehdit tanımlama ve karıştırma için yapay zekâ yetenekleri
KORAL	ASELSAN	Kara Konuşlu elektronik taaruz Sistemi	Düşman radarlarını karıştırma ve yanıltma
HAMLE	ASELSAN	Komutan Asistanı	Taktik seviyede hareket tarzı önerileri için pekiştirmeli öğrenme

Bayraktar TB2T	BAYKAR	SİHA	Arazi referanslı görsel seyir, otonom kalkış/iniş, hedef analizi, acil durumda üsse otomatik dönüş
TOGAN	STM	Taktiksel İHA	GPS olmayan ortamlarda yapay zekâ ile navigasyon
Kargu-2	STM	Kamikaze İHA	Otomatik hedef seçimi ve yüz tanıma için yapay zekâ
Kemankeş	BAYKAR	Mini Akıllı Seyir Füzesi	Otonom uçuş için yapay zekâ destekli otopilot

Kaynak: Cumhurbaşkanlığı Savunma Sanayii Başkanlığı, 2025. https://arge.ssb.gov.tr/TeknolojiYolHaritalari/PublishingImages/Sayfalar/GYZT%20OTA%C4%9E/GYZT_OTAG_Sonuc_Raporu.pdf adresinden 31.12.2025 tarihinde erişildi.

Tablo 1'de Türkiye'de savunma sanayiinde yapay zekâ tabanlı çözümlerin yalnızca tekil bir alana değil, elektronik harp, elektronik destek, karar destek ve otonom mühimmat gibi çok farklı sistem tiplerine yayıldığını göstermektedir. TÜBİTAK BİLGEM tarafından geliştirilen pod sistemlerinde yapay zekâ, tehdit radarlarının tespiti, konumlandırılması ve aynı anda çoklu tehdidin karıştırılması gibi hassas görevlerde kullanılırken, ASELSAN imzalı sistemlerde hem düşman iletişimlerinin analizi hem de taktik seviyede komutana öneri sunan karar destek uygulamaları ön plana çıkmaktadır. BAYKAR ve STM tarafından geliştirilen insansız hava araçları ve kamikaze platformlarda ise yapay zekâ, otonom kalkış ve iniş, hedef analizi, hedef seçimi, yüz tanıma ve GPS olmayan ortamlarda seyrüsefer gibi operasyonel kabiliyetleri güçlendirmektedir. Böylece yapay zekânın, sensör verisinin anlamlandırılmasından taktik karar üretimine kadar tüm görev zincirine nüfuz eden hem kuvvet çarpanı hem de yeni risk alanları yaratan temel bir bileşen hâline geldiği izlenmektedir.

SAVUNMA SANAYİSİNDE YAPAY ZEKÂ TABANLI SİSTEMLERİN KULLANIM ALANLARI

Otonom Sistemler

Savunma sanayiinde yapay zekâ tabanlı sistemlerin kullanımının en görünür olduğu alanlardan biri otonom ve yarı otonom platformlardır. Özellikle insansız hava araçlarında yapay zekâ ile desteklenen algılama, hedefleme ve rota optimizasyonu gibi işlevler, operasyonel etkinliği ve görev esnekliğini önemli ölçüde artırmaktadır. Bununla birlikte bu sistemlerin otonomi düzeyinin yükselmesi, komuta-kontrol bağımlılığının azalması ve gerçek zamanlı kararların makine tarafından verilmesi gibi faktörler, güvenlik ve etik açıdan yeni tartışma alanları doğurmaktadır (Alsadie, 2025). Otonom sistemlerin yapay zekâ bileşenleri, hem siber saldırıların hedefi hâline gelmekte hem de saldırgan aktörler tarafından daha karmaşık tehditler üretmek amacıyla kullanılabilmektedir. Bu durum, savunma odaklı otonom platformların yalnızca fiziksel tehditlere değil, aynı zamanda çok katmanlı siber risklere karşı da dayanıklı biçimde tasarlanmasını gerektirmektedir (Santoso ve Finn, 2024).

Otonom sistemlerde kullanılan gömülü yazılım ve donanımların güvenliği, savunma sanayiinde kritik önem taşımaktadır. Yapay zekâ temelli saldırı tespit ve önleme mekanizmalarının bu sistemlere entegrasyonu, siber saldırıların etkisini azaltmak ve operasyonel sürekliliği güvence altına almak açısından stratejik bir gereklilik olarak değerlendirilmektedir (Oun vd., 2025). Bununla birlikte, otonom platformlarda yapay zekâ tabanlı güvenlik çözümlerinin yüksek doğruluk oranları üretmesine rağmen, model güvenliği, veri bütünlüğü ve açıklanabilirlik gibi alanlarda çeşitli zayıflıkların varlığını sürdürdüğü ifade edilmektedir. Bu nedenle otonom savunma sistemlerinin yalnızca tespit odaklı değil, aynı zamanda erken uyarı ve önleyici güvenlik mimarileriyle desteklenmesi gerekmektedir (Serrano, 2025). Sonuç olarak, otonom sistemlerde yapay zekâ kullanımı savunma kapasitesini artıran belirleyici bir unsur olmakla birlikte, teknolojik üstünlük ile güvenlik kırılganlığı arasındaki hassas dengeyi yönetmeyi zorunlu kılmaktadır. Hem sistem tasarımında hem de operasyonel kullanımda, insan denetiminin ve çok katmanlı güvenlik yaklaşımlarının korunması, bu alandaki risklerin azaltılmasında temel bir ilke olarak öne çıkmaktadır (Santoso ve Finn, 2024; Alsadie, 2025).

Karar Destek Sistemleri

Savunma sanayiinde yapay zekâ tabanlı karar destek sistemleri, özellikle karmaşık ve yüksek belirsizlik içeren operasyonel ortamlarda komutan ve analistlere daha hızlı ve veri temelli değerlendirme yapma olanağı sunmaktadır. Kritik enerji altyapıları, geniş ölçekli ağ yapıları ve çok kaynaklı tehdit istihbaratının analizinde yapay zekâ uygulamalarının, insan operatörlerin tek başına yönetmekte zorlanacağı veri yoğunluğunu işleyerek anlamlı çıktılar üretebildiği görülmektedir (Govea vd., 2024). Bu kapsamda yapay zekâ, yalnızca tehdit tespitinde değil, aynı zamanda risk önceliklendirme ve savunma kaynaklarının dağıtılması gibi alanlarda da karar süreçlerini destekleyen stratejik bir araç hâline gelmektedir (Achuthan vd., 2024). Bununla birlikte karar destek sistemlerinin güvenilirliği, kullanılan verilerin doğruluğu ve model çıktılarının insan denetimiyle birlikte değerlendirilmesi gerekliliği ile yakından ilişkilidir. İnsan kararının tamamen dışlandığı sistemlerin savunma bağlamında öngörülemeyen sonuçlar doğurabileceği vurgulanmakta; bu nedenle yapay zekâ tabanlı karar destek yaklaşımlarının insan uzmanlığıyla birlikte çalışacak şekilde tasarlanması gerektiği belirtilmektedir (Şeker, 2020).

Operasyonel Güvenlik Sistemleri

Yapay zekâ temelli operasyonel güvenlik sistemleri, savunma sanayiinde ağ güvenliği, platform güvenliği ve gömülü sistemlerin korunması gibi kritik alanlarda giderek daha yaygın şekilde kullanılmaktadır. Özellikle otonom ve bağlantılı savunma platformlarında, saldırı tespit sistemlerinin yapay zekâ ile güçlendirilmesi, karmaşık ve düşük izli tehditlerin belirlenmesinde önemli bir üstünlük sağlamaktadır (Dangwal vd., 2024). Benzer biçimde oltalama ve sahte web içeriklerinin belirlenmesine yönelik yapay zekâ modelleri, savunma kurumlarının bilgi güvenliği kültürünün desteklenmesi ve personelin maruz kaldığı siber risklerin azaltılmasına katkı sunmaktadır (Güner ve Takgil, 2025). Bununla birlikte, derin öğrenme tabanlı güvenlik çözümlerinin hem IoT hem de gömülü sistemlerde yüksek doğruluk oranları üretebildiği, ancak bu sistemlerin de kendi içinde model manipülasyonu ve veri güvenliği riskleri taşıdığı ifade edilmektedir (Serrano, 2025). Bu nedenle savunma sanayiinde kullanılan gömülü ve kritik sistemlerin, yalnızca yazılım değil donanım düzeyinde de korunması ve yapay zekâ tabanlı güvenlik çözümlerinin çok katmanlı bir mimari içinde konumlandırılması gerekmektedir (Oun vd., 2025).

İstihbarat

İstihbarat, izleme ve keşif faaliyetleri, yapay zekâ teknolojilerinin savunma sanayiinde en yoğun şekilde konumlandığı alanlardan birini oluşturmaktadır. Yapay zekâ destekli sistemler, insansız hava, kara ve deniz araçlarından elde edilen görüntü, sinyal ve telemetri verilerini gerçek zamanlı olarak işleyebilmekte; bu sayede hedef tespiti, hareket analizi ve anomali belirleme gibi karmaşık süreçler otomatikleştirilebilmektedir (Alsadie, 2025). Bu kapasite, özellikle geniş coğrafi alanlarda yürütülen sürekli gözetleme faaliyetlerinde insan gözüyle fark edilmesi güç olan örüntülerin belirlenmesine ve tehdit unsurlarının erken safhada tespitine olanak sağlamaktadır. Böylece sahaya ilişkin durumsal farkındalık düzeyi artırılmakta, karar mercilerinin daha hızlı ve veri temelli değerlendirmeler yapabilmesi mümkün hâle gelmektedir (Santoso ve Finn, 2024).

Robotik ve otonom sistemlere entegre edilen yapay zekâ çözümleri, ISR (Intelligence, Surveillance, Reconnaissance- İstihbarat, Gözlemleme, Keşif) faaliyetlerinin hızını ve doğruluğunu yükseltmekle birlikte, insan personelin yüksek riskli operasyonlara doğrudan maruz kalmasını da azaltmaktadır. Bu bağlamda yapay zekânın görev planlama, rota optimizasyonu ve risk analizi gibi işlevlerde destekleyici rol üstlenmesi, operasyonel etkinliğin artırılmasına katkı sunmaktadır (Santoso ve Finn, 2024). Denizcilik alanına yönelik çalışmalar ise yapay zekânın liman güvenliği, açık deniz platformlarının izlenmesi ve gemi trafiğinin takibi gibi süreçlerde hem fiziksel hem de siber güvenlik boyutunda kritik rol oynadığını ortaya koymaktadır (Miller vd., 2025). Buna paralel olarak, denizcilik sektöründe yapay zekâ tabanlı siber güvenlik teknolojilerinin karşılaştırmalı olarak ele alındığı araştırmalar, bu teknolojilerin tehdit algılama yeteneğini ve olay müdahale kapasitesini güçlendirdiğini; ancak veri kalitesi, gerçek zamanlı işleme zorunluluğu ve operasyonel koşulların değişkenliği gibi sınırlılıkların dikkatle yönetilmesi gerektiğini vurgulamaktadır (Kumar ve Maharajan, 2024).

Bu çerçevede, istihbarat alanında yapay zekâ kullanımının stratejik üstünlük sağlama potansiyeli taşıdığı, ancak bu sistemlerin güvenilirliği ve sürdürülebilirliğinin veri bütünlüğü, model doğruluğu ve kurumsal denetim mekanizmaları ile yakından ilişkili olduğu söylenebilir. Dolayısıyla yapay zekâ destekli istihbarat uygulamalarında teknolojik gelişmelerin, risk yönetimi ve etik sorumluluk çerçevesiyle birlikte değerlendirilmesi önem taşımaktadır (Alsadie, 2025; Kumar ve Maharajan, 2024).

YAPAY ZEKÂ TABANLI SİSTEMLERDE RİSKLER VE SINIRLILIKLAR

Model Manipülasyonu

Yapay zekâ tabanlı savunma sistemlerinde karşılaşılan en önemli risklerden biri, modellerin kasıtlı olarak yanıltılması ya da çıktılarının manipüle edilmesidir. Özellikle makine öğrenmesi tabanlı saldırı tespit sistemlerinin, küçük fakat hedefli veri oynatmaları ile yanlış sınıflandırmaya yönlendirilebildiği; bu durumun savunma platformlarında kritik sonuçlar doğurabileceği belirtilmektedir (Blowersa ve Williams, 2020). Açıklanabilir yapay zekâ uygulamalarının henüz tam olarak kurumsallaşmamış olması, model kararlarının nasıl alındığının her zaman izlenememesine ve manipülasyon risklerinin geç fark edilmesine yol açabilmektedir (Rjoub vd., 2023). Ayrıca derin öğrenme tabanlı güvenlik sistemlerinde, karşıt saldırılara karşı model direncinin her senaryoda yeterli düzeyde olmadığı ve bu nedenle güvenli mimari tasarımlarının zorunlu hâle geldiği vurgulanmaktadır (Pawlicki vd., 2024). Otonom ve ağ bağlantılı savunma sistemlerinde yer alan yapay zekâ bileşenlerinin, model ve veri manipülasyonuna karşı sertleştirilmemesi durumunda operasyonel bütünlüğün zedelenebileceği ifade edilmektedir (Serrano, 2025; Dangwal vd., 2024).

Veri Güvenliği

Yapay zekâ tabanlı savunma çözümlerinin güvenilirliği, büyük ölçüde kullanılan verinin doğruluğu, bütünlüğü ve güvenliği ile ilişkilidir. Kritik altyapılarda dijital ikiz, sensör ağları ve büyük veri analitiğine dayalı sistemlerin, siber saldırılar yoluyla veri zehirlenmesi ve yetkisiz veri erişimi gibi tehditlere açık olduğu belirtilmektedir (Homaei vd., 2024). Bu durum, yapay zekâ algoritmalarının yanlış ya da manipüle edilmiş verilerle eğitilmesi hâlinde hatalı kararların sistem çapında yayılma riskini artırmaktadır. Enerji ve savunma alanındaki yapay zekâ destekli tehdit tespit sistemlerinde de benzer şekilde veri mahremiyeti ve veri kalitesi kritik bir kırılganlık noktası olarak değerlendirilmektedir (Govea vd., 2024). Oltalama, sahte web içerikleri ve sosyal mühendislik saldırılarının yaygınlaşması, özellikle savunma kurumlarında personel kaynaklı veri sızıntısı ve erişim ihlallerine zemin hazırlayabilmektedir (Güner ve Takgil, 2025). Bu nedenle savunma sanayiinde yapay zekâ tabanlı güvenlik sistemlerinin, veri toplama ve işleme süreçleri de dâhil olmak üzere bütüncül bir güvenlik çerçevesi içinde ele alınması gerektiği vurgulanmaktadır (Şeker, 2020; Malatji, 2024).

Etik Sınırlılıklar

Savunma alanında yapay zekâ kullanımının hızla artması, yalnızca teknik değil aynı zamanda etik ve yönetişim temelli bir tartışmayı da beraberinde getirmektedir. Yapay zekâ sistemlerine duyulan güvenin, sistemlerin gerçekten güvenilir ve denetlenebilir olmasından bağımsız biçimde koşulsuz kabule dönüşmesi durumunda, etik ve hukuki açıdan geri döndürülemez sonuçların ortaya çıkabileceği ifade edilmektedir (Taddeo vd., 2019). Bununla birlikte savunma amaçlı kullanılan yüksek riskli yapay zekâ uygulamalarında, kararların nasıl ve hangi gerekçelerle üretildiğinin tam olarak bilinememesi, şeffaflık ve hesap verebilirlik açısından önemli bir sınırlılık oluşturmaktadır (Martin, 2022). Açıklanabilir yapay zekâ alanındaki mevcut gelişmeler, güvenlik ve etik boyutların güçlendirilmesi için önemli fırsatlar sunmakla birlikte, pratikte henüz standart bir çerçevenin oluşmadığı da vurgulanmaktadır (Rjoub vd., 2023; Pawlicki vd., 2024). Bu nedenle savunma sanayii bağlamında yapay zekâ kullanımının, yalnızca performans ölçütleriyle değil, toplumsal ve etik sorumluluk perspektifiyle de değerlendirilmesi gerekmektedir.

Operasyonel ve Kurumsal Riskler

Yapay zekâ tabanlı sistemlerin savunma sanayiine entegrasyonu, kurumların örgütsel yapıları ve işleyiş süreçleri açısından da çeşitli riskler barındırmaktadır. Özellikle teknolojiye aşırı güven duyulması, insan denetiminin zayıflamasına ve beklenmeyen operasyonel hataların ortaya çıkmasına neden olabilmektedir (Sen, Heim ve Zhu, 2022). Kurumların yapay zekâ çözümlerini benimseme sürecinde teknik yeterlilik, maliyet, yönetsel destek ve yasal uyum gibi unsurlar belirleyici olmakta; bu faktörlerde yaşanan eksiklikler sistemin sürdürülebilirliğini olumsuz etkileyebilmektedir (Kaur vd., 2025). Ayrıca yüksek riskli sektörlerde veri sınırlılığı, gerçek zamanlı işleme gereksinimi ve standart eksikliği gibi etmenler, özellikle denizcilik ve benzeri kritik alanlarda kurumsal karar alma süreçlerini zorlaştırmaktadır (Kumar ve Maharajan, 2024; Miller vd., 2025). Bu çerçevede yapay zekâ, savunma sanayiinde operasyonel verimliliği artıran bir araç olmakla birlikte, kurumsal kapasite ve yönetişim mekanizmaları ile desteklenmediği takdirde yeni kırılganlıklar da yaratabilmektedir (Şeker, 2020).

GÜÇLENDİRME STRATEJİLERİ

Teknolojik Güçlendirme Yaklaşımları

Yapay zekâ tabanlı savunma sistemlerinin güvenli ve sürdürülebilir biçimde kullanılabilmesi, öncelikle teknolojik altyapının çok katmanlı bir güvenlik anlayışıyla güçlendirilmesini gerektirmektedir. Gömülü ve kritik sistemlerde yapay zekâ tabanlı saldırı tespit ve önleme çözümlerinin geliştirilmesi, hem gerçek zamanlı tehdit izleme kapasitesini artırmakta hem de yüksek riskli operasyonlarda sistem dayanıklılığını güçlendirmektedir (Oun vd., 2025). Benzer biçimde robotik ve otonom platformlarda yapay zekâ temelli siber güvenlik çözümlerinin kullanılması, bu sistemlerin fiziksel ve dijital tehditlere karşı birlikte korunmasını zorunlu kılmakta ve güvenlik mimarisinin bütüncül şekilde tasarlanmasını gerektirmektedir (Santoso ve Finn, 2024). Bu çerçevede, yapay zekâ, blokzincir ve bulut bilişim gibi teknolojilerin birlikte kullanılmasıyla merkezi olmayan, daha dirençli ve izlenebilir güvenlik mimarilerinin oluşturulabileceği ifade edilmektedir (Radanliev, 2024). Bununla birlikte, derin öğrenme temelli saldırı tespit sistemlerinin doğruluk düzeylerinin yüksek olmasına rağmen, modellerin kendilerine yönelik manipülasyonlara karşı kırılgan olabildiği ve bu nedenle sürekli test, doğrulama ve güncelleme süreçlerinin kritik bir gereklilik olduğu belirtilmektedir (Serrano, 2025). Otonom ve bağlantılı araçlarda geliştirilen yapay zekâ tabanlı saldırı tespit çözümlerinde de benzer biçimde sistem performansının veri kalitesi ve model sağlamlığıyla yakından ilişkili olduğu vurgulanmaktadır (Dangwal vd., 2024). Ayrıca dijital ikiz ve sensör yoğun altyapılarda yapay zekâ ile birlikte veri bütünlüğünü koruyacak teknolojik önlemlerin alınması gerektiği ileri sürülmektedir (Homaei vd., 2024). Bu yaklaşım, teknolojik güçlendirme stratejilerinin yalnızca yazılımsal değil, sistem mimarisinin tüm katmanlarını kapsayan bir anlayışla ele alınması gerektiğini ortaya koymaktadır.

İnsan-Yapay Zekâ İş birliği

Savunma sanayiinde kullanılan yapay zekâ tabanlı sistemlerin güvenilirliğini artırmanın temel unsurlarından biri, insan ile makine arasında dengeli ve tamamlayıcı bir iş birliği modelinin kurulmasıdır. Kurumların yapay zekâ çözümlerini başarıyla benimsemesi, yalnızca teknik altyapıya değil, aynı zamanda yönetsel destek, çalışan yetkinliği ve örgütsel kültür gibi faktörlere de bağlıdır (Kaur vd., 2025). Bu nedenle yapay zekânın karar süreçlerinde insanı dışlayan değil, insan uzmanlığını destekleyen bir yapı içinde konumlandırılması gerekmektedir. İnsan denetiminin tamamen devre dışı bırakılması, sistemlere aşırı güven nedeniyle kritik hataların göz ardı edilmesine yol açabilmektedir (Sen vd., 2022). Ayrıca literatürde, makine öğrenmesi ve yapay zekâ tabanlı güvenlik çözümlerinin her zaman mutlak ve hatasız sonuçlar üretmediği; özellikle belirsizlik ve veri manipülasyonu koşullarında beklenmedik çıktılar verebildiği vurgulanmaktadır (Blowersa ve Williams, 2020). Bu nedenle güvenlik analistlerinin yapay zekâ sistemlerinin sınırları, önyargıları ve potansiyel hataları konusunda bilinçlendirilmesi, insan-makine etkileşiminin sağlıklı ve eleştirel bir zeminde yürütülmesini sağlayacaktır. Aynı zamanda yapay zekâ uygulamalarının siber güvenlik ve mahremiyet alanlarında sunduğu fırsatların, risk farkındalığı ve güçlü politika çerçeveleri ile değerlendirilmesi de kurumsal kapasitenin önemli bir parçası olarak görülmektedir (Achuthan vd., 2024). Böylece yapay zekâ, savunma sanayiinde insan kararını ikame eden değil, güçlendiren destekleyici bir teknoloji olarak daha güvenli biçimde kullanılabilecektir.

Yönetişim

Yapay zekâ tabanlı savunma sistemlerinin oluşturduğu risklerin yönetilebilmesi için teknik düzenlemelerin ötesine geçen etik ve yönetişim odaklı bir çerçeveye ihtiyaç duyulmaktadır. Yapay zekâ sistemlerine duyulan güvenin, yalnızca performans ölçütlerine değil, aynı zamanda sistemlerin hesap verebilirlik, denetlenebilirlik ve sorumluluk ilkeleriyle uyumuna dayanması gerektiği vurgulanmaktadır (Taddeo vd., 2019). Savunma gibi yüksek riskli alanlarda şeffaflık eksikliğinin, yanlış kararların tespiti ve sorumluluğun belirlenmesini güçleştirdiği; bu nedenle etik yönetişim mekanizmalarının daha da önem kazandığı belirtilmektedir (Martin, 2022). Ayrıca savunma sanayiinin giderek dijitalleşmesi, küresel ölçekte artan siber tehditlerle birleştiğinde, ulusal ve uluslararası düzeyde uyumlu politika ve standart geliştirme ihtiyacını güçlendirmektedir. Kritik altyapılara yönelik saldırıların sayısının ve karmaşıklığının artması, risk değerlendirme ve önleyici güvenlik politikalarının sistematik olarak güçlendirilmesini zorunlu kılmaktadır (Malatji, 2024). Bu bağlamda açıklanabilir yapay zekâ yaklaşımlarının hem etik hem de hukuki boyutlarda hesap verebilirliği artırma potansiyeli taşıdığı; ancak bu alandaki standartların henüz tam anlamıyla olgunlaşmadığı dile getirilmektedir (Rjoub vd., 2023). Dolayısıyla yönetişim, savunma sanayiinde yapay zekâ kullanımının yalnızca teknik düzenleme değil, etik ilkeler, şeffaflık ve kurumsal sorumluluk kültürü ile birlikte ele alınmasını gerektiren bütüncül bir alan olarak öne çıkmaktadır.

Entegre Güvenlik Doktrini

Savunma sanayiinde yapay zekâ tabanlı güvenlik stratejilerinin kalıcı ve etkili olabilmesi için teknoloji, insan ve organizasyonu birlikte ele alan entegre bir güvenlik doktrininin geliştirilmesi gerekmektedir. Bu çerçevede yapay zekâ ile desteklenen çok katmanlı savunma mimarilerinin, yalnızca mevcut tehditlere tepki veren değil, gelecekte ortaya çıkabilecek riskleri de öngörmeye yönelik bir anlayışla tasarlanması önerilmektedir (Radanliev, 2024). Kritik altyapılarda yapay zekâ tabanlı tehdit tespit sistemlerinin başarıyla uygulanabilmesi için veri güvenliği, model güvenliği ve operasyonel güvenlik politikalarının birlikte yapılandırılması gerektiği vurgulanmaktadır (Govea vd., 2024).

Benzer biçimde denizcilik alanında yürütülen çalışmalar, yapay zekâ temelli güvenlik çözümlerinin operasyonel etkinliği artırmakla birlikte, veri kısıtları ve gerçek zamanlı işleme zorunluluğu nedeniyle yeni kurumsal ve teknik gereksinimler yarattığını ortaya koymaktadır (Miller vd., 2025). Savunma amaçlı yapay zekâ uygulamalarında teknolojinin "çift kullanımlı" doğası, bu sistemlerin hem savunma hem de saldırı amaçlı kullanılabileceği gerçeğini gündeme getirmekte; bu durum stratejik risk değerlendirme süreçlerinin önemini artırmaktadır (Yarali vd., 2023). Ayrıca yapay zekâ destekli siber güvenlik çözümlerinin, yalnızca teknik değil, aynı zamanda yönetişim ve etik temelli ilkelerle birlikte ele alınması gerektiği belirtilmektedir (Achuthan vd., 2024; Şeker, 2020). Bu bütüncül yaklaşım, savunma sanayiinde yapay zekânın kontrollü, güvenilir ve sorumlu biçimde kullanılmasını destekleyen kurumsal bir güvenlik kültürünün inşasına katkı sunmaktadır.

SONUÇ

Bu çalışmada yapay zekâ tabanlı sistemlerin savunma sanayiinde giderek artan rolü, siber güvenlik ekseninde kapsamlı biçimde ele alınmıştır. Bulgular genel olarak değerlendirildiğinde, yapay zekânın tehdit tespiti, karar destek, operasyonel güvenlik ve istihbarat süreçlerinde önemli bir kapasite artırımı sağladığı; buna karşılık yeni güvenlik, etik ve yönetişim riskleri de doğurduğu görülmektedir. Özellikle otonom ve ağ bağlantılı savunma

platformlarında yapay zekâ kullanımının yaygınlaşması, bu sistemlerin siber saldırı yüzeyini genişletmekte ve model manipülasyonu, veri bütünlüğünün bozulması ve sistem güvenilirliğinin azalması gibi yeni kırılganlık alanları üretmektedir (Blowersa ve Williams, 2020; Serrano, 2025). Bu durum, yapay zekâ tabanlı savunma uygulamalarında güvenliğin yalnızca teknik değil, bütünsel bir mesele olarak ele alınmasını zorunlu kılmaktadır.

Savunma sanayiinin doğası gereği yüksek riskli ve kritik sonuçlar doğuran karar süreçlerine sahip olması, yapay zekânın bu alandaki kullanımını daha da hassas hale getirmektedir. Güven, hesap verebilirlik ve etik sınırlar bağlamında ortaya çıkan tartışmalar, yapay zekâya mutlak bağımlılığı sorgulayan ve insan denetiminin korunmasını temel ilke olarak vurgulayan bir yönetişim gereksinimine işaret etmektedir (Taddeo vd., 2019; Martin, 2022). Bununla birlikte örgütsel düzeyde benimsemenin, teknik kapasite kadar insan faktörü, kurumsal kültür ve yönetişim çerçeveleriyle de yakından ilişkili olduğu görülmektedir (Kaur vd., 2025). Bu nedenle insan-yapay zekâ iş birliği modelinin dengeli biçimde tasarlanması, savunma sanayiinde sorumlu ve güvenli yapay zekâ kullanımının temel koşulu olarak değerlendirilebilir.

Çalışmanın bir diğer önemli sonucu, yapay zekâ tabanlı savunma sistemlerinde verinin merkezi bir stratejik unsur hâline gelmiş olmasıdır. Veri kalitesi ve güvenliği, model performansını ve saldırılara karşı dayanıklılığı doğrudan belirlemektedir (Homaei vd., 2024; Govea vd., 2024). Veri manipülasyonu ve yanlış yönlendirme riskleri dikkate alındığında, veri yönetişimi, siber güvenliğin ayrılmaz bir bileşeni olarak ele alınmalıdır. Bu noktada hem teknolojik hem de kurumsal düzeyde güçlü denetim mekanizmaları geliştirilmesi gerekmektedir.

Sonuç olarak, savunma sanayiinde yapay zekâ tabanlı sistemlerin güvenli, etik ve sürdürülebilir biçimde kullanılabilmesi için entegre bir güvenlik doktrinine ihtiyaç olduğu söylenebilir. Bu doktrin; teknolojik güçlendirme, insan-makine etkileşiminin dengelenmesi, etik ve hukuki yönetişim ilkelerinin kurumsallaştırılması ve veri güvenliğine dayalı kapsamlı risk yönetiminin birlikte işletilmesini gerektirmektedir (Radanliev, 2024; Achuthan vd., 2024). Böyle bir çerçeve, yapay zekânın savunma sanayiinde sunduğu fırsatlardan en yüksek düzeyde yararlanmayı mümkün kılarken, ortaya çıkabilecek sistemik risklerin de kontrol altına alınmasına katkı sağlayacaktır.

Bu bağlamda gelecekte yapılacak çalışmaların, model güvenliği, açıklanabilirlik, kurumsal yönetişim yapıları ve insan-yapay zekâ etkileşiminin performans ve güvenlik üzerindeki etkileri gibi alanlara odaklanması, literatürdeki önemli boşlukların doldurulmasına ve savunma sanayiinde daha güvenli bir yapay zekâ ekosisteminin geliştirilmesine katkı sunacaktır.

KAYNAKÇA

Achuthan, K., Ramanathan, S., Srinivas, S., & Raman, R. (2024). Advancing cybersecurity and privacy with artificial intelligence: Current trends and future research directions. *Frontiers in Big Data, 7*, 1497535. https://doi.org/10.3389/fdata.2024.1497535

Alsadie, D. (2025). Artificial intelligence-driven unmanned aerial vehicles and cyber threats: A comprehensive review. *Journal of Computer Networks and Communications, 2025*, 8834562. https://doi.org/10.1155/2025/8834562

Blowersa, M., & Williams, C. (2020). Machine learning and cybersecurity: Hype and reality. *IEEE Security & Privacy, 18*(2), 14-20. https://doi.org/10.1109/MSEC.2020.2967500

Dangwal, S., Wazid, M., Nizam, F., Chamola, V., & Das, A. K. (2024). ACID-CAN: Artificial intelligence-based intrusion detection system for CAN-based AIoT vehicles. *Computers & Security, 144*, 103476. https://doi.org/10.1016/j.cose.2023.103476

Govea, J., Gaibor-Naranjo, W., & Villegas-Ch, W. (2024). Threat detection using artificial intelligence in critical energy infrastructure systems: A systematic review and meta-analysis. *Applied Sciences, 14*(2), 665. https://doi.org/10.3390/app14020665

Güner, S., & Takgil, B. (2025). Yapay zeka kullanarak dolandırıcı internet sitelerinin engellenmesi. *Siber Güvenlik ve Dijital Ekonomi Dergisi (Cybersecurity and Digital Economy Journal), 1*(1), 22-28.

Homaei, M. H., Mogollón-Gutiérrez, M., Sancho, J., Avila, C., & Caro, A. (2024). Cybersecurity in digital twins enhanced with artificial intelligence: A survey. *IEEE Access, 12*, 35029-35049. https://doi.org/10.1109/ACCESS.2024.3374021

Kaur, S., Klobucar, T., & Gabrijelcic, T. (2025). Organizational adoption of AI-driven cybersecurity: A TOE framework perspective. *Computers & Security, 140*, 103792. https://doi.org/10.1016/j.cose.2024.103792

Kumar, N., & Maharajan, S. (2024). Comparative analysis of AI based cybersecurity techniques in maritime industry. *International Journal of Intelligent Networks, 5*, 68-76. https://doi.org/10.1016/j.ijinet.2024.01.009

Malatji, M. J. (2024). Understanding CISA cybersecurity alerts through content analysis. *Journal of Cyber Policy, 9*(1), 75-94. https://doi.org/10.1080/23738871.2024.2311730

Martin, K. (2022). Collingridge and the consequences of AI in cybersecurity. *AI and Ethics, 2*(4), 585-592. https://doi.org/10.1007/s43681-022-00149-5

Miller, H., Durlik, M., Kostecka, A., Sokołowska, M., Kozlovska, J., & Zwolak, K. (2025). Artificial intelligence in maritime cybersecurity: A systematic literature review. *Journal of Marine Science and Engineering, 13*(2), 270. https://doi.org/10.3390/jmse13020270

Oun, A. M., Wince, M., Cheng, N., Yu, S., Lee, J.-H., Perez, G. M., Zhang, H., & Shieh, S. (2025). Artificial-intelligence-based cybersecurity for embedded and dependable systems. *IEEE Transactions on Dependable and Secure Computing*. Advance online publication. https://doi.org/10.1109/TDSC.2025.3509940

Pawlicki, M., Pawlicka, A., Kozik, R., & Choras, M. (2024). Advanced insights through systematic analysis: Mapping future research directions and opportunities for xAI in deep learning and artificial intelligence used in cybersecurity. *Neurocomputing, 590*, 127759. https://doi.org/10.1016/j.neucom.2024.127759

Radanliev, P. (2024). Cybersecurity in the metaverse: Artificial intelligence, blockchain and cloud at scale. *Journal of Cybersecurity, 10*(1), tyad045. https://doi.org/10.1093/cybsec/tyad045

Rjoub, G., Bentahar, J., Wahab, O. A., Mizouni, R., Song, A., Cohen, R., Otrok, H., & Mourad, A. (2023). A survey on explainable artificial intelligence for cybersecurity. *IEEE Transactions on Network and Service Management, 20*(4), 5115-5140. https://doi.org/10.1109/TNSM.2023.3282740

Santoso, A., & Finn, D. (2024). AI-driven cybersecurity for robotics and autonomous systems. *Robotics and Computer-Integrated Manufacturing, 87*, 102697. https://doi.org/10.1016/j.rcim.2023.102697

Sen, R., Heim, G., & Zhu, Q. (2022). Artificial intelligence and machine learning in cybersecurity: Applications, challenges, and opportunities for MIS academics. *Communications of the Association for Information Systems, 51*, 179-209. https://doi.org/10.17705/1CAIS.05109

Serrano, D. (2025). CyberAIBot: A deep learning-based IDS framework for IoT cybersecurity. *Sensors, 25*(1), 321. https://doi.org/10.3390/s25010321

Şeker, E. (2020). Yapay zeka tekniklerinin / uygulamalarının siber savunmada kullanımı. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi, 6*(2), 108-115.

T.C. Cumhurbaşkanlığı Savunma Sanayii Başkanlığı, Geleceğin Yapay Zekâ Teknolojileri (GYZT) Odak Teknoloji Ağı (OTAĞ) Sonuç Raporu, 2025; https://arge.ssb.gov.tr/TeknolojiYolHaritalari/PublishingImages/Sayfalar/GYZT%20OTA%C4%9E/GYZT_OTAG_Sonuc_Raporu.pdf adresinden 31.12.2025 tarihinde erişildi.

T.C. Cumhurbaşkanlığı Yatırım ve Finans Ofisi. (2024). *Savunma & Havacılık.* https://invest.gov.tr/tr/sectors/sayfalar/defense-and-aerospace.aspx adresinden 31.12.2025 tarihinde erişildi.

Taddeo, M., McCutcheon, T., & Floridi, L. (2019). Trusting artificial intelligence in cybersecurity is a double-edged sword. *Nature Machine Intelligence, 1*(12), 557-560. https://doi.org/10.1038/s42256-019-0109-1

Yarali, A., Rodocker, E., & Gora, C. (2023). Artificial intelligence in cybersecurity: A dual-nature technology. *2023 International Conference on Computational Science and Computational Intelligence (CSCI)*, 234-240. https://doi.org/10.1109/CSCI62032.2023.00042