Derleme Makalesi

GÜVENLİK VE TEKNİK İSTİHBARATTA YAPAY ZEKA

Cafer ULUÇ[†], Can EYÜPOĞLU[††]

[†] Teknopark İstanbul, İstanbul, Türkiye

[††] Milli Savunma Üniversitesi, Hava Harp Okulu, Bilgisayar Mühendisliği Bölümü, İstanbul, Türkiye

cafer@tutanota.com, caneyupoglu@gmail.com

0000-0003-4756-5757, 0000-0002-6133-8617

Atıf/Citation: Uluç C., Eyüpoğlu C., (2025), GÜVENLİK VE TEKNİK İSTİHBARATTA YAPAY ZEKA, İstanbul Ticaret Üniversitesi Teknoloji ve Uygulamalı Bilimler Dergisi, Cilt 8, No 1, s. 169-183 DOI: 10.56809/icujtas.1638325

ÖZET

Bilinmezden duyulan korku ve endişeyle birlikte -Aristoteles'in Metafizik adlı eserindeki giriş sözünde de yazdığı üzere- *bütün insanlar doğaları gereği bilmeyi arzularlar*. Güvenlik bakış açısıyla yaklaşıldığında, merak etmekten doğan bu bilme isteği, eldeki verileri toplamayı ve bu verilerden fayda üretmek için anlamlı çıktılar üretmeyi hedefler. Bu ifade ile genel bir tanımı yapılan istihbarat, çağın teknolojileriyle bütünleşerek uygulayıcısının elini güçlendirmektedir. Yapay zeka, yaşamın her alanında kendine yer bulmaktadır: Eğitimden tarıma, sağlıktan trafiğe, finanstan afet yönetimine, uzay bilimlerinden siber güvenliğe, kriminalden toplum mühendisliğine, insansız hava/kara/deniz araçlarından sosyal medya platformlarına değin etkin düzeyde kullanılmaktadır. Bu çalışmanın odağında yapay zekanın güvenlik ve istihbarat faaliyetleri bulunmaktadır. Anımsanmalıdır ki, istihbaratın doğası gereği, bu makaledeki konular açık kaynaklara ve akademik yayınlara yansıyan veri ve bilgiler doğrultusunda ele alınmıştır.

Anahtar Kelimeler: Teknik İstihbarat, Yapay Zeka, İstihbarat, Ulusal Güvenlik, Siber Güvenlik

ARTIFICIAL INTELLIGENCE IN SECURITY AND TECHNICAL INTELLIGENCE

ABSTRACT

Along with the fear and anxiety of the unknown -as Aristotle writes in his introduction to his Metaphysics- *all men by nature desire to know*. When approached from a security perspective, this desire to know, which arises from curiosity, aims to collect the available data and produce meaningful outputs to produce benefits from this data. Intelligence, which has a general definition with this statement, strengthens the hand of its practitioner by integrating with the technologies of the age. Artificial intelligence finds its place in every aspect of life: from education to agriculture, from health to traffic, from finance to disaster management, from space sciences to cyber security, from criminal to social engineering, and from unmanned aerial/land/sea vehicles to social media platforms. The focus of this study is on the security and intelligence activities of artificial intelligence. It should be noted that, due to the nature of intelligence, the topics in this article are addressed in line with the data and information reflected in open sources and academic publications.

Keywords: Technical Intelligence, Artificial Intelligence, Intelligence, National Security, Cyber Security

Geliş/Received	**:**	**12.02.2025**
Gözden Geçirme/Revised	**:**	**19.04.2025**
Kabul/Accepted	**:**	**21.04.2025**

1. GİRİŞ

İnternetin sivilleşmesiyle birlikte topluma hızlı biçimde adapte edilen bu teknolojiyle kişisel veriler başta olmak üzere güvenlik riskleri de beraberinde sosyal hayata girmiştir. Kişilerin kendine ait bilgilerini bile isteye internet üzerinden paylaşmaları, istihbaratın temeli olan verinin toplanma ve analiz sürecini de farklı boyutlarda ele alınmasını gerekli kılmıştır. Bu çalışmada da bu değişimin ardılı olan yapay zeka ve teknik istihbaratın bağları ele alınacaktır. Ayrıntılara girmeden önce teknolojinin değiştirdiği ve dönüştürdüğü güvenlik konularına genel bir giriş yapılması uygun görülmüştür.

Değişen ve dönüşen yaklaşımlarla birlikte güvenlik sorunları, geleneksel anlayışta olduğu gibi yalnızca askeri unsurların müdahalesiyle giderilmek istendiğinde sonuçlar yetersiz kalmaktadır. Güvenliğin çok boyutlu bir biçime evrilmesiyle güvenliğe yönelik tehdit ve ihlallerde olduğu gibi güvenliğin sağlanması ve sürdürülmesi de çok yönlü araç ve çok yönlü stratejilerle çevrelenmesi gerekmektedir. Nitekim günümüzdeki ulusal tehditler, tek bir merkezden ibaret değildir; tersine, internetin ve her şeyin internete bağlanabildiği günümüzde olabildiğince merkeziyetsizdir. Üstelik teknolojik gelişimlerle birlikte devlet dışı aktörler teknolojik tabanlı saldırılarda bir devletin siber gücü kadar etkili olabilmektedirler. Literatürde (Altınpınar, 2018) "gizli sınır aşan aktörler" olarak kendine yer bulan bu durumda, yasal bir yaptırım uygulanması ise neredeyse olanaksızdır. Küreselleşmeyle birlikte ulusal güvenlikte yaşanan sorunlar artık kapsamının dışında küresel güvenliğin bir sorunu haline gelmektedir. Yakın coğrafyamızdan bir örnekle Türkiye'nin sınırdaş olduğu ülkelerdeki iç sorunların Türkiye'ye olan yansımaları buna etkili bir örnektir.

Dijital teknolojilerle birlikte iletişim kurmaktan yaşam ve çalışmaya, eğlenceden eğitime değin ciddi bir dönüşüm yaşanmaktadır. 2020'de yaşanan küresel salgın COVID-19 ve sonrasındaki dönüşüm bunun en güncel ve somut örneği olarak etkisini ve dönüşümünü halen sürdürmektedir. 5G teknolojisiyle birlikte uzaktan tıbbi bir ameliyatın dahi yapılacağı gündemdedir. Çalışma gün ve saatleri, öğretimin yöntemi gibi her kesimi ilgilendiren toplumsal paradigmalarda dijital teknolojiler oldukça güçlü bir konumdadır. Bu yönüyle sanal dünya, gerçek dünyadan ayrı olmamakta, yaşanan her gelişme doğrudan fiziki yaşamı etkilemektedir. 2030'lu yıllara doğru giderken insan nüfusunun %90'ının internete bağlı olacağı tahmin edilmektedir (Yanarışık, 2020). Üstelik çevrim içi olanlar yalnızca insanlar değil aynı zamanda internete bağlanabilen nesneler de söz konusudur.

Geleneksel güvenlik faaliyetlerinde olduğu gibi teknoloji tabanlı güvenlikte -örneğin siber güvenlikte- yapay zekanın siber savunma ve saldırı sistemlerine bütünleştirilmesi tercihten öte bir gereklilik arz etmektedir. Siber savunma sistemine entegre edilen yapay zeka ile olası tehditlerin ve yaşanılan saldırıların tespitiyle anında müdahalesi mümkün olmaktadır. Bu yöndeki teknolojiler her ne kadar ileri düzeyde olursa olsun unutulmamalıdır ki güvenlikte en zayıf halka olan insan kadar güçlü olunmaktadır. Geliştirilen ya da geliştirilecek olan sistemlerin yapay zeka ile yarı otonom ya da tam otonom sistemler olması, olabildiğince insan faktörünün (bazı çözümlerde) mümkün ölçüde azaltılması noktasında ifadeler (Şeker, 2020) de mevcuttur.

"Yeni nesil savaş" ile birlikte geleneksel olarak bir savaşın başlangıcı ve bitişi belirsizleşmiş olup kullanılan savaş araç gereçleri de özellikle bilişim teknolojileri tabanlı olarak kendine yer bulmuştur. Beşinci harp sahası olarak nitelenen siber uzay, bir muharebe alanı olarak 7/24 esasına göre barış ve savaş anlarında etkin olarak kullanılmaktadır. Nesnelerin İnternet'i (Internet of Things-IoT), büyük veri ve yapay zeka, gelecek yirmi yılın harp teknolojilerinde en öncelikli ve önem kazanan alanları olacağı alan uzmanlarınca ifade edilmektedir.

Teknolojinin bunca yetenekleri, yalnızca resmi kamu kurum ve kuruluşlarının değil aynı ölçüde terör ve organize suç örgütlerinin ve devlet dışı aktörlerin de ulaşabileceği bir yerdedir. Bugün yasa dışı faaliyet gösteren bu yapılar, yapay zekada olduğu gibi güncel teknoloji kabiliyetlerini donanmaktan geri durmamaktadırlar. Dolayısıyla suç ve suçluyla mücadelede değişen paradigmalar doğrultusunda hareket etmek gerekmektedir (İrdem & Çobanoğlu, 2021). Suçlular, gelişen yeni teknolojilerle birlikte bu teknolojileri suçun icrasında kullanırken yeni suçların da ortaya çıkmasına neden olmaktadırlar (Yanarışık, 2020). "Yeni nesil" suç ve suçlularla "yeni nesil" mücadele zorunluluğu bulunmaktadır (İrdem & Çobanoğlu, 2021). Bir sınırını çizemediğimiz Siber Vatan'ın ve dolayısıyla ulusal güvenliği sağlamanın yolu buradan, yapay zekadan geçmektedir.

Kritik altyapılara yapılabilecek bir saldırıda toplumun büyük kesimi olumsuz etkilenmektedir. Bir hastaneye yapılan saldırıda elektriğin kesildiği, jeneratör gibi acil durumda devreye girecek enerji sistemlerinin de çalışılamaz hale getirildiği senaryoda olacaklar geri dönülmez biçimde olumsuz sonuçlar doğuracaktır. Seçim güvenliğinin siber suçlarla ihlal edilmesi, içme sularının kirletilmesi, iletişim kanallarının bozulması gibi toplumu ve toplum huzurunu doğrudan etkilemek günümüzdeki teknolojik kapasite ile daha bir olası konuma ulaşmıştır (Yanarışık, 2020). Üstelik yapay zeka temelli geliştirilen sistemlerle bu saldırılar kimi zaman otonom olarak dahi

gerçekleştirilebilmektedir. Buradan hareketle siber uzayın güvenliğinin doğrudan doğruya iç güvenliği, buradan da ulusal güvenliği ilgilendirdiği açıkça görülmektedir.

Bilgisayar bilimlerinin alt dallarından biri olan yapay zeka, bir insanın yapabileceği "bazı" görevleri yapabilen bir sistemdir. Bu görevlerin icrasında kimi zaman eşit, kimi zaman daha iyi sonuçlar alınabilmektedir (Şeker, 2020). Elektronik ve mekanik komponentlerin gösterdiği gelişmeler oranındaki etki yapay zekaya da yansımıştır. Sensör, ses ve görüntü gibi mekanik unsurların olabildiğince minyatür boyutlara erişmesiyle birlikte motor ve lityum iyon pillerin ekonomikleşmesi, yapay zeka teknolojilerinin kullanım kolaylığına ve yaygınlaşmasına zemin hazırlamıştır (Ak, 2021). Yapay zeka, internette arama yapıldığında, gelen bir e-postanın zararlı içeriği olup olmadığını anlamada, otomatik olarak ses tanımada, dilden dile çeviride olduğu gibi son kullanıcının bilişim teknolojileri hizmetlerinde etkin olarak kullanılmaktadır. Otonom olarak sürücüsüz otomobillerde, trenlerde, insansız hava araçlarında ise temel güç yine yapay zeka olmaktadır. Yakın gelecekte ise otonom sağlık çalışanlarından (doktor, hemşire, asistan...) hizmet alınması da gündemdedir (Şen & Yurtoğlu, 2020).

Yapay zekanın verileri yüksek hızlı analizi yeteneği özellikle operasyonel alanda -örneğin bir muharebede önceliğin neye göre belirleneceği- anlık veri ya da analiz iletimini sağlayabilmesi sayesinde karar vericinin komuta-kontrolündeki etkinliğine doğrudan katkı sağlamaktadır (Şengöz, 2021). Burada farkında olunmalıdır ki böylesine kritik bir kararı doğrudan doğruya yapay zekaya emanet etmek, mevcut sistemin düşman unsurlarınca ele geçirilmesiyle manipüle edilmeye açık olarak geri dönülmesi olanaksız sonuçlar doğurma potansiyeli taşımaktadır. Operasyonel harekatın planlanmasında yapay zeka, geçmiş ve anlık verileri analiz ederek gerçekleştirilen faaliyetin çerçevesini çıkarabilmektedir. Karar vericiye optimum seçenekleri sunan bir unsur olarak yapay zekanın, karar destek sistemlerinde ciddi kazanımlar oluşturduğu da ortadadır.

Siber uzayın genişlemesi ve bu yolla edinilen verilerdeki çeşitlilik ve veri yoğunluğunda taşınamaz bir yük oluşturmaktadır. Böylesine devasa verinin analizi, uzman personelin (insanın) işlem yeteneğini aşmaktadır (Karasoy, 2022). Bunca veri yükü, insani sınırların çok ötesinde bir sistemi gerekli kılmaktadır (Şen & Yurtoğlu, 2020). Sözün gerçek anlamıyla "dünyanın yükü (verisi)" altında kalmamak adına çağın teknolojik araçlarıyla üretilen verinin aynı yaklaşımla çözümlenmesi gerekir. Nitekim geleneksel yöntemle oluşturulmayan verilerin geleneksel yöntemle karşılanması pratik görünmemektedir. Yapay zeka burada devreye girerek tüm güvenlik alanlarında (bu bir sınır güvenliği ya da siber istihbarat da olabilir) kullanıcısına katma değer üretebilmektedir.

Makale, izleyen bölümlerde yapı olarak şöyle ilerlemektedir: 2. bölümde yapay zekanın nasıl bir durum ve koşulda ortaya çıktığına değinilmektedir. 3. bölümde teknik istihbaratın dönüşümüne odaklanılarak geçmiş ve güncel örnekler üzerinde konu ele alınmaktadır. 4. bölümde yapay zekanın güvenlik ve istihbarattaki kullanımları ele alınarak sınır güvenliği, asayiş, istihbarat ve adli bilişim alanlarındaki kullanımları örneklerle irdelenmektedir. 5. bölümde sonuç olarak makale özetlenmektedir ve 6. bölümde ise yararlanılan kaynaklara yer verilmektedir.

2. HARP SAHASINDA BİR DOĞUM: YAPAY ZEKA

I. ve II. Dünya Savaşları boyunca bilim ve teknolojinin odak noktası ağırlıklı olarak savaştı. Savaşı kazanmaya yönelik bu zorunlu odaklanmanın ise iki ciddi sonucu olmuştu: İlerleyiş ve yıkım (Oruç, 2019). Bilim ve teknoloji alanlarında yaşanan büyük gelişimler kazandığı ilerlemeyle yıkıcı etkisini artırarak aynı oranda can, mal, doğal ve ruhsal kayıplarının yaşanmasına neden olmuşlardır.

Modern anlamda yapay zekanın temelini oluşturan İngiliz matematikçi Alan Turing'in, Almanların kripto iletişim aracı olan Enigma'yı kıracak bir sistem geliştirmesi de II. Dünya Savaşı'nın bir sonucudur. Bu iki büyük savaş döneminde kriptografi makineleri, denizaltı sistemleri, istatistik, fotoğraf makineleri, telsiz cihazlar ve hava araçları "zorunlu bir buluş" olarak ya icat edilmiş ya da var olan teknolojiler ciddi oranda geliştirilmiştir. Bu teknolojiler hem istihbaratta hem de istihbarata karşı koymada etkin biçimde kullanılmaktaydı. Sağlanan faydanın büyüklüğü harp boyunca istihbaratın gücünü ve savaşa olan etkisini ortaya koyarken söz konusu teknolojilerin oluşturacağı katma değer, uygulayıcıların ve karar vericilerin yatırım sağlayacağı bir alan olmaktaydı. Nitekim savaşın galiplerinin ve mağluplarının günümüz teknolojilerindeki hakim gücü, alınan derslerin somut bir çıktısı olarak karşımızda durmaktadır (Oruç, 2019).

II. Dünya Savaşı sonrasında başlayan Soğuk Savaş döneminde ABD, olası bir nükleer tehdide karşın ordunun kendi arasındaki haberleşmesinin kopmaması adına Savunma Bakanlığının ArGe birimi olan Savunma İleri Düzey Araştırma Projeleri Ajansı (Defense Advanced Research Projects Agency-DARPA) öncülüğünde 1960'lı yıllarda İnternet'i icat etti. Ordu içi iletişimi ve istihbaratı üst düzeye taşıyan bu teknoloji zamanla, önce üniversitelere açıldı. Takip eden süreçte, özellikle 1990'lı yıllara gelindiğinde, kamuoyunun kullanımına açılarak "dünyayı saran ağ" haline geldi. Dünyanın en büyük kitlesel yıkımlarının yaşandığı I. ve II. Dünya Savaşlarında korkunç

kayıplarla yorgun düşen uluslar için yeni bir çatışma ortamı (bölgesel çatışmalarla birlikte) siber uzaya taşınmış oldu. Böylece geleneksel savaşların aksine harp sahasına devlet dışı aktörlerin dahli daha mümkün olmuştur. Dahası, bu gibi örgütler, bir devletin erişebileceği teknolojik kabiliyetlerle kendilerini donatabilmekte sorun yaşamamaktadır. Bu durumun temel gerekçesi bilişim teknolojilerinin doğası gereği dinamik bir yaklaşımla hız ve güç kazanmasıdır. Kimi durumlarda kamunun bürokratik ve yasal sınırlamaları olmaksızın hareket edebilen yapılar, devlet dışı aktörlerin siber uzaydaki elini güçlendirmektedir. Buradan hareketle de genelde teknolojinin, özelde internetin bu denli yaygınlaşması ve böylesine üst düzey olanaklar tanımasıyla istihbarat dünyasına yeni bir kavramdan artık söz edebiliyoruz: Siber istihbarat.

Siber istihbaratın günceldeki en büyük kolaylaştırıcısı ise kuşkusuz yapay zeka teknolojileridir. Bir örnekle yakından bakıldığında doğal dil işleme ve diller arası çeviri sistemlerinin geliştirilmesiyle yapay zekanın istihbarat servislerindeki kullanımına değinilebilir: Soğuk Savaş döneminde ABD, Rusya'nın iletişimini deşifre etmek adına Rusçadan İngilizce'ye otonom çeviri imkanına sahip yapay zeka sistemlerinin geliştirilmesine öncelik vermiştir. Söz konusu çeviri, ilgili metinde yer alan sözcüklerin karşılıklarının yazılması ile yapılmamaktadır. Nitekim dil, bir kültürün yapıtaşıdır ve konuşulduğu toprakların geleneğini yansıtır. Dolayısıyla dilden dile çeviri yaparken her iki ülkenin de toplum ve kültür yapısının incelenmesi, çevirinin doğruluğuna doğrudan etki edecektir. Bu da sosyal bilimlerin özellikle insanı ilgilendiren teknolojilerden uzak olmadığına etkin bir örnektir. Bu eksiklikten dolayı çeviri sistemleri, emekleme aşamalarındayken beklentileri karşılayamamıştır. Bu sorun, istihbarat servislerinin kadrolarına dilbilim alanında uzman personellerin istihdamıyla giderilmiştir. Günümüzde devasa boyutlardaki yabancı dillerde yazılan metinlerin oldukça kısa sürede gerek çevirisi gerek analizi yapılabilmektedir. Yapay zeka destekli doğal dil işleme ve çeviri sistemleri her ne kadar ilerlese de -kültürel etkenler dolayısıyla- günün sonunda bir analistin görmesinin gerekliliği alan uzmanlarınca (Oruç, 2019) ifade edilmektedir. Konu istihbarat ve dilbilime gelmişken Milli İstihbarat Teşkilatının "Dil Uzmanı" ünvanıyla alım yaptığına değinmekte yarar vardır.

Tarihsel açıdan Türkiye'ye baktığımızda ise 1991 yılında ülkemizin ilk yapay zeka adı ile açılan bölümü, TÜBİTAK'ın Marmara Araştırma Merkezine (MAM) bağlı olarak kurulan Yapay Zeka Bölümü'dür. Bölüm, MAM olarak Milli Savunma Bakanlığı ArGe Dairesince 1993-1997 yıllarında EUCLID RTP 11.3 projesi kapsamında bir yapay zeka sistemini gerçekleştirmiştir. Proje gereği geliştirilen harp oyunu simülasyonunda 100+ senaryo tasarlanmıştır. 1996 yılında ise Milli Savunma Bakanlığı ArGe Dairesince desteklenen EUCLID RTP 11.7 projesi (Uçuşta Simülasyon) görevi de ilgili bölüm tarafından başarıyla gerçekleştirilmiştir. Söz konusu projede F16 savaş uçağına bütünleştirilebilir simülasyon ile savaş pilotlarının hedeflere yönelik muharebe eğitimleri icra edilebilmektedir (Kocabaş & Öztemel, 1998).

3. TEKNİK İSTİHBARATIN DÖNÜŞÜMÜ

Elçilikler aracılığıyla istihbarat toplanması, günümüzdeki anlamıyla kurulan uluslararası ilişkiler perspektifinden çok önce vardı. Örneğin İtalyanların, 1400'lü yıllarda kurmuş oldukları elçilikler vasıtasıyla başka ülkelerden istihbarat edinmeyi ilk defa sağladıkları ifade edilmektedir (Karasoy, 2022). Venedikli elçilerin, düzenli olarak merkeze ilettiği çeşitli raporlarla aynı zamanda sistematik bir istihbarat ağının kurulmasına da zemin hazırlanmıştır.

I. Dünya Savaşı döneminde kullanımı yaygınlaşan telsiz iletişimi zamanla istihbarat toplama aracı olarak da kullanılmıştır. Sinyal istihbaratı olarak değerlendirilen bu teknoloji özetle "elektromanyetik dalgaların yakalanması ve bu verilerden istihbarat edinilmesi" olarak ifade edilmektedir. I. Dünya Savaşı sürecinde sinyal istihbaratının etkin kullanımıyla elde edilen bir kazanım söz konusudur: Alman ordusunun Rus ordusuna karşın kazandığı doğu cephesi. Üstelik Rus ordusunun Alman ordusundan iki kat büyük olduğu bilinmektedir. Teknolojinin ve insan gücünün bir örneği olan olayda Almanlar, Rusların devasa ordusuna karşın kullandığı ilkel teknolojilerin zafiyetinden yararlandılar. Öyle ki Ruslar, telsizle iletilen mesajlarını şifresiz gönderen altyapı kullanıyorlardı ve Almanların telsiz iletişimini dinleyebileceğini yok saymışlardı. Böylelikle Almanlar, Rusların saldırı planlarını Rus ordusuyla aynı anda öğrenebilmişler, sonuç olarak da kendilerinden sayıca üstün olan Rus ordusunu yenebilmişlerdi (Karasoy, 2022). Bugün, sinyal istihbaratına güncel bir örnek Rusya-Ukrayna Savaşı'ndan verilebilir: Makiivka bölgesinde Ukrayna güçlerince gerçekleştirilen sinyal istihbaratıyla Rus ordusuna mensup askerlerin bulunduğu bir alan tespit edilerek bombalandığı bilinmektedir. Rusya Savunma Bakanlığı, yaptığı resmi açıklamada (Минобороны России, 2023) 63 -kimi kaynaklarda 89- askerin öldüğünü doğruladı. Tespit sırasında olanlar ise şöyle idi: O sırada Rus askerlerinin cep telefonlarıyla sosyal medyaya içerik yükledikleri belirtilmektedir. Nitekim Bakanlık tarafından saldırıya uğramanın nedeni personel tarafından yasağa aykırı olarak cep telefonların açılması ve yoğun biçimde kullanılması olarak ifade edilmektedir (Reuters, 2023).

Sanayi devrimiyle birlikte toplumun yapısı ve yaşayış biçimini değiştiren makineleşmeyle birlikte çatışmanın doğası da bu ölçüde değişime uğramıştır. Bu dönüşüm, literatürde "Dördüncü Nesil Savaş", "Yeni Savaş" ve "Yeni

Nesil Savaş" olarak yer alır. Savaş yaklaşımlarındaki bu değişimin geleneksel olarak güvenlik yaklaşımına (askerin merkezde olduğu güç unsurları) da etki etmiştir. Çatışma, artık cephede konvansiyonel olarak değil bütünüyle tüm kamu kurumlarını ve toplumu hedef alan yapıya evrilmiştir (Karasoy, 2022). Savaşın bu değişen doğası hiç şüphesiz savaşta ve barışta fark etmeksizin düşmana üstün gelmenin anahtarı olan istihbaratı da şekillendirmiştir. Üstelik istihbaratın, ulusal güvenliğin istikrarında her an etkin olması gerekmektedir. Teknik istihbarat ve yapay zekanın geldiği bu noktada dahi istihbaratta insan varlığı, haklı yerini korumaktadır. Nitekim günün sonunda elde edilen veriler, analizi yapılan bilgiler doğrultusunda karar ve hesap verici olan kişi insandır.

Yapay zeka, istihbarat analistinin toplayacağı verilerde, yapacağı sınıflandırma ve analizlerde zaman ve hız açısından pratiklik sağlamaktadır. Yanı sıra yapay zeka, doğal dil işleme, yüz ve ses tanıma, diller arası çeviri yapma, siber uzayda dinleme, izleme ve takip etme gibi yeteneklerle çoğu zaman fiziki takibe gerek bıraktırmadan -bu konuda 4. bölümde bir örnek de verilecektir- gerekli verileri toplayabilmekte, sınıflandırabilmekte, tahminleme ve çıkarımlar yapabilmektedir. Günümüzde sosyal medya istihbaratı oldukça etkili ve geniş ölçekte veri sağlamaktadır. Bugün toplumsal bir hareketlilik önce sosyal medyaya yansımaktadır. Güvenlik güçlerinin yapay zeka destekli sistemleri ilgili platformlardaki verileri toplayarak analiz edebilmektedir. Öte yandan geçmişe dönük verileri de yapay zeka algoritmalarıyla analize dahil edilmesi mümkündür (İrdem & Çobanoğlu, 2021). Kimileri (Şen & Yurtoğlu, 2020), istihbarat açısından sosyal medyayı "bulunmaz bir hazine" olarak yorumlamaktadır. Nitekim sosyal medya, açık kaynak istihbaratının bel kemiğini oluşturmaktadır: Kişilerin birbirleriyle olan bağlantıları, yapılan yorumlar ve beğenilen içerikler, oluşturulan içerikler, kullanılan dil, yapılan yazışmalar.

Kullanıcılar, sosyal medya platformlarında ve anlık yazışma uygulamalarında kendileri ve yakın çevreleriyle ilgili oldukça kritik boyutta bilgilerini paylaşmaktadırlar. İstihbaratın %95'inin açık kaynaktan edinildiği bilindiğine göre (Şen & Yurtoğlu, 2020) internetin istihbarat faaliyetlerindeki boyutu oldukça önem taşımaktadır (UK-RU arasında yaşanan sinyal istihbaratı örneğinde olduğu gibi). Bugün, dünyanın diğer ucundaki bir kişi hakkında istihbarat toplamanın maliyeti yok denecek kadar az olabilmektedir. Oysa internet öncesi dönemde aynı operasyonel faaliyetin gerçekleşmesi için o bölgeyi tanıyan, dilini ve kültürünü bilen ekibin olması ya da bölgede konuşlu personel(ler)in mevcudiyeti gerekirdi. Bu da ek olarak insan ve iş gücünün yanı sıra ciddi zaman ve bütçe demekti. Günümüz teknolojilerinin kapasite ve yetenekleri doğrultusunda siber istihbaratın sunduğu olanaklarla -kimi olaylar için elbette- bir bilgisayar ve birkaç dakika yeterli olabilmektedir (Oruç, 2019). İnternetin nimetlerinin son kullanıcıya neden ücretsiz olarak sunulduğu, tam da bu açıyla bakıldığında açıkça görüldüğü düşünülmektedir.

Yapay zekaya sahip sistemlerdeki algılamalarla olası ya da her an gerçekleşebilecek durumda olan tehditlerin/risklerin tespiti sağlanabilmektedir. Üstelik yapay zeka, söz konusu tehdit ve riskleri düzeylerine göre önceliklendirmekte ve buna göre eyleme geçebilmektedir. Yapay zekanın çıkarımları bir insana göre daha az hata ve daha az maliyet barındırırken yüksek düzeyde hız sağlamaktadır (İrdem & Çobanoğlu, 2021). Her şeyin internete bağlanmasıyla birlikte siber saldırıların yoğunluğu ve hem kamuya hem de topluma yönelik tehditleri de artmaktadır. Dolayısıyla yapay öğrenme (makine öğrenmesi) ve yapay zeka temelli otonom sistemler olası tehditlerin tespitini ve anında müdahalesini otonom yapabilmektedir.

Facebook'a bir fotoğraf yüklendiğinde, fotoğraftaki kişilerin kimler olduğunu söylemesi ya da tanıyor olabilecek kişilerin önerilmesi örneklerinde olduğu gibi ya da bir alışveriş sitesinde müşterinin ilgisini çekebileceğini düşündüğü ürünleri göstermesi ya da YouTube'da izlenilen içeriğe göre video önermesi, Spotify'daki dinlenebilecek müzikler, X'te (Twitter'da) öneri kişi ve gönderiler vd. yapay zekanın günlük yaşamda en çok karşılaşılan örneklerinden birkaçıdır. Bununla birlikte bilinmektedir ki birçok üst düzey teknolojik buluşlar askeri uygulamalar içindir ve sonrasında topluma yayılır. Örnek olarak (STM ThinkTech, 2018), özünde Google'ın otonom aracında kullanılan teknoloji ile bir füzenin ısı izinden hareketle bir hava aracını imha etmesindeki teknoloji benzerlikler taşımaktadır.

İstihbarat faaliyetinin (verinin toplanması, sınıflandırılması, analizi, değerlendirilmesi gibi) bütünüyle siber istihbarat kapsamında yapay zeka yöntemleriyle gerçekleştirilmesi belli oranda mümkündür. Söz konusu bu süreç geleneksel yöntemlere göre oldukça geniş bir alanda, üstelik oldukça düşük maliyette yürütülebilmektedir. Kimi çalışmada (Oruç, 2019) insansız yürütülen bu sürecin insana göre daha az hata payıyla çıkarım yaptığı da kaydedilmektedir.

Günümüzün teknolojik kabiliyetleri doğrultusunda hedefin izlenmesi, dinlenmesi, takip edilmesi oldukça az maliyetli ve yüksek olanaklar sunabilmektedir. Bu doğrultuda istihbarat servisleri özel olarak kulaklık, gözlük gibi günlük yaşamda kullanılagelen nesneleri istihbarat toplama aracına çevirebilmektedirler (Oruç, 2019). Nesnelerin internete bağlanabilmesiyle tüm akıllı cihazlar, kenti saran güvenlik kameraları (esnafın dükkan içi-dışı güvenlik kamerasından KGYS'lere kadar), cebe giren telefonlar, odanın ortasına kurulan televizyonlar, yerleri temizleyen

süpürgeler dahi çevreyi dinleyebilmekte/görüntüleyebilmekte ve "görevi gereği" merkeze iletebilmektedir. Gözetleme faaliyetinin dışında otonom hale gelen cihazlar hedefi tespitinin ardından yine görevi gereği hedefi etkisizleştirme dahi yapabilmektedir.

Çağın petrolü olarak ifade edilen veri, istihbaratın temel yapısını oluşturmaktadır. Örneğin ABD, "İstihbarat Reformu ve Terörizmin Önlenmesi Yasası"nda açıkça belirttiği üzere kaynağına bakılmaksızın yurt içi ve yurt dışından ulusal güvenliği ilgilendiren her türlü veriyi, potansiyel istihbarat olarak görmektedir. Yanı sıra DARPA, yapay zekanın ilk günlerinden beri faaliyetlerinde yapay zekayı -özellikle istihbaratta- desteklemiştir. II. Dünya Savaşı sonrasında başlayan Soğuk Savaş döneminde Sovyetlere karşın dil çevirileri (doğal dil işleme ile) yapay zeka ile yapılmak istenmiş, bu alan için ciddi bütçe ve insan kaynağı yatırımı yapılmıştır. DARPA'nın, yapay zekanın bilimsel bir disiplin olarak ele alındığı yıllarda (1958) kurulmasıyla siber istihbarat başta olmak üzere istihbaratın tüm alanlarında yapay zekanın yer aldığı projeler gerçekleştirmiştir. Günümüzdeki yapısı incelediğinde, ABD İstihbarat Topluluğunun ileri teknoloji araştırmalarını yürüten İstihbarat İleri Araştırma Projeleri Faaliyeti'nin (Intelligence Advanced Research Projects Activity-IARPA) ana görevlerinden ikisi siber güvenlik ve yapay zekadır (Oruç, 2019).

Büyük verinin yapay zeka tarafından toplanması ve sınıflandırılmasıyla birlikte istihbarat analisti, bu gibi rutin sayılan (veri toplama gibi) iş süreçlerine ayırdığı zamanı verinin anlamlandırılmasına, yorumlanmasına ve karara varılmasına ayırabilmektedir. Yapay zeka, büyük veriden yaptığı analizlerle istihbarat analistine analizi yapılmış bilgileri iletmektedir. Analist, elde ettiği çıkarımlarla sonuca ulaşma ve kıymetlendirmeyle birlikte karar verme sürecine odaklanmaktadır. Böylece analist, her gün bir önceki günden daha fazla üretilen veri yükünü yapay zekaya bırakarak zamanını verimli kullanma olanağına sahip olabilmektedirler (Oruç, 2019). Bu noktada şu bilinci de elden bırakmamalı ki bilginin en temel yapısı olan verinin bulanıklaştırılması, çarpıtılması, eksiltilmesi gibi durumlarda ortaya konacak olan çıkarımın ve dönüşümün analiste; onun da karar alıcıya doğru ve isabetli bir çıktı oluşturmayacağı açıktır. Buradan hareketle başlangıç noktası olan verinin edinimi, ondan çıkartılacak anlamlardan daha az önemli olmayıp, dahası, bu yaklaşım da göz önüne alındığında önemi birincil sıradadır.

Bilişim teknolojilerinin -konumuz gereği özelde yapay zekanın- doğası gereği Kara ve Deniz Kuvvetlerinde olduğu gibi niceliği ve baskın gücü fazla olan insan gücüne gereksinim duyulmamaktadır. Dahası siber uzay, birkaç kişilik ekiplerle dahi asimetrik bir çarpan gücüne ulaşabilmektedir. Yapay zekanın da etkin devreye girmesiyle bu durum nüfus olarak düşük ülkelerin işine dahi gelebilmektedir. Bu konuda ABD İstihbarat Direktörü Mike McConnell, ABD'nin elektrik ve ekonomi altyapılarının savunmalarının bozulmasının (hacklenmesinin) bu niyette olan bir ekip için siber uzayın oldukça geniş olanaklar barındırdığını ifade etmesi (Yılmaz, 2020) siber uzayın neden beşinci harp sahası olarak görüldüğünün bir göstergesidir. Bir örnek de Türkiye'den: 2018'de Türk Silahlı Kuvvetlerinin gerçekleştirdiği Zeytin Dalı Harekatının ardından #OpTurkey adı altında ülkemizin kamu kurum ve kuruluşlarına yönelik siber saldırılar yapılmıştır. Saldırıların yapısı ve içeriği analiz edildiğinde varılan noktada siber saldırıları düzenleyen organizasyonla sosyal medya platformlarında sahte haber üretimi, olayların çarpıtılması gibi dezenformasyonların bir merkeze (terör örgütüne) ait olduğu tespit edilmiştir.

İstihbaratın bilimsel bir yaklaşımla incelenmesi ve bu yönde çalışmaların yapılması II. Dünya Savaşından sonraki dönemle başlamıştır (Oruç, 2019). Türkiye özelinde konuya yaklaştığımızda istihbaratın gizemli yönü halen varlığını sürdürürken bu durum bilimsel disiplinden uzak kitap, film, dizi gibi yayınların ortaya çıkmasına neden olmaktadır. İstihbaratın popüler kültürdeki yerinin olumlu sonuçlar doğurduğu da göz ardı edilmemelidir. Nitekim bunca yayın, istihbarat konularının daha görünür hale gelmesine zemin hazırlamıştır (Demircioğlu ve ark., 2021). Bununla birlikte bilimsel içeriklerin artması ve Teşkilat'tan emekli saha deneyimi de olan profesyonel meslek memurlarının akademide yer edinmesiyle yayın üretilmesi gibi gelişmeler de söz konusudur.

4. YAPAY ZEKANIN GÜVENLİK VE İSTİHBARATTAKİ KULLANIMI

Google'ın şirketlerinden olan ve yapay zeka ağırlıklı çalışmalar yürüten Deep Mind, Starcraft adını verdiği oyununu 2016'da duyurmuştur. Oyunda, askeri unsurların komuta ve kontrolüyle oyuncuların aralarındaki mücadelesi işlenmektedir. Oyun içerisinde yapay zekalı oyuncu, ordularıyla gerçek (insan) oyuncularla bir mücadeleye girişmektedir. Deep Mind'ın yaptığı açıklamada (STM ThinkTech, 2018), oyunda karşılaşılan sorunların çözümünü gerçek yaşama uyarladığı ifade edilmektedir. Şirket, yapay zeka temelli geliştirdikleri bu oyunu bir test ortamı olarak kullanmaktadır. Böylece "pekiştirmeli öğrenme" algoritmasıyla yapay zekanın askeri alanda stratejiler geliştirebildiği açıkça görülmektedir.

4.1. Ülkelerin Uygulamalarına Genel Bir Bakış

Teknolojik gelişimlerin hızlandığı ve Soğuk Savaş'ın yaşandığı yıllarda görüldü ki güvenlik, geleneksel yöntem ve çerçevenin dışında bir yaklaşımla sağlanmak durumundadır. Devleti yöneten karar alıcılar böylesine bir hızda

değişen ve gelişen teknolojik gelişimlerle uyumlu olarak gerek iç gerek dış tehditleri önleme, savunma ve savurma ile saldırı kapsamında söz konusu teknolojik araçları ve hizmetleri değerlendirmektedirler. Öyle ki bu durum bir seçenekten çok bir zorunluluk halini almıştır. Nitekim "teknolojik gelişmelerin hızı, insan düşüncesinin önüne geçmeye başlamıştır". 2018'den bu yana devletler, ulusal strateji belgelerinde yapay zekaya yer vermektedirler. Dahası, başlı başına yapay zeka eylem planları dahi kamu tarafında hazırlanıp işe koşulmuştur (İrdem & Çobanoğlu, 2021). Türkiye'nin de duyurduğu Ulusal Yapay Zekâ Stratejisi 2021-2025 bulunmaktadır (T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2021).

Teknolojinin dönüştürücü etkisinde orduların operasyonel kabiliyet ve üstün yönleri değerlendirilirken geleneksel anlamdaki harp silahlarının yanı sıra elektronik harp bileşenleri de dikkate alınmaktadır. Buradan hareketle siber uzay, beşinci harp sahası olarak literatürdeki yerini almıştır. 2016'da Polonya'nın başkenti Varşova'da düzenlenen zirvede siber uzay, NATO tarafından resmi olarak operasyonel bir alan olarak tanımlanmıştır. Günümüzde ABD, siber uzaydaki bir hareketliliği fiziksel den ayrı görmeyeceğini, bir savaş olanı olarak siber uzayı ilan etmiştir (Yılmaz, 2020).

İstihbarat faaliyetleri devletin resmi kurum ve kuruluşlarının yanı sıra resmi olmayan biçimde özel sektör girişimleriyle de sağlanmaktadır. Gelişen teknoloji ihracatı vesilesiyle istihbarat örgütleri, özel sektörün geliştirdiği teknoloji ürün ve hizmetleriyle dünyanın her yerine ulaşabilmektedir. Sosyal medya platformlarının menşei olduğu ülkenin istihbarat servisine veri akışı sağladığı bilinmektedir. Snowden'ın ifşaatları ya da Cambridge Analytica, bu konuda dayanağı olan iki örnektir. Öte yandan Çin'in teknoloji devi Huawei'nin Çin devletince finanse edildiği, hemen hemen diğer ürün ve çözümlerde olduğu gibi, girdiği yerden verileri merkeze aktardığı da yaygın bilinen bir durumdur. ABD istihbarat servislerinin Google ve Gmail'den ilgili merkezlere veri akışının olması gibi Yandex'in de Rus istihbarat servislerine yönelik cömertliği ifade edilmektedir (Oruç, 2019).

Yapay zekanın istihbarat servisine hizmeti yeni değildir. CIA, 1980'li yılların henüz başında iken kurum içi "Yapay Zeka Grubu" kurarak yapay zekanın sunduğu olanaklarla güvenlik, savunma ve istihbaratta nasıl sağlanabilir çerçevesinde diğer kamu kurumlarının katılımlarıyla çalışmalar yapılmıştır. 2020'li yılların ortalarına doğru giderken günümüzdeki istihbarat servislerinin halihazırda yüzlerce yapay zeka temelli projeleri olduğu, bu teknolojik kabiliyetle karşı istihbarat servisinin çalışanlarını izlediği/takip ettiği de bilinmektedir. CIA'dan bir örnekle devam edecek olursak CIA Bilim ve Teknoloji Departmanından Dawn Meyerriecks'in açıklamalarında otuz kadar ülkede bu teknolojilerin etkin olarak CIA tarafından kullanıldığı ifade edilmektedir. İfadeye göre bu teknolojiler öylesine etkili ki direktör yardımcısı Meyerriecks, fiziki anlamda bir takibe gerek duyulmadan "işlerini gördüklerini" söylemektedir. Meyerriecks, istihbarata karşı koyma faaliyetinde yapay zeka ve yapay öğrenmeden yararlandıklarını ifade etmekte ve geliştirdikleri sistem ile operasyonun icrasında büyük kentlerin kamera haritasını çıkardıklarını ve bu bilgiyle istihbarat personelinin ilgili kentin kameralarına karşın önlem alabildiklerini söylemektedir. Bir başka örnekte ise 2016 yılında ABD hükümeti, yapay zekanın kamu kurumlarınca kullanımına ilişkin bildiri yayımlamıştır. ABD güvenlik ve istihbarat servisleri (Federal Bureau of Investigation-FBI, Central Intelligence Agency-CIA, National Security Agency-NSA gibi) bu bildirinin dayanağı ile yapay zeka temelli araştırma ve geliştire projeleriyle birlikte satın alma yoluyla teknik kabiliyete verdiği ağırlığını artırmıştır (Oruç, 2019).

Yapay zekanın güvenlik ve istihbarat alanındaki kullanımına yönelik örneklerin ABD kaynaklı olduğu literatüre yansısa da Çin ve Rusya'nın da bu konudaki yatırımları ve açıkça ilan ettiği hedefleri bulunmaktadır (Oruç, 2019). Bir harekatın planlanması gibi askeri alandaki süreçlerde yapay zekadan yararlanan ülkelerin başında ABD, Rusya ve Çin gelmektedir (Şengöz, 2021; Darıcılı, 2020).

İstihbaratta, savunmada ve silah teknolojilerde yapay zekanın getirilerinin etkin faydasını gören ülkeler arasında bir önde olma rekabeti -Soğuk Savaş dönemindeki uzay sahası gibi- bulunmaktadır. Öyle ki Putin, 2017'de üniversitelilere yönelik gerçekleştirdiği konuşmasında (Oruç, 2019) "yapay zekaya hakim olanın dünyaya hakim olacağını" ifade etmesi bu açık hedefin bir göstergesidir. Rusya, askeri cihazların %30'unu 2025'e kadar robotlaştırmayı hedeflemektedir. Rusya'nın Savunma Güvenlik Kurulu Başkanı Bondarev'in yapay zekanın geleceğin savaşlarında askerin ve pilotun yerini alacağını; askeri alanda kullanılan araç ve sistemlerin yapay zeka tarafından yönetileceği günlerin yakın olduğunu söylemesi yapay zekanın geleceği ve Rusya'nın bu noktadaki hedeflerini ortaya koyması açısından değerlendirilmektedir. 2017'de Fransa, ilan ettiği ulusal savunma stratejisinde yapay zekayı operasyonel üstünlük olarak tanımlamaktadır (Darıcılı, 2020). Çin, 2030'a kadar yapay zeka alanında dünya çapında "birinci inovasyon merkezi" olmayı hedeflemektedir. 2023'te çalışmalarına başlanan DeepSeek (DeepSeek-AI, 2025), 2025'in ilk günlerinde yaptığı çıkış ile ABD kökenli ChatGPT'nin tekelinde bulunan yapay zeka dil modeli alanına ciddi bir alternatif olarak boy göstermiştir. Bu gelişmeyle birlikte denebilir ki Çin, kendisine hedef koyduğu 2030 hedeflerine doğru etkin uygulamalara odaklanmaktadır. DeepSeek'in ortaya çıkışının yalnızca teknolojik bir gelişme olarak görülemeyeceği açıktır. Nitekim ABD Başkanı Trump'ın

danışmanlarından Marc Andreessen'ın DeepSeek-R1 için "yapay zekanın Sputnik anı" yorumu (Hoskins & Imran, 2025) tüm bu çalışmaların aynı zamanda bürokratik, diplomatik, sosyal ve ekonomik etkilerinin bulunduğunu ortaya koyması açısından dikkat çekicidir.

Günümüzde yapay zeka teknolojisi ordular tarafından otonom silahlar çerçevesinde kullanılmaktadır. Örneğin Rus Askeri Sanayii Komitesince onaylanan bir tasarı (İrdem & Çobanoğlu, 2021), bu konuya dikkat çekmektedir: Söz konusu tasarıda Rusya'nın savaş gücünün üçte birlik kısmının bütünüyle otonom sistemler ile donatılmasının 2030'a kadar tamamlanması planlanmaktadır. Bu konu nüfus olarak sorun yaşayan ancak teknolojik olarak ileri olan ülkeler için de bir değerlendirme alanı olarak görülmektedir. Genç nüfusun azlığı nedeniyle Japonya, elindeki üstün sanayii ve teknoloji becerileriyle ulusal güvenliğini sağlama noktasında otonom araç ve sistemleri kullanmaktadır.

2021 yılında T.C. Cumhurbaşkanlığınca yapılan çalışmada (T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi, 2021), gelecek on yılda küresel çapta ve ülkemizde etkisini güçlü olarak gösterecek öncelikli alanlar belirlenmiştir. Bu bağlamda "yapay zeka ve yapay öğrenme, büyük veri ve veri analitiği" teknolojilerinin ekonomiden toplumsal faydaya ve ulusal güvenliğe olan/olacak katkılarına değinilmektedir.

Yapay zekanın gelişmesinin arkasındaki gücün özellikle devletin savunma sanayii ve emniyet kurumlarının araştırma geliştirmeye yönelik finans desteği olduğu ifade edilmektedir (Ak, 2021). Örneğin ABD'li istihbarat servislerinin, istihbaratın bilimsel bir disiplin olarak araştırılması ve geliştirilmesi noktasında üniversitelere destek sağladığı bilinmektedir (Şen & Yurtoğlu, 2020). Bu noktada istihbaratın tüm süreçlerindeki metodolojiler üzerinde akademik çalışmalar yapılmasına önem vermektedir. Dolayısıyla bu desteğin bir diğer çıktısı olarak literatürde ABD odaklı çalışmaların geniş yer tuttuğu görülmektedir.

4.2. Sınır Güvenliği ve Askeri Uygulamalar

Bir ülkenin sınırları, söz konusu ülkenin güvenliğinde ön cephe hattı olarak ifade edilmektedir (Şahiner ve ark., 2021). Dolayısıyla konvansiyonel savaş perspektifinde sınırlar ön cephe olarak yerini korurken yeni nesil teknolojilerle birlikte günümüzde fiziksel sınırlardan da önce siber uzay artık kritik altyapıları ve kamu kurumları ile vatandaşlarının verilerini barındırmasından dolayı öncelikli cephe hattını oluşturmakta, "ilk mermi" önce sanalda atılmaktadır.

Teknolojinin yaşamın her alanına girmesiyle ulusal güvenlik enstrümanları da bu yönde bir değişim/dönüşüm içerisindedir. Bu çok boyutlulukla birlikte ülke sınırlarının güvenliği de salt olarak geleneksel yöntemlerle (kilometreleri bulan duvarlar ve ışıklandırmalar, sınır karakolları, gözetleme kuleleri ve askeri unsurlar vd.) sağlanmasının mümkün olamadığı, gelişen teknolojik yöntemlerle bütünleşik çözümlerin kullanılmasının gerekliliği ifade edilmektedir (Şahiner ve ark., 2021). Nitekim günümüzün yeni nesil savaşlarında bir sınırsızlık söz konusudur. Ülkemizde olduğu gibi sınırlarında sorunlu ülkelerden Türkiye'ye doğru taşınan terörizm, uyuşturucu ve insan kaçakçılığı, yasa dışı göç hareketliliği yaşanmaktadır. Doğrudan iç güvenliği tehdit eden bu gibi unsurlar aynı zamanda ekonomik olarak ülkemizi zor duruma düşürmektedir. Bu ve benzeri açılardan bakıldığında varılan noktada sınır güvenliği, etki alanı içerisindeki olan ülkenin egemenlik haklarının korunması noktasında bir var oluş mücadelesini temsil etmektedir. Sınırlar, ulusal güvenliğin dolayısıyla da ulusal egemenliğin temelini oluşturmaktadır. Bu noktada yapay zeka teknolojileri sözü edilen güvenliğin tüm alanlarıyla bütünleşerek etkin çözümler sunabilen bir teknolojidir.

Peki, yapay zeka sınır güvenliğini sağlamada nasıl iş görebilir? Yapay zeka temelli çözümler (örneğin insansız hava araçlarının devriyesi) tüm gün gerçek zamanlı olarak takip yapabilmekte ve merkeze anında iletebilmektedir. Böylece sınıra yaklaşan terör örgütü mensuplarını ya da yasa dışı geçiş ihlali amacı güden kişilerin tespiti, gerekirse de S/İHA'lar ile engellemesi/etkisiz hale getirilmesi mümkün olabilmektedir. Yanı sıra karar vericiler, sınır güvenliğinde harcanan bütçeyi ve sınıra ayrılan insan gücünü (askeri birlikleri) ülkenin farklı alanlarında daha etkin değerlendirmek istemektedir. Savunma teknolojilerindeki ilerleme, özellikle yapay zekanın sunduğu otonomi, devletlerin bu yöne olan eğilimlerinde gözle görülür bir artış yaşanmaktadır. Bu yönüyle hükümetler, yapay zeka strateji ve eylem planları hazırlamakta ve kamuoyu ile paylaşmaktadırlar. Daha önce sözü edildiği üzere Çin, 2030 yılına kadar yapay zeka teknolojilerinde egemen olmayı devlet politikası olarak ilan ederek bu alanda yapılacak çalışmalar için milyarlarca dolarlık bütçelerle yatırım yapmaktadır. Yatırım yapılan projelere bakıldığında ise ses/yüz tanıma sistemlerinin öncelikli olduğu görülmektedir. Çin, bu sistemleri hem ülke içindeki eyalet sınırlarında hem de ülke sınırlarındaki insan hareketliliğinin izlenmesi ve denetlemesinde kullanmaktadır. ABD tarafında ise Savunma Bakanlığınca yayımlanan Ulusal Savunma Stratejisinde yapay zekanın savaş kabiliyetinin artırımına yönelik uygulamalara yer verilmektedir. Japonya, Fransa ve Hindistan gibi ülkeler de yapay zekada söz ve güç sahibi olma noktasında bir rekabet içerisindedirler. Ülkeler bazında özellikle savunma sanayii çalışmalarında kendine yer edinen yapay zeka, ulusal ve uluslararası ölçekteki strateji ve eylem planlarında

kendine yer bulmaktadır. Nitekim olası bir çatışma ve harp durumunda sivil ya da asker fark etmeksizin insan hayatı doğrudan tehlikededir. Bu durumda kaybın yaşanmamasında ya da az sayı ile durumun savuşturulmasında hareket hızı ve çeviklik önceliklidir. İşbu durumda yapay zeka, karar verme süreçlerinde istatiksel modeller kullanarak karar alıcıya gerekli olan bilgileri elde ettiği geniş veri ağıyla hata payı oldukça az olacak biçimde değerlendirebilmekte, karşılaştırmalı olarak da sunabilmektedir (Şahiner ve ark., 2021).

ABD, Rusya ve Çin'in yapay zeka alanındaki çalışmaları incelediğinde söz konusu ülkelerin askeri sevk ve idare, ulaştırma, karar destek sistemlerindeki otonom çalışmalara olan yatırımları görülmektedir (Ak, 2021). ABD'nin halihazırda yapay zekanın teknik istihbarata olan entegresi bu alanın önemini kavrayan ülkelerce de etkin olarak kullanıldığı görülmektedir. Buna bir güncel örnek de Kore'den: Güney Kore ve Kuzey Kore sınırında insandan arındırılmış bölgede Güney Kore kökenli Samsung'un geliştirdiği SGR-A1 silah sistemi kullanılmaktadır. SGR-A1, güvenlik ve teknik istihbaratta yapay zekanın kullanımına ciddi bir örnek teşkil etmektedir (Oruç, 2019). SGR-A1, ses/görüntü tanıma, izleme, gözetleme gibi işlevlerine ek olarak hedefe yönelik ateş etme görevlerini yapay zeka temelli robotuyla sağlamaktadır. Aynı zamanda bu örnekle birlikte görülmektedir ki yapay zeka, geleceğin savaş aracı olarak robotları nasıl dönüştürmektedir, SGR-A1 bunun açık bir örneğidir. Nöbet sırasında askerlerin zaman içerisinde odaklanmalarında zayıflama olmakta ve performansları düşmektedir. Kimi zaman uyuklamanın da olduğu bilinmektedir. Gayrinizami harp sırasında böylesi bir durumun yaşanmasının bedeli oldukça ağır olmaktadır. Güney Kore, Kuzey Kore'yle olan sınırına 2014 yılında 250 km uzunluğunda, 4 km genişliğindeki insandan arındırılmış bu bölge için geliştirdiği bu koruma sistemiyle hem ısıyı hem de hareketi algılayarak olası tehdit içeren hedefi (insan onayıyla birlikte) etkisizleştirmektedir. Üstelik bu etkisizleştirme 3,2 km uzaktan yapılabilmektedir (STM ThinkTech, 2018).

Güney Kore'de olduğu gibi Hindistan da yapay zeka temelli gözetleme ve ateşleme sistemlerini envanterine katmayı/geliştirmeyi hedeflemektedir. Nitekim Çin ve Pakistan ile uzun sınırlara sahip olan Hindistan, otonom ve insansız hava/kara/deniz araçlarıyla sınırlarını, dolayısıyla ülkesini korumayı istemektedir. Bu amaçla Hindistan Japonya ile yapay zeka alanında iş birliği içerisinde çalışmaktadırlar. Üstelik, bu iş birliği insansız kara ve hava araçları, robotik sistemler gibi askeri alanı kapsamaktadır (Türe & Topuz, 2020). Gittikçe dünya çapında yaygınlaşan yapay zeka temelli savunma sistemlerine bir diğer örnek de Avrupa Birliğinden: Birlik, geliştirdiği iBorderCtrl (Intelligent Portable Control System) projesiyle sınır geçişlerindeki noktalarda yalan tespitini yapmayı hedeflemektedir. iBorderCtrl sistemi (Şahiner ve ark., 2021), Macaristan, Yunanistan ve Letonya arasındaki dört sınır geçiş noktalarında halihazırda kuruludur.

Google'ın üst kuruluşu olan Alphabet'in bir hizmeti olan Kaggle, ABD İç Güvenlik Departmanı ve Ulaştırma Güvenlik Yönetimi'nden edindiği verileri işlemekte ve böylelikle bir yolcunun çantasında/bagajında yasa dışı ve/veya sakıncalı nesnelerin denetimini yapmaktadır (İrdem & Çobanoğlu, 2021). İç güvenliğin sağlanması noktasında bir diğer örnek de sınır güvenliği açısından verilebilir. Ulusal güvenlik genelinde, iç güvenlik özelinde yönetimlerin güvenlik politikalarında, vatandaşın güvenliğini sağlarken teknolojinin tüm yaşama entegresiyle birlikte başta dijitalde tutulan kişisel verilerin korunmasına yönelik uygulamaları bulunmaktadır. Örneğin yüz ve parmak tanıma sistemleri, güvenlik/gözetleme/denetim kameraları gibi teknolojiler veri tabanlarında tutulmakta, anlık ve sonrasında işlenmektedir. Böylesine devasa veri, yapay zeka temelli çözümler ile iç güvenliğin sağlanmasında anlamlı bir bütün sunmaktadır.

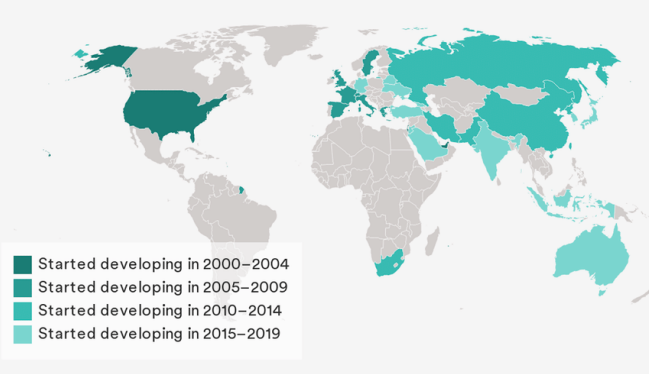
Ulusal güvenlik konuları ve yapısı gereği uluslararası askeri faaliyet alanlarında yapay zeka destekli uygulamalar kullanılmaktadır. Askeriyeyi kapsayacak biçimde yapılan araştırmalardan üretime, bakım onarımdan harekat planlamasına, eğitimden ulaşıma, istihbarattan güzergah planlamasına, elektronik harpten komuta kontrole, haberleşmeden istihbarata karşı koymaya, lojistikten kuvvet dağıtımına değin oldukça yaygın kullanılmaktadır (Kocabaş & Öztemel, 1998).

Yaygın olarak bilindiği üzere insansız hava araçları hem iç güvenlikte hem de sınır ötesinden gelebilecek olası tehditleri önlemede etkin olarak kullanılmaktadır. İHA'lar, yapay zeka teknolojileriyle görüntüleri işleyerek hedef tespitinde bulunabilmektedirler (İrdem & Çobanoğlu, 2021). Böylece kolluk kuvvetlerine ham görüntüleri kıymetlendirerek etkili istihbarat bilgisi oluşturulabilmektedir.

Ülkemizin güney ve doğu sınırlarındaki ülkeler (Suriye, Irak, İran) ile yaşadığı terör, kaçakçılık ve yasa dışı göç hareketliliği; batısında yer alan Yunanistan ile yaşadığı kıta sahanlığı ve Adalar'da olduğu gibi yaşanan aktif sorunlar birer tehdit unsurudur. Farklı cephelerde farklı tehdit unsurlarıyla karşı karşıya kalan ordumuz, gelişen teknolojiyle bütünleşik olarak karşılık vermektedir. Nitekim savunma sanayisindeki gelişim sonucunda gerek düzensiz göçlerin takibinde, gerek enerji güvenliğinin sağlanmasında gerekse de terörle mücadelede iç ve dış operasyonlarda insansız hava araçları kullanılmaktadır (Yetgin & Baştuğ, 2021). İHA'ların karar vericilere yönelik sağladığı istihbarat verilerindeki tutarlılık dolayısıyla ilgili kolluk kuvvetleri ve istihbarat teşkilatları

envanterlerinde insansız hava araçlarına yer vermektedirler. İnsansız hava araçlarından edinilen veriler düzeltme, birleştirme ve anlamlandırma işlemlerinden geçmektedir (Villi & Yakar, 2022). Böylesine karışık ve yüksek boyutlardaki veriler yapay zeka temelli geliştirilen yazılımlar sayesinde kıymetlendirilmektedir.

Son yıllarda gözetleme, çatışma ve harp sahalarında etkin kullanılan insansız hava araçları, yapay zeka teknolojisi ile sınırları denetim altında tutmaktadır (İrdem & Çobanoğlu, 2021). Aşağıdaki görsel, ülkelerin S/İHA'ların güvenlik politikalarındaki yerine dikkat çekmesi açısından değerlendirilebilir.



Şekil 1. S/İHA Geliştiren Ülkelerin Haritada Gösterimi (Chamola ve ark., 2021).

Askeri amaçla kullanılan İHA'lardaki elektro-optik yapılar oldukça gelişmiştir. Özellikle istihbarat faaliyetlerinde keşif amaçlı kullanılan bu tip İHA'lar hedef tespitinin yanı sıra kamuflaj ve düşman unsurun tespitini de yapabilmektedir (Villi & Yakar, 2022). Gece görüşü, hedef üzerinde optik düzeyde yakınlaştırma ve hedef odaklı takip askeri maksatla kullanılan insansız hava araçlarının özelliklerinden birkaçıdır. Yine I. Dünya Savaşı sırasında kullanımı yaygınlaşan uçakların savaşlarda kullanıma girmesiyle ve havadan gözetleme yapılmasıyla birlikte karar vericilere hiç olmadığı kadar farklı bir istihbarat sağlanabilmiştir (Karasoy, 2022).

Yapay zekaya sahip insansız hava araçları günümüzde etkin olarak istihbarat, keşif, gözetleme, tarama, mayın arama gibi görevleri icra edebilmektedir. Sınır güvenliği kapsamında da İHA'lardan yararlanılmaktadır. Geleneksel yöntemlere kaldıraç gücü sağlayan İHA'lar, sınırları anlık olarak gözetlerken silahlı olarak (SİHA) gerekli müdahaleyi de anlık olarak yapabilmektedir. Örneğin, bir geçiş ihlalinin tespitinde geleneksel yöntemde alana askeri unsurların intikal etmesi gerekmektedir. Bu süreç zarfında terörist unsurlar ya da kaçaklar yer değiştirebilmektedirler. SİHA kullanımında ise yasa dışı faaliyetin tespiti ile müdahalesi anlık olarak yapılabilmektedir. Üstelik olası bir sıcak çatışmada güvenlik güçlerinin canı tehlikeye girmemektedir. Ayrıca İHA'larda yer alan kameraların görüş açıları sabit kameralara göre oldukça geniş ve hareketlidir. Düşük ya da yüksek irtifa fark etmeksizin oldukça etkili bir görüş açısına sahiptirler. Bu yetenekleriyle İHA'lar, devriyede olan askeri birliklerden daha fazlasını kapsayabilmektedir (Şahiner ve ark., 2021). Ülkemizin sınır ötesi operasyonlarında İHA'lar terörist unsurları tespit etmekte ve hemen ardından ilgili koordinata intikal ederek şahısları etkisiz hale getirmektedir.

Ay ve Namlı'nın gerçekleştirdiği çalışmada (Ay & Namlı, 2017) uydu ve İHA'dan alınan veriler, görüntü işleme yöntemiyle analiz edilerek ekili arazilere, maden ocaklarına ve orman arazilerine dikilen kaçak yapıların tespiti otonom olarak gerçekleştirilmiştir. Geliştirilen modelin kullanım alanları boş araziler, ormanlarda kaçak ağaç kesimi ve ekili alanlardaki ürünlerin tespiti vb. şeklinde genişletilebilir. Araştırmacılar, çalışmalarında günümüzün en büyük sorunlarından biri olan gıda ve gıda güvenliğine yönelik bir uygulama önermektedirler. Söz konusu araştırmanın sonucuna göre görüntüleri doğru sınıflandırmada %97 oranında doğruluk elde edildiği söylenmektedir. İHA aracılığıyla anlık olarak görüntüyü merkeze iletebilen bu teknoloji ile önceki görüntü ve o an alınan görüntü işlenebilmekte ve merkeze veri aktarımı yapılabilmektedir. Gözetleme maksadıyla etkin olarak kullanılan İHA'lar, yakın zamanda Kahramanmaraş merkezli büyük depremde de kullanılmıştır. İHA'lar kullanılarak elde edilen anlık veriler üzerinde görüntü işleme teknikleri ve yapay zeka algoritmaları ile anlık analiz yapılabilmektedir. Böylece ayrıca bir insanlı iş gücüne gerek kalmaksızın görev icrası mümkün olmaktadır.

Türk Silahlı Kuvvetlerinin envanterinde olan İHA ve SİHA'lar, kontrolün insan ve yapay zeka arasında paylaşıldığı yarı otonom sistemlerdir. Yarı otonom sistemlerde, örneğin, İHA'nın uçuş kalitesiyle ilgili (kanat derecesi gibi) karar komutları yapay zekaya bırakılırken İHA'nın alacağı irtifa ve hareket edeceği yön personel tarafından komuta edilmektedir. Tam otonom sistemlerde insan aradan çıkmakta ve tüm komuta kontrol yetkisi yapay zekaya bırakılmaktadır. Böylece yapay zekaya sahip tam otonom SİHA'lar kendi kendilerine hedefteki bölgeyi tarayabilir, keşif sonrasında elde ettiği verilerin analiziyle birlikte imha dahi edebilmekte, bunun kararını

alabilmektedirler (STM ThinkTech, 2018). Otonom robotlar mayın arama ve arazinin mayından arındırma işlemlerini üstlenerek olası can kayıplarının önüne geçmektedir. Bu robotlar kimyasal risk taşıyan ortamlarda göreve çıkabilir, bir afet durumunda girilemeyecek yerlere girebilir, meskun mahal operasyonlarında kolluk kuvvetlerinin yardımcısı olabilirler (Şengöz, 2021).

4.3. Asayiş ve Adli Bilişim

Siber ortamda fiziki ortama göre suçun daha kolay işlenebilmesi (gelişen teknolojik olanaklar ile az bilgi ile büyük zararlar verilebilmektedir) ve daha kolay saklanılabilmesi; sanal ortamda işlenen suçun olumsuz sonuçları ve cezai yaptırımlarıyla doğrudan ve hemen yüzleşilmemesi, üstelik bu eylemlerin "underground" camiada bir statü artırımı olması gibi etkenler dolayısıyla siber uzaydaki suç oranının fiziki dünyadaki oranından fazla olmasına neden olmaktadır.

Güvenliği sağlamanın temeli, suçun gerçekleşmeden önlenmesinden geçmektedir. Buna rağmen önleyici faaliyetlere olan ilginin ve verilen önemin, suçun aydınlatılmasından daha az olduğu ifade edilmektedir (Ak, 2021). Kolluk güçlerinin yapay zekadan yararlandığı alanlar şöyle sıralanabilir:

1. İşlenen suçların nerede, ne zaman, niçin, nasıl, kim tarafından gerçekleştirildiğini geçmiş vakalardan elde edilen bilgilere dayanarak gelecek olayların tahminlenmesine yönelik analizin yapılması,
2. Görüntü işleme ile biyometriden yararlanılması,
3. Asayişin sağlanmasında devriye görevlerinin optimum düzeyde planlanması.

Yapay zekanın güvenlik güçlerinin "gözü kulağı" olduğu sistemlerden biri de yüz ve ses tanıma ile görüntü işleme teknolojileridir. Güvenlik kameralarından (iş yerinde, hava alanında, sokakta, parkta, hastanede, apartmanda, okulda vb.), uydulardan, insansız hava araçlarından elde edilen görüntüler bu teknoloji kapsamında istihbarat verisi olarak değerlendirilmektedir. Dahası, cep telefonunda yer alan yüz/ses tanıma sistemlerine de istihbarat servislerinin ulaşabildiği kaydedilmektedir (Oruç, 2019). Bu noktada yapay zeka, böylesine devasa boyuttaki verileri, çok yönlü veri tabanlarındaki verilerle görüntü/ses işleme yöntemlerini kullanarak karşılaştırabilmektedir. Örneğin bir hedefin tespiti yapılacaksa çok hızlı tepki süresiyle bunu yapabilmektedir.

Terör örgütleri, dijital kapasitelerine ciddi yatırım yapmakta ve faaliyetlerini dijital ortama taşımaktadırlar. Öyle ki birkaç dilde hazırlanmış web siteleri dahi bulunmaktadır. Örgüt üyeleri iletişimlerini sosyal medya platformlarında, sohbet odalarında, videoların yorum alanlarında, forumlarda ve anlık yazışma uygulamalarında örtülü olarak yürütmektedirler (Yanarışık, 2020). Buradan hareketle kolluk güçlerinin karada gezdiği devriyeler siber ortama da yansıyarak "sanal devriyeler" atılmaktadır (İrdem & Çobanoğlu, 2021).

Terör örgütlerinin finanse edilmesinde yasa dışı para devreye girmektedir. Bu doğrultuda örgüt tarafından kara paranın aklanmasında dijital yollar kullanılmaktadır. Örgüt tarafından fon alımı ve satımı otomatik sistemler aracığıyla çeşitli yollarla yapıldığından bu işlemlerin takibine bir insanın yetişmesi ve analiz etmesi mümkün değildir. Bankalar tarafından konulan filtreleme sistemleri olsa da yetersiz kaldığı bilinmektedir. Yapay zeka bu noktada otonom olarak bu işlemlerin tespitinde kullanılabilmektedir (Şen & Yurtoğlu, 2020).

Yapay zekanın kullanıldığı ve oldukça etkin sonuç veren sistemlerden biri de yüz tanıma sistemleridir. Yüz tanıma sistemleri, özellikle biyometrik olarak elde edilen veriler sayesinde ülkenin giriş ve çıkışlarında yapılan denetimlerde kullanılmaktadır. Bu yöntemle aranan bir kişinin -resmî kayıtlarda olması koşuluyla- sistemi aşması mümkün görünmemektedir. Kameralardan elde edilen veriler, otomatize olarak veri tabanındaki görüntülerle eşleştirilerek bir sonuca varılmaktadır. Rusya'nın 2018'deki Dünya Şampiyonası'nda yüz tanıma sistemini kullandığı bilinmektedir (Şahiner ve ark., 2021).

Yapay zeka ile birlikte kullanılan büyük veri, kolluk güçlerinin verileri anlamlandırmada yararlandığı nitelikli bir teknolojidir. Özellikle iç güvenliğe yönelik olası tehditlerin önceden haber alınması, şüpheli davranışların, kişilerin ve örgütlerin tespiti çerçevesinde sosyal medya platformları başta olmak üzere çevrim içi ortamda bırakılan tüm dijital ayak izleri sürülmektedir. Büyük veriden elde edilen bu ham veriler, veri madenciliği yöntemleri ile işlenmekte ve böylece anlamlandırılmaktadır. Büyük veriden anlam çıkaran yöntemler (veri madenciliği, yapay öğrenme, derin öğrenme vd.) istihbarat faaliyetinde uygulayıcısına ciddi katkılar sunmaktadır. Bu doğrultuda yapay zeka, istihbaratta veri toplama > analiz etme > istihbarat üretme olarak adlandırılan üçlü evrede kullanılmaktadır (İrdem & Çobanoğlu, 2021).

Artan teknolojik olanakların bir çıktısı da veri barındırma olanaklarının artmasıdır. Depolama kapasitesinin artışındaki iyileşme ve düşen maliyetler dijital depolama aygıtlarının kamu işlerinin yanı sıra bireysel olarak günlük yaşamda da ulaşılabilir olmasını sağlamıştır. Bu cihazların yaygınlaşmasıyla, olası bir adli analiz durumunda

incelenecek nesnelerin ve verilerin de sayısı artmaktadır. Böylesine devasa boyuta ulaşan büyük verinin analizi, adli bilişim uzmanlarının çok fazla zamanını almakta ve bu da yargı sürecinin aksamasına neden olmaktadır. Yapay zeka, diğer alanlarda olduğu gibi adli bilişim sürecinde de uygulayıcısına büyük bir kaldıraç gücü sağlamaktadır. Özellikle bilişim suçları kapsamındaki adli süreçlerde dijital delillerin toplanması ve analizinin yapılması fiziki delillerden daha öncelikli olmaktadır. Literatürde bu amaçla geliştirilen modellerin olduğu görülmektedir (Dilber & Çetin, 2021). Veri incelemesinde olabildiğince insansız bir çözüm için rutine binen işlemlerin yapay zeka temelli yapılması hedeflenmektedir. Özellikle bir adli bilişim uzmanının manuel olarak çözmesinde zor olan süreçlerin optimizasyonu yapılmaktadır.

4.4. Endişe Edilen Konular

Bunca yararına rağmen -haklı olarak- yapay zekanın halihazırda oluşturduğu endişeler bulunmaktadır. En nihayetinde otonom davranış modeli yapay zekayı kodlayanların politik/askeri niyetine göre şekillenmektedir. Öte yandan yapay zekanın öğrenme kaynakları olan büyük verinin zehirlenmesi sonucu ortaya çıkan sonuç olumsuz olmaktadır (STM ThinkTech, 2018).

16 Mart 2023'te duyurulan ChatGPT-4'ün teknik raporunda (OpenAI, 2023) ifade edildiği üzere dezenformasyon, siber güvenlik, zararlı içerikler, ekonomik etkiler, konvansiyonel ve konvansiyonel olmayan silahların yayılması gibi oldukça geniş alanda etki düzeyinin olabileceğine değinilmektedir. Yapay zekanın geldiği bu noktada "deepfake" yöntemi internet aracılığıyla oldukça hızlı biçimde yayılma olanağı bulan dezenformasyona kapı aralamaktadır. Yapay zeka, tanım olarak "bir insanın yapabildiği her şeyi yapabilmesi" olduğu kabulüyle kötü niyetli bir insanı da pek iyi taklit edebilmektedir.

Kamu güvenliğinin sağlanmasında vatandaşın kişisel verilerinin korunması ve gizliliği ile mahremiyetine yönelik hassasiyeti ihlal edilmemelidir. Verilerin işlenmesi noktasındaki yapılacak hukuksal düzenlemeler ve bu noktadaki denetim mekanizması önem arz etmektedir (Ak, 2021). Kişisel verilerin korunmasına yönelik etik ihlallerin yapıldığı bilinmektedir. Bu konuda en çarpıcı örnek 2018'de açığa çıkan Cambridge Analtica vakasıdır (Darıcılı, 2024). Büyük verinin yapay zeka sistemleriyle politik amaçlar güdülerek manipüle edilmesi elbette bu örnekle sınırlı değildir. Darıcılı'nın da dikkat çektiği üzere Snowden'ın ifşaatı, ABD'nin Ulusal Güvenlik Ajansı NSA tarafından geliştirilen PRISM yazılımı, kişisel verilerin yapay zeka ile analiziyle yasa dışı kullanımına bir diğer örnektir. Hamas'ın 7 Ekim 2023'te İsrail'e yönelik başlattığı saldırı sonrasında İsrail'in Gazze'ye yönelik başlatılan operasyonlarda yapay zeka destekli bir yaklaşım ortaya koyduğu bilinmektedir. İsrail istihbaratı, geliştirdiği Lavendar adındaki bu yazılım ile "düşman unsurlara" yönelik bombalamaları algoritmalara emanet etmektedir. Bu da binlerce sivilin yaşamlarını yitirmesine neden olmuştur (Darıcılı, 2024).

Yapay zekanın otonomlaşmasına yönelik endişeler de dillendirilmektedir. Kendi kendine karar verebilen silahlı bir robot sisteminin kontrol edilemezliği söz konusudur (Şen & Yurtoğlu, 2020). Nitekim yapay zeka, onu kodlayanın niyetine göre hareket etmektedir ve insan gibi düşünebilen yapay zeka, normal hayattaki kötü insanlar gibi davranabilecektir. Dolayısıyla yapay zeka temelli otonom sistemlerin önleyici güvenlik unsurları olarak değerlendirilmesinde fayda görünmektedir.

Endişe verici ve henüz netlik kazanmayan bir konu da yapay zeka temelli çözümlerde yaşanacak bir sorunda sorumlunun kim olacağı konusudur. Örneğin, istenmeyen bir can ya da mal kaybı yaşandığında yapay zekayı geliştiren yazılımcı mı sorumlu tutulacaktır yoksa komuta kademesindeki subay mı? Bu konularda henüz hukuki bir düzenleme bulunmamaktadır (Şahiner ve ark., 2021).

SONUÇLAR

Yapay zekanın tanımı fen ve sosyal bilimlerle olan temasından dolayı oldukça çeşitlilik göstermektedir. Özünde yapay zeka, insan zekasında olduğu gibi "problem çözme aracı" çerçevesinde yorumlanabilmektedir (STM ThinkTech, 2018).

Masada yapılan harekat planının sahada değişkenlik gösterdiği bilinmektedir. Güvenlik konularının özünde yatan bu gerçek, muharebe ortamının bilinmezlikleri ve her an ortaya çıkan yeni planlarla gözden geçirilmektedir. "İcra edilen faaliyetler, ilk kez çalınan bir bestedir" (Şengöz, 2021). Bu doğrultuda karar verici, mesleki yetkinliklerini bir sanatçı üslubuyla titizlikle işlemelidir.

Denildiği üzere istihbarat, sessiz yürütülen bir savaştır. İstihbaratta esas unsurdan biri de doğruluk ve güncelliktir. Dolayısıyla istihbarat, olabildiğince hızlı biçimde karar vericinin önünde olmalıdır. Yapay zeka, insan üstü bir çeviklikte bunu yapabilmektedir (Yılmaz, 2020). Yapay zeka, özellikle sıcak çatışma anında ya da operasyonel

faaliyet sırasında hızlı ve doğru karar ihtiyacını karşılama olanağı sunmaktadır. Farklı kaynaklardan gelen verileri bir uzmana (insana) göre hızlıca analiz eden yapay zeka sistemleri, karar alıcılar için yüksek kaldıraç gücü sağlamaktadır. Nitekim hızın kritik önemine istinaden bir örnek 1967 yılında gerçekleşen Arap-İsrail savaşıdır. Bu savaşın Mısır tarafınca kaybedilmesinde en büyük üç etkenden birinin hızlı karar alınamaması olarak kaydedilmektedir. Öte yandan otonom sistemlerde insanın olmayışı daha tehlikeli görevlerde daha agresif kararlar alınmasında fayda sağlamaktadır. İnsansız sistemlere gelebilecek bir zarar yalnızca maddi olmakta iken bir can kaybının yanı sıra yetişmiş insan gücü olarak bir savaş pilotunun nitelik kazanması yirmi yılı bulabilmektedir. Bilgisayarlı görü sayesinde keşif faaliyeti yürüten yapay zeka sistemleri, fotoğraf ve video gibi görüntülerle yüz tanıması yaparak aranan şahısların ya da düşman unsurlarının tespitinde kullanılabilmektedir (STM ThinkTech, 2018). Bu teknolojik olanakların bir sonucu olarak yapay zekanın yaygınlaşması ve kamuya açık biçimde sunulmasıyla oldukça farklı bir boyuta evrildiği gözlenmektedir. "Pixels to intelligence" mottosuyla hizmet sağlayan GeoSpy (GeoSpy, 2025), yapay zeka destekli sistemi ile saniyeler içerisinde yüklenen fotoğraftan konum tespiti yapabilmektedir. Bu pratikliğin kolluk güçleri için bir kazanım olduğu düşünülse de birkaç on dolar ile herkesin erişim sağlayabildiği adli bilişim çözümleri, özellikle hassas olan kişisel verilerin kapsamını genişletici bir etkiye neden olmaktadır. Bunun yanı sıra mevcut ses ve fotoğraf/video görüntüsünden yeni içerikler üretilmesi (generative AI) endişe edici unsurların başında gelmektedir.

Güvenliğin çok yönlülüğü ona disiplinler arası bir yaklaşımla bakılmasını gerekli kılmaktadır. Bu doğrultuda sosyal bir varlık olan insanı doğrudan ilgilendiren konularda tarih, edebiyat, ekonomi, siyaset, kültürel yapı, psikoloji gibi sosyal bilimler gerek güvenlik çalışmalarında gerek bu itibarla değerlendirilmek üzere istihbarat faaliyetlerinde kendine yer bulmaktadır. Nitekim tehdit unsuru olan suçu işleyen insanın, örgütlenerek terörist ya da yasa dışı faaliyet amacı güden toplulukların düşünce yapısı ve olası hamleleri ön görülebilir. Örneğin, siber suçlular incelendiğinde (Yanarışık, 2020), fiziki (yüz yüze) işlenen suçlarda yaşanan suçluluk ve pişmanlık hissinin görece daha az yaşandığı, yapılan "işin" bir suç olarak görülmediği, dahası bir ödüllendirme olarak değerlendirildiği görülmektedir. Bu da işlenen suçlardaki artışın bir açıklaması olarak yorumlanmaktadır.

Deneyim birikimi ile insan, makinelerden ve yapay zekadan ayrı olarak pek tabi duyguya sahip bir varlıktır. Teknoloji, günümüzde her ne kadar teknik ve operasyonel kapsamda büyük faydalar sağlamış olsa da güvenlik politikaları çerçevesinde kritik noktada teknik yeteneklerin sosyal düşünce yapısıyla bir arada değerlendirmesi gerekliliği alan çalışmaları yürütenlerce (Özdemir & Kahya, 2021) ortak bir kanıdır. Buradan hareketle geleneksel yöntemle başarılabilen insan istihbaratı kendine has yöntem ve analizlerle haklı yerini korumaktadır.

İstihbaratın analizi sürecinde başat sorun, analizin teslim edileceği kurumun/müşterinin acil olarak talep etmesidir. Oysa analiz raporunun isabeti zamana ve olanakların kullanılabilmesiyle olmaktadır (Şen & Yurtoğlu, 2020). Böylece analist, yazdığı raporda geçmiş tecrübelerinden ve bu deneyimlerden oluşturduğu ön yargılarla çıkarım yapmak durumunda kalmaktadır.

İnsanın tecrübe kazanması oldukça uzun yılları almaktadır. Bununla birlikte bir sonraki kuşağa bu deneyimlerin aktarılması da bir o kadar zor ve uzun zamanları bulmaktadır. Yapay zekalı sistemlerin öğrenmesi ise burada insandan ayrışmaktadır. Yapay öğrenme sistemiyle geliştirilebilir. Yanı sıra sunduğu simülasyon sistemleri sayesinde insanların öğretim görmesinde farklı deneyimler sunabilmektedir. Kolluk güçlerinin eğitim ve öğretimindeki simülasyonlarda muharebe sahalarının tatbiki önceden personele sunulabilmektedir (Şengöz, 2021). Yapay zeka ile harp sahasında düşman unsurlarla gerçekleşecek temastaki olası senaryoların modellemesiyle personelin eğitiminde değerlendirilmektedir (Türe & Topuz, 2020).

Kamusal ve toplumsal olarak bilgi güvenliğinin sağlanmasına yönelik yapay zeka destekli siber güvenlik çözümleri de bütünsel olarak ulusal güvenliğin sağlanmasına ciddi katkılar sağlayabilmektedir (İrdem & Çobanoğlu, 2021). Özellikle e-Devlet uygulamasında olduğu gibi hemen her şeyin dijitalleşmesine yönelik politikanın uygulandığı güncel durumda yapay zeka, uygulayıcısının elini güçlü kılmaktadır.

Sonuç olarak insanlık kadar geçmişi olsa da bilimsel bir disiplin olarak ele alınmaya başlanılan istihbaratın da günümüz anlamında bir teknoloji olarak yapay zekanın da bu anlamdaki birikimi 60~ yılı bulmaktadır. Bu çalışmada, odağa alınan alanlarda kullanıcısına yüksek katma değer sağlayan yapay zeka, güvenlik ve teknik istihbarat çalışmaları için umut ve tehlike vaat ederken fırsat ve riskleri de bünyesinde barındırmaktadır. Her koşulda olduğu gibi bir araç olarak yapay zeka, günün sonunda, kullanıcısının niyeti ölçüsünde biçimlenmektedir.

KAYNAKLAR

Ak, T. (2021). Yapay Zekâ Teknolojileri, Güvenlik ve Kolluk Kuvvetinin Suç Önleme Faaliyetleri. *SDE Akademi Dergisi*, *1*(1), 120-140.

Altınpınar, M. (2018). Sınırsız Güvenlik. *Güvenlik Çalışmaları Dergisi*, *20*(1), 73-86.

Ay, B., & Namlı, E. (2017). Görüntü İşleme Tabanlı İHA ve Uydu Sistemleri Hibrit Yapay Zeka Modeliyle Kaçak Yapıların Tespiti. *Yönetim Bilişim Sistemleri Dergisi*, *3*(2), 114-129.

Chamola, V., Agarwal, A., Gupta, N., Kotesh , P., Naren , N., & Guizani , M. (2021). A Comprehensive Review of Unmanned Aerial Vehicle Attacks and Neutralization Techniques. *Ad Hoc Networks*, *111*(1), 1-26.

Darıcılı, A. B. (2020). Yapay Zekâ Yönetiminin Uluslararası Güvenliğe Etkileri. *Savunma Bilimleri Dergisi*, *19*(1), 49-72.

Darıcılı, A. B. (2024). *Türkiye ve Dünyadan İstihbarat Operasyonları*. İstanbul: Kronik Kitap.

Demircioğlu, İ. H., Özcan, A., Çençen, N., & Yiğit, Y. (2021). *Türk İstihbarat Tarihi.* Yeditepe Yayınevi.

Dilber, İ., & Çetin, A. (2021). Adli Bilişim İncelenme Süreçlerinde Yapay Zeka Kullanımı: VGG16 ile Görüntü Sınıflandırma . *Düzce Üniversitesi Bilim ve Teknoloji Dergisi*, *9*(5), 1695-1706.

İrdem, İ., & Çobanoğlu, S. (2021). Yapay Zekânın İç Güvenlik Yönetimi Üzerine Yansımaları: Siber Güvenlik. *Kamu Yönetimi ve Teknoloji Dergisi*, *3*(2) 175-202.

Karasoy, H. A. (2022). Yeni Nesil Savaş ve Siber İstihbarat. *Güvenlik Bilimleri Dergisi*, *11*(1), 223-240.

Kocabaş, Ş., & Öztemel, E. (1998). Harp Oyunlarında Yapay Zeka Uygulamaları. *Modelleme ve Simülasyon Konferansı.* Ankara.

Oruç, M. A. (2019). İstihbarat ve Yapay Zekâ İlişkisi. *International Social Sciences Studies Journal*, *5*(41), 4224-4234 .

Özdemir, E., & Kahya, M. (2021). İstihbarat ve Güvenlik Çalışmalarında Sosyal Bilimlerin Yeri ve Önemi. *Güvenlik Bilimleri Dergisi*, 2. Uluslararası Güvenlik Kongre Özel Sayısı, 1-14.

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 Zeka Tekniklerinin / Uygulamalarının Siber Savunmada Kullanımı. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi* , *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.

Şengöz, M. (2021). Yapay Zekâ Tabanlı Sistemlerden Üretilen Teknolojilerin Askeri Harekâtın Sevk ve İdaresinde Kullanılmasına Yönelik Bir Değerlendirme. *Nevşehir Hacı Bektaş Veli Üniversitesi SBE Dergisi*, *11*(4), 2159-2174.

Villi, O., & Yakar, M. (2022). İnsansız Hava Araçlarının Kullanım Alanları ve Sensör Tipleri. *Türkiye İnsansız Hava Araçları Dergisi*, *4*(2), 73-100.

Yanarışık, O. (2020). İç Güvenlik ve Siber Güvenlik. *İç Güvenlik Yönetimi ve Polis* (s. 303-323) Ankara: Polis Akademisi.

Yetgin, M. A., & Baştuğ, M. (2021). Devletlerin Değişen Güvenlik Algısında İnsansız Hava Araçları. *Türkiye İnsansız Hava Araçları Dergisi*, *3*(2), 55-64.

Yılmaz, B. A. (2020). Siber Terörizm ve Değişen İstihbarat Anlayışı. *Anadolu Strateji Dergisi*, *2*(1), 65-82.

İNTERNET KAYNAKLARI

Минобороны России. (2023). *Сводка Министерства обороны Российской Федерации о ходе проведения специальной военной операции на территории Украины*. 3.2.2025 tarihinde https://t.me/s/mod_russia/23130 adresinden alındı.

Türe, S., & Topuz, S. (2020). *Yapay Zekâ ve Askeri Uygulamalar.* 9.1.2025 tarihinde https://www.milsoft.com.tr/wp-content/uploads/2020/08/Yapay-Zeka-ve-Askeri-Uygulamalar_v2.2.pdf adresinden alındı.

T.C. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi. (2021). *Ulusal Yapay Zekâ Stratejisi 2021-2025.* 16.1.2025 tarihinde https://cbddo.gov.tr/SharedFolderServer/Genel/File/TR-UlusalYZStratejisi2021-2025.pdf adresinden alındı.

STM ThinkTech. (2018). *Yapay Zeka ve Silahlı Kuvvetlere Etkileri.* Ankara: STM. 8.1.2025 tarihinde https://thinktech.stm.com.tr/tr/yapay-zeka-ve-silahli-kuvvetlere-etkileri adresinden alındı.

GeoSpy. (2025). *Unlock the Power of AI Image Intelligence*. 9.2.2025 tarihinde https://geospy.ai adresinden alındı.

Hoskins, P., & Imran, R.-J. (2025). *Nvidia Shares Sink as Chinese AI App Spooks Markets*. 8.2.2025 tarihinde https://www.bbc.com/news/articles/c0qw7z2v1pgo adresinden alındı.

OpenAI. (2023). *GPT-4 Technical Report.* 15.1.2025 tarihinde https://doi.org/10.48550/arXiv.2303.08774 adresinden alındı.

DeepSeek-AI. (2025). DeepSeek LLM: Scaling Open-Source Language Models with Longtermism. 8.2.2025 tarihinde https://doi.org/10.48550/arXiv.2401.02954 adresinden alındı.

TEŞEKKÜR ve BEYANLAR

Yazarlar çalışmaya eşit oranda katkı sağlamıştır. Bu çalışmada herhangi bir potansiyel çıkar çatışması bulunmamaktadır. Yapılan çalışmada araştırma ve yayın etiğine uyulmuştur.