ARAŞTIRMA

Geliş Tarihi: 07.01.2022
Kabul Tarihi: 15.01.2022

YAPAY ZEKÂNIN İÇ GÜVENLİK YÖNETİMİ ÜZERİNE YANSIMALARI: SİBER GÜVENLİK

Reflections Of Artificial Intelligence On Internal Security Management: Cyber Security

* İbrahim İRDEM ** Sedat ÇOBANOĞLU

Özet

Teknolojinin ve dijitalleşmenin içinde bulunduğumuz yüzyılda ciddi bir ivme kazanarak hayatın her alanına nüfuz etmesiyle birlikte güvenlik sektörü de bu durumdan payını almıştır. Makinelerin insan beyninin yapabildiği her şeyi ve daha ötesini yapabileceği fikri, ön plana çıkarak; oldukça büyük miktarda veriye ve bilgi işlem gücüne sahip yapay zekâ kavramı ve uygulamaları önem kazanmaya başlamıştır. Beşerî zekânın makinelere adaptasyonu ile faaliyetlerin ve olayların hızlı bir şekilde analiz edilebildiği, güvenlik risklerinin tanımlanmasında, tespitinde, önceliklendirilmesinde, tehditlerin risk modellemesine ve algoritmik öğrenme prosedürüne dayalı cihazlarla tahmininde ve bertaraf edilmesinde yapay zekâ kullanımı güvenlik bürokrasisinin karar verici aktörleri açısından güvenliğin ayrılmaz bir parçası haline dönüşmüştür. Bu makale; yapay zekânın iç güvenlik yönetimi üzerindeki yansımalarını değerlendirmekte ve tümdengelimci bir yaklaşım çerçevesinde iç güvenliğin sağlanmasında yapay zekâ uygulamalarının rolünü ve etkisini analiz etmektedir.Spesifik olarak siber güvenliğe odaklanan çalışmada öncelikle yapay zekâ kavramı, yapay zekânın tarihçesi, kullanım alanları detaylı bir şekilde ele alınmakta; akabinde ise yapay zekânın iç güvenlik yönetimi üzerindeki etkileri siber güvenlik üzerinden ele alınmaktadır.

Anahtar Kelimeler: *Yapay Zekâ, İç Güvenlik,Siber Güvenlik*

Abstract

With the penetration of technology and digitalization into all areas of life by gaining a serious momentum in the current century, the security sector has also received its share from this situation. By coming into prominence the idea that machines can do everything that the human brain can do and beyond; the concept and applications of Artificial Intelligance (AI), which has a large amount of data and computing power, have started to gain importance. With the adaptation of human intelligence to machines, there has been a situation where activities and events can be analyzed quickly. The use of artificial intelligence has become an integral part of security for decision-making actors of the security bureaucracy in identifying, detecting, prioritizing security risks, predicting and eliminating threats with devices based on risk modeling and algorithmic learning procedures. This article; evaluates the reflections of artificial intelligence on internal security management and analyzes the role and impact of artificial intelligence applications in providing internal security within the framework of a deductive approach. In the study, which specifically focuses on cyber securtiy, first of all, the concept of artificial intelligence, the history of artificial intelligence, its usage areas are discussed in detail; then, the effects of artificial intelligence on internal security management are discussed through cyber security.

Keywords: *Artificial Intelligence, Homeland Security, Cyber Security*

* İbrahim İRDEM,Dr. Öğr. Üyesi , , Polis Akademisi Başkanlığı Güvenlik Bilimleri Enstitüsü Müdürlüğü, ibrahimirdem33@gmail.com (https://orcid.org/0000-0003-0559-3418)
** Sedat ÇOBANOĞLU, Dr., Bağımsız Araştırmacı, drsedatcobanoglu@gmail.com (https://orcid.org/0000-0001-8357-885X)

1. Giriş

Asırlardır insanoğlu kendi yaşamını kolaylaştırmak ve daha güvenli bir yerde yaşayabilmek amacıyla pek çok alanda önemli kazanımlar sağlamıştır. Bu kazanımların en önemli çıktılarından birisi de son yüzyıl içinde küreselleşmenin de etkisiyle hızlı bir şekilde tüm yer küreye nüfuz eden önemli teknolojik gelişmelerdir. Böylece toplumsal ihtiyaca göre teknolojik gelişmelerden önemli ölçüde faydalanılmaya başlanmıştır. Yegane varlık olan "insan aklı"nın farklı bir aygıta/robota aktarılması merakı, bu teknolojik devrimlerin bir sonucu olmuştur. Bu köklü değişime neden olan olgu, yapay zekâ (artificial intelligence, AI) olarak adlandırılmaktadır. Günümüzde yapay zekâ hakkında farklı alanlarda pek çok çalışma yapılmaktadır. Hem kamu sektöründe hem de özel sektörde yapay zekâ, etkin bir şekilde kullanılmaya başlanmıştır. Bu alanlardaki işlerin/faaliyetlerin etkin, verimli ve güvenli yapılabilmesi için yapay zekâ çalışmalarına önem verilmektedir.

Soğuk Savaş'ın bitiminden itibaren güvenlik çalışmaları genişlemeye ve çeşitlenmeye başlamış, bu da günümüzün küresel sisteminde tehditleri salt askerî tehdit olmaktan çıkartarak çok yönlü ve karmaşık bir dinamiğe evirmiştir (Karakoç-Dora, 2021: 145). Artık hükümetler, hem içeriden hem de dışarıdan gelebilecek kamu düzenini olumsuz etkileyebilecek unsurlara karşı iç güvenliklerini sağlamak amacıyla geleneksel yöntemlerin yanı sıra küresel bağlamda gelişen teknoloji temelli yeni yöntemleri de kullanmaya çalışmaktadırlar. Özelllikle iç güvenliğe tehdit unsuru oluşabilecek faktörlere yönelik teknolojik gelişme ve değişimleri takip etmek bir zorunluluk haline gelmiştir. Bu nedenle devlet, küreselleşme sürecinde ortaya çıkan ya da çıkabilecek olası yeni tehdit unsurlarını bertaraf etmek amacıyla her türlü tedbiri almaktadır. Bu tedbirler arasında yenilikçi yaklaşımlar önemle takip edilmektedir. Çünkü teknolojik gelişmelerin hızı, insan düşüncesinin ötesine geçmeye başlamıştır. Bu nedenle yapay zekânın iç güvenlik politikalarında kullanılması, günümüz hükümet politikalarında bir zorunluluk olmuştur.

Bu çalışma, iç güvenlik politikaları çerçevesinde yapay zekâ kullanımının hangi uygulamalarla nasıl sağlanacağını ve küresel süreçte ne gibi uygulamaların olduğunu sorgulamaktadır. Öncelikle yapay zekâ, yapay zekânın tarihçesi ve yapay zekânın çeşitleri incelenerek kuramsal bir çerçeve oluşturulmuştur. Ardından yapay zekânın uygulama/kullanım alanlarından örnekler verilmiş ve iç güvenlik yönetiminde yapay zekânın yansımaları uygulamalar üzerinden tartışılmıştır. Çalışmada spesifik olarak siber güvenlik üzerine odaklanılmıştır. Çalışmada veriler, ikincil kaynaklar üzerinden toplanmış olup, keşfedici bir derleme çalışması niteliğindedir. Bu çalışmanın, iç güvenlik alan yazınına katkı sağlaması amaçlanmıştır.

2. Kuramsal Çerçeve

2.1. Yapay Zekâ

İnsanoğlunun teknolojiyle olan imtihanı sonucunda yeni bir çalışma alanı daha ortaya çıkmıştır. Yapay zekâ kavramının net bir tanımı olmasa da bu alan üzerine kafa yoranların/düşünenlerin çok olması nedeniyle farklı tanımlamalar mevcuttur. Bu farklılıkların kökeninde insan aklı ile bilimsel düşünceyi bir nesne üzerinde tatbik etme denemelerinin farklı alanlarda kullanılma çabası yatmaktadır.

Yapay zekâ, pek çok konu başlığı altında incelenmektedir. Yapay sinir ağları, uzman sistemler, bulanık mantık ve genetik algoritmalar gibi konular bu alanda ön plana çıkmaktadır. Yapay zekâ farklı disiplinler tarafından çalışılmaktadır. Örneğin; sağlık, eğitim, bilgisayar mühendisliği ve elektronik bilimleri gibi. Günümüzde yapay zekâ çalışmaları daha da yaygınlaşmaya devam etmektedir. Akademik çalışmalar, gazeteler ve konferanslar gibi "bilgi tartışma ve üretme" platformlarından, sosyal bilimlerden fen bilimlerine kadar birçok çalışma alanında yapay zekâ konusu üzerine tartışmalar mevcuttur. Yapay zekâ konusunun farklı alanlarda çalışılması sebebiyle günümüzde birçok farklı tanım ortaya çıkmıştır.

Yapay zekâ; bilim ve mühendislik alanıdır. Bu çalışma alanı; çevre üzerinde etkili olan, uyum, öğrenme, planlama, problem çözme, doğal dil süreçleri ve algılama gibi insan davranışındaki zekâ ile ilişkilendirdiğimiz özellikleri sergileyen gelişen sistemlerin teorik ve pratik ile ilgili süreçlerini kapsamaktadır (Tecuci, 2012:168). Yapay zekâ, evrendeki kullanılabilir aklın/zekânın işlenmesi ve bilgi türlerinin toplanması sürecinde mekanik bir simülasyon sistemidir. Bu süreç, bilginin toplanması ve yorumlanmasını içermektedir. Dahası eyleme geçilerek zekâya uygun hale dönüştürülmesi sürecidir. Yapay zekânın tanımında yaklaşık kırk yılı aşkın bir zaman diliminde hızlı değişimler yaşanmıştır. İlk tanımlar robotlar, kameralar ve bilgisayarlar gibi mekanik aletler üzerine odaklanırken, daha sonra simülasyon, taklit ve benzerlik kavramlarıyla şekillenmiştir. Makinelerden bilgisayarlara doğru bir tanımlama değişimi gözlenmiştir (Grewal, 2014:13). Tanımlardaki farklılıkların içeriğine genel olarak bakıldığında yapay zekâ, kullanıldığı alana ve tanımını yapan kişiye fayda sağlayacak biçimde kurgulanmıştır (Yampolskiy, 2020:68). Sonuç olarak yapay zekâ kavramı birçok alanda yaygın bir şekilde kullanılmaya devam edilmektedir. Bu nedenle kavramın kullanıldığı alana göre farklı tanımlarla karşılaşmak mümkündür.

2.2. Yapay Zekânın Tarihçesi

Cansız nesnelerin akıllı varlıklar olarak hayata geçirilmesi fikrinin temelleri oldukça uzun zamana yayılmıştır. Eski Yunanlıların robotlar hakkında efsaneleri var olagelmiştir. Çinli ve Mısırlı mühendisler ise kendiliğinden hareket eden makineler icat etmişlerdir. Modern anlamda yapay zekâ çalışmalarının başlangıcı, klasik dönem filozofların in-

san düşüncesini sembolik bir sistem olarak tanımlama girişimlerine kadar götürülebilir (Lewis ve Writer, 2014). Batı bilimindeki gelişmelerin yanı sıra Anadolu topraklarında makineleşme ve akıllı varlıklaşmanın öncülerinden El Cezeri, bu alandaki çalışmalarıyla örnek teşkil etmektedir. Sibernetik alanın kurucusu, fizikçi, mucit ve dahi bir mühendis olan El Cezeri kısa adı "Kitab-ül Hiyel" olan eserinde kırktan fazla "insan gibi hareket eden" otomat/robot çizmiş, bunları nasıl yaptığını detaylı bir şekilde anlatmış ve bunları hayata geçirmiştir. El Cezeri, robot biliminde çalışmalar yapan ilk bilim insanı olmanın yanında, kendi tasarımı makinelerin üretim algoritmalarını aktaran ilk algoritma kitabını yazmış bir bilim insanı olarak da bilinmektedir (Okçu, 2021: 218).

1769 yılında matematik, hukuk, fizik, teoloji ve felsefenin alt alanlarında önemli katkılar sağlayan Leibniz, seri olarak çeşitli hesaplamalar yapabilen "Step Reckoner" adında, dört aritmetik işlem yapabilen ilk mekanik cihazı icat etmiştir. Böylece insan zihninin yapabileceği fonksiyonları bir makinanın da yapabileceği fikri ortaya çıkmıştır. 1847 yılında ise yapılan matematik çalışmalarında, zihin matematiksel olarak incelenmiş ve mantık sembollerinin, cebirsel semboller olarak ifade edildiği keşfedilmiş ve "çağdaş mantık kuramı" yeniden inşa edilmiştir. Bir diğer matematik bilimci İngiliz Turing tarafından "Turing Machine" şeklinde adlandırılan bir makine tarif edilmiştir. Hazırladığı çalışmasında Turing, bu makinanın her türlü işlemi taklit etmek ve herhangi bir diziyi hesaplamak için tek bir makine icat etmenin mümkün olduğunu söylemiştir (Önder ve Saygılı, 2018: 640).

Turing tarafından 1950 yılında yazılan "Computing Machinery and Intelligence" isimli taklit oyunu kurgusunda "Makineler düşünebilir mi?" sorusuna cevap aranmıştır. İnsanın bir bilgisayar gibi çalıştığından hareket edilmiştir. Dijital bilgisayarların da ötesinde bu düşüncede, makinelerin bir insan bilgisayarı/insan beyni (human computer) tarafından her türlü faaliyeti yerine getirilebileceğinden bahsedilmiştir. Turing'e göre dijital bilgisayar düşüncesi oldukça eskidir. Turing, Cambridge Üniversitesi'nde 1828 ve 1839 yılları arasında Matematik Profesörü olan Charles Babbage'ın Analitik Makine/Motor olarak adlandırılan bir planının olduğunu, fakat bu planını gerçekleştiremediğini ifade etmiştir (Turing, 1950: 433, 436).

Dartmouth Üniversitesi'nde 1956 yılında yapılan bir konferansta John McCarthy, yapay zekâ tanımının doğrudan insan hafızası ile ilgili olmadığını belirtmiştir. McCarthy'ye göre belirli bir sorunun çözülmesi gerekliyse, yapay zekâ çalışan araştırmacılar, insanlarda gözlemlenmeyen yöntemleri serbetçe kullanabilmektedir. Modern bilgisayar biliminde akıllı bilgi sistemleriyle uğraşan bir alan bulunmaktadır. Bu alan, yapay sinir ağları alanıdır. Bu ağlar, insan beyninin benzerliğinden oluşturulan öğrenme yeteneği olan matematiksel bir model olarak betimlenmektedir (Doroganov ve Baumgarten, 2013: 132). Yapay zekâ kavramının temelleri henüz resmi olarak kabul edilmese de, ilk kez 1956 yılındaki bu konferansta atılmıştır (Lewis ve Writer, 2014).

Yapay zekâ alanında 1960'lı yıllardan günümüze birtakım gelişmeler yaşanmıştır. Örnek verilecek olursa (Türkçe Yayın, 2018);

1961-İlk endüstriyel robot olan Unimate, New Jersey'deki General Motors fabrikasında bir montaj hattı üzerinde çalışmaya başlamıştır.

1964-Daniel Bobrow, "Bir Bilgisayar Sorun Çözme Sistemi için Doğal Dil Girişleri " başlıklı MIT doktora tezini tamamlamış ve doğal bir dil anlama bilgisayar programı olan STUDENT geliştirilmiştir.

- 1965-Joseph Weizenbaum ELIZA programını geliştirmiştir.
- 1966-Shakey robotu, kendi hareketlerinin sorumluluğunu alabilen ilk robot olarak nitelendirilmiştir.
- 1970-İlk antropomorfik robot olan WABOT-1, Japonya'daki Waseda Üniversitesi'nde icat edilmiştir. Bu robot; kontrol sistemi, görme sistemi ve konuşma sistemi içeriyordu.
- 1979-Stanford Cart, beş saat içinde insan müdahalesi olmadan sandalye dolu bir odanın içerisinden başarılı bir şekilde geçerek, otonom bir aracın en eski örneklerinden biri haline gelmiştir.
- 1988-Rollo Carpenter, "doğal insan sohbetlerini ilginç, eğlenceli ve mizahi bir şekilde taklit etmek" için sohbet botu Jabberwacky'yi geliştirmiştir.
- 1997-Deep Blue, bir dünya satranç şampiyonu yenen ilk bilgisayar satranç oyun programı olmuştur.
- 2000-Yapay olarak akıllı bir insan robotu olarak tasarlanan Honda'nın ASIMO robotu, bir insan gibi hızlı bir şekilde yürüyebilme, bir restoran ortamında tepsileri müşterilere sunabilme özelliklerine sahip olmuştur.
- 2009-Google sürücüsüz araç geliştirmeye başlamıştır. 2014 yılında, Nevada'da ABD eyaletinde kendi kendine sürüş testi yapan ilk araba olmuştur. Watson, hızlı cevap verebilen bir konuşma makinesi yapmış ve bu makine iki dil şampiyonunu yenmiştir.
- 2015-Google Project Wing'i kuran ekibin girişimi Skydio dronelar için "yapay zeka" geliştirdiğini duyurmuştur.
- 2017-Google video içeriğini tanıyıp aranabilir hale getiren "machine learning" API'ını yayılamıştır.

Tablo 1. Yapay Zekânın Tarihsel Gelişimi

1950	Çalışmaların başlaması
1955	McCarthy tarafından yapay zekâ teriminin kullanımı
1974	Bilgisayarların hızlanması ve ulaşılabilir olması
1980	Yapay zekâ yılı
2000	Yapay zekânın başarıya ulaşmasının sınır noktası

Kaynak: Data Flair, 2019.

Sonuç olarak yapay zekâ çalışmaları, insanın kendi aklını bir nesneye aktarma çabasıyla özellikle teknolojik gelişmelere koşut bir şekilde hızla ilerlemektedir. Yapay zekânın tarihsel çizgisinde gelişen pek çok olay ve gelişme mevcuttur. Bu alanda çalışanlar, farklı bilim dallarına yeni kapılar açmış ve yapay zekânın çeşitlenmesine olanak sağlamışlardır.

2.3. Yapay Zekânın Çeşitleri ve Bu Alanda Sık Kullanılan Bazı Kavramlar

Teknolojik gelişmeler devam ettikçe yapay zekâ alanında çalışmalara bağlı olarak yeni gelişmeler ortaya çıkmaktadır. Yapay zekânın tek bir tanımının olmadığı gibi farklı yaklaşımlarla farklı çıkarımların elde edilmesiyle yapay zekanın çeşitleri de ortaya çıkmıştır. Örneğin Avrupa Parlamentosu çalışmalarında yapay zekâ konusundaki çalışmaların nasıl ilerlediğine ve geliştiğine dair yapılan bir araştırmada ise yapay zekânın iki temel safhada farklı tiplerde geliştiğinden bahsedilmiştir. Birinci safhada yapay zekânın sembolik bir yanı olduğuna dikkat çekilmiştir. İlk safhada "uzman sistemler", "bulanık mantık" ve "iyi ve eski moda yapay zekâ" şeklinde türlerden bahsedilmiştir. İkinci safhada ise "makine öğrenme süreci" anlatılmıştır. Bu safhada yapay sinir ağları ve derin öğrenme, dil çalışmaları, yapay zekânın geliştirilmesi, yapay zekânın bir sanat olması, büyük veri ve bilgi madenciliği gibi kavramlar ön plana çıkmaktadır. Gelecek safhalarda ise durumsal yapay zekâ, robotik yapay zekâ ve kuantum yapay zekâ gibi farklı yeni çalışma alanlarının ortaya çıkacağı iddia edilmiştir (Boucher, 2019:1-2).

Yapay zekâ çalışmalarında günümüzde sıklıkla kullanılan ve öne çıkan bazı kavramları şu şekilde açıklamak mümkündür:

Uzman sistemler, özel bir alana odaklanarak belirli bir problemin çözülebilmesi maksadıyla kullanılan bilgisayar programlarıdır. Bu sistemlerin kökeni, insan zekâsının bilgiyi işleme sürecinin makine tarafından otomatik olarak gerçekleştirilebilmesi amacıyla sürdürülen çalışmalara dayanmaktadır. Bunu yapabilmek için uzmanların sahip olduğu bilgi ve tecrübelerin bilgisayara aktarılabilmesi ve bilgisayar tarafından bu bilgilerin saklanması gerekmektedir. Böylelikle uzman sistemler, bilgi tabanında saklanan verileri kullanarak insanın karar verme sürecine benzer bir yapıyla belirlenen bir probleme çözüm üretmektedir (İçen ve Günay, 2014: 39).

Bulanık mantık, klasik küme teorisinin bir genellemesi olan bulanık kümelerin matematiksel teorisine dayanan 1965 yılında *Lotfi Zadeh* tarafından *Boolean* mantığının bir uzantısıdır. Bu yöntem, bir durumun doğrulanmasında "seviye" belirleyerek, durumun doğru veya yanlıştan başka bir durumda olmasını sağlamaktadır. Böylece bulanık mantık, yanlışlıkları ve belirsizlikleri hesaba katmayı mümkün kılan akıl yürütmek ya da muhakeme edebilmek için çok değerli bir esneklik sağlamaktadır (Dernoncourt, 2013: 1).

Yapay sinir ağlarının ortaya çıkışı, insan beyninin üstün özellikleri üzerinde bilim adamlarının çalışmasına ve beynin nörofiziksel yapısından esinlenerek matematiksel modelleme çıkarma çabalarına dayanmaktadır. İnsan beyninin bütün davranışlarını tam olarak modelleyebilmek için fiziksel bileşenlerinin doğru olarak modellenmesi gerektiği düşüncesi ile çeşitli yapay hücre ve ağ modelleri geliştirilmiştir. Böylece yapay sinir ağları denen yeni ve günümüz bilgisayarlarının algoritmik hesaplama yönteminden farklı bir bilim dalı ortaya çıkmıştır (Ataseven, 2013: 102).

Makine öğrenme teknolojisi, modern teknolojinin birçok yönünü güçlendirmektedir. Örneğin sosyal ağlardaki web taramalarından içerik filtrelemeye, e-ticaret web sitelerindeki önerilere kadar pek çok makine öğrenme etkisi görülebilir. Makine öğrenme sistemleri resimlerdeki nesneleri tanımlamak için kullanılmakta ve konuşmaları metinlere çevirmekte, nesneleri eşleştirmeler yapmakta, kullanıcıların ilgilerine göre onlara ürünler göndermekte ve arama sonuçlarında arayan kişiye istediği sonuçları sunabilmektedir. Artan bir şekilde devam eden bu uygulamalar, *derin öğrenme* olarak adlandırılan teknik sınıfa girmektedir (LeCun, Bengio ve Hinton, 2015: 436).

Büyük veri ve veri madenciliği kavramları da yapay zekâyla doğrudan bağlantılıdır. Büyük veri; ağırlıklı olarak çeşitli ve kendi içinde bağımsız kaynaklardan gelen dinamik, karmaşık, belirsiz, tamamlanmamış, ayrık ve yığın halindeki bilgi kümelerinden oluşan verileri tanımlamak için kullanılmaktadır. Büyük veri için temel kaynaklar; iş uygulamaları, kamusal ağlar ve sosyal medya gibi alanlardır. Büyük veri madenciliği ise büyük data veri setlerinden oluşan bilgilerin işlenmesini içermektedir (Sherin, Uma, Saranya ve Vani, 2014: 854). Böylelikle veri madenciliği iş dünyası, tıp, bilim ve mühendislik alanlarında geniş ölçekte kullanılmaktadır. Örneğin; hükümetler, sosyal medya ağlarında, bloglarda, online işlemlerde ve diğer bilgi kaynaklarında devletin ihtiyaçlarını karşılamak, olası tehditleri ve beklentileri tahmin etmek ve şüpheli grupları tespit etmek amacıyla veri madenciliği yapmaktadır (Che, Safran ve Peng, 2013: 4).

Yapay Zeka İşletim Sistemi veri alımı ve analizi sağlayan yapay zekâ destekli uygulamaların ve çözümlerin kullanımını sağlayan ortak bir yazılım altyapısıdır. Bilgisayar donanım ve yazılım kaynaklarını yöneten ve genel yapay zekâ aracılığıyla bilgisayar programları için ortak hizmetler sunan yazılım biçimidir. Yapay zekâ işletim sistemi aslında bir bilgisayar sistemindeki sistem yazılımının bir parçasıdır. Klasik anlamdaki işletim sistemi ile benzerlik taşıyan ve yapay zekâ ile çalışan aiWARE dünyadaki ilk yapay zekâ işletim sistemidir.

ABD menşeli bir şirket olan Veritone tarafından geliştirilmiştir. Yapay zekâ teknolojilerinin gereksinim duyduğu motorlara sahip olan aiWARE ses, görüntü, video, metin vb. gibi karmaşık, yapılandırılmamış verileri okuma yeteneğini birleştiren ve önemli içgörülerin hızlı analizini sağlamak için yapay zekayı kullanan tek platformlu bir yaklaşımı temsil etmektedir. "aiWare", özellikle uçtan uca süreç otomasyonunu yürütmek için gelişmiş akıllı otomasyon ile entegre olma yeteneğine sahiptir (Gutierrez, 2021). Bu bağlamda aiWARE uygulamasının; yüz tanıma, ses parmak izi, logo algılama, pkala tanıma ve nesne algılama gibi geleceğe yönelik yapay zeka hizmetleri (bilişsel yetenekler) sunması beklenmektedir (Python Dünyası, 2020).

3. Yapay Zekanın Kullanım Alanları/Uygulamaları

Yapay zekâ toplumsal yaşamda birçok şeyi etkilemekte ve değiştirmektedir. Örneğin, 1950'lerden bu yana birisinin zaman içinde yolculuk ettiği ve 2019 yılına geldiği düşünüldüğünde; insanların Facebook, Instagram ve Twitter gibi sosyal medya kanallarına olan bağımlılığını gördüğünde oldukça şaşkına döneceğini tahmin etmek mümkündür. Aynı zamanda bu kişi, akıllı telefonların şehirlerde dolaşmak için nasıl kullanıldığını, Alexa ve Cortana gibi sanal dijital asistanların sorulan sorulara nasıl cevap verdiğini görse ne derece hayret içinde kalacağı tahmin edilebilir. Bu nedenle yapay zekânın tüm insanlar için artık günlük hayatın ayrılmaz bir parçası olduğuna şüphe yoktur. Dahası finansal kurumlar, kamu kurumları, medya şirketleri ve sigorta şirketleri, yapay zekâyı kendi yararlarına kullanmanın yollarını bulmuşlardır. Dolandırıcılıkların tespitinden, doğal dil işleme ve yasal süreçlerin takibine kadar birçok alanda yapay zekânın kullanımı oldukça geniş bir alanı kapsamaktadır (Marr, 2020). Yapay zekâ hakkında Tesla ve SpaceX CEO'su Elon Musk, yapay zekânın herhangi bir insandan daha zeki olacağını ve 2025 yılı itibarıyla insanoğlunu geride bırakacağını iddia etmiş ve yapay zekâ teknolojisinin insanlığı önemli ölçüde değiştireceğini ifade etmiştir (Moran, 2020). Yapay zeka uygulamaları Tablo 2'de sunulduğu gibi küresel pek çok şirket aktif olarak kullanmaktadır.

Tablo 2. Yapay Zekâ Kullanan Şirketler ve Yapay Zekâ Uygulamaları

	Teknoloji /Platformlar	Yapay Zekâ Uygulamaları
Google Deepmind	Arama Motoru, Haritalar Reklamlar, Gmail, Android, Google Chrome ve Youtube	İnsansız Arabalar
	Derin Q-Ağlar	Bilgisayar Programı Alpha Go, Derin Öğrenme odaklı oyunlar: DQN, İnsan Sesi Çalışmaları: Wavenet
OpenAI	Kar amacı gütmeyen Kuruluşlar, Evrimsel Algoritmalar, Derin Sinir Ağları	Derin Sinir Ağları ile çalışan Evrimsel Algoritmik Sistemler, Testbeds
IBM	Bilgisayar Donanım ve Yazılım Üreticisi Barındırma ve Danışma Hizmetleri Bilişsel Hesaplama	Deep Blue: Dünya'daki Satranç şampiyonunu yenen ilk program
Facebook	Sosyal Ağ Hizmeti	Uygulamalı Makine Öğrenme İnsan Bilgisayar Etkileşimi
Apple	Bilgisayar Donanım ve Yazılım Tüketici Elektronik Ürünler Online Hizmetler	Siri: Sanal Danışman İnsansız Arabalar
Amazon	Bulut Hesaplama Online Parakende Hizmetler Elektronik Ürün ve Hizmetler	Alexa: Sanal Danışman Amazon Yapay Zekâ Programı
Microsoft	Geliştirme, Üretme ve Lisans Bilgisayar Donanım ve Yazılım Tüketici Elektronik Ürünleri	Microsoft Azur Cortana

Kaynak: Perez, Deligianni ve Ravi, 2017:15.

Ayrıca Yapay zekâ uygulamalarına sağlık, teknoloji ve savunma gibi pek çok alanda rastlamak mümkündür. Sağlık alanındaki yapay zekâ uygulamalarına bakıldığında genel olarak tıbbi görüntüleme, tıbbi kayıt, ilaç sektörü, robot uygulamaları, büyük veri analizi, erken tanı ve tedavi, hatasız uygulamanın sağlanması ve gereksiz tedavilerin önüne geçilmesi gibi konular üzerine çalışmalar yoğunlaşılmıştır. Derin öğrenme teknolojisini kullanarak radyoloji ve patoloji görüntüleri, kan testleri ve EKG'ler gibi analiz işlemlerinde yapay zekâ kullanılmaktadır (Uzun, 2020: 86, 89).

Yapay zekânın kullanıldığı bir diğer uygulama çeşidi de insansız araçlardır. Bu araçlar, artık birçok konuda insanlara yardımcı olan araçların yerini almaktadır. Robotlar evdeki ve ofislerdeki temizlik işlerini otomatik olarak vakum sistemleriyle yerine getirmektedir. Günümüzde "chatbot"lar hayatımızı kolaylaştırmak amacıyla birçok alanda programa yüklenen bilgiler sayesinde günlük ajanda olarak kullanılmakta, gidilecek yer hakkında bilgi vermekte, konuşulduğunda doğrudan konuyla ilgili cevap vermektedir. Sağlık alanında birçok bilgi yüklenen robotik sistemler, hastalara teşhisler koyarak hastalıkların erken tedavisinde önemli rol oynamaktadır (Zanzotto, 2019: 243).

Yapay zekânın kullanım alanları arasında sanal asistanlar da bulunmaktadır. Örneğin Tablo 2'de de gösterildiği gibi Apple firması tarafından üretilen SİRİ ve Amazon firması tarafından tanıtılan ALEXA programı bu alanda önemli uygulamalar arasındadır. Sağlık alanında COGİTO, TESLA otonom araçları, öğrenme, karar verme, daha rahat ve konforlu tatil planı yapma için tatil firmaları tarafından kullanılan BOXEVER vb. birçok sanal asistan yapay zekâyı kullanmaktadır. Yapay zekâ sayesinde hizmet veren bu uygulamalar, büyük şirketlerden bireylere kadar her alanda günlük hayatın ayrılmaz birer parçası haline gelmiştir (Yefimçik, 2019).

Dahası bilgisayar teknolojisindeki gelişmelerle sürrealist bilgisayarlar, yapay zekâyla kelimeleri resimlere dönüştürmeye başlamıştır. Bu yapay zekâ gelişimi, OpenAI şirketi uzmanları tarafından geliştirilmiştir. Uzmanlar bilinen sinir ağları GPT-3'e DALL E isimli yeni bir modül ekleyerek daha da geliştirmişlerdir. Örneğin GPT aktif bir şekilde kullanılmaktadır. Bu sinir ağları "chatbot" olarak mevcut durumda kullanılmaktadır. Bir kişi, chatbota soru sorduğunda yalnızca bildiği soruları sistem cevaplamaktadır. Fakat DALL E modülüyle birlikte kelimeler artık resimlere dökülmektedir. Örneğin "Köpek yangın esnasında çocuğu nasıl kurtardı?" sorusuna yeni yapay zekâ sistemi, bu olayı resimleştirerek görsel hale çevirmektedir (Glyantsev, 2021).

Yapay zekânın uygulama alanlarından birisi de eğitim alanıdır. Örneğin Çin merkezli yapay zekâ destekli uyarlanabilir eğitim sağlayıcısı olan SquirrelAI, her öğrenciye ayrı ayrı yapay zekâ öğretmeni sağlayabilmek amacıyla çalışmalarını sürdürmektedir. ABD merkezli McGraw-Hil tarafından uyarlanabilir yapay zekâ eğitim programı olan ALEKS geliştirilmiştir. Yine ABD'de IBM tarafından tasarlanan Watson isimli yapay zekâ programı 2010 yılında kullanılmaya başlanmış ve program kendisini geliştirerek günümüzde sadece okullarda değil, bütün işletmeler için birçok alanda kullanılmaya başlanmıştır. Bu program sayesinde öğrencilere kişiselleştirilmiş öğrenme fırsatı sunulurken, öğrencinin öğrenme potansiyeli ortaya çıkarılmakta ve verimliliğin en üst düzeye çıkarılması hedeflenmektedir (İşler ve Kılıç, 2021: 6).

Yapay zekâ çeşitli uygulama alanlarında görüldüğü üzere toplumsal hayat üzerinde ciddi avantajlar sağlamaktadır. Yapay zekânın yakın gelecekte daha da geliştirilmesi diğer alanlarda olduğu gibi trafik güvenliği açısından da yarar sağlayacaktır. Araçların

güvenliği artacak ve trafikte birçok karmaşıklık ortadan kalkacaktır. Benzer şekilde yapay zekâdan belki başka bir çalışmanın konusunu oluşturabilecek kamu bürokrasisi de etkilenecek; yapay zekâ uygulamaları geleneksel yönetim anlayışının önemli özelliklerinden birisi olan bürokratik çıkmazların önüne geçilmesinde etkili olacaktır. En basit haliyle uzun zaman alan monoton işlerin hızlanmasına katkı sağlayacaktır. Çeşitli algoritmaların kullanılmasıyla karar alma süreçlerinin güçlendirilmesine ve bazı karmaşık girdilerin kullanılması yoluyla karar ağacı çıkartılıp örgütlerde daha kolay karar alma sürecinin gerçekleşmesine imkan tanıyacaktır (Randall, 2019).

4. Yapay Zekânın İç Güvenlik Yönetimi Üzerine Yansımaları

İnsan zekâsının ve aklının bilgisayar programları ve yazılımları tarafından taklit edilmesine dayanan yapay zekâ; bir sistemin harici verileri doğru bir şekilde yorumlama, bu tür verilerden öğrenme ve bu öğrendiklerini esnek adaptasyon yoluyla belirli hedeflere ve görevlere ulaşmak için kullanma kabiliyetidir. Yapay zekâ; iç güvenlik aktörlerinin ve örgütlerinin iç güvenliğe ilişkin faaliyet yürütme tarzını değiştirme potansiyeli olan, teknoloji ve dijitalleşmeden maksimum derecede istifade eden, günümüz çağının paradigma değiştiricisi, yeni bir oyun kurucusu haline gelmiştir. Savunma, istihbarat, kamu güvenliği, terörle mücadele, acil müdahale, ekonomi güvenliği, sınır gözetimi ve bu çalışmada odaklanılan siber güvenlik gibi iç güvenliğin neredeyse hemen hemen her yönü, yapay zekâ tarafından şekillenebilmektedir (Homeland Security Research Corporation, 2020).

4.1. İç Güvenlik Yönetiminde Yapay Zeka Uygulamaları

2018 yılı itibarıyla dünya üzerinde birçok ülke, yapay zekâ uygulamalarına yönelik ulusal stratejiler belirlemişlerdir. Örneğin; ABD, İtalya, İngiltere, Rusya Federasyonu, Güney Kore, Polonya, Almanya, Arjantin, Avusturya, Avustralya, Yeni Zelenda, Brezilya, Kanada,Şili, Fransa, Danimarka, Estonya, Finlandiya, Hindistan, İrlanda, Japonya, Kenya, Litvanya, Malezya, Meksika, Hollanda, Norveç, Suudi Arabistan, Sırbistan, Singapur, İspanya, İsveç, Tunus, Birleşik Arap Emirlikleri ve Uruguay devletleri ulusal strateji olarak yapay zekâ çalışmalarına devlet politikalarında yer vermişlerdir (Future of Life Institute, 2021). Dolayısıyla son yıllarda iç güvenlik yönteminde teknoloji tabanlı yeni yöntemlere ihtiyaç duyulduğu ve küresel bağlamda birçok ülkenin yapay zekâ uygulamalarını devlet politikası seviyesinde yasal çerçeveye aldıkları söylenebilir.

Dijital toplumun sağlıklı bir biçimde işleyebilmesi için toplumun siber saldırılara karşı minimum seviyede olumsuz etkilenmesi gerekmektedir. Bu nedenle devletler siber güvenliği öncelikli güvenlik alanı olarak görmektedir. Öyle ki siber güvenlik ve yapay zekânın iki önemli güvenlik çıktısı vardır: yapay zekâ temelli çözümlerde güvenlik ve geliştirilmiş siber güvenlik için yapay zekâya dayalı güvenliktir. Yapay zekâ uygulamaları; sensörler, iletişim ağları, bilgi merkezleri, büyük veri ve software aracılığıyla geniş uygulama alanı bulmaktadır. Norveç Ulusal Güvenlik Otoritesi'nin temel prensipleri,

Norveç kamu ve özel örgütleri için birçok çözüm sunmaktadır. Norveç hükümeti, 2019 yılında siber güvenliğin sağlanması amacıyla ulusal güvenlik stratejisi çalışması hazırlamıştır (Norwegian Ministry of Local Government and Modernization, 2019: 64, 65):

Öte yandan ABD internet tabanlı geliştirilen yapay zekâ uygulamalarına yönelik güvenlik temelli bazı uygulamalar oluşturulmuştur. Örneğin "Affectiva" programı, yapay zekâyı kullanarak insanların duygularını, bilişsel durumlarını, hareketlerini ve insanların kullandığı diğer nesneleri anlayabilmektedir. Bu program için yapay zekâ teknolojisiyle 90 farklı ülkeden 10 milyon yüz ve ses analiz edilmiştir. Böylece bir tür veri havuzu oluşturulmuştur. Bir başka uygulama ise bir IP soft şirketi olan Amelia'dır. Yapay zekâ kullanılarak bu uygulamayla insanın duygu, ifade ve anlayışını en iyi biçimde ifade eden bir program oluşturulmaya çalışılmaktadır. Bunların yanı sıra Darktrace, Fetch.ai, Skymind ve SparkCognition da yapay zekâ uygulamalarından bazılarıdır (Dawns, 2021).

Yapay zekâ, otonom silah sistemlerinde ordular tarafından da kullanılmaya başlanmıştır. Artık yapay zekâ tabanlı 35 dolarlık bir bilgisayar, simülatör savaşında ABD'de eğitilmiş bir savaş pilotunu yenebilmektedir. Rus Askeri Sanayi Komitesi, 2030 yılına kadar Rus savaş gücünün yüzde 30'luk kısmını tamamen uzaktan kontrol edilebilen otonom robotik platformlarla donatmasına yönelik bir planı onaylamıştır. Diğer ülkelerin de benzer şekilde ulusal güvenlik ve demografi sorunlarına çözüm aramaya yönelik amaçları vardır. Örneğin Japonya ve İsrail gibi ileri sanayii ve teknoloji altyapısına sahip olan ülkelerin demografik sorunları olduğundan bu ülkeler, ulusal güvenliklerini sağlamak amacıyla otonom silah sistemlerine odaklanmaktadırlar (Allen ve Chan, 2017: 21).

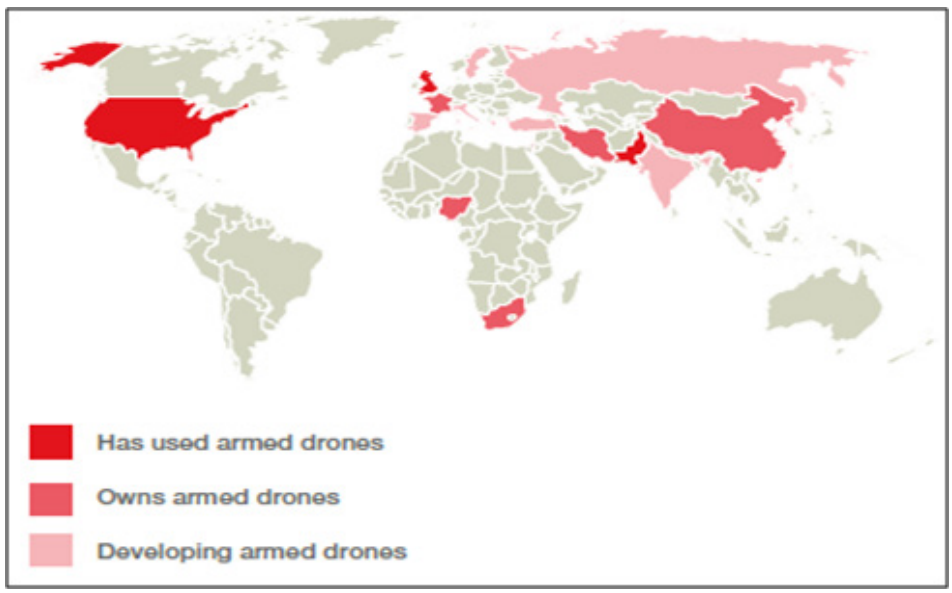
İnsansız hava araçları, yeni nesil kablosuz iletişim ağları için gelecek vaat eden teknolojilerden biri olarak kabul edilmektedir. Bu araçların, hareketlilikleri ve görüş hattı bağlantıları kurma yetenekleri, onları birçok potansiyel uygulama için önemli sorun çözme aracı haline getirmiştir. Aynı şekilde, yapay zekâ günümüzde hızla gelişmeye devam etmektedir ve özellikle mevcut verilerle yapılan çalışmalarda oldukça önemli başarılar elde edilmiştir. İnsansız hava araçlarının etkin bir şekilde kullanılması ile ilgili çeşitli problemlerin çözülmesinde yapay zeka algoritmaları uygulanarak, bu hava araçlarına "zekâ" entegre edilmeye başlanmıştır (Lahmeri, Kishk ve Alouini, 2021: 1015).

İç güvenliğin sağlanmasında önemli bir alan olan bilgi güvenliğinin yapay zekâ uygulamalarıyla yakın ilişkili olduğunu söylemek mümkündür. Çünkü hem devletin hem de özel sektörün bilgi güvenliklerinin korunması amacıyla kullanılan birçok uygulama bulunmaktadır. Siber saldırılara karşı virüs programları örnek olarak gösterilebilir. Virüs programlarına yüklenen verilerle, dışarıdan gelebilecek "hackleme" saldırılarına karşı savunma oluşturulmaktadır. Böylece yapay zekâ yüklü sistemler kullanılarak kurumsal veriler korunmaktadır. "Endpoint detection and response (EDR), NDR (Network Detection and Response), UEBA (User and Entity Behavior Analytics) ve TIP (Threat Intelligence Platform) gibi uygulamalar, bilgi güvenliğini sağlayan dijital dünyanın uygulamaları arasında yer almaktadır (Şabanov, 2020).

"Ses kayıt algoritmaları" uygulaması, ABD Sahil Güvenlik Birimleri tarafından kullanılmaktadır. Bu uygulamayla fiziksel görünümlerin oluşturulması amacıyla sesler analiz edilmektedir. Bu durum, kriminal incelemelerde hatalı sinyallerin ortadan kaldırılmasına yardımcı olmaktadır. Diğer bir uygulama "makine öğrenimi için açık kaynak verileri" uygulamasıdır. Bu uygulama sayesinde Alphabet şirketi KAGGLE platformuyla birlikte ABD İç Güvenlik Departmanı, Ulaştırma Güvenlik Yönetiminden aldığı verilerle, yasadışı ve tehlikeli malların kontrol edilmesi amacıyla yolcu bagajlarını inceleyerek daha iyi algoritmalar geliştirmeye çalışmaktadır. Dahası ABD'de sınır güvenliğinin sağlanmasında yapay zekâ sistemleri kullanılmaktadır. Sınır güvenliğinde insansız hava araçları ve yer robotları gözlem amaçlı kullanılmaktadır (Horowitz vd., 2018: 12). Ayrıca ABD Silahlı Kuvvetleri, yapay zekâ kullanılan otonom araçlar ve otonom silahlar üzerine çalışmalarını sürdürmektedir. ABD Hava Kuvvetleri'nin yanı sıra, Deniz ve Kara Kuvvetlerinde de otonom araçların prototip testlerine başlanmıştır. Örneğin Çok Amaçlı Taktik Ulaşım aracı üzerine çalışmalar sürdürülmektedir (Hoadly ve Lucas, 2018: 11,12).

Dünya üzerinde yapay zeka kullanan güvenlik temelli pek çok araştırma vardır. Örneğin, bir çalışmada yapay zekânın etik boyutuna dikkat çekilmiştir. Çalışmada dünya üzerinde yapay zekânın güvenlik ve silahlanma boyutuna karşı etkileri incelenmiştir. Şekil-1'de görüldüğü gibi ülkelerin güvenlik politikalarında bir araç olarak kullanılan ve geliştirilmeye çalışılan silahlı insansız hava araçları gösterilmiştir (Perez vd., 2017:39).

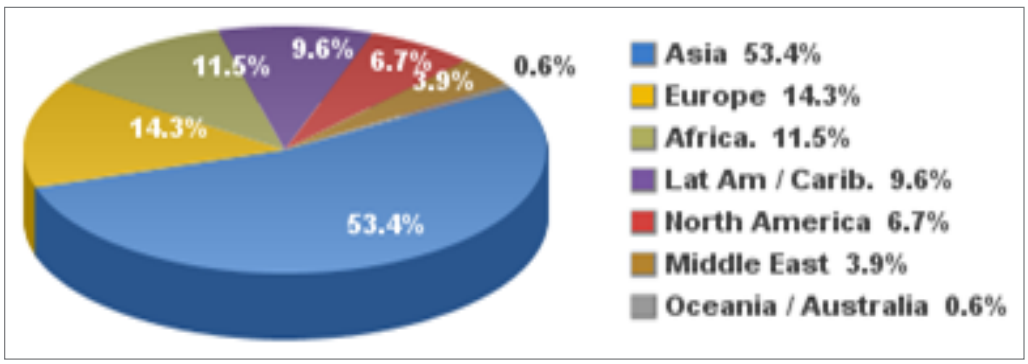
Şekil 1. 2017 Yılında Dünya Üzerinde Silahlı Dronların Kullanımı



Kaynak: Perez vd., 2017:37.

Şen ve Yurtoğlu (2020), güvenlik ve teknoloji bağlamında yapay zekânın istihbarat analizindeki yerini ve önemini inceleyen bir çalışma yapmıştır. Bu çalışmada, teknoloji ve güvenlik arasındaki ilişkiye dikkat çekilmiş olup, siber güvenlik çalışmalarının da bu süreçten bağımsız olmayacağına vurgu yapılmıştır. Bu anlamda siber güvenliğin hem devletler hem de bireyler için önemli bir güvenlik alanı olduğu belirtilmiştir (Şen ve Yurtoğlu, 2020:23-26). Şekil-2'de gösterildiği gibi dünyada 31 Mart 2021 tarihinde internet kullanıcı sayısı 5 milyarı geçmiştir. Bu durumda internet kullanımının artması yapay zekâ uygulamalarını doğrudan arttıracağı gibi, siber güvenlik alanında da yapay zekânın daha etkin kullanılmasına neden olacaktır.

Şekil 2. 2021 Yılında Dünya Üzerinde İnternet Kullanıcı Sayısı



Kaynak: Internet World Stats, 2021

Dolayısıyla yapay zekânın kullanılmasıyla sosyal medya, arama motorları ve bilgi belge arşivleri gibi çeşitli kaynakları Büyük Veri çerçevesinde kullanılmaktadır. Büyük Veri, istihbarat analizlerine önemli katkı sağlamaktadır. Ayrıca Veri Madenciliği (*Data Mining*), Veri Bilimi (*Data Science*), Makine Öğrenmesi (*Machine Learning*), Derin Öğrenme (*Deep Learning*) gibi terimlerde bu alanda kullanılan teknikler arasındadır (Şen ve Yurtoğlu, 2020:27). Yazarlar, yapay zekânın istihbaratın üç evresinde (veri toplama, analiz etme ve istihbarat üretme) kullanılabileceğini belirtmişlerdir (Şen ve Yurtoğlu, 2020:45).

Türkiye'de yapay zekâ konusunda çalışmalar son dört yılda yediye katlanmıştır. Türkiye Yapay Zekâ İnisiyatifi (TRAI) verilerine göre Türkiye'de yapay zekâ konusundaki girişim sayısı 164'e ulaşmıştır. Bunun yarısı görüntü işleme ve makine öğrenmesi alanında faaliyet göstermekle birlikte öngörü ve veri analitiği, arama asistanı ve arama motoru, doğal dil işleme, chatbot ve diyalogsal yapay zeka, optimizasyon, otonom araç, robotik süreç otomasyonu ve akıllı platform alanı gibi kategorilerde yapay zekâ uygulamaları ile karşılaşılmaktadır (Haber Türk, 2021). Ayrıca, Türkiye'de ilk defa yapay zekâ konusunda yol haritası niteliğinde Ulusal Yapay Zekâ Stratejisi (2021-2025) Cumhurbaşkanlığı Genelgesi ile Resmi Gazete'de yayımlanmış, yapay zekâ konusunda ilk ve en kapsamlı metin olmuştur. Cumhurbaşkanlığı Dijital Dönüşüm Ofisi Başkanlığı (CBDDO) ve Sanayi ve

Teknoloji Bakanlığı tarafından hazırlanan Türkiye'nin yapay zekâ stratejisi; yapay zekâ uzmanı yetiştirme, yapay zekâ konusunda istihdamı artırma, araştırma, girişimcilik ve yeniliği destekleme, kaliteli veriye ve teknik altyapıya erişim, sosyo-ekonomik uyumu hızlandıracak düzenlemeler yapmak, uluslararası iş birliklerini güçlendirmek ve yapısal ve işgücü dönüşümünü hızlandırmak olarak belirlenmiş; bu öncelikler bağlamında da 24 amaç ve 119 tedbir belirtilmiştir (CBDDO, 2021).

Türkiye'de iç güvenlik alanına yönelik siber savunma yazılımları geliştirilmekte, Türk Bilim Vakfı (TBV), Türkiye Bilişim Sanayicileri Derneği (TUBİSAD) ve Türk Elektronik Sanayicileri Derneği (TESİD) gibi sivil toplum kuruşları ve Dijital Türkiye Platformu gibi platformların işbirliği ile vatandaşı, devleti ve iş dünyasını kapsayan bütüncül bir dijital dönüşüm gerçekleştirmesini sağlayacak politika önerileri oluşturulmaktadır (TÜBİSAD, 2019). Cumhurbaşkanlığı Savunma Sanayii Başkanlığı (CBSSB) koordinasyonunda Sürü İHA sistemleri konusunda projeler yürütülmekte, Sürü İHA Teknoloji Geliştirme ve Gösterim Projesi kapsamında mikro ölçekli firmalar ve KOBİ'lerin katılımıyla insansız platformların Sürü konseptinde kullanımına yönelik algoritma ve yazılımların geliştirilmesi hedeflenmektedir. İHA'lar sınır ötesinden iç güvenliğe yönelebilecek tehditlerin berteraf edilmesinde etkili rol oynamakta, görüntü işleme algoritmaları ile yapay zekâ ve makine işleme tekniklerinden yararlanarak hedef tespitini hassasiyetle yapabilmekte, istihbarat/görüntü kıymetlendirme çözümleriyle entegre şekilde çalışabilmektedir (Anadolu Ajansı, 2020).

Cumhurbaşkanlığı Bilim, Teknoloji ve Yenilik Politikaları Kurulu tarafından önümüzdeki on yıl içerisinde dünyada ve Türkiye'de etkisini derinden hissettirecek öncelikli alanların belirlenmesine ilişkin çalışmada 'yapay zekâ ve makine öğrenmesi' ile 'büyük veri ve veri analitiği' konularının ekonomik etki, sosyal fayda ve ulusal güvenlik açısından en etkili alanlar olduğu saptanmıştır (Sanayi ve Teknoloji Bakanlığı ve CBDDO, 2021: 37). Kurul'un bünyesinde hazırlanan "Yapay Zekâ Teknoloji Yol Haritası" çerçevesinde teknolojiler özelinde hedefler belirlenmiş, AR-GE projeleri ve geliştirilen ürün ya da teknolojilerin öncelikli uygulamaları ele alınmıştır. Bu kapsamda yapay zekâ alanında TÜBİTAK tarafından özel sektöre verilen destekler ve dağılımlar incelendiğinde Ocak 2007 ila Mart 2020 arası dönemde 1290 proje gerçekleştiği görülmektedir. Proje sayısı, bütçesi ve kullanım alanları incelendiğinde ilk beş sırada "sanayinin dijital dönüşümü ve ileri imalat sistemleri", "ticarete dijital dönüşüm", "akıllı yaşam ve sağlık", "oyun, medya ve eğlence", "finans sektöründe dijital dönüşüm" gelmektedir. Altıncı sırada ise 1290 projenin 67'sini oluşturan ve 116.823.161 TL'lik bütçeye (1.566.647.146 TL'lik genel bütçesnin yüzde 7'si) sahip "savunma ve güvenlik" alanı gelmektedir (Sanayi ve Teknoloji Bakanlığı ve CBDDO, 2021:46). Bu kapsamda Savunma Sanayii Başkanlığı tarafından savunma ve güvenlik konseptinde çeşitli sorun alanlarına ve ihtiyaçlara yönelik yapay Zekâ teknolojileri içeren AR-GE projeleri şu şekildedir (Sanayi ve Teknoloji Bakanlığı ve CBDDO,2021: 55):

- Sosyal Medya Anomali Tespiti, Olay Takibi ve Analizi
- Derin Öğrenme Büyük Veri Analiz Platformu
- Sosyal Medya Analizi Performans Geliştirilmesi
- Küresel Konumlama Sistemi Bağımsız Otonom Seyrüsefer Geliştirilmesi
- Radar ile Tespit Edilen Su Üstü Hedeflerin Sınıflandırılması ve Kimliklendirilmesi
- İşbirlikçi Robotlar ile Otonom Keşif, Güdüm ve Seyrüsefer
- Hareket Tarzı Geliştiren Yapay Zekâlı Komutan Asistanı
- Kara Araçları İçin Yapay Zekâ Destekli Atış Kontrol ve Otonom Sürüş
- Yazılım Tanımlı Ağlarda Yapay Zekâ Temelli Zafiyet Tespiti ve Engelleme
- Küresel Zafiyet Analizi

Devletin ve vatandaşlarının her türden krizden ve tehditten korunması anlamına gelen ulusal güvenlik kavramını da içerisinde barındıran iç güvenlik; hem bir devletin egemenlik sahasındaki ülke sınırları içerisinde ortaya çıkabilecek hem de sınır ötesi aktörlerden gelebilecek güvenliğe yönelik saldırılardan korunması ve barışın tesis edilmesi durumudur (İrdem, 2020: 24-26). Dolayısıyla iç güvenlik alanında yapay zekâ uygulamaları günümüzde, farklı projeler ve programlar çerçevesinde hızla gelişen teknolojiye koşut bir biçimde yaygınlaşmaya devam etmektedir. İç güvenlik uygulamaları kapsamında kişisel verilerin korunması; insan yüz tanıma sistemlerinin yaygınlaşması; sensörlerin, kamera sistemlerinin ve bilgi merkezlerinin kurulması; büyük veri ve siber savunma çalışmalarının hızlanması ve insansız hava araçlarının kullanılmaya başlanması yapay zekâ kullanılan temel iç güvenlik uygulama alanları arasındadır. Böylece gelişen ve değişen dijital toplumun güvenlik ihtiyacı, yeni şartlara uygun olarak yapay zekâ uygulamalarıyla pekçok ülkede hayata geçirilmiştir.

Günümüzde teknolojik gelişmelerin hızlı bir şekilde artması, bilişim, iletişim ve bilgi güvenliğinin sağlanmasına yönelik talepleri kaydadeğer ölçüde artırmıştır. Bu sebeple, iç güvenlik yönetiminde siber güvenliğin sağlanması, çağımızda bilgi toplumunun en temel tartışma konusu haline dönüşmüştür. Böylelikle iç güvenlik temelli yapay zekâ uygulamalarından siber güvenliğin sağlanması, devletlerin güvenlik politikalarının başat konusu olmuştur.

5. Yapay Zekâ ve Siber Güvenlik

Sistemleri, ağları, verileri, programları çeşitlenen siber saldırılardan korumak ve siber ortamda karşılaşılabilecek her türlü tehdidi berteraf etmeye odaklanan siber güvenlik konusu 21'inci yüzyılın en önemli güvenlik sorunlarından birisi haline gelmiştir.

Siber suçların sayısının, boyutunun ve gizliliğinin gün geçtikçe arttığı günümüzde devletler, güvenlik politikalarında siber güvenliği mutlaka göz önünde bulundurmak durumunda kalmaktadır. Siber ortamdaki bilişim sistemlerine yönelik saldıların önlenmesini, siber ortamda işlenen verinin gizlilik, bütünlük ve erişilebilirliğinin güvence altına alınmasını, saldırıların ve siber güvenlik olaylarının tespit edilmesini, bu tespitlere karşı tepki mekanizmasının devreye sokulmasını ve akabinde de gerçekleşen bir siber güvenlik sorunu ile karşı karşıya kalındığında olay öncesi duruma tekrar dönülmesini esas alan siber güvenlik; devletin bekası, bilgi güvenliğinin sağlanması ve gelişen teknolojilerin ortaya çıkardığı sorunlar karşısında gerekli önlemlerin alınmasını sağlamaktadır (Erendor, 2019: 155).

Tablo 3. Siber Güvenlik Tehditleri, Aktöreler ve Amaçlar

Tehditin Seviyesi	Aktör	Amaç
Ulusal Güvenliğe Yönelik Tehditler	Bilgi Savaşçısı (Siber Asker)	Bir devletin karar verme kabiliyetinin kısıtlanması, ülkede kaosa ve psikolojik terör ortamı yaratmak.
	Ulusal İstihbarat Görevlisi (Siber Casus)	Siyasi, ekonomik, askeri üstünlükler kazanmak maksadıyla bilgi sızdırmak.
Devletler ve Özel Sektör Tarafından Karşılaşılan Müşterek Tehditler	Siber Terörist	Eylemlerinin kitleler tarafından görünür olmasını sağlama; politik değişiklikler yaratmak.
	Endüstriyet Casusluk	Rekabet üstünlüğü elde etmek.
	Organize Suç	***İntikam dürtüsüyle hareket e***tmek, maddi kazanç sağlamak; kurumsal/politik değişikler yapmak.
Yerel Tehditler	Kurumsal Hacker'lar	Maddi kazanç sağlamak; heyecan / meydan okumak; tanıtım yapmak ve prestij kazanmak.
	Eğlence Amaçlı Hacker'lar	Heyecan, meydan okumak.

Kaynak: Karasoy, 2021: 23.

Saldırıları tespit etmenin ve suçluları yakalayabilmenin oldukça zor olduğu siber güvenlik anlayışında saldırılar çeşitli yöntemlerle gerçekleştirildiğinden kamu hizmetlerinin aksatılmasından halkın refahının ve güvenliğinin tehlika altına girmesine kadar olumsuz çıktılarla karşılaşılmaktadır. Siber saldırılarla veriler çalınabilmekte, ulusal

güvenlik bilgisayar programlarına müdahalede bulunulabilmekte, acil servisler, elektrik dağıtım sistemleri, telekominikasyon kanalları, su dağıtım ağları, mali sistemler ve hava alanları kapatılabilmektedir (Yanarışık, 2020:304). Bilhassa yapay zekâ destekli saldırılar siber saldırıların daha tehlikeli bir boyut kazanmasına neden olabilmektedir. Yapay zekâ otonom araçlar ve insansız hava araçları da dahil olmak üzere çok sayıda sistemi ele geçirerek bu sistemleri potansiyel silahlara çevirmek için kullanılabilmektedir (Yanarışık, 2020: 308). Bu nedenle dijital çağda devletlerin ortaya çıkması muhtemel sorunlarla karşılaşmaması veya tehditleri elimine etmesi için yapay zekâ tabanlı siber güvenlik uygulamalarına önem vermesi gerekmektedir. Siber güvenlik sistemlerinin daha güçlü bir yapıya kavuşturulması ve siber güvenlikle ilgili strateji belirlenmesi proaktif ve reaktif anlamda siber güvenliğin sağlanmasında etkin rol oynamaktadır.

Yukarıdaki tablo incelendiğinde ulusal güvenliğe yönelik tehditler tehdit seviyesinin en üstünde yer almaktadır. İkinci seviyeyi devletler ve özel sektör kuruluşları tarafından karşılaşılan ortak tehdit alanları oluşturmakta, üçüncü seviyeyi ise diğer ikisine kıyasla daha az tehdit seviyesine haiz lokal tehditler oluşturmaktadır. Her ne kadar tehditlerin seviyesi ve amacı birtakım farklılıklar içerse de devletler veya devlet dışı başkaca aktörler tarafından gerçekleştirilen siber saldırılar yıkıcı sonuçlar doğurabilmekte, geleneksel savaş ve saldırı konseptini dönüştürmektedir.

Yapay zekâ, gelişen teknoloji ve siber ortam güvenlik yönetimi sürecinde maruz kalınan tehditlerin doğasını ve çevresini değiştirerek kamu düzenini bozan suç şebekelerinin yöntemlerinde değişiklikler meydana getirmektedir. Devletler gerek dış güvenlik bağlamında gerekse iç güvenlik bağlamında çeşitli aktörler (devletler, devlet dışı örgütler, korsanlar, suç örgütleri vb.) tarafından gerçekleştirilen saldırılara ve hibrit tehditlere açık hale gelmekte, dijital medyada yürütülen dezenformasyon ve algı operasyonları ile karşılaşmaktadır. Ayrıca çok uluslu şirketler tarafından vatandaşların sosyal medya paylaşımlarının depolanması ya da bireylerin sosyal medya üzerinden manipüle edilmesi veri güvenliğini ve toplumsal güvenliği olumsuz etkilemektedir. Bu nedenle iç güvenlik yönetiminde devletlere düşen önemli görevlerden birisi de bir yandan ülkenin stratejik kurumlarına, eğitim, sağlık, güvenlik, ekonomi gibi alt yapılarına yönelik saldırıların bertaraf edilmesi, diğer yandan da bireylerin dijital kişiliğinin korunması anlamına gelen dijital güvenliğinin muhafaza edilmesidir.

Dijitalleşme ile birlikte gelişen teknolojiler milyonlarca veri kümesini hızla analiz etme ve kötü amaçlı yazılım tehditlerinden kimlik avı saldırısıyla sonuçlanabilecek gölgeli davranışlara kadar çok çeşitli siber tehditleri izleme yeteneğine sahip olduğundan, yapay zeka ve makine öğrenimi artık bilgi güvenliği için gerekli hale gelmiştir. Hızla gelişen siber saldırıların ve teknolojik cihazların hızla artmasıyla yapay zeka ve makine öğrenimi, siber suçlulardan haberdar olmayı sağlamakta, tehdit algılamayı otomatikleştirmekte ve geleneksel yazılım odaklı veya manuel tekniklerden daha etkili sonuç vermektedir (Belani, 2021).

Yapay zekâ veya insan yapımı bilinç ve makine öğrenimi programlaması, önceki olayların sonuçları aracılığıyla öğrenmekte ve belirlenen hedefe ulaşmada kolaylık sağlamaktadır. Bunun yanında dijital saldırıların önlenmesinde güvenlik uzmanları tarafından yapay zekâ tabanlı cihazlar kullanılsa da makine öğrenimi ile birlikte insan yapımı zeka, sohbet robotları aracılığıyla çok miktarda spam/yanlış beyan/kimlik avı mesajı göndermekten, spekülasyon yapan yapay zeka destekli gizli anahtara ve kriptografik saldırılar yürütmeye kadar birçok saldırı biçimini gerçekleştirmek için de kullanılabilmektedir (Kumar, Saini ve Cuong, 2021:9). Ancak tehditlerin berteraf edilmesi de yapay zekâ ile entegre siber güvenlik mekanizmalarının geliştirilmesine bağlıdır. ***Çünkü*** siber tehditlere ilişkin yapay zekâ tabanlı programlar önceliklendirme yaparak herhangi bir saldırıda nelerin kullanılbileceğine, olabilecek potansiyel tehditlerle ilgili gelişmeleri değerlendirmeye, bir saldırı gerçekleşmeden önce güvenlik açıklarının tespitine, zayıf yönlerin geliştirilmesi için planlama yapılmasına yardımcı olmaya ve bir saldırı meydana geldiğinde veya saldırı riski uyarısı alındığında hızlı yanıt vermeye fayda sağlamaktadır. Ayrıca siber saldırılarda makine öğrenme algoritmaları ile denetimsiz öğrenme tekniklerinden yararlanılması kötü niyetli bir kod ile o kodun parçaları arasında ilişkilendirmede bulunma yeteneği sağlamaktadır. Bir başka deyişle, gerçekleşmesi engellenen saldırıdan elde edilen verilerle sorumlu aktörleri hakkında çıkarımda bulunulabilmektedir (Reşitoğlu, 2021).

Farkındalığı ve tehditle mücadelede etkinliği artırmak ve gerçek zamanlı tepkiler vermek için yapay zekâdan yararlanan siber güvenlik uygulamaları tehditlerinin belirsiz olduğu, saldırgan-savunucu asimitrelerini değiştiren saldırılar karşısında kendi kendine uyarlamayı içermektedir. Şöyle ki, rakibin zayıf yönlerini belirleyebilmekte, gözlem yöntemlerininden ve öğrenilen derslerden yararlanarak saldırı türlerini sınıflandırabilmekte ve uyarlanabilir yanıtları (tutarsızlıkların tespiti ve nasıl onarılacağının bilinmesi) geliştirebilmektedir (National Science and Technololgy Council, 2020: 5). Esasında kısaca siber güvenlik alanında yapay zekâ uygulamalarının önceden tespit, tahmin ve yanıt verme olarak üç temel işlevi yerine getirdiği söylenebilir.

Milyarlaca bilginin depolandığı, tüm iletişim ağlarını içeren, insanlara, devletlere, devlet dışı aktörlere ve suç örgütlerine ev sahipliği yapan siber uzayda siber güvenlik tehditleri ile mücadelede yapay zekâ siber güvenliğin önemli bir bileşeni ve ayrılmaz bir parçası olmuştur. 10 ülke ve yedi ayrı iş sektöründe *"Siber Güvenliği Yapay Zekâ ile Yeniden Keşfetmek: Dijital Güvenlikte Yeni Sınır"* başlıklı bir araştırma kapsamında bilgi güvenliği, siber güvenlik, BT operasyonlarından 850 üst düzey yönetici ile birlikte endüstri mühendisi ve akademisyenlerle anket ve derinlemesine mülakatlar yapılmış; araştırma sonucunda katılımcıların ***büyük çoğunluğu***nun yapay zekânın siber güvenliğin geleceği için anahtar bir unsur olduğu sonucuna ulaşılmıştır. Ayrıca araştırma sonucuna göre (Capgemini Research Institute, 2019):

- Katılımcıların %64'ü yapay zekânın ihlalleri tespit etme ve bunlara yanıt verme maliyetini ortalama %12 oranında azalttığını söylemiş,
- Katılımcıların %74'ü yapay zekânın daha hızlı yanıt süresi sağladığını söyleyerek; tehditleri tespit etmek, ihlalleri gidermek ve güvenlik açığı olan konularda eksiklikleri gidermek için geçen süreyi %12 oranında azalttığını dile getirmiş,
- Katılımcıların %69'u yapay zekânın ihlalleri tespit etme doğruluğunu geliştirdiğini söylemiş ve
- Katılımcıların %60'ı, siber güvenlik analistlerinin verimliliğini artırdığını, yanlış pozitifleri analiz etmek için harcadıkları zamanı azalttığını ve üretkenliği artırdığını belirtmişlerdir.

Siber tehditlerin kapsam ve boyutunun artması, belirsizlikleri bünyesinde bulundurması, suç veya terör örgütlerinin eleman devşirme, propaganda ve algı operasyonları faaliyetlerini siber ortama taşıması siber güvenliğin önemli bir parçası olan siber istihbaratı da gündeme getirmektedir. Elektronik ortamdaki tehdit ve saldırıların izlenmesi, analiz edilerek karşı önlemlerin alınması anlamına gelen siber istihbarat gerek hızı gerekse maliyeti dolayısıyla yeni bir istihbarat faaliyeti olarak tercih edilmektedir (Karaağaç, 2018:60). ABD Güvenlik Şirketi Mandiant tarafından yayımlanan 18 Şubat 2013 tarihli raporda Çin Halk Kurtuluş Ordusu'nun Şangay'ın Pudong Bölgesinde yer alan 12 katlı binada 2006'da beri bilgisayar ağ güvenliğinden sorumlu yüzlerce personelle faaliyet gösterdiği bilinmektedir. Çin'in beş yıllık kalkınma planında yer alan 20 sektörden 141 şirkete siber casusluk yapılarak bilgilerinin sızdırıldığı; şirketlerin yüzlerce terebaytlık mavi kopyasının, iş planının, fiyatlama ve kullanıcı bilglerinin, e-posta adres ve iletişim bilgilerinin ele geçirildiği belirtilmiştir (Yılmaz, 2019: 259).

Yapay zekâ istihbarat örgütlerinin ve analistçilerinin verileri hızlı toplamasını, işlemesini, sınıflandırmasını ve analiz edilmesini kolaylaştırmaktadır. Böylece zaman ve kapasite bakımından avantaj sağlanmaktadır. Yapay zekâdan istihbarat faaliyetlerinde doğal dil işleme ve çeviri sistemleri; yüz tanıma, ses tanıma ve görüntü işleme, akıllı silah sistemleri, veri toplama ve analizi gibi alanlarda yararlanılabilmekte; siber ortamda ise izleme, dinleme, takip ve tararssut eylemleri fiziki takibe gerek kalmayacak şekilde akıllı sistemler marifetiyle daha kolay gerçekleştirilmektedir (Oruç, 2019: 4228-4230). ***Örneğin; toplumsal olayların daha önceden tespit edilebilmesi veya gerçekleşen olaylara ilişkin geriye dönük araştırma yapılabilmesi için twitter gibi sosyal medya verileri analiz edilebilmektedir. Çünkü kitleler günümüzde artık mesajlaşmalar veya paylaşımlar yoluyla sosyal medya üzerinden harekete geçmekte ve organize olmaktadır (***Savaş ve Topaloğlu, 2015: 67). Sosyal medya verileri üzerinden yürütülen siber istihbarat faaliyetleri olayların aydınlatılmasına katkı sağlamaktadır.

Hem özel sektör şirketleri tarafından hem de devletler tarafından siber saldırıla-

ra yanıt vermek amacıyla siber güvenlik alanında yapay zekâ uygulamalarına dönük yatırımlar, projeler ve çalışmalar gerçekleştirilmektedir. Yapay zekânın siber güvenlik pazarındaki payının 2020'den 2027'ye kadar yüzde 23.6'lık birleşik yıllık büyüme hızı ile (CAGR) 2027 yılına kadar 46.3 milyar dolara ulaşması beklenmektedir (Meticulous Research, 2021). Nesnelerin internetinin artan şekilde benimsenmesi ve buna paralel olarak bağlı elektronik cihazların yaygınlaşması, artan siber güvenlik tehditleri, Wi-Fi ağlarının güvenlik tehdilerine artan savunmasızlığı, sosyal medya kullanıcısının gittikçe artması siber güvenlik alanında yapay zekâ pazarının artmasının temel sebepleri olarak nitelendirilebilir.

Cybersecuriy Venture adlı siber güvenlik şirketi tarafından yapılan bir araştırmada siber saldırıların dünya ekonomisine verdiği zararın 2015 yılında 3 trilyon dolar olduğu, 2021'de bunun 6 trilyon dolara ulaşacağı ve 2022 yılı itibariyle siber güvenlik harcamalarının 133.7 milyar doları bulacağı belirtilerek Covid-19 pandemisi ile birlikte siber suçlarda yüzde 300 artış olduğu, hatta her 39 saniyede bir siber güvenlik olayı yaşandığı belirtilmiştir (Hürriyet, 2020). Siber saldırıların artması ve karşı karşıya kalınan siber güvenlik sorunları yapay zekâ tabanlı platfformlara ve çözümümlemelere ihtiyaç olduğunu göstermektedir. Makine öğrenmesi ve yapay zekâ teknolojileri üzerine inşa edilen otomasyonlar sayesinde tehditlerin tespiti, tahmini ve müdahalesi daha kolay olabilmektedir.

6. Sonuç

Yapay zekâ konusu 1950'lerde özerk bir araştırma alanı olarak ele alınmaya başlamış, fen bilimlerinden sosyal bilimlere kadar çok sayıda disiplini etkilemiştir. Etkilenen disiplinler içerisinde yapay zek***â***nın tezahür ettiği konulardan birisi de kamu yönetiminde özel bir incelemeye ihtiyaç duyulan iç güvenlik yönetimi olmuştur.

Yapay zekâ, iç güvenlik yönetiminden sorumlu aktörlerin operasyonel ve örgütsel faaliyetlerini şekillendirmekte, örgüt yapısını inşa ederken bilgi iletişim teknolojilerinden ve dijitalleşmeden azami derecede faydalanmasını sağlamakta, proaktif ve reaktif önlemler içermektedir. Yapay zekâ araçlarına entegre edilmiş algılama sistemlerine bağlı olarak risk ve tehditlerin kolaylıkla tespiti sağlanmakta, risk ve tehditler önceliklendirilebilmekte, tahmin edilebilmekte ve bertaraf edilebilmektedir. Yapay zekâ insan hatalarından olabildiğince arınmış şekilde güvenlik yönetimini daha kolay, daha hızlı, daha az maliyetli hale getirmektedir**.**

İç güvenlik yönetiminde yapay zekâ kullanımı devletlerin yeni teknolojilere uyum sağlama ve teknoloji geliştirme kapasitesi ile yakından ilgilidir. Çünkü; yalnızca teknolojik gelişmelere uyum sağlayabilen devletler veya yeni teknolojik atılımlar yapabilen devletler yapay zekâyı iç güvenlik yönetiminde etkili bir şekilde kullanabileceklerdir. Terör örgütlerinin, organize suç örgütlerinin, algı operasyonları yürüten aktörlerin gerek eleman temininde gerekse faaliyetlerinde küreselleşmenin beraberinde getirdiği

teknolojik ilerlemelerden faydalanarak siber ortamda kendisine alan açtığı günümüzde devletlerin kolluk birimleri tarafından karada gerçekleştirilen devriyelerin yerini siber/sanal devriyeler; görevlerini ifa ederken zorunlu olarak taşıdıkları silah, tabanca, tüfek gibi teçhizatların yerini de teknolojik araç ve gereçler almaktadır. Dolayısıyla illegal faaliyetler yürüten aktörlere karşı önlem almak, suç ve suçluyla mücadelede üstünlük sağlamak için devletler tarafından yeni teknolojilere uyum sağlamak, bu alandaki yatırımları desteklemek ve bunlardan istifade etmek oldukça önem taşımaktadır.

İç güvenlik yönetiminde yapay zekâ kullanımı teknolojik gelişmeleri yakından takip ederek siber ortamda manevra kabiliyeti geliştiren organize suç örgütleri, terör örgütleri, siber korsanlar vb. gibi illegal yapılanmalar karşısında geride kalmamak, suç ve suçluyla mücadelede üstünlük kazanmak için bir zaruret haline gelmiştir. İçinde bulunduğumuz dijital çağda yalnızca toprak parçası ile sınırlı olmayan siber vatanın güvenliği için yapay zekâ araçlarının kullanımı bir tercih değil, zorunluluk doğurmaktadır. Dolayısıyla, iç güvenlik teşkilatları tarafından en çok hassasiyet gösterilmesi gereken hususların başında yapay zekâ ve bilgi iletişim teknolojilerini yönetsel sürece tatbik etmek gelmelidir.

Sonuç olarak hızla gelişen teknolojik gelişmeler çerçevesinde, yapay zekânın iç güvenlik politikalarına etkisinin artarak devam edeceği söylenebilir. Dijital toplum ya da bilgi toplumu temelinde siber güvenliğin sağlanmasında ise teknik olarak yapay zekâ uygulamaları, gelişmeye ve çeşitlenmeye devam edecektir.

Etik Beyanı: Bu çalışmanın tüm hazırlanma süreçlerinde etik kurallara uyulduğunu yazar beyan eder. Aksi bir durumun tespiti halinde Kamu Yönetimi ve Teknoloji Dergisinin hiçbir sorumluluğu olmayıp, tüm sorumluluk çalış-manın yazarlarına aittir.

Yazar Katkıları: İbrahim İrdem ve Sedat Çobanoğlu çalışmanın tüm bölümlerinde ve aşamalarında katkı sağlamışlardır. Yazarlar esere eşit oranda katkı sunmuştur.

Çıkar Beyanı: Yazarlar ya da herhangi bir kurum/ kuruluş arasında çıkar çatışması yoktur.

Teşekkür: Yayın sürecinde katkısı olan hakemlere teşekkür ederiz.

Ethics Statement: The author declares that the ethical rules are followed in all preparation processes of this study. In the event of a contrary situation, the Journal of Public Administration and Technology has no responsibility and all responsibility belongs to the author of the study.

Author Contributions: İbrahim İrdem and Sedat Çobanoğlu have contributed to all parts and stages of the study. The authors contributed equally to the study.

Conflict of Interest: There is no conflict of interest among the authors and/or any institution.

Acknowledgement: We would like to thank the referees who contributed to the publication process

Kaynakça

Allen, G. & Chan, T. (2017) *Artificial Intelligence and National Security*, Belfer Center for Science and International Affairs, Harvard Kennedy School, Massachusetts.

Anadolu Ajansı (2020), *Yapay Zeka Destekli İHA Sürüsü Geliyor,* https://www.aa.com.tr/tr/bilim-teknoloji/yapay-zeka-destekli-iha-surusu-geliyor/2048808, Erişim Tarihi: 16.08.2021.

Ataseven, B. (2013) "Yapay Sinir Ağları ile Öngörü Modellenmesi", Öneri Dergisi, 10(39), s. 101-115.

Belani, G. (2021), *The Use of Artificial Intelligence in Cybersecurity: A Review,* https://www.computer.org/publications/tech-news/trends/the-use-of-artificial-intelligence-in-cybersecurity, Erişim Tarihi: 24.12.2021.

Boucher, P. (2019) *How Artificial Intelligence Works*?. EPRS/European Parliamentary Research Service Brifing, s. 1-10.

Capgemini Research Institute (2019), *Reinventing Cybersecurity with Artificial Intelligence the New Frontier in Digital Security,* https://www.capgemini.com/wp-content/uploads/2019/07/AI-in-Cybersecurity_Report_20190711_V06.pdf, Erişim Tarihi: 23.12.2021.

CBDDO (2021) *Türkiye'nin İlk Yapay Zekâ Stratejisi*, https://cbddo.gov.tr/haberler/6126/turkiye-nin-ilk-yapay-zeka-stratejisi, Erişim Tarihi: 22.08.2021.

Che, D.; Safran, M. & Peng, Z. (2013) "From Big Data to Big Data Mining: Challenges, Issues, and Opportunities", in. *International Conference on Database Systems for Advanced Applications*, (Ed.) Bonghee Hong, Xiaofeng Meng, Lei Chen, Werner Winiwarter, and Wei Song, Berlin: Springer. ss. 1-15.

Data Flair (2019), *History of Artificial Intelligence-AI of the Past, Present and the Future!,* https://data-flair.training/blogs/history-of-artificial-intelligence/, Erişim Tarihi: 06.12.2020.

Dawns, R. (2021), *Featured: AI News' list of Innovative Companies to Watch in 2021,* https://artificialintelligence-news.com/2021/03/03/featured-ai-news-list-of-innovative-companies-to-watch-in-2021/, Erişim Tarihi: 10.05.2021.

Dernoncourt, F. (2013) "Introduction to Fuzzy Logic", *MIT,* s. 1-21.

Doroganov, V. S. İ. & Baumgarten, M. İ. (2013) "Vozmojnie Problemi, Voznikayuşçie Pri Sozdanii Iskustvennogo Intellekta", *Vestnik Kuzbastkogo Gosudarstvennogo Tehniçeskogo Universiteta*, 98(4), ss. 132-135.

Erendor, M. E. (2019) "Siber Güvenlik, Siber İstihbarat ve Devletlerin Ulusal Güvenliğinin Sağlanmasında Siber İstihbaratın Rolü", iç. *Kamu Güvenliği Politikaları: Yerelden Küresele*, (Ed.) Hasan Acar, Ankara: Nobel Yayınevi. ss. 169-200.

Future of Life Institute (2021), *National and International AI Strategies,* https://futureoflife.org/national-international-ai-strategies/?cn-reloaded=1, Erişim Tarihi: 10.05.2021.

Glyantsev, A. (2021), *Kompyuter-Sürrealist:İskustvennıy İntellekt Prevraşaet Slova na Risunki (Bilgisayar Sürrealist: Yapay Zeka Kelimeleri Resimlere Dönüştürüyor),* https://www.vesti.ru/nauka/article/2507581, Erişim Tarihi: 17.01.2021.

Grewal, D. S. (2014) "A Critical Conceptual Analysis of Definitions of Artificial Intelligence as Applicable to Computer Engineering", *IOSR Journal of Computer Engineering,* 16(2), ss. 9-13.

Gutierrez, D. D. (2021), *An Enterprise AI Platform as an Path Toward Intelligence Process Automation,* https://insidebigdata.com/2021/11/02/an-enterprise-ai-platform-as-a-path-toward-intelligence-process-automation/, Erişim Tarihi: 23.12.2021.

Haber Türk (2021), *Türkiye'de Yapay Zekâ Ekosistemi 4 Yılda 7'ye Katlandı,* https://www.haberturk.com/iste-turkiye-yapay-zeka-haritasi-haberler-2968031-teknoloji, Erişim Tarihi: 16.08.2021.

Hoadly, D.S. & Lucas, N. J. (2018) *Artificial Intelligence and National Security*, Congressional Research Service Report, s. 1-38.

Homeland Security Research Corporation (2020) *Artificial Intelligence Market with COVID-19 Impact in Homeland Security & Public Safety 2020-2025*, Report of Homeland Security Research Corporation.

Horowitz, M.; Scharre, P.; Allen, G.C.; Frederick, K.; Cho, A. & Saravalle, E. (2018) *Artificial Intelligence and International Security,* Center for a New American Security's series on Artificial Intelligence and International Security, s. 1-27.

Hürriyet (2020), *Yapay Zekâ, Kendisi ile Mücadelesini Sürdürecek,* https://www.hurriyet.com.tr/teknoloji/yapay-zeka-kendisi-ile-mucadelesini-surdurecek-41662416, Erişim Tarihi: 25.12.2021.

Internet World Stats (2021), https://www.internetworldstats.com/stats.htm, Erişim Tarihi: 25.12.2021.

İçen, D. ve Günay, S. (2014) "Uzman Sistemler ve İstatistik", İstatistikçiler Dergisi: İstatistik & Aktüerya, 7, 37-45.

İrdem, İ. (2020) "İç Güvenlik, Kamu Düzeni ve Yeni Kamu Hizmeti Perspektifinden Güvenlik Yönetimi", iç. *İç Güvenlik Yönetimi ve Polislik*, (Ed.) İbrahim İrdem, Ankara: Polis Akademisi Yayınları. ss. 17-45.

İşler, B. & Kılıç, M.Y. (2021) "Eğitimde Yapay Zeka Kullanımı ve Gelişimi", *Yeni Medya Elektronik Dergi,* 5(1), s. 1-11.

Karaağaç, Y. (2018) *Geçmişten Geleceğe İstihbarat Gizli Servisler, Örtülü Operasyonlar ve Savaş Stratejisi*, İstanbul: İskenderiye Kitap.

Karakoç-Dora, Z. (2021) "Borders, Terror and Immigration: the ISIS Case", iç. *Security Issues in the Context of Political Violence and Terrorism of the 21st Century*, (Ed.) Hasan Acar ve Halil Emre Deniş, Newcastle: Cambridge Scholars Publishing. ss. 143-153.

Karasoy, H. A. (2021) *Kamu Güvenliğinde Yeni Paradigmalar: Hibrit Savaş Asimetrik Savaş Vekâlet Savaşı İstihbarat ve Terörle Mücadele*, Ankara: Nobel Yayıncılık.

Kumar, G.; Saini, D. K. & Cuong, N.H.H. (2021) *Cyber Defense Mechanisms Security, Privacy and Challanges*, New York: CRR Press.

Lahmeri, M. A.; Kishk, M. A. & Alouini, M. S. (2021) "Artificial Intelligence for UAV-enabled Wireless Networks: A Survey", *IEEE Open Journal of the Communications Society*, 24(1), s. 1015-1040.

LeCun, Y.,; Bengio, Y. & Hinton, G. (2015) "Deep Learning", *Nature,* 521(7553), s. 436-444.

Lewis, T. & Writer, S. (2014), *A Brief History of Artificial Intelligence,* https://www.livescience.com/49007-history-of-artificial-intelligence.html, Erişim Tarihi: 06.12.2020.

Marr, B. (2020), *What is the Importance of Artificial Intelligence (AI),* https://bernardmarr.com/default.asp?contentID=1829, Erişim Tarihi: 08.12.2020.

Meticulous Research (2021) *AI in Cybersecurity Market by Technology (ML, NLP), Security (Endpoint, Cloud), Application (DLP, UTM, IAM, IDP), Industry (Retail, Government, Automotive, BFSI, IT, Healthcare, Education), and Geography - Global Forecast to 2027*, Report of Meticulous Market Research Pvt. Ltd.

Moran, M. (2020), *Elon Musk says AI will be Smarter than Humans within 5 Years - and It'll Get 'Weird',* https://www.dailystar.co.uk/news/world-news/elon-musk-says-ai-smarter-22421942, Erişim Tarihi: 06.12.2020.

National Science and Technology Council (2020) *Artificial Intelligence and Cybersecurity: Opportunities and Challenges Technical Workshop Summary Report*, A report by the Networking & Information Technology Research and Development Subcommittee of The National Scıence & Technology Council, s. 1-10.

Norwegian Ministry of Local Government and Modernization (2019), ***National Strategy for Artificial Intelligence***, https://www.regjeringen.no/contentassets/1febbbb2c4fd4b7d92c67ddd353b6ae8/en-gb/pdfs/ki-strategi_en.pdf, Erişim Tarihi: 10.05.2021.

Okçu, M. (2021) "Bildiğimiz Kamu Yönetiminin Sonu: Kamu Yönetiminde Yapay Zekâ ve Dijital Dönüşüm", iç. *21. Yüzyılda Türk Kamu Yönetiminin Değişimi*, (Ed.) Aysun Öcal ve Yasemin Hayta, Ankara: Detay Yayıncılık. ss.215-256.

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

Önder, M. & Saygılı H. (2018) "Yapay Zeka ve Kamu Yönetimindeki Yansımaları", *Türk İdare Dergisi,* 487, s. 629-668.

Perez, J. A.; F. Deligianni, D. & Ravi, G. Y. (2017) *Artificial Intelligence and Robotics*, UK: EPSRC UK-RAS Network.

Python Dünyası (2020), *Aiware Yapay Zeka İşletim Sistemi,* https://pythondunyasi.com/aiware-yapay-zeka-isletim-sistemi/, Erişim Tarihi: 25.12.2021.

Randall, E. (2019), *5 Reasons Why Artificial Intelligence is Important to You,* https://readwrite.com/2019/10/09/5-reasons-why-artificial-intelligence-is-important-to-you/, Erişim Tarihi: 08.12.2020.

Reşitoğlu, Ş. N. (2021), *Siber Güvenlikte Yapay Zekâ Etkisi*, https://www.tuicakademi.org/siber-guvenlikte-yapay-zeka-etkisi/, Erişim Tarihi: 25.12.2021.

Sanayi ve Teknoloji Bakanlığı & CBDDO (2021), *Ulusal Yapay Zekâ Stratejisi,* https://cbddo.gov.tr/UYZS, Erişim Tarihi: 20.12.2021.

Savaş, S. & Topaloğlu, N. (2015) "Sosyal Medya Verileri Üzerinden Siber İstihbarat Faaliyetleri", iç. 8*. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı Bildiriler Kitabı*, Ankara: ODTÜ Yayınları, ss. 1-7.

Sherin, A.; Uma, S.; Saranya, K. & Vani, S. (2014) "Survey on Big Data Mining Platforms, Algorithms and Challenges", *Journal of Computer Science & Engineering Technology,* 5(9), s. 854-862.

Şabanov, A. (2020), *Primeneniye Tehnologiy Iskustvennogo Intellekta v İnformatsionnoy Bezopasnosti,* https://www.anti-malware.ru/analytics/Technology_Analysis/using-artificial-intelligence-technologies-in-information-security, Erişim Tarihi: 29.05.2021.

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

Tecuci, G. (2012) "Artificial Intelligence", *WIREs Computational Statistics,* 4(2), s. 168-180.

Turing, A. M. (1950) "Computing Machinery and Intelligence", *Mind*, 59(236), s. 433-460.

TÜBİSAD (2019), *DTP: Dijital Türkiye İçin Bağlanabilirlik, Siber Güvenlik ve Yapay Zekâ Kritik Önemde,* https://www.tubisad.org.tr/tr/tubisad/detay/DTP-Dijital-Turkiye-Icin-Baglanabilirlik-Siber-Guvenlik-ve-Yapay-Zeka-Kritik-Onemde/19/1870/0, Erişim Tarihi: 16.08.2021.

Türkçe Yayın (2018), *Yapay Zekânın Tarihçesi ve Gelişim Süreci,* https://medium.com/t%C3%BCrkiye/yapay-zekan%C4%B1n-tarih%C3%A7esi-ve-geli%C5%9Fim-s%C3%BCreci-cb4c73deb01d, Erişim Tarihi: 22.08.2021.

Uzun, T. (2020) "Yapay Zeka ve Sağlık Uygulamaları", *Katip Çelebi Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,* 3(1), s. 80-92.

Yampolskiy, R. V. (2020) "On Defining Differences between Intelligence and Artificial Intelligence", *Journal of Artificial General Intelligence*, 11(2), s. 68-70.

Yanarışık, O. (2020) "*İç Güvenlik ve Siber Güvenlik",* iç. İç Güvenlik Yönetimi ve Polislik, (Ed.) İbrahim İrdem, Ankara: Polis Akademisi Yayınları. ss. 302-327.

Yefimçik, A. (2019), *10 Vpeçatlyayuşçih Primerov Ispolzovaniya Iskustvennogo Intellekta v Jiszni,* https://www.kv.by/post/1056728-10-vpechatlyayushchih-primerov-ispolzovaniya-iskusstvennogo-intellekta-v-zhizni, Erişim Tarihi: 10.12.2020.

Yılmaz, S. (2019) *Temel İstihbarat Toplama - Analiz ve Operasyonlar*, Ankara: Kripto Kitapları.

Zanzotto, F. M. (2019) "Viewpoint: Human-in-the-loop Artificial Intelligence", *Journal of Artificial Intelligence Research*, 64, s. 243-252.