



# k@ytek

## KAMU YÖNETİMİ VE TEKNOLOJİ DERGİSİ

THE JOURNAL OF PUBLIC ADMINISTRATION AND TECHNOLOGY

Cilt / Vol: 3 Sayı / No: 2 Yıl / Year: 2021 e-ISSN 2687-6485

KAMU YÖNETİMİ VE TEKNOLOJİ DERGİSİ  
THE JOURNAL OF PUBLIC ADMINISTRATION AND TECHNOLOGY

Türkiye’de Uzaktan Eğitim Politikaları  
Distance Education Policies In Turkey  
*Hasan Alpay KARASOY / Emin CEBE / Pelin BABAĞLU*

Eğitimde Teknolojinin Kullanımı  
Use of Technology in Education  
*Umay Tuba CURACI*

Yapay Zekanın İç Güvenlik Yönetimi Üzerine Yansımaları: Siber Güvenlik  
Reflections Of Artificial Intelligence On Internal Security Management:  
Cyber Security  
*İbrahim İRDEM / Sedat ÇOBANOĞLU*

Uluslararası Denizcilik Örgütü (IMO) Hukuki Araçlarının Otonom Gemilere  
Uygulanabilirliği Üzerine Kısa Bir Değerlendirme  
A Brief Review of the Applicability of International Maritime Organization  
(IMO) Legal Instruments to Autonomous Ships  
*Ali Erdem ŞAHİN*

Siber Ordular ve Siber Savaşlar  
Cyber Armies And Cyber Wars  
*Meryem ORAK*



# k@ytek

## KAMU YÖNETİMİ VE TEKNOLOJİ DERGİSİ

JOURNAL OF PUBLIC ADMINISTRATION AND TECHNOLOGY

KAYTEK DERGİSİ • CİLT/VOL: 3 • SAYI/ISSUE: 2 • YIL/YEAR: 2021



KAMU YÖNETİMİ VE TEKNOLOJİ  
HAKEMLİ DERGİSİ



# k@ytek

## KAMU YÖNETİMİ VE TEKNOLOJİ DERGİSİ JOURNAL OF PUBLIC ADMINISTRATION AND TECHNOLOGY

KAYTEK DERGİSİ • CİLT/VOL: 3 • SAYI/ISSUE: 2 • YIL/YEAR: 2021

### KAMU YÖNETİMİ VE TEKNOLOJİ DERGİSİ(k@ytek)

**Dergi İmtiyaz Sahibi (Publisher)**  
Kamu Bilişim Derneği adına  
Doç. Dr. İzzet Gökhan ÖZBİLGİN

**Editörler (Editors-in-Chief)**  
Prof. Dr. Doğan Nadi LEBLEBİCİ  
Doç. Dr. İzzet Gökhan ÖZBİLGİN

**Editör Yardımcısı (Assistant Editor)**  
Doç. Dr. Cenay BABAĞLU  
Doç. Dr. Oğuzhan Erdoğan

**Yayın Kurulu (Editorial Board):**  
Prof. Dr. Doğan Nadi LEBLEBİCİ  
Doç. Dr. İzzet Gökhan ÖZBİLGİN  
Doç. Dr. Cenay BABAĞLU  
Dr. Meltem İMAMOĞLU  
Dr. R. Erdem ERKUL

**Yazım ve Dil Editörü  
Spelling and Language Editor**  
Arş. Gör. Abdullah GENCO

**Dergi Sekreteri (Secretary)**  
Arş. Gör. Tuncay ÇOLAK

**Yayın Türü**  
Sürelili yayın  
"Kamu Yönetimi ve Teknoloji  
Dergisi"  
altı (6) ayda bir yayımlanır.

**Yayın Dili**  
Türkçe ve İngilizce

**Tasarım**  
Ajans Düş Pınarı

**İletişim/Contact**  
Kamu Bilişim Derneği,  
Çetin Emeç Bulvarı  
4. Cad. No: 3/16 A. Öveçler/ANKARA  
Tel: 0555 800 05 27  
e-posta: bilgi@kdb.org.tr

<https://dergipark.org.tr/tr/pub/kaytek>  
Doğan Nadi Leblebici: nadi@hacettepe.edu.tr  
Cenay Babaoğlu: cenaybabaoglu@gmail.com

### Tarandığı Dizinler / Endeksler / (Abstracting / Indexing)



Kamu Yönetimi ve Teknoloji Dergisi yılda iki kez Kamu Bilişim Derneği tarafından yayınlanan hakemli, ulusal bir dergidir. Dergiye yönelik makale talepleri DERGIPARK üzerinden değerlendirilmektedir. Gönderilen metinler editörler tarafından bilimsel anlatım ve yazım kuralları açısından incelenir. Ardından kör hakem uygulaması yapılarak her yazı en az iki hakeme gönderilir. Hakemlerin kararları doğrultusunda yazı kabul ya da ret edilir. Dergide yayınlanan tüm yazı ve görüşler yalnızca yazar(lar)a aittir. Dergi sahibi, yayıncı ya da editörler yazarların görüşlerinden sorumlu tutulamaz.

## Bilim ve Danışma Kurulu

Prof. Dr. Türksel Bengşir	Ankara Hacı Bayram Veli Üniversitesi
Prof. Dr. Alptekin Erkollar	Swiss Federal Institute of Technology
Prof. Dr. Jane Fountain	University of Massachusetts
Prof. Dr. Dimitris Gouscos	University of Athens
Prof. Dr. Vahap Tecim	Dokuz Eylül Üniversitesi
Prof. Dr. Hikmet Kavruk	Gelişim Üniversitesi
Prof. Dr. Peter Parycek	Danube University
Prof. Dr. Mete Yıldız	Hacettepe Üniversitesi
Prof. Dr. William Webster	University of Stirling
Doç. Dr. Laura Alcaide Munoz	University of Granada
Doç. Dr. Hasan Alpay Karasoy	Selçuk Üniversitesi
Doç. Dr. Aysu Kes Erkul	Hacettepe Üniversitesi
Doç. Dr. Uğur Sadioğlu	Hacettepe Üniversitesi
Doç. Dr. Nilay Yavuz	Orta Doğu Teknik Üniversitesi
Dr. Meltem İmamoğlu	Türk Hava Kurumu Üniversitesi
Dr. Özkan Leblebici	

## Bu Sayının Hakemleri

Prof. Dr. Hikmet KAVRUK

Prof. Dr. Mustafa Kemal ÖKTEM

Doç. Dr. Altuğ Murat KÖKTAŞ

Doç. Dr. Şerife PEKKÜÇÜKŞEN

Doç. Dr. Vedat YILMAZ

Doç. Dr. Yıldız ATMACA

Doç. Dr. Yusuf PUSTU

Dr. Öğr. Üyesi Oğuzhan YANARIŞIK

Dr. Öğr. Üyesi Serkan GÜNDOĞDU





# EDİTÖRDEN

Dergimizin yeni sayısında tüm okuyucularımızı saygıyla selamlıyoruz. Oyunun kurallarının sürekli olarak değiştiği bu dünyada, örgütlerin teknolojik gelişmeleri izleyebilme ve yönetim sistemlerine entegre etme fonksiyonu adeta bir satranç maçındaki vezir kadar oyun kazanmak için önemlidir. Bu nedenle gerek kamu yönetimleri gerekse özel yönetimler, teknolojiyi hem adaptasyon hem de sorun çözme aracı olarak kullanarak dijitalleşmeye önem vermektedirler. Kamu Yönetimi ve Teknoloji Dergisi olarak, biz de örgütlerin dijitalleşme süreçlerinde kuramsal gelişmelerin ve uygulama deneyimlerinin paylaşılması adına bir platform görevi görmeye devam ediyoruz. 2017 yılında başlayan çalışmalarımızda bir yandan Kamu Yönetimi ve Teknoloji Zirvelerini düzenlemeye diğer yandan dergimizi büyötmeye devam ediyoruz. Bu sayede hem akademik disiplin bağlamında hem de kamu politikası uygulayıcılarının pratikleri üzerinden teknoloji ve kamu yönetimi ilişkisini değerlendirmeyi ve bu konuda çözümler üretmek katkı sağlamayı hedefliyoruz.

Tüm bu çalışmaların bir sonucu olarak Kamu Yönetimi ve Teknoloji Dergisi'nin üçüncü cildinin ikinci sayısını sizlerin beğenisine sunmanın mutluluğunu yaşıyoruz. Bu sayımızda;

Hasan Alpay Karasoy, Emin Cebe ve Pelin Babaoğlu'nun birlikte kaleme aldıkları **“Türkiye’de Uzaktan Eğitim Politikaları”** isimli makalede uzaktan eğitimin avantaj ve dezavantajlarını belirtmişler sonrasında dünyada ve Türkiye’deki uzaktan eğitim politikalarının mevcut durumlarını ele alarak ve ilgili politika alanındaki durum üzerinden değerlendirmeler yaparak alana katkı sağlamışlardır.

**“Eğitimde Teknolojinin Kullanımı”** başlıklı ikinci çalışmada Umay Tuba Curacı, teknolojinin eğitimde kullanılmasına ilişkin mevcut durumu değerlendirilerek geleceğe dair öngörölere yer vermiştir.

İbrahim İrdem ve Sedat Çobanoğlu'nun birlikte yazdıkları **“Yapay Zekânın İç Güvenlik Yönetimi Üzerine Yansımaları: Siber Güvenlik”** başlıklı makalelerinde yapay zekânın iç güvenlik yönetimi üzerindeki etkisi özellikle de siber güvenlik üzerindeki etkisi değerlendirilmekte ve tündengeçimci bir yaklaşım çerçevesinde iç güvenliğin sağlanmasında yapay zekâ uygulamalarının rolü ve etkisi tartışılmaktadır.

Ali Erdem Şahin tarafından kaleme alınan ve Denizcilik Örgütü'nün (“IMO”) yasal araçları olan SOLAS, COLREG, MARPOL ve STCW metinlerinin yeni sistemle çelişebilecek maddelerini incelendiği, ardından bu hukuki araçların uygulanabilirlik dereceleri kısaca değerlendirdiği **“Uluslararası Denizcilik Örgütü (IMO) Hukuki Araçlarının Otonom Gemilere Uygulanabilirliği Üzerine Kısa Bir Değerlendirme”** başlıklı makalesiyle alana katkı sağlamıştır.

Son olarak Meryem Orak'ın kaleme aldığı **“Siber Ordular ve Siber Savaşlar”** isimli makalede siber güvenlik ve siber ordu kavramlarına dair literatür incelenerek dünyada bu alanda atılım yapan devletlerden olan ABD, Rusya ve İran'daki durum ortaya konmuş ardından da siber güvenlik alanında Türkiye'nin kurumsal ve altyapı girişimleri ele alınmıştır.

Birbirinden değerli bu çalışmaların teknoloji ve kamu yönetimi alanlarında çalışan araştırmacılara, kamu yönetiminde görev alan bürokratlara, kamu politikası oluşturma sürecinde rol alan paydaşlara ve konunun ilgilisi tüm okuyuculara faydalı olmasını temenni ediyoruz. Gelecekteki sayılarımızda siz değerli kullanıcılarımızın da çalışmalarına yer vermeyi ümit ediyoruz.

Saygılarımızla.



# İÇİNDEKİLER / CONTENTS

## ARAŞTIRMA

### **Türkiye’de Uzaktan Eğitim Politikaları**

Distance Education Policies In Turkey / 143

*Hasan Alpay KARASOY / Emin CEBE / Pelin BABAÖĞLU*

## DERLEME

### **Eğitimde Teknolojinin Kullanımı**

Use of Technology in Education / 166

*Umay Tuba CURACI*

## ARAŞTIRMA

### **Yapay Zekanın İç Güvenlik Yönetimi Üzerine Yansımaları: Siber Güvenlik**

Reflections Of Artificial Intelligence On Internal Security Management: Cyber Security / 175

*İbrahim İRDEM / Sedat ÇOBANOĞLU*

## DERLEME

### **Uluslararası Denizcilik Örgütü (IMO) Hukuki Araçlarının Otonom Gemilere Uygulanabilirliği Üzerine Kısa Bir Değerlendirme**

A Brief Review of the Applicability of International Maritime Organization (IMO) Legal Instruments to Autonomous Ships / 203

*Ali Erdem ŞAHİN*

### **Siber Ordular ve Siber Savaşlar**

Cyber Armies And Cyber Wars / 214

*Meryem ORAK*



## TÜRKİYE'DE UZAKTAN EĞİTİM POLİTİKALARI

## Distance Education Policies In Turkey

---

\*Doç. Dr. Hasan Alpay KARASOY / \*\* Emin CEBE / \*\*\* Pelin BABAĞLU

---

**Özet**

Uzaktan eğitim modelleri pek çok ülkenin eğitim politikalarında önemli bir yer tutmaktadır. Yaşanılan COVID-19 salgını, uzaktan eğitimin önemini bir kez daha ortaya koymuştur. Salgın öncesinde gelişmiş bir uzaktan eğitim altyapısı bulunan ülkeler bu süreçte eğitim sisteminin devamını sağlayabilmişlerdir. Bu altyapıya sahip olmayan kimi ülkeler ise eğitim sistemlerinde ciddi sıkıntılar ile karşılaşmışlardır. Kamu politikaları alanında önemli konu başlıklarından biri olan eğitim alanı da bu açıdan dikkat çekmektedir. Salgın sonrası dönemde uzaktan eğitim sistemlerinin yaygınlaşacağı ve bu alana yapılan yatırımların artacağı öngörülmektedir. Bu nedenle bu çalışmada uzaktan eğitim kavramı ele alınacak, tarihçesi ile birlikte avantaj ve kısıtlılıkları ortaya konulmaya çalışılacaktır. Konuyla ilgili ulusal ve uluslararası literatür taranarak Dünyada ve Türkiye'de mevcut durum ele alınmış ve ilgili politika alanındaki durum üzerinden değerlendirmeler yapılmıştır. Ulaşılan bulgular sonucunda eğitim alanında oluşturulan kamu politikalarının etkilerini ve pandemi gibi olağan üstü durumlarda kamu politikası oluşturabilmenin önemini ortaya koymak amaçlanmıştır.

**Anahtar Kelimeler:** Uzaktan Eğitim, Eğitim Politikaları, Kamu Politikaları, COVID-19, Dijitalleşme

**Abstract**

Distance education systems play an essential role in the education policies of many countries. The COVID-19 pandemic has once again demonstrated the importance of distance education. Countries that had a developed distance education infrastructure before the epidemic ensured the continuation of the education system in this process. Some countries that do not have this infrastructure have faced severe problems in their education systems. The field of education, which is one of the critical issues in public policy, draws attention in this respect. It is expected that distance education systems will become widespread, and investments in this field will increase in the post-pandemic period. Therefore, this study will focus on the concept of distance education, and the potential use of DE systems will be discussed, and its advantages and limitations will be revealed along with its history. The current situation in the world and in Turkey has been discussed by scanning the national and international literature on the subject and evaluations have been made on the situation in the relevant policy area. As a result of the findings, it is aimed to reveal the effects of public policies created in the field of education and the importance of creating public policy in extraordinary situations such as pandemics.

**Keywords:** Distance Education, Education Policies, Public Policies, COVID-19, Digitalization

---

\*Hasan Alpay KARASOY, Doç. Dr. , Selçuk Üniversitesi, dr.alpaykarasoy@gmail.com (<https://orcid.org/0000-0002-3813-2960>)

\*\* Emin CEBE, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü, Siyaset Bilimi ve Kamu Yönetimi YL Öğrencisi, emincebe98@hotmail.com (<https://orcid.org/0000-0002-6421-8004>)

\*\*\* Pelin BABAĞLU, Öğr. Gör., Isparta Uygulamalı Bilimler Üniversitesi, Uzaktan Eğitim MYO, pelinbabaoglu@isparta.edu.tr (<https://orcid.org/0000-0002-7542-1323>)

## GİRİŞ

Kitlesel eğitim yaklaşımının bir gereği olarak hayat boyu öğrenme süreci toplumların üzerinde oldukça fazla durduğu bir olgu olarak karşımıza çıkmaktadır. Uzaktan eğitim modelleri bu ‘hayat boyu öğrenme’ olgusunu destekleyen en güçlü sistemlerin başında gelmektedir. Bu nedenle pek çok karar verici eğitim politikaları içerisinde uzaktan eğitime gerekli önemi vermeye çalışmaktadır. Son yıllarda artan teknolojiler ile uzaktan eğitim daha az maliyetli, daha kolay ulaşılabilir ve daha kullanışlı hale gelmiştir. Ancak teknolojik dezavantajların da bulunduğunu belirtmek gerekir. 2019 yılından itibaren tüm dünyada etkisini gösteren korona virüs salgını sonrasında pek çok ülkede zorunlu kapanmalar yaşanmıştır. Bu kapanmalardan en çok etkilenen alanların başında ise eğitim gelmektedir. Uzaktan eğitim bu noktada uğranılan zararları minimum düzeye indirgeyerek eğitim sürecinin devam etmesinde kilit önemde olmuştur. Teknolojik olanakları etkin kullanarak dünya genelinde milyonlarca öğrenci evlerinden eğitimlerine devam edebilmişlerdir.

Ülkeler genç nüfuslarını nitelikli yetişkin bireyler haline gelmeleri ve ülkeleri için fayda sağlamaları amacıyla her yıl oldukça yüklü miktarlarda bütçe ayırarak eğitmek istemektedirler. Ancak günümüz dünyasında gelinen noktada eğitim denilen sürecin bir başlangıcı veya sonu olmadığı görülmüştür. İnsan varlık olarak dünyaya geldiği andan itibaren bir şeyler öğrenmeye başlar ve bu dünyadan ayrılana kadar bu öğrenme süreci devam eder. Eğitimin bu sürekli yönü nedeni ile ‘hayat boyu öğrenme’ denilen kavram ortaya çıkmıştır. Günümüz rekabet dünyasında gerek bireyler gerekse de devletler var olan konumlarını korumak ve geliştirmek için sürekli bir değişim ve gelişim içerisinde olmak zorundadır. Ancak eğitim alanında başat aktör olan devlet kurumunun bu hayat boyu öğrenme sürecinde belli başlı kısıtlılıkları vardır. Söz gelimi küçük yaşlarda eğitim kurumu olan ‘okul’lara alınan bireyler bu okullarda belli bir yaşa kadar eğitilebilmektedirler. Üstelik her bireyin eğitim süreci devlete belli bir maliyet yüklemektedir. Belli bir yaşa gelen bireyler okullardan aldıkları eğitimler ile hayata başlamaktadır. Ancak hayat sürekli değişmekte ve dönüşmektedir. Okullarda aldığı eğitim ile mezun olan bir birey birkaç yıl sonra değişen dünyada aldığı eğitimin ve öğrendiği şeylerin değiştiğini, bunların artık bir işine yaramadığını görmektedir. Son yıllarda tüm dünyada artan işsizlik oranlarının ardında bu gibi nedenler sayılabilir. Örneğin teknolojinin ve bilgisayarların bu denli hayatımıza girmediği dönemlerde alınan pek çok eğitim teknolojinin hayatlarımızın vazgeçilmezi olduğu günümüzde işlevsiz kalmış durumdadır. Önümüzdeki yıllarda da günümüzde alınan mevcut eğitimlerin belli bölümünün işlevsizleşeceği öngörülmektedir. Bu nedenler ile devletler vatandaşlarını rekabetçi dünyada daima sistem içerisinde yeterli donanıma sahip bir şekilde hazırlamak zorundadır. Devletlerin vatandaşlarını hayat boyu öğrenme süreci ile daima kalifiye halde tutabilmesi için kullanabileceği yollardan en dikkat çekenini ise uzaktan eğitimidir. Uzaktan eğitim okul yılları bitmiş pek çok bireye gündelik hayatlarında eğitimlerine devam edebilme olanağı

sağlayabilir. Okul dönemlerinde ise öğrencilerin okullara bağımlılığını azaltarak kendi istedikleri alanlarda uzmanlaşma imkânı sunmakta ve okula yardımcı bir destekleyici işlevi görebilmektedir.

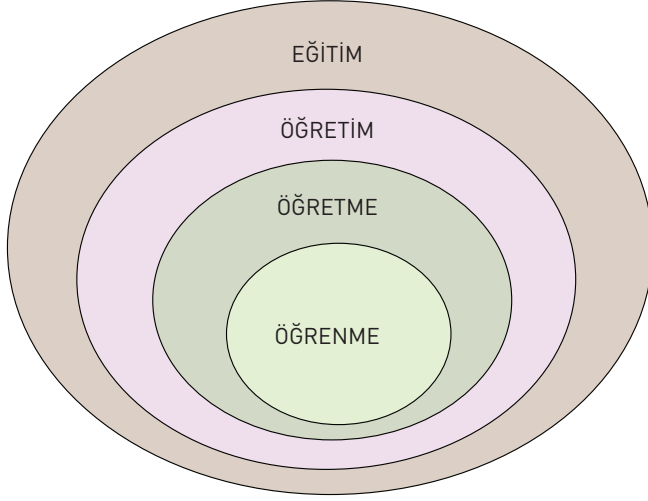
2019 yılında Çin'in Wuhan kentinden tüm dünyaya yayılan korona virüs (Covid-19) salgını uzaktan eğitimin farklı bir boyutunun ortaya çıkmasına neden olmuştur. Bu süreçte pek çok ülkede okullara ara verilmek zorunda kalınmıştır (Koç, 2021). Salgın öncesi uzaktan eğitim altyapısı güçlü olan ülkeler bu kapanma dönemlerinde öğrencilere uzaktan eğitim vererek eğitim sisteminin sürekliliğini koruyabilmişlerdir. Ancak bazı ülkelerin ise eğitim sistemleri bu süreçten çok kötü etkilenmiş ve eğitim faaliyetleri durma noktasına gelmiştir. Yaşanan pandemi dönemi uzaktan eğitim uygulamalarının önemini ortaya koymuştur (Türk Eğitim Derneği, 2020). Salgın sonrası 'yeni dünya'da devam etmesi beklenen politikalarından birisi de uzaktan eğitimidir. Pek çok ülke bu alana dikkatini çekmiş ve yatırımlar yapmıştır. Gerek devletler gerekse de özel şirketler uzaktan eğitim altyapılarını güçlendirmek için bütçelerinden büyük miktarlar ayırmaya başlamışlardır. Bu gibi gelişmeler önümüzdeki yıllarda uzaktan eğitim alanının önemini arttırmaya devam edeceği öngörülerine neden olmaktadır. Bu nedenle alanın incelenmesi gereği duyulmuştur.

Çalışmada öncelikle alanın kavramsal temelleri üzerinde durulmuştur. Daha sonra ise kavramın tarihsel gelişimi ele alınmıştır. Kavramın dünyadaki durumunu anlamak amacı ile dünyada gelişimi ve diğer ülkelerdeki durumu incelenmiştir. Bu incelemenin ardından odak noktası Türkiye'ye kaydırılmıştır. Türkiye'de alanın gelişimi, mevzuat konusu, ne tür aktörlerin yer aldığı incelenmiştir. Sonuç kısmına geçmeden önce ayrı bir başlık halinde sorun alanları ve çözüm önerileri sunulmuştur.

## 1. UZAKTAN EĞİTİM

Uzaktan Eğitim kavramını tanımlamak için kavramın merkezinde bulunan "eğitim" in tanımlanması gerekmektedir. Eğitim ilk insanlardan itibaren var olan bir olgudur. Eğitim ile insanlar öncelikli olarak yeme-içme gibi temel hayatta kalma becerilerini öğrenmektedirler. Bu nedenle eğitim için temelde bir 'öğrenme' faaliyeti olduğunu söylemek yanlış olmayacaktır. Eğitimin temel amacı insan gelişimidir. İnsan beyni doğada kapasitesi ile en ileri beyindir. Bu ileri kapasite sayesinde insanlar çevrelerini gözlemleyerek, düşünerek, araştırarak ve sorgulayarak 'bilgi' denilen metaları ortaya çıkarmaktadır. Bu bilgiler nesiller boyunca aktarılmaktadır (Etlioğlu, 2009:32-36; Şen, 2021; 26-31). Bu aktarım eğitim yolu ile olmaktadır. Eğitim, öğretme, öğretme ve öğrenme arasındaki iç içe geçen ilişki şekil 1'de görülmektedir.

### Şekil1: Eğitim



Kaynak: (Etlioğlu, 2009: 35)

Uzaktan Eğitim teriminin diğer önemli kavramı ise ‘uzaktan’ olmasıdır. Bu kavram geleneksel yöntemler ile yüz yüze yapılan eğitim faaliyetleri yerine bir takım eğitim faaliyetlerinin eğitici ile öğrencinin fiziksel olarak yan yana olmasının gerekmediğini ifade etmektedir. Uzak mesafelerden iletişim kurmanın oldukça kolaylaştığı günümüzde bu terimin anlamı daha çok belirginleşmektedir. Günümüzde teknolojinin geldiği noktada internet bağlantısı olan her yerde anlık iletişimler kurulabilmektedir. Görsel ve işitsel teknolojileri kullanarak eğitim faaliyetleri senkron veya asenkron şekilde yürütülebilmektedir(Avcı, 2021: 75; İşcan, 2020: 5)

İki terimin birleşiminden ortaya çıkan uzaktan eğitim kavramı, öğretim elemanı ile öğrenen olarak eğitimin iki ucunda yer alan öğelerin zamansal ve mekânsal sınırlılıklarını esnekletiren bir kavramdır (Akdemir, 2011: 5). Söz gelimi bu kavram ile klasik eğitim faaliyetlerinden olan sınıf ortamı sanal ortama taşınabilmektedir. Eğitici ve öğrenci arasındaki aynı mekanda ve aynı zamanda bulunma zorunluluğunun ortadan kalkmasına uzaktan eğitim denilebilir.

United States Distance Learning Association (USDLA)’ a göre Uzaktan Eğitimin tanımı (Özbay, 2015: 378);

*“Uydu, video, audio grafik, bilgisayar, çoklu ortam teknolojisi gibi elektronik araçların yardımıyla, eğitimin uzaktaki öğrencilere ulaştırılmasıdır. Uzaktan Eğitim uygulamalarında öğretmen ve öğrencinin birbirlerinden coğrafi olarak uzak olması nedeniyle eğitim programında elektronik araçların ya da yazılı materyal ve matbu malzemelerin kullanılması gerekir. Uzaktan eğitimi, öğretmenleri içine alan öğretim ile öğrencileri içine alan öğrenim olmak üzere iki temel bölümden oluştuğunu belirtir.”*



Uzaktan eğitim modelinin dayandığı kuramları ele alındığında Bağımsızlık Kuramı, Özerklik Kuramı, Endüstrileşme Kuramı, İletişim ve Etkileşim Kuramı, Androgoloji/Yetişkin Eğitimi Kuramı ve Transaksiyonel Uzaklık Kuramı öne çıkan başlıklar olarak sıralanabilir (Etlüoğlu, 2019: 57-61; Bal, 2017: 73-94; Düzenli, 2019: 27-32). Bu kuramlar kısaca incelendiğinde;

- *Bağımsızlık Kuramı*: Öğrenenlerin kendi bağımsızlıklarına vurgu yapılmaktadır. Öğrenen konumunda olan bireyle bağımsız iradeleri ile öğrenme sürecine katılırlar. Wedemeyer tarafından geliştirilmiştir.
- *Özerklik Kuramı*: Moore tarafından geliştirilen bu kuramda öğrencilerin karar verme noktasında özerk iradelerini kullanabilmeleri vurgulanmıştır.
- *Endüstrileşme Kuramı*: Otto Peters tarafından geliştirilen kuramda uzaktan eğitim endüstri devrimi sonucu ortaya çıkan kitlesel eğitim hareketinin bir sonucu olarak ortaya çıkmıştır.
- *İletişim ve Etkileşim Kuramı*: Holmberg, eğitim sürecinde iletişim ve etkileşimin önemine vurgu yapmaktadır. Uzaktan eğitim modelinde de bu öğelerin güçlendirildiğini belirtmektedir.
- *Androgoloji/Yetişkin Eğitimi Kuramı*: Knowles'in kuramına göre uzaktan eğitimin amaçlarından biri de iş hayatlarına başlamış olan yetişkinlerin eğitimlerine devam edebilmesini sağlamaktır.
- *Transaksiyonel Uzaklık Kuramı*: Moore tarafından geliştirilen ikinci kuramdır. Bu kuram öğrenen ve öğretene arasında sadece fiziksel bir mesafe değil psikolojik bir mesafenin de bulunduğuna dikkat çekmektedir.
- *Eşitlik Kuramı*: Simonson tarafından geliştirilen kuramda öğrenme ortamlarının eşitliğinden ziyade eşit öğrenme deneyimlerine önem verilmesi gerektiği vurgulanmıştır.
- *İşbirlikçi Özgürlük Kuramı*: Uzaktan eğitim sürecinde özgürlüklerin bir gereksinim olduğu ancak bu özgürlüğün aşırı bireysellik doğurmasının zararlı olabileceği belirtilmiştir. Buna göre özgürlükler iş birliği ile desteklenmelidir. Bu sayede bireyler hem özgürlüğü hem de iş birliği ile öğrenmeyi sağlamış olacaklardır.

Yukarıdaki kuramlardan da hareketle uzaktan eğitim sürecinin dört adet bileşeninden söz etmek mümkündür. Bunlar e-içerik, öğrenme yönetim sistemleri, sanal sınıf ortamı ve ölçme-değerlendirmelerdir (Aksoy, 2018: 5). Öncelikle uzaktan eğitimin içerik olarak geleneksel eğitimden ayrışması gerekmektedir. Kitaplar vb. geleneksel eğitim içerikleri uzaktan eğitime uygun değildir. Bu nedenle teknolojinin yardımı ile uzaktan eğitimde içerikler elektronikleştirilmelidir. Video içerikleri, elektronik kitaplar, sanal sınavlar bunlara örnek verilebilir. Öğrenme yönetim sistemleri ise uzaktan eğitim sü-

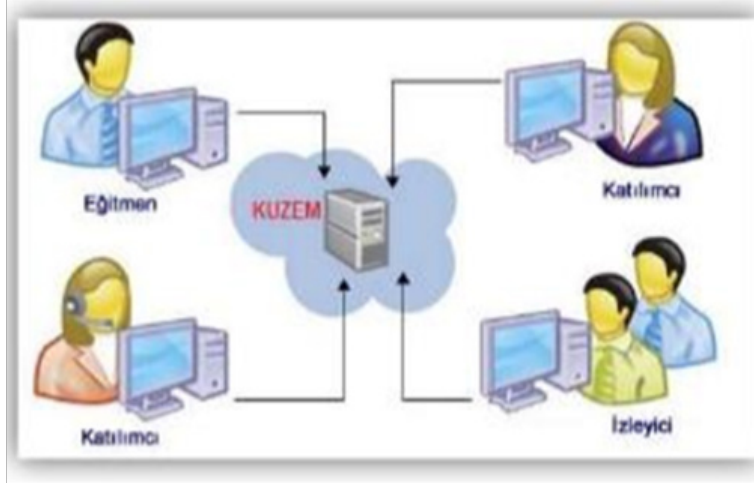
recinde sistemin yönetimini, evrak işlemlerini, kurumsal işlemleri ve sınav işlemlerini gerçekleştirebilmeyi mümkün kılan programlardır. Aynı zamanda bu sistemler ders içeriklerinin organizasyonun sağlanabildiği, etkileşim araçlarını bünyesinde taşıyan, öğretici ve öğrencilerin eğitim takibine ve öğrencilerin eğitim sürecinin kişiselleştirebilmelerine olanak sağlayan bütüncül sistemlerdir (Öztürk, Vd., 2017:82). Sanal sınıflar ise öğrenci ile öğretim elemanlarının fiziksel olmayan bir ortamda farklı zamanlarda ve farklı yerlerde bir araya gelebildiği ortamlardır. Son olarak ise eğitim sisteminin önemli unsurlarından olan eğitimin başarısını ortaya koyan ölçme-değerlendirme faaliyetleri uzaktan eğitim sürecinde önemli bir yer tutmaktadır.

**Şekil 2: Uzaktan Eğitim Bileşenleri**



Kaynak: Demir, 2014:207

Uzaktan eğitimin genel yapısına bakıldığında ise süreç içerisinde temel aktör olarak eğitmen ve öğrencinin yer aldığı görülmektedir. Ancak bazı durumlarda bu iki temel aktörün yanı sıra farklı aktörlerin de sürece dâhil olduğu görülmektedir. Uzaktan eğitim sürecine dahil olan diğer aktörler katılımcılar ve izleyicilerdir. Eğitim faaliyetleri sırasında bazı durumlarda eğitmen tarafından sürece olumlu katkısı olabileceği düşünülen katılımcılar uzaktan eğitim sürecine dahil edilebilmektedir. Aynı şekilde öğrenci konumunda olan bazı bireylerde uzaktan eğitim sürecinin belirli bir bölümüne katılarak izleyici konumunda daha sınırlı bir konu hakkında bilgi edinebilir.

**Şekil 3: Uzaktan Eğitim Yapısı**

Kaynak: [Aksoy, 2018: 5]

Buraya kadar olan kısımda anlatılanlardan yola çıkarak uzaktan eğitimin özelliklerini sıralamak gerekirse ilk dikkat çeken özellik uzaktan eğitimde eğitim görevlisi ve öğrencilerin farklı yerlerde bulunmasıdır. Süreç içerisinde her iki aktörde farklı konumlardan eğitime dahil olmaktadır. İkinci özellik uzaktan eğitim kitlesinin ortaya çıkmasında daha çok geleneksel örgün eğitimde faydalanamayan veya bu örgün eğitime destek olarak uzaktan eğitim modelini kullananlar dikkat çekmektedir. Üçüncü özellik ise teknolojik olanaklara ve kullanım tercihine göre sürecin senkron veya asenkron şeklinde olabilmesidir. Dördüncü özellik uzaktan eğitim modelinin zaman, mekan, yaş ve konu gibi unsurlarda sağladığı esnekliktir. Bu esneklik birçok avantajı da beraberinde getirebilmektedir. Beşinci özellik, uzaktan eğitim modelinde örgün eğitim modelinin aksine dijital içeriklerin bulunmasıdır. Örgün eğitimdeki kitap, defter, not vb. birçok materyal uzaktan eğitim sürecinde dijital ortama taşınmıştır. Altıncı özellik ise uzaktan eğitim modeli iletişimi engelleyen uzaklık, zamansal uyum, kapasite gibi pek çok soruna karşı etkili bir çözüm sunmaktadır. Söz gelimi normal şartlarda coğrafi uzaklık gibi nedenlerle gerçekleştirilemeyecek olan eğitim faaliyetleri uzaktan eğitim sayesinde mümkün olabilmektedir. Son olarak ise uzaktan eğitim özellikle 21. Yüzyılda gelişen teknolojiler ile tamamen teknoloji tabanlı bir hale gelmiştir (Ergenç, 2021: 80; Aksoy, 2018: 6; Akyürek, 2020: 3).

Uzaktan Eğitim modelinin barındırdığı birtakım avantajlar ve dezavantajlar bulunmaktadır. Uzaktan eğitimin ilk avantajı maliyet konusundadır. Fiziki olarak pek çok hazırlığın ve masrafın yapıldığı örgün eğitime oranla uzaktan eğitim sadece teknolojik bir maliyete sahiptir. Başka bir açıdan ise örgün eğitime oranla zamansal ve mekansal bir

bağımsızlık sağlamaktadır (Garrison, 2003: 52–54). Günümüz kitle eğitim amaçları için ise uzaktan eğitim modeli oldukça uygundur. Günümüz iletişim teknolojileri ile geniş kitlelere uzaktan eğitim verilebilmektedir. Uzaktan eğitim modeli engelli bireyler gibi dezavantajlı grupların eğitimi içinde oldukça uygun bir modeldir. Bu sayede hükümetlerin eğitim politikalarında daha fazla etkinlik ve verimlilik sağlamak mümkündür. Uzaktan eğitim sayesinde üniversiteler gibi bilgi üreten kurumların ürettikleri bilgiler kurum içerisinde kalmadan daha geniş kitlelere ulaştırılabilir. Bu sayede paylaşılan bilgi ile bilimin ilerleyişi hızlanacaktır. Politika alanının önemli özelliklerinden biri de sürekli olmasıdır. Uzaktan eğitim modeli sayesinde eğitim politikalarında süreklilik sağlamak mümkündür. İçinde yaşadığımız pandemi dönemi bunun en güzel örneğidir. Uzaktan eğitimin diğer avantajlarına değinecek olursak bireysel gelişimi izleme noktasında verimli bir modeldir. Ayrıca teknolojinin ucuzlayıp yaygınlaşması ile paralel şekilde modelinde yaygınlaşması ve daha erişilebilir hale gelmesi önemli bir avantajdır. Tüm bunları yanı sıra uzaktan eğitim modeli geleneksel eğitim modelini destekler bir niteliğe sahiptir. Bu model sayesinde örgün eğitimdeki pek çok öğrencinin eksikleri için destek sunulabilir. Öğrenciler ekstra olarak ilgi duydukları alanlarda uzaktan eğitim yoluyla eğitim alabilirler (Altınsoy, 2019: 8; Ataş, 2017: 16; Etlioğlu, 2019: 61; Balıkçioğlu, Vd., 2019: 464).

Sayılan tüm avantajların yanında uzaktan eğitim modelinin bazı kısıtlılıkları ve dezavantajları da bulunmaktadır. Bunlardan ilki bireyler için oldukça önemli olan sosyalleşmenin uzaktan eğitim modelinde yeterince gelişmiyor olmasıdır. Toplum içerisinde tecrübeye dayalı olarak gelişen bazı davranış kalıpları için uzaktan eğitim modeli ciddi kısıtlılıklar içermektedir. Örgün eğitimde öğrencilerden alınan geri bildirim(feedback) uzaktan eğitim sürecinde kısıtlı olarak alınabilmektedir. Sınırlı geri bildirim imkanı önemli bir dezavantaj oluşturmaktadır. Öbür taraftan ise örgün eğitime destek olan uzaktan eğitim modelinde bireylerin dinlenme vakitleri uzaktan eğitime ayrılabilir. Bu da bireylerde stres artışına ve mutsuzluğa yol açabilmektedir. Uzaktan eğitimin kısıtlı yönlerinde biri de teknoloji ile olan simbiyotik bağılılığıdır. Bu bağılık neticesinde teknolojiye ulaşamayan veya kullanamayan dezavantajlı gruplar ortaya çıkabilmektedir. Ayrıca gerekli teknolojik altyapının kurulum ve bakım masrafları da modelin kısıtlılıkları arasında sayılabilir (Akyürek, 2020: 4-5; Etlioğlu, 2019: 62; Ataş, 2017: 17).

## 2. UZAKTAN EĞİTİMDE TARİHSEL GELİŞİM

Uzaktan eğitimin yaklaşık 300 yıllık bir geçmişi olduğu kabul edilmektedir. En eski uzaktan eğitim örneği olarak 1728 yılında Amerika Boston’da gazeteye ilan vererek mektup ile steno(hızlı yazı yazma) dersleri vereceğini söyleyen Caleb Phillipps gösterilmektedir. Daha sonraki süreçte 1833 yılında İsveç’te bir gazete ilanı ile kompozisyon yazma dersi verileceği ilan edilmiştir. 1840 yılında ise Isaac Pitman’ın İngiltere’de mektup ile steno dersleri verdiği bilinmektedir. 1843 yılında “Fonografik Mektup Topluluğu”

kurulmuştur. Böylece mektup ile uzaktan eğitim sistemli bir yapıya bürünmüştür. 1856 yılında Berlin’de mektup ile eğitim veren bir uzaktan eğitim kurumu kurulmuştur. 1920’li yıllara kadar yazışmalar yoluyla devam eden uzaktan eğitim radyonun icadı ile farklı bir noktaya evrilmiştir. 1921 yılına Latter Day Saints Üniversitesi radyo teknolojisini kullanarak eğitsel yayınlar yapmaya başlamıştır. Teknolojinin gelişmesiyle televizyonların ortaya çıkması uzaktan eğitime farklı bir boyut kazandırmıştır. 1934 yılında Iowa State Üniversitesi televizyon üzerinden öğretici yayınlar yapmaya başlamıştır. İkinci dünya savaşının ardından ise radyo ve televizyon teknolojisi tüm dünyada yaygınlık kazanmış ve böylece uzaktan eğitim faaliyetleri kitlesel bir nitelik kazanmaya başlamıştır. Uzaktan eğitimin niteliklerinin ortaya çıkması ile birlikte bu alana olan ilgi artmıştır. Tüm dünyada bu alana yönelik araştırmalar yapılmaya başlanmıştır. 1969 yılında İngiltere’de “İngiliz Açık Üniversitesi” kurulmuş, böylece uzaktan eğitimin yükseköğretimde de kullanılabilceği anlaşılmıştır. Bunun sonucu olarak tüm dünyada uzaktan eğitim veren yükseköğretim kurumlarına başlanmıştır. 1979 yılında “Çin TV Üniversitesi Sistemi”, 1982 yılında Türkiye’de Anadolu Üniversitesi, 1985 yılında “İndira Gandhi Ulusal Açık Üniversitesi” kurulan dikkat çekici uzaktan eğitim kuruluşlarıdır. 1970-80’li yıllarda Telekomünikasyon teknolojilerinin devreye girmeye başlamasıyla uzaktan eğitim yeni bir boyut kazanmıştır. 1990’lı yıllarda internetinde kullanılmaya başlaması ile o zamana kadar evde bireysel çaba ile yürütülen uzaktan eğitim faaliyetleri birçok bireyin farklı yerlerden bağlanabildiği bir tele-konferans sistemine dönüşmüştür (Düzenli, 2019: 9-11; Enfiyeci, 2019: 11; Aksoy, 2019: 9; ataş, 2017: 13-14; Demir, 2014: 204-205).

Çevrimiçi eğitim hizmeti olarak Phonix Üniversitesi’nin 1989 yılında kullanmaya başladığı “CompuServe” alanın ilk örneğidir. P. Sloan Vakfı tarafından ise 1992 yılında Asenkron Öğrenme Ağları geliştirilmiştir. 1997 yılına gelindiğinde ülkede pek çok üniversite uzaktan eğitim vermeye başlamıştır. 1998 yılında ise New York Üniversitesi “NYU Online” hizmetini etkin hale getirerek uzaktan eğitime dâhil olmuştur. 2000’li yıllardan sonra ise bu alanda sunulan hizmetler katlanarak artmıştır (Etlioğlu, 2019: 46-47).

Miller’in (2021) yaptığı araştırmaya göre Amerika Birleşik Devletleri’nde 226 yılına kadar uzaktan eğitim endüstrisinin büyüklüğünün 370 milyar doları geçmesi beklenmektedir. Raporda Amerika’da yapılan üniversite kayıtlarında uzaktan eğitim veren kurumlara yapılan kayıtların her yıl giderek arttığı gözlemlenmektedir.

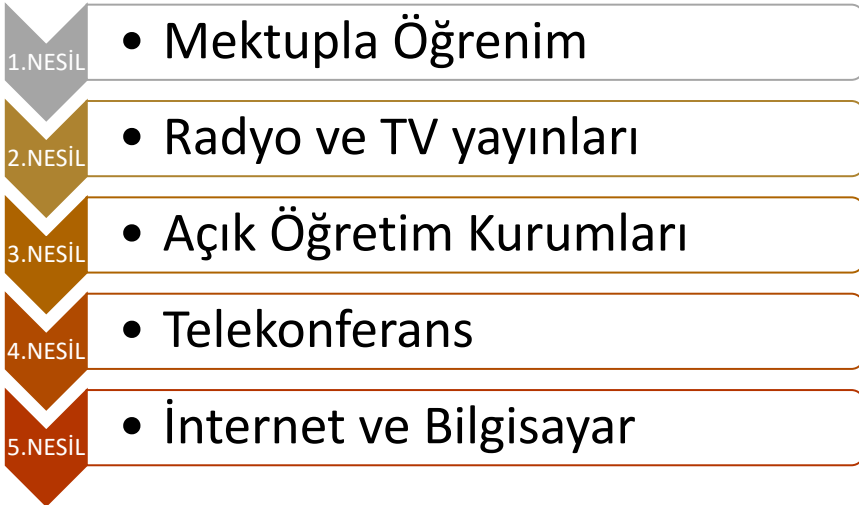
11 Mart 2021 Perşembe günü Başkan Biden tarafından imzalanan “Amerikan Kurtarma Planı” ile birlikte Amerika’da pandemiden etkilenen eğitim sektörüne yönelik büyük miktarda bir fon artışı hedeflenmektedir. Bu artış ile pandemi sürecinde eğitim alanında olumsuz etkilenen bireylerin eksik kaldığı noktalarda uzaktan eğitim modeli yardımıyla desteleme eğitimleri yapılması planlanmaktadır (American Rescue Plan, 2021).

Amerika Birleşik Devletleri’nde yükseköğretim kurumlarında en fazla uzaktan eğitim alanına yer veren üniversiteler ise şu şekilde sıralanmaktadır ([www.distancelearningportal.com](http://www.distancelearningportal.com), 2021):

1. John Hopkins University
2. Northwestern University
3. University of California, Los Angeles (UCLA)
4. New York University
5. University of Texas at Austin
6. Georgia Institute of Technology
7. Boston University
8. The Ohio State University
9. University of Maryland
10. University of Pittsburgh

İngiltere’de uzaktan eğitim alanında önde gelen kurumlardan biri Oxford Üniversitesidir. Üniversite çeşitli konularda birçok çevrimiçi uzaktan eğitim olanağı sunmaktadır (Etlioğlu, 2019: 47-48). Çin’deki yüksek nüfusun eğitim ihtiyacını karşılamak için “Çin Eğitim ve Araştırma Ağı (CERNET- China Education and Research Network)” kurulmuştur (Etlioğlu, 2019: 49). Çin’in uzaktan eğitim altyapısı pandemi döneminde oldukça yüksek olan nüfusunun eğitim ihtiyacını karşılayabilmesini sağlamıştır. Tüm bu tarihsel süreçlere bakıldığında uzaktan eğitimin tarihsel gelişimin beş nesle ayırmak mümkündür:

**Şekil 4: Tarihsel Gelişim**



Kaynak: (Aksoy, 2018: 9)

1. Nesilde Mektup yoluyla uzaktan eğitim faaliyetleri ile karşılaşılmaktadır. 2. Nesilde Radyo ve Televizyon Teknolojilerinin devreye girmesiyle yeni bir dönemin başladığı görülmektedir. 3. Nesilde Açık Öğretim Kurumlarının ortaya çıkmaya başladığı görülmektedir. 4. Nesilde telekomünikasyon teknolojilerindeki gelişmeler sayesinde telekonferans döneminin başladığı görülmektedir. 5. Nesilde ise İnternet ve Bilgisayar teknolojilerinin ortaya çıkması ve yaygınlaşmasıyla sürecin daha farklı ve daha güçlü bir yöne evrildiği görülmektedir. Bu gelişim çizgisi uzaktan eğitim sisteminin teknoloji ve çağın ihtiyaçları doğrultusunda şekillenen bir olgu olarak karşımıza çıktığını göstermektedir. Teknolojik olanaklar bir yandan uzaktan eğitimin verimliliği ve yaygınlığı üzerine olumlu bir etki ederken diğer yandan toplumda artan eğitim ihtiyaçları doğrultusunda da gittikçe talep gören bir seçenek haline gelmiştir. Günümüzde ise teknolojinin geldiği nokta ve artan öğrenme ihtiyacı uzaktan eğitimi eğitimin her kademesinde bir alternatif olarak değerli, eğitimin bir parçası olarak karşımıza çıkarmaktadır (Çivril, Vd., 2018: 42).

### 3. TÜRKİYE'DE UZAKTAN EĞİTİM

Türkiye’de uzaktan eğitim konusu ilk kez 1924 yılında gündeme gelmiştir. Dewey tarafından sunulan raporda ülkenin her yerindeki öğretmenlerin uzaktan eğitim yolu ile koordine edilmesi ve eğitilmesini önermesi ile konu gündeme gelmiştir. 1939 yılında ise toplanan Milli Eğitim Şurasında konu tekrar gündeme gelmiştir. Türkiye’de uzaktan eğitim alanında özel sektör bazlı ilk faaliyet ise bir dil kurumu olan FONON tarafından gerçekleştirilmiştir. Kuruluş, Milli Eğitim Bakanlığında aldığı özel izin ile 1953 yılında bir açıköğretim kurumu oluşturmuştur. Bu kurum yıllarca uzaktan dil eğitimi vermiştir. 1956 yılına gelindiğinde ise Ankara Üniversitesi Banka ve Ticaret Hukuku Enstitüsü uzaktan eğitime yönelik girişimlerde bulunmuştur. 1974 tarihinde YAYKUR (Yaygın Yükseköğretim Kurumu) vasıtası ile televizyon yayını yoluyla lise mezunu bireylere ön lisans mezunu olma imkanı tanınmıştır. 1976-1977 yıllarında Eskişehir İktisadi ve Ticari İlimler Akademisinin gerçekleştirdiği uzaktan eğitim faaliyetleri alanın gelişmesine katkıda bulunmuştur. Uzaktan Eğitim faaliyetlerinin sistemli bir bütün haline gelmesi Açıköğretim Fakültelerinin kurulması ile olmuştur. 20 Temmuz 1982 yılında çıkarılan 41 sayılı KHK ile Anadolu Üniversitesi’ne açıköğretim faaliyetleri yapabilme yetkisi tanınmıştır. Bu doğrultuda Türkiye’de modern anlamda uzaktan eğitim faaliyetleri Anadolu Üniversitesi ile başlamıştır. Daha sonra ODTÜ tarafından uzaktan eğitimle sertifikalı programları açılmaya başlamıştır. 1991 yılında ise Fırat Üniversitesi kendi TV yayın istasyonunu kurarak TV üzerinden uzaktan eğitim faaliyetlerine başlamıştır. 1992 yılında Açıköğretim Lisesi, 1997 yılında ise Açık İlköğretim Okulu kurulmuştur. Üniversitelere uzaktan eğitim faaliyetleri yetkisi veren yasa 14 Aralık 1999 tarihinde çıkarılan 23906 sayılı “Üniversitelerarası İletişim ve Bilgi Teknolojilerine Dayalı Uzaktan Yükseköğretim Yönetmeliği”dir. Bu yönetmelik ile “Enformatik Milli Komitesi” kurulmuştur. Bu komite üniversitelere bağımsız kredi açma imkanı vermiştir. Bu süreçle birlikte Ahmet Yesevi Üniversitesi ile Anadolu Üniversitesi iş birliği ile uzaktan eğitim faaliyetlerinin kapsa-

minini arttırmıştır. 2000’li yıllardan sonra ise uzaktan eğitim faaliyetlerinde ciddi bir artış yaşanmıştır. 2005 yılında ise YÖK tarafında Uzaktan Eğitim Komisyonu kurulmuştur. 2009 yılında İstanbul Üniversitesi uzaktan eğitim hizmeti sunmaya başlamıştır. Aynı yıl Atatürk Üniversitesi Uzaktan Eğitim Uygulama ve Araştırma Merkezi (ATAUZEM) kurulmuştur. Ayrıca 2011 yılında Atatürk Üniversitesi Açıköğretim Fakültesi de açılmıştır. Türkiye’de uzaktan eğitim faaliyetleri genel olarak üniversitelerin kendi bünyelerinde çıkardığı yönetmelikler ile düzenlenmektedir (Etlioğlu, 2019: 53-57; Aksoy, 2018: 11-14; Ataş, 2017: 87-90; Bozkurt, 2017: 87-90; Kaya, 2020: 38-42).

Türkiye’de uzaktan eğitim faaliyetleri genellikle üniversiteler bünyesinde sürdürülmektedir. Anadolu Üniversitesi, Atatürk Üniversitesi ve İstanbul Üniversitesi uzaktan eğitim hizmeti veren en büyük üniversitelerdir (Akarsu, 2019: 49-61). Türkiye’de üniversitelerin koordinasyonu ile görevli olan Yüksek Öğretim Kurumu (YÖK) uzaktan eğitim faaliyetlerinde de yetkilere sahiptir. YÖK bünyesinde bulunan Uzaktan Eğitim Kurulu ile bu yetkilerini kullanmaktadır. Uzaktan eğitim konusunda yetkileri bulunan ve etkin faaliyetleri olan diğer kuruluş ise Milli Eğitim Bakanlığı’dır. Bakanlık kurduğu Eğitim Bilişim Ağı (EBA) ile uzaktan eğitim faaliyetlerini tek çatı altında birleştirmiştir. EBA, bünyesinde çok çeşitli dijital içerikler sunarak öğrencilere fayda sağlamaktadır (Yaman, 2021: 3304). Son olarak ise özel kuruluşlar dikkat çekmektedir. Türkiye’de eğitim alanında güçlü bir özel sektör bulunmaktadır. Bu sektör gerek özel okullarıyla gerekse de özel üniversite veya kursları ile uzaktan eğitim hizmeti vermektedir.

### Şekil 5: Türkiye’de Uzaktan Eğitim Aktörleri



Kaynak: (Ataş, 2017)



Türkiye’de Temmuz 2019 yılında yayımlanan 11. Kalkınma Planında üç adet maddenin uzaktan eğitim alanıyla ilgili olması dikkat çekicidir. Söz konusu maddelerde ilki planın ikinci bölümünde yer alan “Rekabetçi Üretim ve Verimlilik” başlığı altındadır. Söz konusu başlık altında “Yüksek Kurumsal Kapasite” başlığıyla verilen maddede “*Verimlilik konusunda uzaktan eğitim platformu kurulacaktır*” (md. 312.3) ibaresi yer almaktadır. Kalkınma planında uzaktan eğitim konulu ikinci madde “Nitelikli İnsan, Güçlü Toplum” başlığı altında “*Engellilerin meslek edinmesine yönelik uzaktan eğitim programları geliştirilecektir*” (md. 572.1) şeklindedir. Uzaktan eğitimin engellilere yönelik politikalarda kullanılması politika belgesinin dikkat çekici bir yönüdür. Politika belgesinde yer alan uzaktan eğitimle ilgili son madde ise “Hukuk Devleti, Demokratikleşme ve İyi Yönetişim” başlıklı bölümde yer alan “*Hizmet içi eğitim uygulaması, kamu çalışanlarının mesleki ve temel becerilerini artıran uzaktan eğitim sistemleri kullanılmak suretiyle kolayca erişilebilen bir yapıya dönüştürülecektir*” (md. 806.3) maddesidir (Strateji ve Bütçe Başkanlığı, 2019).

Türkiye’de uzaktan eğitim alanında en önemli aktörlerden biri Yükseköğretim Kurulu(YÖK)’dur. Bu nedenle bu kurumun politika belgelerini incelemek Türkiye’de uzaktan eğitim alanındaki politika süreci hakkında önemli bilgiler sunmaktadır. Çalışma kapsamında kuruma ait ulaşılabilen en eski politika belgesi 23 Mart 1996 tarihinde yayınlanan belgedir. Bu belgede Türk yükseköğretiminin mevcut durumu incelenmiş ve sorun alanları ile çözüm önerileri sunulmuştur. Belge incelendiğinde uzaktan eğitim kavramının belgede dört kez kullanıldığı görülmektedir. İlki temel sorunlar alanında iki yıllık eğitim veren kurumların bazı eğitimleri uzaktan eğitim yöntemiyle verebileceğinden bahsetmektedir. Devamında ise uzaktan eğitim yöntemlerinin giderek yaygınlaştığı vurgulanmaktadır (YÖK, 1996). 1996 yılında uzaktan eğitim alanının tüm dünyada hızlı gelişimi Türkiye’de de yansımalarını bulmuş ve YÖK’ün politika belgelerine bu durum yansımıştır.

YÖK’ün konu ile ilgili diğer önemli politika belgesi ise Şubat 2007 yılında yayınlanan “Türkiye’nin Yükseköğretim Stratejisi” isimli politika belgesidir. Söz konusu belgede 2007 yılı itibari ile Türkiye’nin yükseköğretim sistemi hakkında bilgiler sunulmaktadır. Bu bilgiler içerisinde uzaktan eğitim alanının da bulunması dikkat çekicidir. Belgede, Türkiye’nin Anadolu Üniversitesi gibi üniversiteler bünyesinde yürüttüğü uzaktan eğitim faaliyetleri sayesinde dünyada bu alanda önemli bir yere sahip olduğu belirtilmektedir. Politika belgesinde belirlenen kapasite sorunu gibi sorun alanlarına yönelik uzaktan eğitim modelinin etkinliği bir çözüm olabileceği belirtilmektedir. Ayrıca belgede ‘yaşam boyu öğrenme’nin artan önemi vurgulanmış ve bu artışın beraberinde uzaktan eğitim sistemlerinde bir gelişmeyi tetikleyeceği belirtilmiştir. Belgede 1999 yılında “Enformatik Milli Komitesi” kurulmasına rağmen istenilen gelişmelerin sağlanamadığı noktasında bir özeleştiri de yapılmıştır. Son olarak ise belgede 2007 itibari ile Türkiye’de yükseköğrenim içerisinde uzaktan eğitimin payının %30’un üzerinde olduğu vurgulanmıştır (YÖK, 2007).

Pandemi dönemine girildikten sonra YÖK tarafından yeni koşullar çerçevesinde uzaktan eğitimi kapsamlı şekilde ele alan bir belge yayınlanmıştır. “Küresel Salgında Yeni Normalleşme Süreci” başlıklı bu belgede pandemi döneminde yükseköğretim sisteminde meydana gelen değişimler ele alınmaktadır. Söz konusu politika belgesinde dikkat çekici nokta salgın sonrasında da ‘karma’ bir eğitim modelinin uygulanabileceğidir. Pandemi döneminde uzaktan eğitimin verimliliğinin ortaya çıkmasıyla beraber örgün eğitimin çevrimiçi uzaktan eğitim ile desteklenebileceği belirtilmiştir. Belgede pandemi döneminde sorun yaşayan alanlardan olan ‘uygulamalı eğitimler’e de değiştirilmiş olması önemlidir. Uzaktan eğitimin tek taraflı olmaması gerektiği ve bu doğrultuda etkileşimi artırıcı şekilde düzenlenmesi gerektiği vurgulanmıştır. Hayat boyu öğrenme sürecine destek olarak bir “açık kaynak ekosistemi” belgede vurgulanan diğer bir önemli noktadır. YÖK tarafından üniversitelere altyapı desteği sağlanması gerektiği vurgulanan belgede üniversitelere konu ile ilgili araştırma ve AR-GE faaliyetlerini arttırmaları tavsiye edilmektedir. Belgede uzaktan eğitim modeline uygun insan kaynağına da yer verilmiştir. Bu doğrultuda bu model üzerinden ders verecek olan eğitimcilerin yeterliliklerinin iyileştirilmesi noktasında çalışmalara önem verilmesi gerektiği ifade edilmiştir. Uzaktan eğitim modelinden istenilen verimin alınabilmesi için yapılanma ve organizasyonun önemi olduğu ve bu nedenle üniversitelere önemli görevler düştüğü görülmektedir. Uzaktan eğitim sürecinde bireylerin psikolojik yıpranmalarına da değinilen belgede bu konu ile ilgili ders dışı çevrimiçi etkinlikler tavsiye edilmiştir. YÖK tarafından alınan kararla “salgından bağımsız olarak” eğitim programlarında %40 oranının da uzaktan eğitim zorunluluğu getirilmiştir. Belgede bu kararın salgından bağımsız bir karar olduğu önemle vurgulanmıştır. Ölçme-değerlendirme noktasında ise geleneksel yöntemlerin kullanılması gerektiği ancak bunların yanı sıra yeni yöntemlerinde uygulanması gerektiği belirtilmiştir (YÖK, 2020). Uzaktan eğitim modelini konu alan söz konusu belge alana yönelik en dikkat çekici politika belgesi olarak öne çıkmaktadır.

Günümüzde gelinen noktada uzaktan eğitim ve teknoloji arasında simbiyotik bir ilişki bulunmaktadır. Günümüzde mevcut olan uzaktan eğitim uygulamalarının tamamı teknoloji tabanlıdır. Bu nedenle bir ülkede uzaktan eğitim alanını incelerken söz konusu ülkenin teknolojik altyapısını göz önünde bulundurmak gerekmektedir. Türkiye’de de teknolojik durumu anlamak uzaktan eğitim sisteminin başarı düzeyi ile ilgili fikir sahibi olabilmek açısından önemlidir. Türkiye İstatistik Kurumunun 25 Ağustos 2020 tarihinde yayınladığı “*Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması, 2020*” (TUIK, 2020) başlıklı araştırma bu konu ile ilgili önemli veriler içermektedir. Söz konusu araştırmaya göre Türkiye’de internet kullanan bireylerin oranı %79,0’a yükselmiştir. Bu oranın geçen yılın aynı döneminde %75,3 olduğuna araştırmada dikkat çekilmiştir. Araştırmadaki diğer önemli veri ise ‘evden internete erişim imkânıdır. Bu veri ise 2020 itibarı ile %90,7’ye ulaşmıştır. 2019 yılında ise bu oran %88,3 olduğu görülmektedir. Son olarak ise araştırmada Türkiye’de genişbant ile internete erişim sağlayan hanelerin oranı

%89,9 olarak belirtilmiştir. Bu veriler göstermektedir ki Türkiye’de uzaktan eğitim alanında gerekli olan teknoloji kullanımı üst düzeyde mevcuttur.

Türkiye’de 13 Mart 2021 tarihinde Çin’de ortaya çıkan ve tüm dünyaya yayılan Koronavirüs (Covid-19) salgını nedeni ile tüm ülkede eğitime ara verilmiştir. Aradan geçen 1 yıllık süreçte ülkede eğitim-öğretim faaliyetleri uzaktan eğitim yoluyla devam ettirilmiştir. Bu süreçte Milli Eğitim Bakanlığının EBA ([www.eba.gov.tr](http://www.eba.gov.tr)) sistemi önemli katkılar sağlamıştır. İlköğretim, ortaöğretim ve lise düzeylerinde öğrenciler bu süreçte EBA sistemi üzerinden derslerine devam edebilmişlerdir. Yükseköğretim öğrencileri ise bu süreçte üniversitelerin UZEM sistemleri üzerinden eğitimlerine devam etmişlerdir (Avcı ve Akdeniz, 2021: 120). Can, 2020;Koç, 2021)

### Şekil 6: MEB ve YÖK Öğrenci Verileri (2020)

MEB Öğrenci Sayısı	
Toplam İçerisinde Açık Öğretim Sayısı	1.583.805
Toplam	18.241.881
YÖK Öğrenci Sayısı	
Önlisans Öğrenci Sayısı	3.002.964
Lisans Öğrenci Sayısı	4.538.926
Yüksek Lisans Öğrenci Sayısı	297.001
Doktora Öğrenci Sayısı	101.242
Toplam İçerisinde Açıköğretim Programları Öğrenci Sayısı	4.199.801
Toplam	7.940.133

Kaynak: (MEB, 2020; YÖK, 2020)

Şekil 6’da görülen öğrenci sayıları Türkiye’de uzaktan eğitim sisteminin bir tercihten çok zamanla zorunluluk haline geleceğini göstermektedir. Bu oranda yüksek bir nüfusu eğitmek için yalnızca geleneksel yollardan yararlanmak yeterli olmayacaktır. Bu nedenle önümüzdeki süreçte Türkiye’de uzaktan eğitim önemini giderek artacağını iddia etmek yanlış olmayacaktır. Babaoğlu ve Öktem’in (2017: 11) araştırması neticesinde Türkiye’de uzaktan eğitim sisteminin büyükşehirlerde daha fazla geliştiği ortaya çıkmıştır. Bu olgunun temelinde büyükşehirlerde teknolojik altyapı imkânlarının gelişmiş olması, yoğun nüfus alanları ve büyük üniversitelerin varlığı gibi nedenler sayılabilir.

Küresel salgınların insanlık tarihine her zaman önemli etkileri olmuştur. Covid-19 pandemisi de tüm dünyaya birçok sıkıntının beraberinde yenilikler de getirmiştir. Türkiye’de tüm dünya ile bu süreçte birçok yeniliğe ve dönüşüme sahne olmuştur. 2000’lerden sonra dijitalleşen dünyada dijitalleşmeye karşı olan direnç pandemi dönemi ile birlikte kırılmış görülmektedir. Türkiye’de bu 16 Mart 2020 sonrası eğitimin tüm kademelerinde uzaktan eğitime zorunlu bir geçiş deneyimi yaşanmıştır. Özellikle yükseköğretim seviyesinde eğitim veren yaklaşık 3.000 tane kurum içinden öğrenci, akademik ve idari personel dahil 3 milyondan fazla kişinin direkt ya da dolaylı olarak etkilenmesine neden olmuştur (Yamamoto ve Altun, 2020: 26). Bu deneyim sırasında teknolojiden ulaşıldığı kadar faydalanılarak sürecin olumsuzlukları minimuma indirgenmeye çalışılmıştır. Pandemi öncesi eğitimde teknoloji kullanımını yaygınlaştırırken pandemiyle yüksek bir ivme kazanmıştır. Bu süreçte ilk ve ortaokullarda, liselerde ve üniversitelerde büyük orandan uzaktan eğitim ile derslere devam edilmiştir. Üniversitelerde lisans, yüksek lisans ve doktora gibi eğitimler uzaktan eğitim teknolojileri ile devam ettirilmiştir. Bu dönemde birçok konferans ve sempozyum teknolojik imkanlar sayesinde geniş kitlelere ulaşabilmiştir. Türkiye’de pandemi süreciyle birlikte pek çok bireyin normal şartlarda ulaşamayacağı eğitimler ücretsiz bir şekilde halka sunulmuştur. Bütün bunlar pandemi ile birlikte Türkiye’de uzaktan eğitim alanında yeni gelişmelerin ortaya çıktığını ve pandemi sonrasında da bu gelişmelerin devam edeceğini göstermektedir (Babaoğlu ve Kulaç, 2021).

#### 4. SORUNLAR VE ÇÖZÜM ÖNERİLERİ

Türkiye’de uzaktan eğitim alanında en önemli avantaj uzun yıllara dayanan altyapıdır. 1980’li yıllardan itibaren üniversiteler bünyesinde başlayan ve daha sonra yaygınlaşan sistem neticesinde alanda tecrübeleri kurum ve eğitmenler mevcuttur. Uzaktan eğitim için olmazsa olmazlardan hizmet sağlayıcı sistemler Türkiye’de gelişmiştir. EBA ve üniversitelerin UZEM sistemleri bunlara güzel örneklerdir. Türkiye’nin uzaktan eğitimde güçlü yanlarından biri de insan kaynağının teknolojiye olan uyumudur. 2000’li yıllardan sonra ülke genelinde yayılan teknolojiler neticesinde başta yeni nesiller olmak üzere pek çok bireyde teknoloji ile uyumluluk görülmektedir. Türkiye’de Milli Eğitim Bakanlığı (MEB) ve Yükseköğretim Kurulu (YÖK) gibi kuruluşlar alanın güçlü yanlarından biridir. Bu kurumların alana yönelik yetkilerinin bulunması önemlidir. Eğitim sistemine en yakın olan kurumların yetkiyi kullanması güçlü bir yöndür. Son olarak ise uzun yıllardır teknolojilerin etkin kullanımı neticesinde dijital içerik alanında önemli bir birikim elde edilebilmiştir. Günümüz itibari ile sanal ortamda pek çok içeriğe (video, ses, metin, uygulama vb.) ulaşılabilmektedir (Türk Eğitim Derneği, 2020).

Tüm bu avantajların yanı sıra pandemi sürecinin göstermiş olduğu bazı sorun alanları da mevcuttur. En büyük ve önemli sorun alanı altyapı eksikliğidir. Günümüz teknolojilerinin hayatlarımıza girmesi ile uzaktan eğitim ve teknoloji simbiyotik bir ilişki içe-

risine girmiştir. Bu nedenle internet vb. altyapı sorunları ciddi sorunlardır. Öte yandan bazı durumlarda altyapı yeterli olsa dahi teknoloji kullanımı istenilen düzeylere ulaşmamaktadır. Özellikle belli bir yaş grubu üzeri teknolojik kullanımda isteksiz davranabilmektedir. Teknolojik istekliliği yüksek ancak teknolojiye erişemeyen dezavantajlı gruplardan söz etmek mümkündür. Bu bağlamda maddi vb. nedenler ile dezavantajlı gruplar mevcuttur. Uzaktan eğitimde eğitici önemli bir unsurdur. Geleneksel eğitim sistemine alışkın pek çok eğitimci uzaktan eğitim sürecinde uyum problemi yaşamaktadır. Sürecin diğer önemli aktörü de eğitilen bireylerdir. Bu bireylerde özellikle asenkron gibi etkileşimsiz derslerde derslere olan ilgilerini kaybedebilmektedirler. Uzaktan eğitimde sorun teşkil eden alanlardan biri de uygulamalı alanlardır. Pek çok uygulama gerektiren eğitim uzaktan eğitim sistemi ile verilememektedir. Son olarak ise geleneksel eğitim sisteminin ölçme-değerlendirme uygulamaları uzaktan eğitim sistemine uygun değildir (Türk Eğitim Derneği, 2020)

Tüm bu sorun alanlarından yola çıkarak oluşturulan çözüm önerileri:

### Şekil 7: Çözüm Önerileri

<b>Daha Fazla Araştırma ve İnceleme</b>	Alana yönelik çalışmalar yapılmalıdır. Öğretmen ve öğrencilere süreçte yaşadıkları sorunlar sorulmalıdır. Bunun için saha araştırmaları yoluyla geri bildirimler alınmalıdır.
<b>Sorunlar Kategorize Edilmeli</b>	Dezavantajlı gruplar tespit edilmelidir. Bu grupların dezavantajları iyi bir şekilde kategorize edilmeli ve bu kategorilere göre çözüm sunulmalıdır. Örneğin sorun teknoloji yetersizliği mi yoksa teknoloji kullanımında yaşanan sorunlar mı? Sorun alanlarının kategorize edilmesi çözüm stratejilerinde avantaj sağlayacaktır.
<b>Psikolojik Yön Önemli</b>	Alanın teknik yönünün yanı sıra insani yönüne de önem verilmelidir. Özellikle pandemi dönemlerinde birçok öğretmen ve öğrenci uzun vakitler evlerinde kalmak zorunda kalmışlardır. Bu bireylerde stres düzeyinin artmasına ve başarısızlığı tetiklemesine neden olmaktadır. Bu nedenle uzaktan eğitimi yalnızca eğitim faaliyetlerine kullanmakla yetinmemeli; psikolojik destek ve bireysel koçluk hizmetleri gibi faaliyetler ile bireyleri uzaktan eğitime zihinsel olarak da hazır hale getirmek gerekmektedir.
<b>Eğitimcilere Teknik Destek</b>	Birçok öğretmen son dönemde yaşanan zorunlu uzaktan eğitime geçiş sürecinde uyum problemleri yaşamaktadır. Bu sorunu ortadan kaldırmak için eğitim görevlilerinin sorun yaşadıkları anlarda teknik destek alabilecekleri çağrı merkezleri kurulmalıdır. Ayrıca uyum problemini aşmak için hizmet içi eğitimler verilmelidir. Son olarak ise öğretmenlerin karşılaştığı sorun alanları tespit edilmeli, bu alanların niteliklerine göre çözümler geliştirilmelidir.

<b>Daha Fazla Etkileşim</b>	Uzaktan eğitimin kısıtlı yönlerinden birisi sosyalleşmeyi ve etkileşimi sınırlamasıdır. Bu sınırlamayı engellemek için uzaktan eğitimde mümkün oldukça canlı video konferans dersler tercih edilmeli, asenkron şekilde gerçekleştirilen eğitimden kaçınılmalıdır.
<b>Uygulamalı Alanlar</b>	Uygulamalı alanların yaşadığı problemler göz önünde bulundurulmalı, uygulamalı derslerin telafisi yüz yüze eğitim döneminde yapılmalıdır. Uygulamalı eğitim alması gereken bireylerin bu eğitimleri teorik olarak uzaktan eğitim yoluyla alıp meslek hayatlarına başlamaları engellenmelidir.
<b>Yeni Ölçme-Değerlendirme Yöntemleri</b>	Uzaktan eğitim sürecinde yaşanan sıkıntıların başında ölçme-değerlendirme gelmektedir. Geleneksel sistemdeki sınavların uzaktan eğitimde uygulanması güçtür. Bu nedenle uzaktan eğitime yönelik yeni ölçme-değerlendirme yöntemleri geliştirilmelidir. Öğrenciyi düşünmeye ve araştırma yapmaya yönlendiren proje yöntemleri buna güzel bir örnektir.

Küreselleşen dünyamızda teknolojinin hayatımızın vazgeçilmez bir parçası olduğu aşikârdır. Teknoloji geliştikçe hemen her alanda etkisini hissettirmektedir. Uzaktan eğitim alanı da hiç şüphesiz teknolojinin önemli rol oynadığı bir alandır. Artan dünya nüfusu, yaşanan küresel salgınlar ve kitlesel eğitim hedefleri uzaktan eğitimin önemini her geçen gün arttırmaktadır. Bu nedenle uzaktan eğitim konusunda daha fazla çalışma yapmak, alana yönelik sorunları tespit etmek ve çözüm önerileri geliştirmek başta ülkemiz olmak üzere tüm dünya için önemli bir meseledir.

## SONUÇ

Uzaktan eğitimin yaklaşık üç yüz yıllık bir geçmişi olduğu kabul edilmektedir. Aradan geçen dönemde uzaktan eğitim önemini giderek arttırmıştır. Özellikle içinde bulunduğumuz pandemi dönemi uzaktan eğitimin önemini bir kez daha gözler önüne sermiştir. Devletler vatandaşlarını nitelikli bireyler haline getirerek kalkınmak ve büyümek istemektedirler. Dolayısıyla eğitim faaliyetlerine büyük bütçeler ayırmaktadırlar. Bu nedenle eğitim alanı kamu politikalarında önemli bir yer işgal etmektedir. Sanayi Devrimi sonrasında kitlesel üretim sürecine giren dünyada bu üretimi gerçekleştirmek için tüm bireylere belli bir eğitim verilmesi gerekmektedir. Bu eğitim ancak kitlesel bir eğitim ile gerçekleştirilebilir. Bu nedenle pek çok ülkede belli bir eğitim düzeyine kadar okula devam etme zorunluluğu vardır. Ancak son yıllarda yaşanan dönüşümler eğitim faaliyetinin bir başlangıç veya sonunun olmadığını göstermiştir. Değişen ve gelişen dünyada bireylerin hayat boyu öğrenme alışkanlığı edinmesi gerektiği anlaşılmıştır. Çok hızlı gelişen teknoloji nedeni ile kazanılan niteliklerin birkaç yıl sonra bir önemi kalmayabilmektedir. Bu nedenle bireylerin eğitimlerinin süreklilik kazanması bir zorunluluktur. Ancak özellikle belli bir yaşta sonra bireylere geleneksel eğitim yöntemleri ile eğitim

verilmesi oldukça güçtür. Bunun nedeni çalışma hayatına giren bireylerin zamanlarının büyük kısmını işlerine ayırmalarıdır. Bu noktada devletler eğitim politikalarında uzaktan eğitimden yararlanarak vatandaşlarını hayat boyu öğrenme süreçlerine dahil edebilmektedir. Tüm bunların yanı sıra uzaktan eğitim geleneksel eğitimin önemli bir destekleyicisidir. Öğrencilerin bireysel çalışmalarında uzaktan eğitimin faydalarından yararlanmasıyla gelişmelerini hızlandırmaları mümkündür. Tüm bu avantajlar uzaktan eğitim faaliyetlerinin önemini ortaya koymaktadır.

Mektup yolu ile başlayan uzaktan eğitim daha sonra radyo ve televizyon teknolojilerinin gelişmesi ile yeni bir boyut kazanmıştır. Eğitici radyo ve TV yayınları yapılmasının faydalarının görülmesi üzerine Açık Öğretim Kurumları kurulmaya başlamıştır. Bu alanda İngiltere ve Amerika Birleşik Devletleri'ndeki gelişmeler öncü sayılmaktadır. Bilgi ve iletişim teknolojilerinin gelişmesiyle uzaktan eğitimde tele-konferans yöntemleri uygulanmaya başlamıştır. Son olarak ise internet ve bilgisayarın hayatlarımıza girmesi ile uzaktan eğitim faaliyetleri oldukça yaygınlaşmıştır. Teknolojinin ucuzlayıp yaygınlaşmasıyla paralel şekilde uzaktan eğitim faaliyetleri de ucuzlayıp yaygınlaşmaktadır. 2019 sonundan itibaren dünyada yaşanan pandemi süreci uzaktan eğitim faaliyetleri üzerinde önemli sonuçlar doğurmuştur. Bu dönemde birçok ülke yüz yüze eğitim faaliyetlerine ara vermek zorunda kalmıştır. Bu ülkeler içerisinde uzaktan eğitim altyapısı yeterli olanlar eğitim faaliyetlerine devam edebilmiştir. Uzaktan eğitim altyapısı güçlü olmayan ülkeler ise pek çok sorun yaşamıştır. Pandemi sonrası dünyada pandemi döneminde yaygın kullanılan teknolojilerden kullanılmaya devam edilecek gibi gözükten uzaktan eğitim bu nedenle pek çok çalışmaya konu olmuştur. Bu nedenle uzaktan eğitime gerekli önemin verilmesi gerekmektedir.

Türkiye'de Cumhuriyetin ilk yıllarında çeşitli raporlarda uzaktan eğitim ile ilgili açıklamalara rastlamak mümkündür. Ancak modern anlamda uzaktan eğitim faaliyetlerinin gerçekleşmesi 1980 sonrası üniversiteler bünyesinde kurulan açıköğretim fakülteleri ile olmuştur. Bu bağlamda Anadolu Üniversitesi Türkiye'de modern uzaktan eğitimin ilk örneğidir. Daha sonra pek çok üniversitede uzaktan eğitim faaliyetleri yaygınlaşmıştır. Günümüzde Anadolu Üniversitesi, İstanbul Üniversitesi ve Atatürk Üniversitesi geniş uzaktan eğitim faaliyetleri ile dikkat çekmektedir. Türkiye'de uzaktan eğitim ile ilgili mevzuat düzenlemeleri genel olarak üniversitelerin bünyelerinde çıkarılan yönetmelikler ile düzenlenmektedir. Aktörlere bakıldığında ise MEB, YÖK, Üniversiteler ve Özel Kurumların öne çıktığı görülmektedir.

Çalışmada Türkiye'de uzaktan eğitim alanına dair güçlü yanlar, sorun alanları ve çözüm önerileri de sıralanmıştır. Bu bağlamda uzaktan eğitim geleceğin önemli konularındandır. Alanla ilgili çalışma sayısının artması ve alana olan ilginin yükselmesi ümit edilmektedir.

---

**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 çalışmanın yazarlarına aittir.

**Yazar Katkıları:** Hasan Alpay Karasoy, Emin Cebe ve Pelin Babaoğlu 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:** Hasan Alpay Karasoy, Emin Cebe and Pelin Babaoğlu 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**

- Akarsu, M. (2019). *Türkiye’de Açık Öğretim Fakültelerinde Kalite Kültürü: İstanbul Üniversitesi Açık ve Uzaktan Eğitim Fakültesi(AUZEK) Örneği*, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, İstanbul.
- Akdemir, Ö. (2011). “Yükseköğretimimizde Uzaktan Eğitim” , *Yükseköğretim ve Bilim Dergisi*, 1(2), s. 69-71.
- Aksoy, H. (2018). *Uzaktan Eğitimde Merkezi Sınav Sistemi*, Kırıkkale Üniversitesi Fen Bilimleri Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Kırıkkale.
- Akyürek, M. İ. (2020). “Uzaktan Eğitim: Bir Alanyazın Taraması”, *Medeniyet Araştırmaları Dergisi*, 4(1), s. 1-9.
- Altınsoy, F. (2019). *Uzaktan Eğitim Öğrencilerinin Başarılarının Yapay Zekâ Teknikleri ile Tahmini*, Süleyman Demirel Üniversitesi Fen Bilimleri Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Isparta.
- Ataş, B. (2017). Açık ve Uzaktan Yükseköğretimde Öğrenme Ortamlarında Videonun Kullanımı: Türkiye’deki Uygulamalara İlişkin Değerlendirmeler, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Eskişehir.
- Avcı, A. (2021). “Pandemi (Covid-19) Üniversite Öğrencileri ve Uzaktan Eğitim Deneyimi”, *HABİTUS Toplum Bilim Dergisi*, (2), s. 71-84.
- Avcı, F., Akdeniz, E. C. (2020). “Koronavirüs (Covid-19) Salgın ve Uzaktan Eğitim Sürecinde Karşılaşılan Sorunlar Konusunda Öğretmenlerin Değerlendirmeleri” , *Uluslararası Sosyal Bilimler ve Eğitim Dergisi*, 3(4), s. 117-154.
- Babaoğlu, C. ve Kulaç, O.(2021). “The Covid-19 pandemic’s effect on digitalization and internationalization policies of Turkish higher education” , *ç. Higher Education Policies for Developing Digital Skills to Respond to the Covid-19 Crisis: European and Global Perspectives* (Ed. Nina Tomažević, Dejan Ravšelj, Aleksander Aristovnik), Belçum; European Liberal Forum asbl.
- Babaoğlu, C., Öktem, M. K. (2017) “E-Learning in Higher Education System: An Analysis of Turkish Case” , in. *Open and Distance Learning for Sustainable Growth in Emerging Nations* (Edt: Umesh Chandra Pandey ve Verlaxmi Indrakanti), Hersey/PA:IGI, s. 1-17.
- Bal, Z. E. (2017). *Yükseköğretimde Dijitalleşmenin Uzaktan Öğrenime Etkileri*, İstanbul Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doktora Tezi, İstanbul.
- Balıkçioğlu, N., Çınar, D., & Nilüfer, N. (2019). “Üniversite Öğrencilerinin Uzaktan Eğitim Derslerindeki Memnuniyet Araştırması: Aşık Veysel Meslek Yüksekokulu Örneği”. *C.Ü. İktisadi ve İdari Bilimler Dergisi*, 20 (1), s. 462-473.
- Best Online Masters in the USA (2021). <https://www.distancelearningportal.com/articles/1307/10-us-universities-offering-top-distance-education.html> . Erişim Tarihi: 30.05.2021.

- Bozkurt, A. (2017). “Türkiye’de Uzaktan Eğitimin Dünü, Bugünü ve Yarını”. *Anadolu Üniversitesi AUAd*, 3(2), s. 85-124.
- Can, E. (2020). “Coronavirüs (Covid-19) Pandemisi ve Pedagojik Yansımaları: Türkiye’de Açık ve Uzaktan Eğitim Uygulamaları” , *Anadolu Üniversitesi AUAd*, 6(2), s. 11-53.
- Çivril, H., Aruğaslan, E., & Özaydın Özkara, B. (2018). “Uzaktan Eğitim Öğrencilerinin Uzaktan Eğitime Yönelik Algıları: Bir Metafor Analizi” , *Eğitim Teknolojisi Kuram Ve Uygulama*, 8(1), s.39-59.
- Demir, E. (2014). “Uzaktan Eğitime Genel Bir Bakış” , *Dumlupınar Üniversitesi Sosyal Bilimler Dergisi*, (39), s. 203-212.
- Düzenli, H. (2019). *Açık ve Uzaktan Öğrenme Bağlamında Verilen Bir Çevrimiçi Dersin Etkinlik Kuramı Çerçevesinde İncelenmesi*, Eskişehir Anadolu Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Eskişehir.
- Enfiyeci, T. (2019). *Çevrimiçi Ortamlarda Lisansüstü Uzaktan Eğitim Öğrencilerinin Topluluk Hissi, Motivasyon ve Akademik Başarısı Arasındaki İlişki: Ahmet Yesevi Üniversitesi Örneği, Gazi Üniversitesi Eğitim Bilimleri Enstitüsü Yayınlanmamış Yüksek Lisans Tezi*. Ankara.
- Ergenç, İ. E. (2021). *Çevrimiçi (Online) Uzaktan Eğitim Hizmetlerinde E-Hizmet Kalitesi Boyutları; Bir Kalite Fonksiyon Göçerimi ve AHP Uygulaması*, İzmir Katip Çelebi Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doktora Tezi, İzmir.
- Etlioğlu, M. (2019). *E-Öğrenmede Öğrenci Tutumu ve Akademik Başarı Arasındaki İlişkide Öğrenci Duyuşsal Özelliklerinin Aracılık Rolünün İncelenmesi*, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doktora Tezi, Konya.
- Garrison, D. R. (2003). “E-Learning in the 21st Century: A Frameworkfor Research and Practice” , Londra: Routhledge.
- İşcan, A. (2020). *Uzaktan Lisansüstü Eğitimde Sınav Otomasyonlarının Geliştirilmesi: Anadolu Üniversitesi Örneği*, Eskişehir Anadolu Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Eskişehir.
- Kaya, F. (2020). *Yükseköğretimde Atatürk İlkeleri ve İnkılâp Tarihi Dersinin Uzaktan Eğitim Yoluyla Verilmesine İlişkin Öğrenci Görüşleri (Kastamonu Üniversitesi Örneği)*, Kastamonu Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Yüksek Lisans Tezi, Kastamonu.
- Koç, E. S. (2021). “Nasıl Bir Uzaktan Eğitim? 1 Yılın Sonunda Yapılan Çalışmaların Değerlendirilmesi” , *International Anatolia Academic Online Journal Social Sciences Journal*, 7(2), s.13-26.
- Miller, C. (2021). *Online Education Statistics*. <https://educationdata.org/online-education-statistics> . Erişim Tarihi: 20.05.2021.

- Millî Eğitim Bakanlığı(2020). *Millî Eğitim İstatistikleri Örgün Eğitim 2019-2020*, [http://sgb.meb.gov.tr/www/icerik\\_goruntule.php?KNO=396](http://sgb.meb.gov.tr/www/icerik_goruntule.php?KNO=396) , Erişim Tarihi: 12.06.2021.
- Office Of Elementary & Secondary Education (2021). American Rescue Plan. <https://oese.ed.gov/offices/american-rescue-plan/> , Erişim Tarihi: 30.05.2021.
- Özbay, Ö. (2015). "Dünyada ve Türkiye'de Uzaktan Eğitimin Güncel Durumu" , *INESJOURNAL*, 2(5), s. 376-394.
- Strateji ve Bütçe Başkanlığı (2019). *On Birinci Kalkınma Planı*, <https://www.sbb.gov.tr/wp-content/uploads/2019/07/OnbirinciKalkinmaPlani.pdf> Erişim Tarihi: 11. 06. 2021
- Şen, O. (2021). *Uzaktan Eğitim Yoluyla Gerçekleştirilen Yönetici Eğitimi Faaliyetlerinin Yayılım Süreçlerinin İncelenmesi*, Eskişehir Osmangazi Üniversitesi Sosyal Bilimler Enstitüsü Yayınlanmamış Doktora Tezi. Eskişehir.
- Türk Eğitim Derneği (2020). *Covid-19 Sürecinde Eğitim Uzaktan Öğrenme, Sorunlar ve Çözüm Önerileri*, Ankara: TEDEM.
- Türkiye İstatistik Kurumu (2020). *Hanehalkı Bilişim Teknolojileri (BT) Kullanım Araştırması, 2020*, [https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-\(-BT\)-Kullanim-Arastirmasi-2020-33679](https://data.tuik.gov.tr/Bulten/Index?p=Hanehalki-Bilisim-Teknolojileri-(-BT)-Kullanim-Arastirmasi-2020-33679) , Erişim Tarihi: 11.06.2021.
- Yamamoto, T. G., & Altun, D. (2020). "Coronavirüs Ve Çevrimiçi (Online) Eğitimin Önlenebilir Yükselişi" , *Üniversite Araştırmaları Dergisi*, 3(1), s. 25-34.
- Yaman, B. (2021). "Covid-19 Pandemisi Sürecinde Türkiye ve Çin'de Uzaktan Eğitim Süreç ve Uygulamalarının İncelenmesi" , *OPUS*, 17(Pandemi Özel Sayısı), s. 3297-3309.
- Yükseköğretim Kurulu(1996). *Türk Yükseköğretiminin 1-Bugünkü Durumu, Sorunları, Çözüm Önerileri 2-Türk Cumhuriyetleri ile Türk ve Akarba Topluluklarından Gelen Öğrencilerin Sorunları, Çözüm Önerileri 3-2547 Sayılı Yükseköğretim Kurumu Kanununda Değişiklik Yapılması Hakkında Kanun Taslağı Önerisi*, <https://www.yok.gov.tr/Documents/Yayinlar/Yayinlarimiz/turk-yuksekogretiminin-1-2-3.pdf> , Erişim Tarihi: 12.06.2021.
- Yükseköğretim Kurulu(2007). *Türkiye'nin Yükseköğretim Stratejisi*, <https://www.yok.gov.tr/Documents/Yayinlar/Yayinlarimiz/Turkiyenin-yuksekogretim-stratejisi.pdf> , Erişim Tarihi: 12.06.2021.
- Yükseköğretim Kurulu(2020). *Küresel Salgında Yeni Normalleşme Süreci*, <https://www.yok.gov.tr/Documents/Yayinlar/Yayinlarimiz/2020/kuresel-salginda-yeni-normallesme-sureci-2020.pdf> , Erişim Tarihi: 12.06.2021.
- Yükseköğretim Kurulu(2020). *Yükseköğretim Bilgi Yönetim Sistemi*, <https://istatistik.yok.gov.tr/> , Erişim Tarihi: 12.06.2021.

# EĞİTİMDE TEKNOLOJİNİN KULLANIMI

## Use of Technology in Education

\* Umay Tuba CURACI

### Özet

Teknolojinin kamu yönetimi dönüşümünde itici güç olduğu yadsınamaz bir gerçek olarak hep var olmaktadır. Ülkeler teknolojiye uyum sağlamak için kendi dinamikleri doğrultusunda çalışmalar yapmaktadır. Ancak, Covid 19 Pandemisi gibi bir kriz tüm dünyada ülkelerin teknoloji potansiyellerini tespit etmeleri bakımından önemli bir etken olurken bir yandan da sosyal mesafe zorunluluğu teknolojinin kullanımını gerekli hale getirmiştir. Özellikle eğitim alanında bu durum daha etkili bir şekilde hissedilmiştir. Eğitim ve teknoloji eski dönemlerden beri birbirine yakın iki kavram olarak görülmektedir. Sadece bahsi geçen kriz dönemlerinde değil yaşamın ilk yıllarından itibaren insan gelişiminde önemli rol oynamıştır. Globalleşme ve öncelikle internet olmak üzere, teknolojilerin gelişmesiyle birlikte farklı bir boyuta ulaşmış ve yeni teknolojilerin eğitim yöntemlerini değiştirme süreci ile birlikte yeni boyutlara ulaşmaya devam etmektedir. Bu kapsamda, alanyazınında eğitimde teknolojinin geleceğine ilişkin birçok öngörü de yer almaktadır. Bu makalede teknolojinin eğitimde kullanılmasına ilişkin mevcut durum değerlendirilerek geleceğe dair öngörlere yer verilmiştir.

### Abstract

It is undeniable that technology is the driving force in the transformation of public administration. Countries are working in line with their dynamics to adapt to technology. However, while a crisis such as the Covid 19 Pandemic is an effective factor for countries all over the world to identify their technology potential, terms of the necessity of social distance have made the use of technology necessary. This situation has been felt more effectively in the education field. Since ancient times, education and technology have been seen as two closely related concepts. It has played an important role in human development not only during the mentioned crisis periods but also from the first years of life. With globalization and the development of technologies, primarily the internet, it has reached a different dimension and the process of changing the education methods of new technologies continues to reach new dimensions. There are many predictions of technology in education in the literature in this context. In this article, a framework for the use of technology in education is drawn and predictions for the future are given.

**Anahtar Kelimeler:** Eğitim, Teknoloji, Eğitim Teknolojileri, Eğitimde Dönüşüm

**Keywords:** Education, Technology, Educational Technologies, Transformation in Education

\* Umay Tuba CURACI, Yüksek Lisans Öğrencisi, Hacettepe Üniversitesi Sosyal Bilimler Enstitüsü, Siyaset Bilimi ve Kamu Yönetimi Anabilim Dalı, Kamu Yönetimi Tezli Yüksek Lisans Programı, umaycuraci@hacettepe.edu.tr, ORCID: 0000-0003-3545-0346

## 1. GİRİŞ

Türk Dil Kurumu'nun tanımına göre teknoloji, "İnsanın maddi çevresini denetlemek ve değiştirmek amacıyla geliştirdiği araç gereçlerle bunlara ilişkin bilgilerin tümü." olarak tanımlanmıştır. Eğitim ise "Çocukların ve gençlerin toplum yaşayışında yerlerini almaları için gerekli bilgi, beceri ve anlayışları elde etmelerine, kişiliklerini geliştirmelerine okul içinde veya dışında, doğrudan veya dolaylı yardım etme, terbiye" olarak tanımlanmaktadır. Eğitim için demografik olarak dar bir tanım yapılmış olsa da teknoloji ile eğitimin bir araya gelmesi kaçınılmaz olarak görünmektedir. Bu anlamda, her iki kavram literatürde sık sık yan yana gelmektedir. Kimi araştırmacılar tarafından "eğitim teknolojisi" olarak adlandırılırken, kimileri ise "öğretim teknolojileri" kavramının kullanılması tercih edilmiştir (Karademirci, 2010).

Eğitim teknolojisi kavram olarak farklı isimler aldığı gibi araştırmacıların farklı bakış açılarından kaynaklanan farklı tanımlara da sahip olmuştur. Bu tanımlar, "Çevre ayarlanmasında belli öğrenmeleri kılavuzlamak için belli öğretme yöntemleri kullanırken, öğretmenin dersinin gereğince belli eğitim araç ve gereçlerinden yararlanma işlemi" gibi klasik bir yaklaşımla yapılabilmektedir. Diğer yandan "Davranış bilimlerinin iletişim ve öğrenmeyle ilgili verilerine dayalı olarak eğitimle ilgili ulaşılabılır insan gücü ve insan gücü dışı kaynakları akıllıca ve ustaca kullanıp, sonuçları değerlendirerek, bireyleri eğitimin özel amaçlarına ulaştırma yollarını inceleyen bilim dalı" gibi disiplinler arası bir yaklaşım doğrultusunda tanımlar da bulunmaktadır (Sürek, 2018).

Kronolojik olarak değerlendirildiğinde, eğitim teknolojisi 18. yüzyılın başlarında araç olarak görülmüştür. 1960 yılından sonra bir yöntem olarak belirlenmiş; "tasarım ve öğrenme" olarak tanımlanmıştır. Bu dönemde davranışçı ekolün etkisi altında kaldığı, 1990'lı yıllardan sonra ise davranışçı yaklaşımın dışındaki farklı öğrenme kuramları ve bilgisayar teknolojilerinde meydana gelen ilerlemelerden etkilendiği görülmüştür (Karademirci, 2010).

Eğitim, öğrenmeye odaklı olarak herkesin öncelikle yaşantısını sürdürebilmesi için temel beceriler kazandıran bir süreçtir. Okul öncesinde dönemsel özelliklere göre yöntem ve teknikler farklılıklar gösterse de eğitim alanında kullanılan teknoloji günün şartlarına göre değişmektedir. Yaşamın ilk dönemlerinde itibaren alınan temel eğitimde yürümeyi öğrenmek için kullanılan yürüteçler de teknolojinin bir ürünüdür, ilkokulda kullanılan abaküsler de. Dolayısıyla teknoloji, bulunduğu zamanın şartları kapsamında, eğitimde her zaman önemli bir yerde bulunmaktadır. Bu çalışmada, geçmişten günümüze teknolojinin eğitimde kullanımı konusu açıklanmaya çalışılacak olup gelecekte hangi noktalara ulaşılabileceğine dair öngörüler yapılacaktır.

## 2. EĞİTİM TEKNOLOJİSİNİN TARİHSEL GELİŞİMİ

Yazılı, sözlü iletişim bakımından bulunduğu dönemin şartlarına göre teknolojinin eğitim alanında kullanımı eski çağlara dayanmaktadır. İlk bulunduğu zamanlar için teknolojik anlamda büyük bir adım olan radyo 1900'lerin ilk yarısında eğitimde kullanılmaya başlanmıştır. 1900'lerin ikinci yarısından itibaren ise televizyon ve video gibi radyoyu takip eden icatlar açık öğretim alanında popülerlik kazanmıştır (Bates, 2015).

Ülkelerin gelişmişlik düzeylerinin seviyesi, bilişim teknolojilerinin toplumda yaygın ve kullanımıyla ölçülebilmektedir. Dolayısıyla, ülkeler de dünyadaki gelişmelere uyum sağlayabilmek adına teknoloji ile eğitimi entegre etmek için proje ve çalışmalarını yoğunlaştırmışlardır. Dünya'da internet hızının geliştirilmesi, internete bağlı teknolojilerde ilerleme sağlanması, bilgisayar kullanımının yaygınlaşmasıyla birlikte 1990'ların ikinci yarısından itibaren teknoloji yön değiştirerek, eğitim sektöründe de aktif bir şekilde kullanılmaya başlanmıştır. 2000'li yıllardan itibaren pek çok ülkede de eğitimde dijitalleşme hız kazanmıştır (Genç, 2019).

Eğitimin internet teknolojileri ile buluşması, televizyon ile tek taraflı verilen açık öğretimden, interaktif uzaktan eğitime dönüşümü de sağlamıştır. Bu dönüşümden en çok etkilenen düzey ise yüksek öğretim olmuştur. Uluslararası boyut kazanan uzaktan eğitim, özellikle yüksek öğretimde yapısal değişikliklere neden olmuş, yaklaşım ve uygulamalar anlamında yeniden yapılanmalar meydana gelmiştir (Kapucu Kocatürk ve Uşun, 2020).

Türkiye'de ise eğitimde teknolojinin kullanımına ilişkin çalışmaların, Cumhuriyetin başlangıç dönemlerinden itibaren yapıldığı görülmektedir. Ancak, teknolojinin kapsamlı kullanımı 1970'li yılların başlarından itibaren başlamıştır. Milli eğitim mevzuatında düzenlemeler yapılmıştır. "1973 yılında yürürlüğe giren 1739 sayılı Milli Eğitim Temel Kanunu"nun 13'üncü maddesinde "Her derece ve türdeki ders programları ve eğitim metotlarıyla ders araç ve gereçleri bilimsel ve teknolojik esaslara ve yeniliklere, çevre ve ülke ihtiyaçlarına göre sürekli olarak geliştirilir. Eğitimde verimliliğin artırılması ve sürekli olarak gelişme ve yenileşmenin sağlanması bilimsel araştırma ve değerlendirmelere dayalı olarak yapılır." hükmü yer almıştır. Kalkınma Planlarında eğitimde bilim ve teknolojiye uyum sağlanmasına ilişkin hedefler yer almıştır. Örneğin, 6'ncı ve 7'nci Beş Yıllık Kalkınma Planlarında yaşanan bilimsel ve teknolojik gelişmeler doğrultusunda öğretim programlarında güncelleme yapılması gerekliliği vurgulanmıştır. (Genç, 2019).

Tüm Dünyada "dijital dönüşüm"ün hızlandığı 21. yüzyılla beraber Türkiye'de de eğitimde dünya ile benzer teknolojiler kullanılmaya başlanmıştır. Türkiye'de de teknolojinin eğitim alanında kullanımına ivme kazandırmıştır. "10'uncu Beş Yıllık Kalkınma Planı Eğitimde Kalitenin Artırılması Özel İhtisas Komisyon Raporu"nda eğitimde bilişim teknolojilerinin ağırlık kazanması ve bu kapsamda eğitim kurumlarının altyapı düzenlemelerinin yapılması konusunda çalışmaların devam ettiği belirtilmiştir. Raporda, "Bilişim teknolojileri sınıflarının kurulması yoluyla eğitimin kalitesini arttırmak" amacıyla

“Avrupa Yatırım Bankası” kredisi ile 2006-2011 döneminde gerçekleştirilen “Eğitim Çerçevesi II.Faz” projesinden bahsedilmiştir. Tüm bu çalışmalarla birlikte, “eğitimde fırsat eşitliğini sağlamak” ve “okullardaki teknolojiyi iyileştirmek” için hazırlanan “Fırsatları Artırma Teknolojiyi İyileştirme Hareketi (FATİH) Projesi”nin, 2010 yılında uygulanmaya koyulduğu; bu kapsamda “ilk ve ortaöğretimde tüm okulların dersliğine dizüstü bilgisayar, projeksiyon, internet bağlantısı ve akıllı tahtanın donatılması”nın hedeflendiği belirtilmiştir. Ayrıca, söz konusu rapora göre “09.2011 tarihinde yayımlanan 652 sayılı Kanun Hükmünde Kararname ile birlikte MEB merkez teşkilatının yapısı önemli ölçüde değişmiştir. Bu çerçevede, merkez teşkilatı, daha etkin ve etkili çalışabilmesi için küçültülmüştür. Ayrıca, eğitim niteliğini artırma potansiyeli taşıyan kimi yeni birimler kurulmuştur.” (Kalkınma Bakanlığı, 2014).

Türkiye’de Cumhurbaşkanlığı Sistemine geçilmesiyle beraber “10/7/2018 tarihli ve 30474 sayılı Resmi Gazete’de yayımlanan 1 sayılı Cumhurbaşkanlığı Kararnamesinin 311. maddesi”nde Milli Eğitim Bakanlığının “Yenilik ve Eğitim Teknolojileri Genel Müdürlüğü”nün görevleri şu şekilde belirlenmiştir:

“MADDE 311 - (1) Yenilik ve Eğitim Teknolojileri Genel Müdürlüğünün görev ve yetkileri şunlardır:

- a. Eğitim ve öğretimin teknoloji ile desteklenmesine yönelik işleri yürütmek,
- b. Eğitim ve öğretim faaliyetlerinde bilişim teknolojileri ile bilişim ürünlerinin kullanılmasına yönelik çalışmalar yürütmek,
- c. Yaygın eğitim ve öğretime yönelik olarak bilgi ve iletişim teknolojilerine dayalı program, film ve benzeri yayınları hazırlamak veya hazırlatmak, yayınlamak veya yayınlattmak,
- ç. Eğitim ve öğretimde uygulanan yeni teknoloji ve gelişmeleri izlemek ve değerlendirmek,
- d. Eğitim ve öğretimde teknolojik imkânların tüm yurt çapında etkin ve yaygın biçimde kullanılmasını ve her öğrencinin bilgi teknolojilerinden yararlanmasını sağlamak,
- e. Bakan tarafından verilen diğer görevleri yapmak.”(Cumhurbaşkanlığı, 2018)

Bu kapsamda, milli eğitim kapsamında, Cumhurbaşkanlığı Sisteminde eğitimde dijitalleşme adımlarının hızla atılacağı da öngörülebilmektedir.

Koronavirüs (Kovid-19) salgını ile birlikte sınıf eğitimine ara verilme zorunluluğu ortaya çıkmıştır. Virüs tedbirlerinden dolayı bu ara dönemde, eğitimin kesintisiz ve “sürdürülebilir” olması gerekliliği kapsamında yürütülen uzaktan eğitim faaliyetleri doğrultusunda “mevzuat, altyapı insan kaynakları, içerik ve uygulama” gibi temel alanlarda İlk ve orta öğretimle beraber yükseköğretim kurumlarını da kapsayacak çalışmalar yapılmıştır (Telli ve Altun, 2020).

Bu kapsamda, Yüksek Öğretim Kurulu “bahar dönemiyle sınırlı olmak kaydıyla, tüm alanlarda uzaktan öğretim yapma imkânı sağlanmıştır.” Ayrıca, uzaktan eğitime ilişkin olarak gerekli mevzuat ve yapısal uyum çalışmaları yapmıştır (Telli ve Altun, 2020). İlk ve orta dereceli eğitimde ise uzaktan eğitimi sağlamak amacıyla “Milli Eğitim Bakanlığı” tarafından hazırlanan “Eğitim Bilişim Ağı (EBA)” aktif olarak kullanılmaya başlanmıştır. Milli Eğitim Bakanı tarafından “9 ve 12. sınıflar” yine aynı Ağ üzerinden canlı sınıf eğitimlerinin yapılacağı belirtilmiştir. Ancak, diğer düzeylerdeki öğrenciler için farklı platformlar üzerinden yapılan uzaktan eğitimlerde veri güvenliği riskine dikkat çekilmiştir (MEB, 2020). Ulusal boyutta tüm ihtiyaç duyulan tüm alanlarla birlikte eğitimde de veri güvenliği riski göz önüne alınarak, yerli video konferans yazılımları üretilmeye başlanmıştır.

“Anadolu Ajansı”nın bir haberine göre “Türk savunma sanayisinin yazılım tabanlı çözüm merkezlerinden **HAVELSAN**, yeni tip koronavirüs (Kovid-19) salgınına karşı alınan tedbirlerle birlikte artan ihtiyacı dikkate alarak, yerli ve güvenli bir video konferans ürünü” geliştirmiştir (AnadoluAjansı, 2020). “HAVELSAN Diyalog” ismini almış olan bu yazılım HAVELSAN’ın web sayfasında şu şekilde tanımlanmıştır: “kurulumu ve yönetimi kolay, güvenli, yüksek kalitede görüntülü ve sesli görüşme imkanı sağlayan yerli bir video konferans çözümüdür.” (HAVELSAN, 2010)

### 3. EĞİTİMDE TEKNOLOJİNİN GELECEĞİ

“Eğitimde teknoloji kullanımı, öğrenciye görsel, işitsel, dokunsal tüm algılarını kullanabilme imkanı sağlamaktadır bu da öğrendiklerini daha kalıcı hale getirmektedir. Yapılan araştırmalar, zaman kavramının sabit tutulduğu şekilde, insanlar okuduklarının %10’unu, duyduklarının %20’sini, gördüklerinin de %30’unu hatırlarken aynı zamanda hem görüp hem duyduklarının %50’sini hatırlamaktadır. Aynı zamanda söylediklerinin %90’ını hatırlamaktadırlar” (Metin, 2018). Yani, Öğrenmenin kalıcı ve etkili olabilmesinin, beş duyardan ne kadarını kullandığıyla orantılı olduğu görülmektedir. Eğitimde çoklu zeka kuramlarının, öğrenme, gelişim ve başarı üzerinde olumlu etkilerinin fark edilmesi, çoklu uyaranlarla eğitimin verimliliğinin yüksekliğine dair bulgular elde edilmesi, teknolojinin yönünü bu alanlara çevirmiştir.

Günümüz teknolojileri olan “Sanal Gerçeklik”, Simülasyonlar” ve “Artırılmış Gerçeklik”, çoklu algıyı harekete geçirerek, duyuların daha verimli kullanımını sağlamaktadır. Dolayısıyla, uygulama eğitimlerinde mekânsal ve zamansal maliyetleri yüksek olan “pilotluk eğitimleri”, “mühendislik uygulama eğitimleri”, “tıp eğitimi” gibi alanlarda bu teknolojilerin kullanılması daha az maliyetli, zaman ve mekan kısıtının olmadığı, etkili öğrenmeyi teşvik eden bir eğitim ortamının oluşturulmasında fayda sağlayabilmektedir (Arkan, 2018). Ayrıca, eğitim risklerin düşürülmesi de ayrı bir fayda olarak sayılabilmektedir. Dolayısıyla eğitimde teknoloji kullanımı, eğitim teknolojisi veya farklı teknolojilerin eğitime uyarlanması gibi konulara ilişkin çalışmaların geniş bir alanda yapılabilecek özelliğe sahip görünmektedir.



Medyada çıkan haberler ve yazılar göz önüne alındığında, eğitimde kullanılacak teknolojilerin, genel itibarıyla “artırılmış gerçeklikle sınıf ortamlarının oluşturulması”, “interaktif elektronik ortamları” mümkün hale getiren teknolojilerin kullanılması, “çoklu dokunmatik kontrole sahip yüzeyler” in geliştirilmesi, “sanal gerçeklik gözlükleri”nin eğitim ortamlarına taşınmasının hızlanması gibi öngörüler mevcuttur (Kaplanseren, 2013).

Bunların yanı sıra eğitimin ev ortamında sanal sınıflarda yapılmasının yaygınlaşması, okul ortamında yapılan derslerin teknolojik olarak kişiselleştirilmiş sınıflarda yapılması, “bulut bilişim”in kitapların yerini alması da tahminler arasında yer almaktadır. Ayrıca, gelişen teknolojinin meslekleri de değiştireceğine, “robot tamircisi, drone pilotu, yapay zeka psikoloğu vs.” gibi mesleklerin ortaya çıkabileceğine dair fikirler bulunmaktadır. Bu mesleklerin ortaya çıkmasıyla beraber, eğitimin de bu yönde değişeceği görüşleri de dikkat çekmektedir (Kurt, 2018).

#### 4. SONUÇ

Fütürist yazar “Alvin Toffler”, eğitimin değişimiyle ilgili “Üçüncü Dalga Geliyor” kitabında “Bugün İkinci Dalga eğitim modelleri, her yerde sorgulanıyor. Üçüncü Dalga, eğitimin mutlaka sınıfta yapılması gerektiği yönündeki İkinci Dalga görüşüne meydan okuyor. Bugün, öğrenimi çalışmayla, politik mücadeleyle, toplum hizmetiyle ve hatta oyunla birleştirmemiz gerekiyor. Eğitim hakkındaki tüm geleneksel varsayımlarımız gerek zengin ve gerekse yoksul ülkelerde yeniden incelenmek zorunda.” sözleriyle sınıf eğitiminin gelecekte tercih edilmeyecek bir yöntem olacağına dair iddialarını dile getirmiştir. Dolayısıyla, gelecek planlarında, okul binalarının geniş yer alması çok da anlamlı bulunmamaktadır. Eğitimin, teknolojinin de etkisiyle daha küresel bir anlam kazanılacağı düşünülmektedir. Teknoloji ile birlikte mekan ve zaman kısıtının ortadan kalkması, bir anda birden çok yüksek öğretim kurumunda eğitim görme imkanını ortaya çıkarması mümkündür. Tahminlerin gerçekleşmemesi olası olsa da bugünden farklı olacağına kesin gözüyle bakılmaktadır (Şirazduvarı, 2017). Özellikle etkilerinin bir süre de hissedileceği kesin olan Covid-19 Pandemisi teknoloji yardımıyla eğitimde zaman ve mekan zorunluluğunun sorgulanmasını sağlamıştır. Teknolojinin eğitim üzerindeki etkileri sadece zaman ve mekan yönünden değil; aynı zamanda eğitimin maliyeti ve niteliği açısından da değerlendirilmelidir. Teknoloji sayesinde erişilebilen kaynakların sayısındaki artış eğitimin kalitesini artırmakta ve eğitimin içeriğini yerel-bölgesel düzeyden çıkarıp küresel boyuta taşımaktadır. Eğitimde teknoloji kullanımı için yapılan altyapı yatırımlarının artması coğrafi olarak ülkenin her noktasındaki öğrenciler için eşit imkanları sunmaktadır. Ancak bireyler arasındaki gelir farklılıkları, sosyal ve kültürel eşitsizlikler, insan kaynağının henüz teknoloji okuryazarlığında yeterli seviyeye ulaşmamış olması eğitimde teknoloji kullanımından alınacak verimi düşüren ve çözülmesi gereken problemler olarak öne çıkmaktadır. Gerekli kamu politikalarının oluşturulması, yatırımların yapılması, ilgili kamu kurumları ve özel sektör kuruluşlarının koordine edilmesi eğitimde teknolojinin kullanılmasını yaygınlaştırmak ve alınacak verimi maksimum düzeye çıkarmak için atılması gereken öncelikli adımlardır.

---

**Etik Beyanı:** Bu alıřmanın tm hazırlanma srelerinde etik kurallara uyulduđunu yazar beyan eder. Aksi bir durumu tespiti halinde Kamu Ynetimi ve Teknoloji Dergisinin hibir sorumluluđu olmayıp, tm sorumluluk alıřmanın yazarlarına aittir.

**Yazar Katkıları:** Umay Tuba Curacı alıřmanın tamamında tek bařına katkı sunmuřtur.

**ıkar Beyanı:** Yazar ya da herhangi bir kurum/ kuruluř arasında ıkar atıřması yoktur.

**Teřekkr:** Yayın srecinde katkısı olan hakemlere teřekkr ederim.

**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:** Umay Tuba Curacı has contributed to all parts and stages of the study

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

**Acknowledgement:** I would like to thank the referees who contributed to the publication process.

**KAYNAKÇA**

- AnadoluAjansı. (2020). HAVELSAN Türkiye'yi yerli yazılımla konuşturmaya hazırlanıyor. Erişim Adresi: <https://www.aa.com.tr/tr/bilim-teknoloji/havel-san-turkiyeyi-yerli-yazilimla-konusturmaya-hazirlaniyor/1828037> (Erişim Tarihi: 07.06.2020)
- Arkan, A. (2018). Teknoloji, Eğitim ve Gelecek. Siyaset, Ekonomi ve Toplum Araştırmaları Vakfı (SETA). Erişim Adresi: <https://www.setav.org/teknoloji-egitim-ve-gelecek/> (Erişim Tarihi: 10.06.2020)
- Bates, A. W. T. (2015). *Dijital Çağda Öğretim*. Çeviren: M. Adnan İn M. Adnan & G. Y. Güven (Eds.), <https://pressbooks.bccampus.ca/tonybates> Erişim Tarihi: 12.06.2020
- Cumhurbaşkanlığı. 1 Sayılı Cumhurbaşkanlığı Teşkilatı Hakkında Cumhurbaşkanlığı Kararnamesi. R. Gazete [Sayı:30474 Tarih: 10.07.2018]
- Genç, Z. (2019). *Fırsat Eşitliği Bağlamında Eğitimde Teknoloji: Fatih Projesi Örneği*. (Yüksek Lisans Tezi). Kocaeli Üniversitesi Sosyal Bilimler Enstitüsü Çalışma Ekonomisi ABD, Kocaeli.
- HAVELSAN. (2010). HAVELSAN Diyalog Tanıtım. Erişim Adresi: <https://www.havel-san.com.tr/content/files/uploads/4362/HAVELSANDiyalog.pdf> (Erişim Tarihi: 08.06.2020)
- Kalkınma Bakanlığı. (2014). 10. Kalkınma Planı Eğitim Sisteminin Kalitesinin Artırılması Özel İhtisas Komisyonu Raporu. Erişim Adresi: [http://www.sbb.gov.tr/wp-content/uploads/2018/10/10\\_EgitimSistemininKalitesininArtirilmesi-1.pdf](http://www.sbb.gov.tr/wp-content/uploads/2018/10/10_EgitimSistemininKalitesininArtirilmesi-1.pdf) (Erişim Tarihi: 11.06.2020)
- Kaplanseren, E. (2013). Geleceğin eğitimi teknolojiden geçiyor. Hürriyet. Erişim Adresi: <https://www.hurriyet.com.tr/gelecegin-egitimi-teknolojiden-geciyor-23227927> (Erişim Tarihi: 12.06.2020)
- Kapucu Kocatürk, N. ve Uşun, S. (2020). Üniversitelerde Ortak Zorunlu Derstlerin Öğretiminde Uzaktan Eğitim Uygulamaları. *Açıköğretim Uygulamaları ve Araştırmaları Dergisi*, 6(1), 8-27.
- Karademirci, A. H. (2010). Öğretim teknolojileri: Tanımı ve tarihsel gelişimine yeniden bakmak. *Akademik Bilişim'10*, 496.
- Kurt, C. (2018). Gelecekteki Eğitim Teknolojisiyle İlgili 6 Senaryo. İstanbul İşletme Enstitüsü. Erişim Adresi: <https://www.iienstitu.com/blog/gelecekteki-egitim-teknolojisiyle-ilgili-6-senaryo> (Erişim Tarihi: 12.06.2020)
- MEB. (2020). Canlı Sınıf Yazılımlarına İlişkin Açıklama. Erişim Adresi: <http://www.meb.gov.tr/canli-sinif-yazilimlarina-iliskin-aciklama/haber/20654/tr> (Erişim Tarihi: 08.06.2020)

- Metin, E. (2018). *Eđitimde Teknoloji Kullanımı Öğretmen Eđitimi: Bir Durum Çalışması*. (Yüksek Lisans Tezi). Bahçeşehir Üniversitesi Eğitim Bilimleri Enstitüsü İstanbul.
- Sürek, G. (2018). *Eđitimde Teknoloji Uygulamalarına İlişkin Ortaokul ve Lise Bilişim Teknolojileri Öğretmenlerinin Görüşlerinin İncelenmesi (Şanlıurfa İli Örneđi)*. (Yüksek Lisans Tezi Yüksek Lisans Tezi). İnönü Üniversitesi Eğitim Bilimleri Enstitüsü, Malatya
- Şirazduvarı. (2017). Gelecekte Eğitim Nasıl Olacak? Erişim Adresi: <https://sirazduvari.com/gelecekte-egitim-nasil-olacak/> (Erişim Tarihi: 12.06.2020)
- Telli, S. G. ve Altun, D. (2020). Coronavirüs ve Çevrimiçi (Online) Eđitimin Önlenemeyen Yükselişİ. *Üniversite Araştırmaları Dergisi*, 3(1), 25-34.

# 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 dengeli 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.

### 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 Intelligence (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 security, 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.

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

**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 çıktılarında 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 aygıt/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. Özellikle 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 sorulamaktadır. 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 kullanıma 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 zekâyâ 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. Makinelere bilgisayarlar 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 olagelmıştır. 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 getirebileceğinden bahsedilmiştir. Turing’e göre dijital bilgisayar düşüncesi oldukça eskidir. Turing, Cambridge Üniversitesi’nde 1828 ve 1839 yılları arasında Matematik Profesörü olan Charles Babbage’in 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 gerekiyorsa, 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'nı 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 zekânın 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 amacıyla 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 nesnelere tanımlamak için kullanılmakta ve konuşmaları metinlere çevirmekte, nesnelere 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 zekâyı 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 Zekânın 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 düşünülürken; 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**

	<b>Teknoloji /Platformlar</b>	<b>Yapay Zekâ Uygulamaları</b>
<b>Google Deepmind</b>	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
<b>OpenAI</b>	Kar amacı gütmeyen Kuruluşlar, Evrimsel Algoritmalar, Derin Sinir Ağları	Derin Sinir Ağları ile çalışan Evrimsel Algoritmik Sistemler, Testbeds
<b>IBM</b>	Bilgisayar Donanım ve Yazılım Üreticisi Barındırma ve Danışma Hizmetleri Bilişsel Hesaplama	Deep Blue: Dünya'daki Satranç şampiyonunu yenen ilk program
<b>Facebook</b>	Sosyal Ağ Hizmeti	Uygulamalı Makine Öğrenme İnsan Bilgisayar Etkileşimi
<b>Apple</b>	Bilgisayar Donanım ve Yazılım Tüketici Elektronik Ürünler Online Hizmetler	Siri: Sanal Danışman İnsansız Arabalar
<b>Amazon</b>	Bulut Hesaplama Online Parakende Hizmetler Elektronik Ürün ve Hizmetler	Alexa: Sanal Danışman Amazon Yapay Zekâ Programı
<b>Microsoft</b>	Geliştirme, Üretim 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 yoğunlaşmıştır. 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 Zelanda, 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 güvenlidir. 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 nesnelere 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 odaklanmaktadır (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).

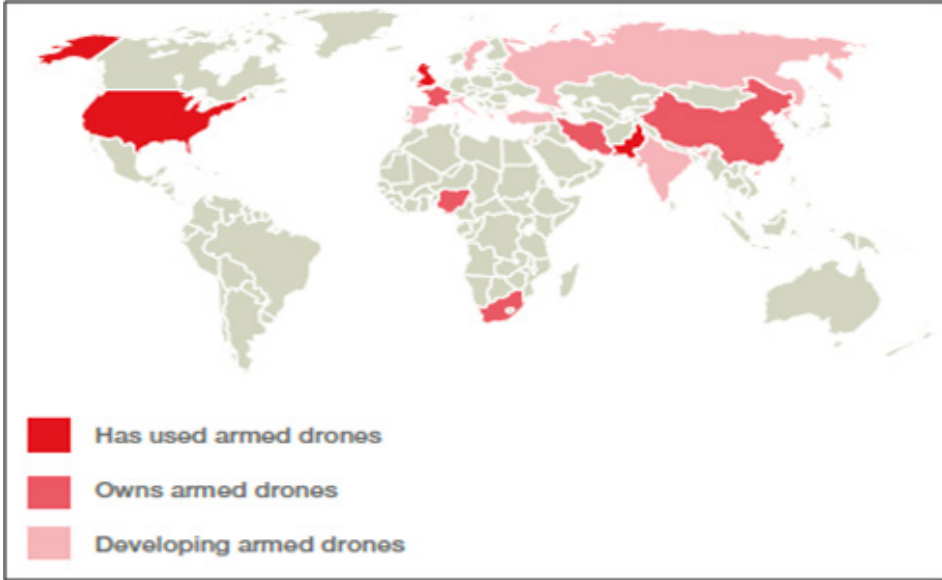
İç güvenliğin sağlanmasında önemli bir alan olan bilgi güvenliğinin yapay zekâ uygulamalarıyla yakın ilişkili olduğunu söylemek mümkündür. Çünkü hem devletin hem de özel sektörün bilgi güvenliklerinin korunması amacıyla kullanılan birçok uygulama bulunmaktadır. Siber saldırılara karşı virüs programları 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 görünümünün 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).

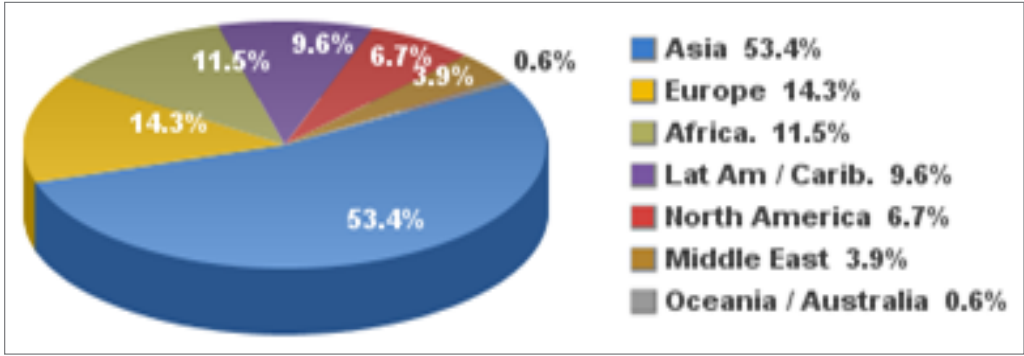
### Şekil 1. 2017 Yılında Dünya Üzerinde Silahlı Dronların Kullanımı



**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 arttıracığı 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 kuruluşları ve Dijital Türkiye Platformu gibi platformların işbirliği ile vatandaş, devleti ve iş dünyasını kapsayan bütüncül bir dijital dönüşüm gerçekleştirmesini sağlayacak politika önerileri oluşturulmaktadır (TUBİSAD, 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 bertaraf 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 bütçesinin 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 bulundurmada kalmaktadır. Siber ortamdaki bilişim sistemlerine yönelik saldırıların 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, Aktörelere ve Amaçlar**

Tehditin Seviyesi	Aktör	Amaç
<b>Ulusal Güvenliği Yönelik Tehditler</b>	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 amacıyla bilgi sızdırmak.
<b>Devletler ve Özel Sektör Tarafından Karşılaşılan Müsterek Tehditler</b>	Siber Terörist	Eylemlerinin kitleler tarafından görünür olmasını sağlama; politik değişiklikler yaratmak.
	Endüstriyel Casusluk	Rekabet üstünlüğü elde etmek.
	Organize Suç	<i>İntikam dürtüsüyle hareket</i> etmek, maddi kazanç sağlamak; kurumsal/politik değişiklikler yapmak.
<b>Yerel Tehditler</b>	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 karşılaşmaktadır. Siber saldırılarla veriler çalınabilmekte, ulusal

güvenlik bilgisayar programlarına müdahalede bulunulabilmekte, acil servisler, elektrik dağıtım sistemleri, telekomünikasyon 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 kullanılabilir (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 nedene 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 gölge 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 vermektir (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 kullanılabilir. (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 kullanılabileceğine, 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 ilişkilendirilmede 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 asimetrelerini değiştiren saldırılar karşısında kendi kendine uyarlamayı içermektedir. Şöyle ki, rakibin zayıf yönlerini belirleyebilmekte, gözlem yöntemlerinden ve öğrenilen derslerden yararlanarak saldırı türlerini sınıflandırabilmekte ve uyarlanabilir yanıtları (tutarsızlıkların tespiti ve nasıl onarılacağına bilinmesi) geliştirebilmektedir (National Science and Technology Council, 2020: 5). Esasında kısaca siber güvenlik alanında yapay zekâ uygulamalarının önceden tespit, tahmin ve yanıt verme olarak üç temel işlevi yerine getirdiği söylenebilir.

Milyarlara 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 çoğunluğunun** yapay zekânın siber güvenliğin geleceği için anahtar bir unsur olduğu sonucuna ulaşılmıştır. Ayrıca araştırma sonucuna göre (Cappemini 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 bilgilerinin, e-posta adres ve iletişim bilgilerinin ele geçirildiği belirtilmiştir (Yılmaz, 2019: 259).

Yapay zekâ istihbarat örgütlerinin ve analistçilerinin verileri hızlı toplamasını, işlemlerini, 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 tarafsız 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 tehditlerine 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 itibarıyla 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 platformlara ve çözümlerle 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 zekânın 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 çalışmanın 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-ih-a-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](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) "Vozmojnje 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://futureof-life.org/national-international-ai-strategies/?cn-reloaded=1>, Erişim Tarihi: 10.05.2021.

Glyantsev, A. (2021), *Kompyuter-Sürrealist:İskustvenniy İntellekt Prevrşayet 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 Sürdürecektir*, <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 Deniz, 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 Challenges*, 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 Science & Technology Council, s. 1-10.

Norwegian Ministry of Local Government and Modernization (2019), **National Strategy for Artificial Intelligence**, [https://www.regjeringen.no/contentassets/1febbbb-2c4fd4b7d92c67ddd353b6ae8/en-gb/pdfs/ki-strategi\\_en.pdf](https://www.regjeringen.no/contentassets/1febbbb-2c4fd4b7d92c67ddd353b6ae8/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](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 Zekâ'nın 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%BCrci-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 Vpechatlyayuşçih 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.



# ULUSLARARASI DENİZCİLİK ÖRGÜTÜ (IMO) HUKUKİ ARAÇLARININ OTONOM GEMİLERE UYGULANABİLİRLİĞİ ÜZERİNE KISA BİR DEĞERLENDİRME

## A Brief Review of the Applicability of International Maritime Organization (IMO) Legal Instruments to Autonomous Ships

\* Ali Erdem ŞAHİN

### Özet

"Dijital Çağ" olarak da adlandırılan günümüzde, hemen hemen her sektörün değişim ve dönüşümünü teknolojik gelişmeler temelinde şekillendirdiği görülmektedir. Bu anlamda denizcilik dünyası da gemi yürütmeye ilişkin olarak öngördüğü otonom, yarı-otonom ve uzaktan kontrol gibi yenilikçi sistemlerle bu trendi takip etmektedir. Ancak yeniliklerin bu derece köklü olduğu durumlarda mevcut hukuksal çerçevenin daha önce öngörülmemiş meselelere ne şekilde cevap vereceğinin sınanması büyük önem arz eder. Bu çalışmada, insan unsurunun azaltılmasına dayanan gemi modelleri ve operasyonları tanımlandıktan sonra Uluslararası Denizcilik Örgütü'nün ("IMO") yasal araçları olan SOLAS, COLREG, MARPOL ve STCW metinlerinin yeni sistemle çelişebilecek maddeleri incelenmiş, ardından uygulanabilirlik dereceleri kısaca değerlendirilmiştir.

### Abstract

Nowadays, which is called the "digital age", it has been seen that almost every sector shapes its change and transformation on the basis of technological developments. In this sense, the maritime world has followed this trend with innovative systems such as autonomous, fully autonomous, and remote-control, in order to operate ships. However, in cases where innovations are radical, it is of great importance to test how the current legal framework will respond to issues that were not foreseen before. In this study, after having defined ship models and operations based on reducing the human factor, the provisions of the legal instruments of the International Maritime Organization ("IMO"), namely, SOLAS, COLREG, MARPOL and STCW that may conflict with the new systems were examined, and then the degree of applicability was briefly evaluated.

**Anahtar Kelimeler:** Denizcilik, Otonom, Tam Otonom, Uzaktan-Kontrol, IMO.

**Keywords:** Maritime, Autonomous, Fully Autonomous, Remote-Control, IMO.

\* Ali Erdem ŞAHİN, Anayasa Mahkemesi Başkanlığı, Hakim-Raportör,  
alierdemshn@hotmail.com (<https://orcid.org/0000-0003-0559-3418>)

## 1. Introduction

This century is known to be an age of technology. Every field has been surrounded by rapid technological developments, and the maritime world is not an exception to resist this movement. A set of tools have been already implemented thus far such as sonars, global positioning, and early warning systems and so on. Beyond the scope of this, the latest innovations have been focused on autonomous systems to operate vessels by reducing the proportion of human interventions or even eliminating the human factor.

There has also been ongoing experimental, and military-based research within the maritime industry but it has been shifted from small-scale to large-scale in terms of intended use in the last few years. For instance, Rolls-Royce, one of the major players in the high-tech engine sector, revealed plans for autonomous vessels and envisaged that the first vessel would be floated in the 2020 timeframe (Buchholz, 2018). Moreover, the European Commission has initiated a new research project on the autonomous ships to see the probability of actualisation of this idea (Rødseth and Burmeister, 2012:4) and the selected project name is "Maritime Unmanned Navigation through Intelligence in Networks" (MUNIN) which aims to develop technology for unmanned vessels (MUNIN, n.d.). In this sense, it can be said that autonomous technologies related to ships have gained a feature that concerns everyone rather than a specific segment in terms of usage and regulations.

On the other hand, the outcomes of such initiatives will create a regulation problem as the character of the matter evolved from domestic to international ground, and there is no possibility to tackle the issue with the help of the legislation that has been governed by local authorities solely anymore. Nonetheless, it is possible that the current international legislation, primarily in wording, has some shortcomings in covering the characteristics of unmanned ships. As a matter of fact, the current legislation is designed only for traditional navigation. Therefore, it is beneficial to analyze the extent to which current regulations can respond to innovations.

In this essay, primarily unmanned ships and their operations will be scrutinized. After that, the current legal instruments of the International Maritime Organization ("IMO") will be examined in terms of the contradictive provisions which is related to manning, and finally the degree of applicability will be assessed. Whilst performing analysis, it will be assumed that foremost safety issues such as possible communication and signal delays have already been solved by MUNIN. Otherwise, there will not be a solid ground to investigate the compliance degree between current regulations and unmanned vessels.

## 2. Unmanned Vessels: Definition and Operations

An autonomous ship is a ship that has some level of automation and self-governance (Nordahl and Rødseth, 2017:5). There are different labels which represent the autonomous ships, and they could be used interchangeably such as unmanned ships, unmanned craft, unmanned maritime vehicles and so on. Thus, the term of the unmanned vessel ("UV") might be a preferable option as it emphasises the two features explicitly that there is no crew on the board and no hesitations about either it is a ship or not (Veal, 2017:2).

According to Lloyds registration, there are seven levels of autonomy from AL0 to AL6, and through the AL6 the degree of human intervention will be declined (Lloyd's Register, 2016). Besides this, the unmanned ships are classified generally under three sub-categories due to the operational specialities which are a remote-based operation, autonomous operation, automated (fully autonomous) operation (MUNIN, n.d.).

Due to the remote-based operative system, relevant data will be collected by the advanced data-gathering devices and then will be transmitted from UV to the shore control centre ("SCC"), is located somewhere apart from the ship, in order to navigate the UV (Hooydonk, 2014:404).

Under automated operation, the UV have owned its decision-making system and reflexive specialities to manage its own voyage plan without human intervention except for uploading the target destination into the UV's onboard computer (Pritchett, 2015:199).

Autonomous operation system is a hybrid of remotely operated and fully autonomous systems (Pritchett, 2015:200). Routine manoeuvres within the context of the instructions can be performed by advanced onboard computers which are under the supervision of the operator in case of emergency or necessary corrections (Hooydonk, 2014:404).

## 3. Could unmanned ships be accepted as a ship within traditional meaning?

The maritime legal framework is composed of considerable conventions which incorporate the various definitions regarding the ships. When determining the status of such an innovative concept in the light of the current legal framework, the threshold movement has to be focused on the previous definitions in order to provide wording detection whether it includes any restrictions or not? The definitions of the ships are changeable among the conventions as they have particular subjects to concentrate (Hooydonk, 2014:406), however, some of them does not point out any wording expressly.

International Convention for the Safety of Life at Sea, London, 1 November 1974 ("SOLAS") Regulation 2 does not incorporate the precise definition of a vessel. Therefore, it could be assumed that there are no restrictive reasons to exclude unmanned vessels from the SOLAS about crew requirements notably.

International Convention On Salvage, London, 28 April 1989 , Article 1(b) defines vessel as “any ship or craft, or any structure capable of navigation”. International Regulations for Preventing Collision at Sea London, 20 October, 1972 (“COLREGs”), Rule 3(a) describes vessels as “every description of water craft, including non-displacement craft, WIG craft and seaplanes, used or capable of being used as a means of transportation on water”. International Convention for the Prevention of Pollution from Ships London, 2 November 1973 (“MARPOL”) Article 2(4) defines the ship as “a vessel of any type whatsoever operating in the marine environment and includes hydrofoil boats, air-cushion vehicles, submersibles, floating craft and fixed or floating platforms”.

The unique speciality of the unmanned ships is not to have needs of any crew on board for operating the vessel. In the light of those definitions which have been examined thus far to see what parameters consist of the essence of being a vessel and the sample of conventions have pointed out that none of them put forward a pre-requisite stipulation in terms of manning. As a result, there is no exclusion for UV to entitle having rights and also performing duties in comparison to traditionally crewed ships.

#### **4. The compliance of existing IMO instruments in terms of unmanned ships**

As it has been mentioned above, the discussion regarding the vessel status of UV has been successfully finalized with the help of the vessel definitions. However, there are still some provision problems which have to be tackled. These shortcomings are stemmed from the nature of UV. That is to say, related provisions have been designed for regular ships which have already had the crews, but UV does not have any. Therefore, there is a necessity to address the related provisions to decide the degree of applicability each of them.

On the other hand, the analysis will be made by considering the remote-based and autonomous vessels' points of view. Upon contemplating the automated operations, it can be seen that there will be no stable ground for making a comparison between the traditional crew and artificial intelligence (AI) as long as the blur status of the AI will be enlightened in terms of human-specific skills.

#### **4.1 SOLAS**

The first edition of the SOLAS was adopted in 1914 after the Titanic disaster, and it has been continued to update with new versions and to add such amendments hitherto. The purpose of this convention is to provide safety of life at sea by generating minimum standardization regarding the construction, the safety tools and the operating procedures (SOLAS, 1974). Therefore it has a pivotal role in regulating maritime safety.

Upon having considered the UV's nature, Chapter V has to be examined among the other chapters as the manning-based provisions mainly are covered by this chapter.

Chapter V-Regulation 14 is incorporated with the wording of “sufficiently and efficiently manned” for Reg.14(1) and “establishing the appropriate minimum safe manning and issuing a document” for Reg.14(2).

There are two options to interpret Reg.14(1). If preferring the strict way and accepting the minimum standard as appearing at least one crew on board physically, there would be no chance to navigate for UV. The second option is to concentrate the capability of UV without considering the traditional manning. Therefore, it can be assumed that as long as the provision has a chance to be fulfilled by the SCC or advanced computers which are under the supervision of the operator in case of emergency, the absence of crew in the ship would not affect the sufficiency. Moreover, after the credibility is fully gained in the future by UV, this requirements would be remembered as a deterrent nothing more (Pritchett, 2015:203).

On the other hand, Reg.14(2) prescribes that appropriate minimum safe manning document has to be issued and the last resort of this decision is the flag state regarding whether its eligible or not to be merit (Ringbom et al., 2016:43). Therefore, the flag state has to be convinced by the UV, but there is an uncertainty about under what criteria should be taken into account to reach such a decision. As a result, the provision would need to be amended in order to a resurgence in the degree of applicability.

Chapter V-Regulation 22(3) refers to the level of visibility which has to be a significant part of the ship design to maintain the safe navigation. Most of the ships have already implemented the advanced technology to enhance the visibility possibilities instead of hiring more crew to achieve it. Therefore, the provision has a higher degree of applicability. However, there might be added some amendments about the location points of the sensors to avoid the possible signal blockers as well as the regular ships which dealing with the poor eyesight by moving containers vicinity of the navigating bridge .

Chapter V-Regulation 33(1) refers to the liability of shipmaster in distress situation at sea and the entering reason of failure into the logbook in case of not being able to assist to the persons in distress. It can be seen that the applicability of the first part of this provision is not possible with respect to today’s technology. As providing assistance in certain matters is a considerably complicated process to manage and human intervention has to be performed by the ship crew, and this time SCC cannot be the substitution of actual crew. Therefore, in this case, there would be needed some serious amendments.

On the other hand, the second part of the provision would be amended by adding an electronic version of log-book for UV.

## 4.2 COLREG

The standards of navigational rules are determined by the COLREG constitutively (Baatz, 2014:228) which also known amongst mariners as The Rules of the Road (McLaughlin, 2011:111). This convention was entered into force in 1972, and the purpose is to procure prevention of collisions at sea (COLREG, 1972).

UV have to cope with some contradictive standards against its nature prescribed by COLREG. For example, Rule 2 deals with the responsibility matters that there will be no privilege whomever causes the neglect of precaution in terms of taking responsibility; Rule 5 is about the look-out instructions that every vessel has to have a proper look-out by sight and hearing in order to avoid risk of collision; Rule 6 refers to the safe speed that every vessel has to proceed safe speed in order to take proper precaution against unforeseen conditions; Rule 8 deals with the action to avoid collision that points out the success of this aim highly correlated with following the rules and the good seamanship.

Rule 2 and 8 are about the good seamanship issue. This concept is designed for the actual sailors to demonstrate the requirement of taking necessary precautions by the ordinary practice of seamen. In this sense, the capability of UV might become a controversial matter in terms of situational awareness and human judgement in the decision-making loop as they have SCC rather than a traditional crew (CMI, 2018:14-15). Even though, as long as the rules are carried out responsibly and contemporaneously by SCC, the rules would have a higher degree of applicability.

The subject of a proper look-out is primarily related to the visibility matters which has been discussed similarly under the section of SOLAS (Chapter V-Reg.22). In this case, the issue is the wording of "sight and hearing" which has to be necessitated by human factor. Even if UV does not have an actual crew, possible adrift stuff or multiple mobile objects at sea might have readily detected by the future advanced sensor technology (Pritchett, 2015:205) and gathering data might have assessed on time by SCC. Thus, the wording of sight and hearing might be accepted as a negligible.

There are significant parameters which have to be taken into account by determining the safe speed such as visibility, traffic density and so on due to Rule 6. Nevertheless, it is anticipated that most UV will travel at higher speeds than many manned vessels and they are not dumb. (McLaughlin, 2011:111) In this case, there is a probability of radar range-scale problem as the radar might be inadequate to detect closer objects whilst UV is floating, but it can be tackled by using two different scales of radars (Cockcroft and Lameijer, 2004:31-32). As a result, the safe speed issue once again might be solved with the help of technology and SCC.

### 4.3 MARPOL

The standards of prevention of pollution were determined by the MARPOL constitutively. This Convention was entered into force in 1973, and it has been continued to update with amendments. The Convention is comprised of regulations aimed at hindering and reducing pollution from ships whether caused by accidental pollution or that from regular operations.

The provisions of MARPOL will have to be implemented by UV as their manned counterparts, even though the adaptation would not be relatively straightforward, upon considering the other IMO regulations regarding unmanned operations (CMI, 2018:17). Because according to this convention, the matter of the manning is the least concern among other conventions of IMO.

### 4.4 STCW

Convention on Standards of Training, Certification and Watchkeeping for Seafarers ("STCW") was adopted in 1978, and the purpose of the convention was to prescribe minimum standards concerning training, certification and watchkeeping for seafarers (STCW, 1978).

UV have to cope with some contradictive standards against their nature prescribed by STCW. For example, Article III emphasises that "seafarers serving on board seagoing ships entitled to fly the flag of a Party". Chapter VIII is composed of watchkeeping regulations such as "at no time shall the bridge be left unattended", "keep the watch on the bridge" and "in no circumstances leave the bridge until properly relieved" as well as SOLAS and COLREG also have similar sections, but this time human actions are directly described.

It can be accepted that there is a significant disparity between shore-based controllers and seafarers in terms of using information technology ("IT") skills and the convention was designed for dealing with seafarers rather than unmanned operations (CMI, 2018:17). For this reason, there is no need to raise an assumption for demonstrating the substitution between seafarers and SCC personnel.

Furthermore, there is an open spot which enables retaining or adopting other educational and training arrangements for particular types of ships due to the Article IX(1) and this would pave the way for fulfilling the training requirements concerning UV. As a result, the nature STCW is not applicable for UV and need to have serious amendments to comply with UV (Ringbom et al., 2016:47-48).

## 5. Conclusion

In this article, firstly UV was defined, and then diversification was made with respect to operative features. Later on, the status of UV was investigated with the help of sample legal ship definitions and not being reached any exclusions for UV. After this challenge, contradictive provisions of current legal instruments of IMO was examined one by one in terms of compliance with the UV's nature, and then the degree of applicability was assessed.

The findings of this essay can be divided into two parts. First, the perspective of remote-based and autonomous vessels, and the second is the point of view of the automated vessels.

According to the first one, every convention has its applicability degree. Whilst making analysis, substitution possibilities between traditional manning and SCC have been contemplated. Accordingly, whether negligible or not there is a need to make some amendments. And if the necessary amendments are fulfilled by IMO with the help of tacit acceptance (Baatz, 2014:333), compliance with conventions will be provided readily or it might be tried to establish new conventions as STCW-F<sup>1</sup>, but this time the adequate ratification number might be a problem. Therefore, amendments seem to be the best option to take.

On the other hand, the second one is a highly complicated matter regarding status. Upon being assessed all of the conventions, it can be seen that the traditional manning approach was adopted by IMO. Hence, there will be no chance to assess compliance, unless the status of the AI becomes definite. Therefore, the new legal ground has to be constituted instead of heading an adaptation for automated operations.

1 Special version of STCW for fishing personnel.



---

**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 çalışmanın yazarlarına aittir.

**Yazar Katkıları:** Ali Erdem Şahin çalışmanın tamamında tek başına katkı sunmuştur.

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

**Teşekkür:** Yayın sürecinde katkısı olan hakemlere teşekkür ederim.

**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:** Ali Erdem Şahin has contributed to all parts and stages of the study

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

**Acknowledgement:** I would like to thank the referees who contributed to the publication process.

## Bibliography

International Convention for the Safety of Life at Sea, London, 1 November 1974 'SOLAS,1974'(Imo.org,) [http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-\(SOLAS\),-1974.aspx](http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Safety-of-Life-at-Sea-(SOLAS),-1974.aspx)

International Regulations for Preventing Collision at Sea London, 20 October, 1972 'COLREG' (Imo.org,) <http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/COLREG.aspx>

International Convention for the Prevention of Pollution from Ships London, 2 November 1973 'MARPOL' (Imo.org,) [http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Prevention-of-Pollution-from-Ships-\(MARPOL\).aspx](http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-for-the-Prevention-of-Pollution-from-Ships-(MARPOL).aspx)

Convention on Standards of Training, Certification and Watchkeeping for Seafarers 7 July 1978 'STCW' (Imo.org) [http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-on-Standards-of-Training,-Certification-and-Watchkeeping-for-Seafarers-\(STCW\).aspx](http://www.imo.org/en/About/Conventions/ListOfConventions/Pages/International-Convention-on-Standards-of-Training,-Certification-and-Watchkeeping-for-Seafarers-(STCW).aspx)

### Secondary Sources

Baatz Y. (2014) *Maritime Law* (3rd ed), Informa Law from Routledge.

Cockcroft A, J Lameijer. (2004). *A Guide To The Collision Avoidance Rules* (6th ed.) Elsevier Butterworth-Heinemann.

Hooydonk, E. (2014). The law of unmanned merchant shipping – an exploration. *JIML*, 20(1). 403-423.

McLaughlin, R. (2011). Unmanned Naval Vehicles at Sea: USVs, UUVs, and the Adequacy of the Law. *Journal of Law, Information and Science*, 21(2), 100-115.

Pritchett, P. W. (2015). Ghost Ships: Why the Law Should Embrace Unmanned Vessel Technology. *Tulane Maritime Law Journal*, 40(1), 197-226.

Ringbom H., Collin F and Viljanen M. (2016). AAWA, Remote and Autonomous Ships: The Next Steps. *Rolls-Royce plc*. 35-54.

[https://www.rolls-royce.com/~/\\_media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/aawa-whitepaper-210616.pdf](https://www.rolls-royce.com/~/_media/Files/R/Rolls-Royce/documents/customers/marine/ship-intel/aawa-whitepaper-210616.pdf)

Rødseth Ø. J. and Burmeister H-C. (2012). Developments Toward the Unmanned Ship. *Semantic Scholar*. 1-16. <https://pdfs.semanticscholar.org/6a8a/771d52e210f36d48cd345a13aab294d83780.pdf>

Veal, R. (2017). Unmanned ships on the IMO work agenda. *Lloyd's Shipping & Trade Law*. 17. 1-4.

Buchholz K. (2018). Rolls-Royce Sets Sail with Autonomous Ship Technology.

<https://www.sae.org/news/2018/04/rolls-royce-sets-sail-with-autonomous-ship-technology>

CMI. (2018). International Working Group Position Paper On Unmanned Ships and The International Regulatory Framework Regulatory Framework. <https://comitemaritime.org/wp-content/uploads/2018/05/CMI-Position-Paper-on-Unmanned-Ships.pdf>

Lloyd's Register. (2016). LR defines 'autonomy levels' for ship design and operation. <https://www.lr.org/en/latest-news/lr-defines-autonomy-levels-for-ship-design-and-operation>

MUNIN, (n.d.). About. <http://www.unmanned-ship.org/munin/about>.

MUNIN, (n.d.). The Autonomous Ship. <http://www.unmanned-ship.org/munin/about/the-autonomus-ship>

Nordahl H and Rødseth Ø. (2017). Definition for Autonomous Merchant Ships. 1-21. <https://nfas.autonomous-ship.org/wp-content/uploads/2020/09/autonom-defs.pdf>

# SİBER ORDULAR VE SİBER SAVAŞLAR

## Cyber Armies And Cyber Wars

\*Meryem ORAK

### Özet

Gelişen dünya teknolojileri karşısında geleneksel ordular ve geleneksel silahların yanında siber ordu ve siber silahlar da devreye girmeye başlamıştır. Rekabet ve yarış sanal dünyada devam etmekte olup hem devlet hem de devlet dışı aktörler, kozlarını bu platformda da paylaşmaktadırlar. Genellikle ülkelerin resmi web sitelerine yapılan saldırılarla birlikte ayrıca o ülke adına faaliyet gösteren firmalar ya da o ülke vatandaşları da bizzat siber orduların hedefi olabilmektedir. Bu bakımdan yalnızca resmi aktörlerin değil ülke için önemli ticari firmaların ve vatandaşların da korunması önem arz etmektedir. Devletler bu bağlamda savunma sistemlerini yapılandırmakta ve siber bir dünyada daha etkili olabilmek adına ordularını bu çerçevede geliştirmektedirler. Bu çalışmada siber güvenlik ve siber ordu kavramlarına dair literatür incelenerek dünyada bu alanda atılım yapan devletlerden olan ABD, Rusya ve İran'daki durum ortaya konulmuştur. Son olarak da siber güvenlik alanında Türkiye'nin kurumsal ve altyapı girişimleri ele alınmıştır.

### Abstract

In the face of developing world technologies, besides traditional armies and traditional weapons, cyber army and cyber weapons have started to come into play. Competition and race continues in the virtual world, and both state and non-state actors share their trump cards on this platform. In addition to attacks on the official websites of countries, companies operating on behalf of that country or citizens of that country can also be the target of cyber armies. In this respect, it is important to protect not only official actors but also important commercial companies and citizens for the country. In this context, states are structuring their defense systems and developing their armies within this framework in order to be more effective in a cyber world. In this study, the literature on the concepts of cyber security and cyber army has been examined and the situation in the USA, Russia and Iran, which are among the states that have made a breakthrough in this field in the world, has been revealed. Finally, Turkey's institutional and infrastructure initiatives in the field of cyber security are discussed.

**Anahtar Kelimeler:** Siber güvenlik, Siber ordu, Siber savaş

**Keywords:** Cyber security, Cyber army, Cyber warfare

Meryem ORAK, Yüksek Lisans Öğrencisi, Bartın Üniversitesi, meryem\_orak@icloud.com

## Giriş

Siber ordu kavramı ele alınmadan önce siber orduların temel iki bileşeni olarak iletişim sistemleri ile askeri kurumların ilişkisine değinilmesi gerekmektedir. Günümüze kadar geliştirilen pek çok teknoloji ve bunlarla bağlantılı cihazlar öncelikle askeri alanda kullanılmış olup ardından sivil alana yayılmıştır. Bunun başlıca örnekleri ise bilindiği üzere bilgisayar sistemleri ve internettir. Bilgisayar teknolojisine dair kavramların ortaya çıkışı 2. Dünya Savaşı yıllarına kadar götürülebilir. 2. Dünya Savaşı esnasında iletişim kurmak için Almanlar tarafından kullanılan ve Enigma ismi verilen bir makine bünyesinde barındırdığı kompleks sistemler ile bilgisayar teknolojisine benzer özellikler taşımaktaydı. Enigma'yı kısaca, 1. Dünya Savaşı sonlarında Alman bilim adamı Arthur Scherbius tarafından geliştirilen, düşman kuvvetlerinin iletilen mesajları okumasını engelleyecek şekilde şifreleme yöntemleri kullanan karmaşık bir makine olarak tanımlamak mümkündür.

2. Dünya Savaşı'nın başlarında bir takım mesajlar çözülmüş olsa da Enigma Almanlar tarafından sürekli geliştirilmiş ve bir Enigma'nın bir algoritması çözülene kadar yenisi oluşturulmuştur. Böylece istihbarat ve haberleşme gibi çok önemli iki alanda Almanya düşman kuvvetlere karşı avantaj sağlamıştır.

Savaş henüz patlak vermeden önce şifreli mesajları okumak amacıyla İngiliz hükümeti tarafından Bletchley Park ismi verilen bir grup kurulmuştur. Bu gruba 1938 yılında Alan Turing de davet edilmiştir. Turing doktora öğrenimi sırasında gerçekleştirmiş olduğu çalışmalarla Bletchley Park'ta oldukça faydalı olmuştur. Turing ve arkadaşları Enigma'nın mesajlarını kısmen çözmüş olsalar da her gün yenilenen algoritmalarından dolayı şifre çözmeyi sürekli hale getirebilecek bir karşı makine yapmak için çalışmalarını sürdürmüşlerdir. Aynı dönemde Adolf Hitler'in generalleri ile iletişim kurması için geliştirilen Geheimschreiber isimli bir makinenin de varlığından söz edilmekteydi. Dolayısıyla hem Enigma hem de Geheimschreiber için ayrı ayrı çalışmalar yürütülüyordu. Alan Turing'in zekası ve önceki çalışmaları bu konuda oldukça fayda sağlamış ve günümüz bilgisayarlarının atası kabul edilebilecek Clossus isimli makine bu dönemde geliştirilmiştir. Clossus bir mesajdaki 25000 karakteri anlık olarak tarayıp anlamlı mesajları ayırt edebilen icat edildiği dönem için oldukça gelişmiş bir makine olarak öne çıkmaktaydı. Bu sebeple iki ayrı makine yapılmadan Clossus ile hem Enigma'nın hem de Geheimschreiber'in gönderdiği mesajlar çözülebilmekteydi. Dönemin savaş uzmanları tarafından Turing'in oluşturmuş olduğu makinenin, savaşı 2 yıl daha erken bitirdiği ve milyonlarca hayatı kurtardığı ifade edilmektedir (Copeland, 2004, s. 232).

İnternetin gelişimine bakıldığında yine askeri kurumların bu teknolojiye öncülük ettiği görülebilir. 1969 yılında Amerika Savunma Bakanlığı'nın kurmuş olduğu "The Advanced Research Projects Agency Network" yani daha yaygın ismiyle "ARPANET" dünyanın ilk paket dağıtım ağı yani internet ağı olarak kabul edilir. Savunma Bakanlığı öncülüğünde;

Kaliforniya Üniversitesi Los Angeles Yerleşkesi, Kaliforniya Üniversitesi Santa Barbara Yerleşkesi, Utah Üniversitesi, Stanford Araştırma Enstitüsü arasında ilk bilgisayar bağlantısı oluşturuldu. Kurulan protokolde gönderilen ilk ileti ise "lo" idi. Aslında gönderilmek istenen "login" kelimesiydi ancak gönderilen ilk iki harften sonra sistemlerde meydana gelen sorunlardan ötürü diğer harfler saatler sonra gönderilebilmiştir. Sonrasında ise ağ bağlantıları genişletilmiş, ordu ardından üniversiteler ve diğer devlet kurumları, internet aracılığı ile bağlantı kurmaya başlamıştır (Lukasik, 2011, s. 12).

Bunun yanında siber bir ordu fikri de zaman zaman ortaya atılmıştır Genellikle bilim kurgu filmlerinin konusu olmakla beraber yakın zamanda bunun artık gerçekleşebileceği görülmüş ve siber ordu çalışmaları hız kazanmıştır. Bunun öncülerinden biri de Amerika Birleşik Devletleri olarak karşımıza çıkmaktadır.

### **a) Amerika Birleşik Devletleri**

Amerika Birleşik Devletleri, ordusu bünyesinde siber saldırılarına ilk olarak resmi bir yapılanmaya girmeden çok önce başlamıştır. Bunun ilk örneği ise 1. Körfez Savaşı sırasında yaşanmıştır. ABD bünyesinde faaliyet gösteren siber birimler Irak ordusunun kara, deniz ve hava kuvvetleri arasındaki koordinasyonu keserek savaş esnasında önemli bir üstünlük elde etmişlerdir. Ayrıca kriptolu telsiz frekanslarına sızarak frekansları karıştırmış ve Irak ordusunu yanlış noktalara yönlendirmişlerdir.

2. Körfez Savaşı esnasında da ABD mevcut siber gücünü ölçme imkanı bulmuştur. Bu defa yalnızca telsizlere değil Irak ordusunun diğer tüm haberleşme birimlerine sızma faaliyetleri gerçekleştirilmiş ve propaganda faaliyetleri bu yolla gerçekleştirilmiştir. Ele geçirilen haberleşme araçları ile görevli subayları psikolojik olarak etkileyecek ve ABD ordusuna teslim olmasını sağlayacak nitelikte mesajlar paylaşılmıştır (DARICILI, 2017, s. 341).

Amerika Birleşik Devletleri, özellikle 11 Eylül 2001'de yaşamış olduğu saldırılar sebebiyle bir histeriye kapılmış ve devletin ve de özellikle güvenlik birimlerinin etkinliğini oldukça etkin bir seviyeye çıkarmıştır. Başta fiziki silah envanterini genişletmekle başlayıp askeri müdahalelerle devam eden bu süreç, ordunun da yapılanmasını beraberinde getirmiştir. Bu bağlamda, öncelikle mevcut Uzay Komutanlığı bir dönüşüm geçirmiş ve uzayda etkinlik sağlama amacı yanında bir de siber güvenlikle ilgili görevler edinmiştir. Ancak 2008 yılına gelindiğinde ABD bunun yeterli olmayacağına kanaat getirmiş ve bir siber komutanlık kurulmasına yönelik çalışmalara başlamıştır ve 23 Haziran 2009 tarihine gelindiğinde United States Cyber Command (USCYBERCOM) resmi adıyla, Amerika Birleşik Devletleri Siber Komutanlığı'nı kurmuştur. Birleşik Devletler Siber Komutanlığı'nın görevleri ise şu şekilde belirlenmiştir:

- Savunma Bakanlığı'na bağlı bilişim ve bilgi ağlarını korumak ve bu noktada gerekli operasyonları gerçekleştirmek.

- Verilecek görevler doğrultusunda mevcut tüm sahalarda geniş ölçekli askeri siber operasyonlar düzenlemek.
- ABD'nin ve müttefik devletlerin internetteki dolaşım özgürlüğünü sağlarken düşman devletlerin faaliyetlerini baskılamak ve kısıtlamak amacıyla etkinliklerde bulunmak, planlar yapmak, koordinasyon faaliyetleri gerçekleştirmek ve bütünlük sağlamak olarak belirlenmiştir.
- Askeri ve sivil diğer otoriteler ile bilgi paylaşımında bulunmak, gerçekleşen ya da gerçekleştirilmesi planlanan operasyonlara dair bilgilendirmede bulunmak.
- Diğer ordu birimleri ile koordinasyon içerisinde hareket etmek.

11 Ekim 2012 tarihine New York'ta gerçekleşen bir konferansta ABD Savunma Bakanı Leon Panetta gelecek yıllarda ABD'nin siber bir Pearl Harbor tehlikesiyle karşı karşıya olduğunu ve bir takım düşman odaklarının ABD'nin kritik altyapısını siber yolla vurmak istediğini belirtmiştir. Pek çok altyapı faaliyetinin bilişim sistemleri üzerinden yürüdüğünü belirtmiş ve olası bir siber saldırı sonucunda elektrik, su gibi ve hatta ulaşım faaliyetlerinin kontrolü gibi bir takım durumların ciddi tehlikeye girebileceğini belirtmiştir. Tüm bu risklerden ötürü olası siber saldırılara karşı siber güvenliğin önemini vurgulayan Panetta siber ordunun bu tehlikelerin ortaya çıkması halinde anında karşılık vermesinin önemine dikkat çekmiştir (Yayla, 2013, s. 186-187).

ABD Siber Komutanlığı Ordu Siber Komutanlığı, Filo Siber Komutanlığı, Sahil Güvenlik Siber Komutanlığı ve Hava Kuvvetleri Siber Komutanlığı 4 alt birimden oluşmaktadır. 2013'te USCYBERCOM'da görev yapan asker sayısı 5000 olarak açıklanmıştır. Ancak bunun sonraki senelerde 21 bine çıkarılacağı iddia edilmektedir. Siber ordu ilk büyük muharip savaşını 29 Nisan 2016 tarihinde Irak Şam İslam Devleti (İŞİD) isimli örgüte karşı gerçekleştirmiştir. Özellikle internet alanında oldukça etkin olan İŞİD bu tarihten sonra bu alanda da bir savaş içerisine girmiştir. Birleşik Devletler Siber Komutanlığı'na bağlı birimler İŞİD'in faaliyet gösterdiği internet alanlarını izlemeye almış, internet üzerinden gerçekleşen para akışlarını kesintiye uğratmış ve propaganda yapmasını engellemeye yönelik girişimlerde bulunmuş ve oldukça önemli başarılar elde etmiştir (DARICILI, 2017, s. 341-342).

Geniş ölçekli siber savaş son zamanlarda ise ABD ve İran arasında yaşanmaktadır. 2015 yılına doğru başta İran olmak üzere pek çok ülkedeki devlet kurumlarına ait bilişim sistemleri Stuxnet ismi verilen bir virüsten etkilenmiştir. Windows işletim sistemleri üzerinden yayılan virüs kısa zamanda onlarca ülkede bilişim sistemlerine kritik ölçülerde zararlar vermiştir. Özellikle nükleer enerji sektöründe kullanılan sistemleri hedef alan virüs, reaktörlerdeki olağandışı durumların görülmesini engelleyerek nükleer felakete davetiye çıkarmıştır. Eski bir NSA (United States National Security Agency) çalışanı olan Edward Snowden, Stuxnet'in ABD ve İsrail ortaklığı sonucu ortaya çıkan bir virüs olduğunu ve tamamen İran'ın nükleer faaliyetlerin sekteye uğratmaya yönelik ola-

arak geliştirildiğini söylemiştir. Nitekim virüsün zararlarına bakıldığında en çok etkilenen ülkenin %58,85 ile İran olduğu görülmektedir. İran milyonlarca dolar zarar etmiştir. Ayrıca nükleer santrallerindeki santrifüjleme makineleri olağanüstü hızlarda dönerek parçalanmıştır (Yazıcı, 2015). Bu yaşanan gelişmeleri siber savaşların ilk önemli adımları olarak görmek mümkündür.

20 Haziran 2019 tarihinde Amerika'ya ait bir casus insansız hava aracı İran tarafından düşürülmüştür. Söz konusu dönem için mevcut olan en yüksek teknolojiye sahip izleme ekipmanlarına sahip hava aracının değeri 120 milyon dolar olarak belirtilmiştir. 2016 yılında ABD'ye ait RQ-170 model insansız hava aracı yine İran tarafından düşürülmüş ve İran siber ordusu tarafından aracın kriptografisi çözülmüş ve aynı özelliklerde araçlar İran tarafından üretilmeye başlanmıştır. Silah olmayan orijinal modeline silah aparatları da ekleyerek mevcut RQ-170'i daha da geliştirilmiştir (Aksan, 2019). 20 Haziran 2019 tarihinde düşürülen hava aracının da benzer bir durumla karşı karşıya kalmasını istemeyen ABD bu noktada İran ile bir siber savaşa başlamıştır. ABD'nin siber savaş tehdidinin akabinde ilk saldırılar ise İran'dan gelmiştir. Amerikan hükümeti ve birtakım Amerikan şirketleri hedef alınmıştır. Amerika Birleşik Devletleri siber ordusu ise İran'ın petrol tankerlerini hedef almasına yönelik geliştirdiği sistemlere zarar vermiştir. İran kendi kurmuş olduğu takip sistemleri ile körfezde gerçekleşen petrol nakliyesini takip edebiliyordu ve bu doğrultuda bir takım casus programlar geliştirmişti. Amerika Birleşik Devletleri bu programları hedef almış ve ilgili veri tabanını silmiştir (Sözen, 2019).

Birleşik Devletler Siber Ordusu genellikle Ulusal Güvenlik Ajansı ile beraber hareket etmektedir. Ulusal Güvenlik Ajansı'nın başkanı ise aynı zamanda siber ordunun da komutanıdır.

## **b) Rusya Federasyonu**

Rusya'nın Amerika'da olduğu gibi resmi bir siber ordu yapılanması mevcut değildir. Rusya ordusu hava, kara, deniz, uzay ve stratejik füze kuvvetleri olmak üzere 5 kuvvet komutanlığından oluşmaktadır. Resmi bir komutanlık kurulmamış olmasına rağmen Rusya'nın da siber alandaki devlet ölçekli faaliyetleri oldukça eskiye götürülebilir. 1980'lerde SSCB ordusunda görev yapan Mareşal Nikolai tarafından "Askeri Meselelerde Devrim" ismi verilen bir program başlatılmış ve ordu faaliyetleri ilk kez sanal alana da taşınmıştır. Oluşturulan bu programda ordunun otomasyona geçmesi, orduda bilişim eğitimlerinin sağlanması, bilgisayar envanterin çıkarılması gibi bir takım durumların gerçekleşmesi söz konusu olsa da ilerideki gelişmeler açısından öncü bir nitelik taşımıştır. Rusya siber ordu konusunda atılımı ise 1. Körfez Savaşı sonrası gerçekleştirmek istemiştir. Savaş esnasında Amerika'nın kullandığı siber faaliyetlerin etkisine şahitlik eden ve durumu yakinen izleyen Sovyetler Birliği, siber ordu konusunda adım atmak istemiştir ancak iç siyasi çalkantılar ve ardından gelen dağılma dönemi ile psikolojik, sosyolojik ve ekonomik anlamda çöküntüye uğrayan Rusya'nın yeniden toparlanması



oldukça uzun sürmüştür. Ancak 2000'lere gelindiğinde yeniden bu tartışmalar gündeme alınabilmiştir (Darıcılı & Özdal, 2017, s. 124).

09.09.2000 tarihinde Rusya Enformasyon Güvenliği Doktrini yayınlanmıştır. Doktrin- de bilgi güvenliği, amaçlar, sanal gelecek gibi pek çok konu ele alınmıştır. Rusya Enfor- masyon Güvenliği Doktrini Rusya'nın siber güç olma yolundaki ilk belgesi olarak kabul edilmektedir.

12 Mayıs 2009 tarihinde "2020'ye Doğru Ulusal Güvenlik Strateji Belgesi" ilan edil- miştir. Bu belge Rus istihbaratına bir rehber görevi görmek ve ulusal güvenlikteki ge- rekli rolleri ortaya koyması açısından önemlidir. Belgede, gelişen teknolojinin aynı za- manda pek çok riski de beraberinde getirdiğine değinilmiştir.

2011'de ise "Bilgi Çağında Rus Silahlı Kuvvetleri'nin Faaliyetlerine İlişkin Kavramsal Görüşler" isimli bir belge yayımlanmıştır. Rus Siber Savaş Doktrini olarak da belirtilen bu belgede siber savaşın mantığına vurgu yapılmıştır. Buna göre ulusal bilgi sistem- lerine zarar veren, hükümeti ve toplumu bu yolla etkilemeye çalışan, Rus kültürünü, sosyolojisini ve ekonomisini yok etmeye çalışanlara karşı gerçekleştirilecek enformatik faaliyetler siber savaşın mantığını oluşturmaktadır (Darıcılı & Özdal, 2017, s. 125).

Rusya'da resmi bir siber komutanlık olmamasına karşın ordunun ve istihbarat ser- visinin bünyesinde siber yapılanmalar mevcuttur. Siber savunma; Federalnaya Slujba Bezopasnosti (Rusya Federal Güvenlik Servisi/FSB), SluzhbaVneshney Razvedki (Rusya İstihbarat Servisi/SVR) ve Glavnoye Razvedyvatel'noye Upravleniye'nin (Rusya Askeri İstihbarat Kurumu/GRU) müşterek faaliyetleri ile yürütülmektedir.

FSB (Rusya Federal Güvenlik Servisi) devlet güvenliğine yönelik faaliyetlere karşı istihbarat toplamakla görevlidir. KGB'nin devamı niteliğinde olan kurum özellikle ayrı- lıkçı grupların durumlarını kontrol altında tutmaya çalışmaktadır. Fakat bunun yanında FSB'nin siber güvenlik ile ilgili rolü de bulunmaktadır. Bu bağlamda, Rusya vatandaşı veya yabancı kişilerin telekomünikasyon bilgilerini kontrol etmek görevlerinden bir ta- nesidir. FSB'nin Rusya içi siber etkinliğinin fazla olduğu bilinmektedir.

SVR (Rusya İstihbarat Servisi) ise ülke dışındaki istihbarat faaliyetlerinden sorum- lu olan kurumdur. Genellikle GRU ile birlikte istihbarat toplamakta olan SVR başta SSCB'den ayrılan ülkeler olmak üzere, Suriye, Küba, Vietnam gibi pek çok ülkede espi- yonaj faaliyeti göstermektedir. Rus menşei bir takım yazılımlar ve uygulamalar vasita- sıyla uluslararası casusluk faaliyetlerinde bulunduğu iddia edilmektedir.

GRU (Rusya Askeri İstihbarat Kurumu) ise genellikle diğer istihbarat örgütleri ara- sındaki dengeyi sağlamakla görevlidir.

2014 yılında Sergei Shoigu Rus ordusunun siber savunmasını şu sözlerle aktarmış- tır: "Rus ordusu siber tehditler karşısında giderek bağımsız bir yapılanmaya kavuşmak-

tadır. Hükümet olarak bu amaçla 500 milyon dolar bütçe ayırdık. Faaliyetler hem yurt içi hem de yurtdışında sürecektir. Bunun için insan kaynağı envanterini genişletip yazılım uzmanları ve yabancı dil bilen personel istihdam edeceğiz” demiştir (Darıcı & Özdal, 2017, s. 131).

Sonraki yıllarda ise yazılım alanında uzmanlaşan üniversite öğrencilerinin orduya katılmasına yönelik girişimlerde bulunulmuştur. Alanında uzman bilgisayar mühendislerine, programcılara, web tasarımcılarına, orduya katılmak için gereken bir takım kriterlerden muaf olacak şekilde, orduya katılmaları için teklifler götürülmüştür (Saygun, 2017).

Son yıllarda ise Rus devlet kurumlarına ait internet siteleri ise oldukça fazla siber saldırıya maruz kalmıştır. Saldırıları genellikle Amerika ve Avrupa ölçekli olmuştur. Rusya Federal Eğitim ve Bilim Denetim Servisi'nin resmi sitesi Haziran 2019'da saldırıya uğramış ve bir süre lise öğrencilerinin katılmış olduğu sınavlara erişim sağlanamamıştır (Sputnik News, 2019). Saldırı daha büyük sonuçlar yaratmadan atılırsa da Rusya'da bu konuda ciddi çalışmalar yapılması gerektiği konusunu bir kez daha gündeme getirmiştir.

Tüm bu tehditler neticesinde oldukça radikal bir adım atan Rusya bir süredir gerçekleştirmeyi planladığı internet uygulamasını 24 Aralık'ta düzenlemiş ve bu tarihte tüm dünya ile olan internet bağlantısını kesmiştir. Kimi kaynaklar bunun bir siber saldırı tatbikatı olduğunu belirtirken Rusya ise ülkenin ulusal internet altyapısının küresel DNS'ye bağlı kalmadan çalışıp çalışmayacağına yönelik bir deneme yapıldığını ve sonucun olumlu olduğunu belirtmiştir. Buna göre olası bir siber saldırı altında Rusya istediği anda uluslararası internet ağından ayrılabilir (Baki, 2019). Hem Rus devlet kurumuna ait internet siteleri hem de Rusya ölçekli firmalara ait internet sitelerini kapsayacak şekilde kurulan bu intranet ağı olası siber saldırılardan ülkenin en az zararı görmesini sağlayacak.

### c) İran

Ortadoğu coğrafyasına bakıldığında zaman etrafında en fazla düşman unsuru bulunan ülkelerden birisi İran'dır. Bu durum GSYH ile karşılaştırıldığında İran'ın savunma harcamalarının daima yüksek bir harcama kalemi oluşturmasına yol açmaktadır. İran, bir caydırıcılık unsuru olarak da elinde daima nükleer gücü bulundurmaktadır; ancak İran'ın varlığı ve savunma harcamaları da diğer ülkeler açısından bir tehdit unsuru olarak kabul edilmektedir. Bundan ötürü İran İslam Devrimi'nden beri süregelen adı konulmamış bir savaş hali yaşanmaktadır. Bu kimi zaman İran-Irak Savaşı gibi sıcak çatışma halinde yaşansa da çoğu zaman ambargolar veya bir takım engellemelerle devam etmektedir.

İran'ın yeni savaş düzeninin sanal dünyaya da taşındığını idrak etmesi 2010'ların başlarında olmuştur. İran'daki, başta nükleer tesislerdeki bilgisayarlar olmak üzere, pek çok bilgisayarda Flame ismi verilen bir virüs keşfedilmiştir. O zamana değin geliştirilen virüsler genellikle bilgisayar sistemlerini çökertmek için kullanılırken bu virüs bilgisayar ara birimlerini çalıştırabilecek bir takım özelliklere sahiptir. Öyle ki bilgisayarda

mevcut mikrofon özelliklerini açarak virüsün etkileşim halinde olduğu programcıya ses kayıtları başta olmak üzere tüm bilgisayar verilerini gönderebilmekteydi. İran Petrol Bakanlığı virüsten kimin sorumlu olduğunu bilmediklerini ifade etse de İsrail Başbakan Yardımcısı Moşe Yalon'un İran'ın nükleer çalışmalarını bertaraf etmek için siber saldırıların olabileceğini söylemesi olayın failinin kim/kimler olduğunu özetler nitelikte olmuştur (Köylü, 2012).

İran siber dünyada da etkinliği artırmak istemiş ve ilk büyük saldırısını Ağustos 2012 tarihinde gerçekleştirmiştir. Suudi Arabistan'a ait petrol şirketi Saudi Aramco'yu hedef alan siber saldırılar başlatılmıştır. Saldırıların sonucunda kuruma ait bilgisayarların yarısı (30 bin adet bilgisayar) devre dışı bırakılmış ve bilgisayarlardaki mevcut veriler silinmiştir. Ancak verilerin kopyalanıp kopyalanmadığı bilgisine ulaşılamamıştır. Hemen ardından Katar'ın doğalgaz şirketi Ragas da bu virüsün hedefi olmuştur. Aramco kadar ciddi etkileri olmamakla birlikte Ragas da bu virüsten büyük oranda zarar görmüştür. İran resmi bir açıklama yapmamış olsa da virüsün içeriği ve saldırı zamanlaması İran'ı işaret etmektedir. Virüsün kodlarında İran'ın kutsal değerlerine ait ifadeler geçmekte olup saldırının Kadir gecesi düzenlenmesi ve aynı zamanda saldırıyı gerçekleştiren grubun kendilerine "Hz. Ali'nin Kılıcı" ismini takmış olması gibi pek çok unsur şüpheleri doğrudan İran'a yöneltmektedir. Virüsün bulaştığı bilgisayarlarda ise yanmış bir Amerikan bayrağı resmi bulunmakta idi (Çelik, 2014).

Bu olaydan 4 yıl sonra Aralık 2016 tarihinde yine aynı firmalar bu virüsün saldırısına uğramış ancak verilen zararlar ilgili bir açıklama yapılmamıştır. Bu defa bilgisayarlara ise boğularak hayatını kaybeden 4 yaşındaki Suriyeli mülteci Aylan Kurdi'nin fotoğrafı konulmuştur (Çelik, 2016).

İran'da çok güçlü bir siber saldırı ekibinin olduğu bilinmekle beraber İran'da da Rusya'da olduğu gibi ordu içerisinde resmi bir yapılanma mevcut değildir. İran resmi makamlarınca bu konu ile ilgili bir açıklama yapılmazken son yıllarda İranlı hacker sayısındaki artış dikkat çekmiştir. APT33 isimli bir hacker grubunun İran'ın resmi siber ordusu olduğu iddia edilmektedir; ancak İran tarafından henüz resmi bir açıklama yapılmamıştır. Genellikle havacılık ve enerji sektöründe faaliyet gösteren Suudi ve Amerikan kuruluşlarını hedef alan APT33 grubunun son olarak, Amerikalı mail servisi Microsoft Outlook'u saldırı düzenlendiği bilinmektedir. Amerika Birleşik Devletleri Siber Komutanlığı ise güvenlik açıklamaları konusunda endişelerini aktarmış ve güvenlik açıklarından yararlanarak sızmaların genellikle İran destekli APT33 tarafından gerçekleştirildiğini belirtmiştir (Yinanç, 2019).

#### **d) Türkiye**

Türkiye'de de uzun zamandır siber alana yönelik çalışmalar hız kazanmış ve bir siber komutanlık kurulmasına yönelik çalışmalar yapılmıştır. Ancak henüz kara, deniz ve hava kuvvetlerine bir kuvvet komutanlığı olarak siber komutanlık eklenmemiştir. 2012 yılında TSK Siber Savunma Merkezi Başkanlığı kurulmuştur. Bu kurum 2013 ta-

rihinde “TSK Siber Savunma Komutanlığı”na dönüştürülmüştür. Ancak Siber Savunma Komutanlığı'nın amacı Türk Silahlı Kuvvetleri'nin ve Genelkurmay Başkanlığı'nın internet sitelerini korumak ve olası saldırıları engellemek olarak tanımlanmıştır. Yani bir sanal muharebeden ziyade savunma işlevi ile donatılmıştır. TSK yetkilileri nükleer saldırı tehditlerinden sonra siber saldırıların dünyadaki en büyük ikinci tehdit unsuru haline geldiğini belirtmiş ve NATO ile müşterek halde siber savunmanın gerçekleştirildiğini belirtmiştir (Uslu, 2016). Ardından Cumhurbaşkanlığı Savunma Sanayi Başkanlığı bünyesinde Siber Savunma Merkezi Projesi için çalışmalara başlanmış ve 2018'in ilk yarısında ordunun gerekli siber donanıma sahip olması için gereken faaliyetlerin gerçekleştirilmesi planlanmıştır (T.C. Savunma Sanayii Başkanlığı , 2016). Ancak istenen başarı sağlanamamıştır.

Türkiye’de henüz silahlı kuvvetlere bağlı bir siber bir kuvvet komutanlığı bulunmamakla birlikte bir siber ordu kurulması için bakanlıklarda da çalışmalar gerçekleştirilmiştir. 2013 yılında başta Ulaştırma Denizcilik ve Haberleşme Bakanlığı'na bağlı olarak kurulan, ardından Bilgi Teknolojileri ve İletişim Kurumu bünyesinde devam eden Ulusal Siber Olaylara Müdahale Merkezi (USOM) kurulmuştur. Kurum, siber saldırılarının tespit ve bertaraf edilmesinde kamu ve özel kişiler arası koordinasyonun sağlanmasında görev yapmaktadır. Ayrıca 2017 yılında yaptığı bir konuşmada Ulaştırma, Denizcilik ve Haberleşme Bakanı Ahmet Arslan tarafından Türkiye'nin çeşitli devlet kurumlarında 13 bin beyaz şapkalı hackerin görev yaptığı ifade edilmiştir (Babacan, 2017). Bununla beraber 2013 yılında Emniyet Genel Müdürlüğü bünyesinde Siber Suçlarla Mücadele Daire Başkanlığı kurulmuştur. Bu birimin öncelikli amacı internette ve internet vasıtasıyla gerçekleşen suçlarla mücadele olarak tanımlanmıştır. Siber ordu niteliği taşımasa da siber suçlara karşı caydırıcılık sağlaması açısından faydalı bir girişim olarak görülmektedir.

Türkiye'ye yönelik siber saldırılar genellikle bankacılık veya hizmet sektöründeki firmalara yönelik olmuştur. 28 Ekim 2019 tarihinde Garanti BBVA'ya yönelik bir takım siber saldırılar gerçekleşmiştir. Kurum yöneticileri müşterilerine ait bilgilerin çalındığını; yalnızca internet servislerinde bir takım yoğunlukların yaşandığını dile getirmişlerdir (Hürriyet, 2019).

26 Aralık 2019 tarihinde ise Kişisel Verileri Koruma Kurumu, Türkiye'nin en büyük e-alışveriş sitelerinden biri olan n11.com'dan üyesi olan 832 adet müşterinin e-posta adresinin çalındığını duyurmuştur. İnternet ortamında yapılan alışverişlerde kişilerden cep telefonu numaraları, ev adresleri, bazı özel bilgilerinin istendiği düşünüldüğünde oldukça büyük oranda bir veri sızıntısı riskinin olduğu öngörülmektedir (KVKK, 2019).

Tüm bu sebeplerle Türkiye'nin profesyonel anlamda bir siber komutanlığa sahip olması bir zorunluluk arz etmektedir. Özellikle son zamanlarda gerçekleştirilen saldırılarda nükleer santrallerin ve enerji santrallerinin başlıca hedefler olduğu görülmektedir. Türkiye nükleer enerji konusunda henüz yeterli bilgi birikimine sahip olmamakla birlikte hali hazırda Sinop ve Mersin'de iki adet nükleer santral yapım projesine sahiptir. Nükleer santrallerin Türkiye'ye için getirilerinin oldukça fazla olacağı düşünülmektedir.

Bundan ötürü olası saldırılar karşısında da Türkiye'nin kendisini korumak ve gerekli caydırıcılığı sağlamak adına ordu bünyesinde bir yapılanmaya gitmesi konusunda zorunluluk doğmaktadır. Sadece nükleer enerji değil günümüzde gelişen elektrikli otomobillerden yapay uydulara kadar pek çok sistem siber tehdit altındadır. Örneğin, Chris Roberts isimli bir siber güvenlik uzmanı NASA'nın internet sistemlerine girerek buradan Uluslararası Uzay İstasyonu'na giriş protokollerini elde edebilmiştir (Tolga Yanık, 2019). Türkiye'nin de son yıllarda Göktürk uyduları aracılığı ile bu alanda yatırım yaptığı düşünüldüğünde yine bir korunma ihtiyacı ortaya çıkmaktadır.

### e) Sonuç

Hem ülkemizde hem de dünyada artık önü alınamaz bir şekilde teknolojiyle bütünleşme durumu yaşanmaktadır. Bunun yararları gündelik hayatın pek çok noktasında kendini göstermektedir. Örneğin, akıllı telefonlar ile binlerce kilometre mesafedeki insanlarla sesli ve görüntülü iletişim kurulabilmekte veya onlarca kitabın içerikleri küçük cihazlara yüklenerek her an ulaşılabilir olmaktadır. Teknolojinin faydaları oldukça uzun bir liste oluşturacaktır. Aynı şekilde teknolojinin zararları ve yarattığı riskler azımsanmayacak bir miktara ulaşmaktadır. Örneğin, 2019 yılında gerçekleştirilen bir araştırmada insanların %67'sinin online alışverişi tercih ettiği gözlenmiştir (Sakarya & Yardımcı, 2019). Böylesine büyük bir rakam dolandırıcılık ve hırsızlık yöntemlerinin de sanal ortamlara taşınmasına yol açmıştır. Bunun yanında sosyal medya kullanımı beraberinde insanların özel bilgilerinin istismarı gibi durumları da gündeme getirmiştir. Fakat yaratacağı büyük olumsuzluklar ve etki alanının genişliğinden ötürü devletler seviyesinde yaşanan siber güvenlik sorunları bireysel risklerden daha öncelikli olmaktadır. ABD tarafından İranlı General Kasım Süleymani'ye düzenlenen suikast sonrası dünya gündeminde ilk dillendirilen konu İran'ın siber bir saldırı hazırlığı yapıp yapmadığı olmuştur (Seldin, 2020). Bir savaş senaryosunda dahi ilk ortaya atılan durum fiziki saldırı değil sanal bir saldırı durumu olmuştur. Bu durum dahi gelecekte siber saldırıların ve siber savaşların rolüne dair bir ipucu niteliğindedir.

Sonuç olarak savaş paradigmasında geleneksel orduların halen en etkin güç olmasının yanında bu ordulara aynı zamanda siber orduların da eklenmesi bir zorunluluk haline gelmektedir. Devletlerin, kurumların ve kişilerin internet üzerinde de bir mevcudiyeti bulunmaktadır ve tıpkı fiziksel olarak bunların korunması gerektiği gibi sanal anlamda da korunması bir gereklilik arz etmektedir. Bu bakımdan özellikle ülkemiz bünyesinde geç kalınmadan gerekli donanım sağlanmalı ve etkin bir siber ordu kurulmasına yönelik çalışmalara başlanmalıdır. Ancak siber ordu kurmak tek başına yeterli bir girişim olmayacaktır. Teknoloji ve insan kaynağı bakımından sürekliliğin sağlanması, kullanılan teknolojinin millileştirilmesi, bu alanda faaliyet gösteren kamu kurumlarının ve özel sektör kuruluşlarının koordine edilmesi, yükseköğrenim seviyesinde AR-GE faaliyetlerinin teşvik edilmesi siber orduların kurulması ve güçlendirilmesi için stratejik öneme sahip adımlar olarak öne çıkmaktadır.

---

**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 çalışmanın yazarlarına aittir.

**Yazar Katkıları:** Meryem Orak çalışmanın tamamında tek başına katkı sunmuştur.

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

**Teşekkür:** Yayın sürecinde katkısı olan hakemlere teşekkür ederim.

**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:** Meryem Orak has contributed to all parts and stages of the study

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

**Acknowledgement:** I would like to thank the referees who contributed to the publication process.

## Kaynakça

Aksan, S. (2019, Haziran 20). *Yeni Şafak*. Aralık 31, 2019 tarihinde <https://www.yeni-safak.com/gundem/iranin-abd-ucagini-dusurmesi-nasil-sonuclar-doguracak-3495626> adresinden alındı

Babacan, N. (2017, Mayıs 17). *Hürriyet*. Ocak 17, 2020 tarihinde <http://www.hurriyet.com.tr/gundem/13-bin-hackerla-siber-ordu-40461432> adresinden alındı

Baki, O. (2019, Aralık 23). *Webtekno*. Aralık 31, 2019 tarihinde <https://www.webtekno.com/rusya-kuresel-internet-agiyla-baglantisini-kesti-h82374.html> adresinden alındı

Copeland, B. J. (2004). *The Essential Turing*. New York: Oxford University Press.

Çelik, M. (2014, Ağustos 29). *Siber Bülten*. Aralık 31, 2019 tarihinde <https://siberbulten.com/makale-analiz/turkiyenin-kacan-son-firsati-suudi-siber-komutanligi/> adresinden alındı

Çelik, M. (2016, Aralık 26). *Siber Bülten*. Aralık 31, 2019 tarihinde <https://siberbulten.com/uluslararası-iliskiler/shamoon-kabusu-4-yil-sonra-geri-dondu/> adresinden alındı

Darıcı, A. B., & Özdal, B. (2017). Rusya Federasyonu'nun Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi. *Bilig*, 121-146.

DARICILI, D. A. (2017). *Amerika Birleşik Devletleri'nin Siber Kapasitesinde Rol Oynayan Kurumsal Yapı İlanlarının Analizi*. Bursa: Dora Basım Yayım Ltd. Şti.

Köylü, H. (2012, Mayıs 12). *Deutsche Welle* Türkçe. Aralık 31, 2019 tarihinde <https://www.dw.com/tr/en-tehlikeli-vir%C3%BCs-flame/a-15988868> adresinden alındı

Lukasik, S. J. (2011). Why the Arpanet Was Built. *IEEE Computer Society*, 4-21.

Sakarya, G., & Yardımcı, N. (2019, Mart 29). *TRT Haber*. Ocak 16, 2020 tarihinde <https://www.trthaber.com/haber/yasam/turkiye-alisverisi-internette-mi-yoksa-magazadan-mi-yapiyor-410153.html> adresinden alındı

Saygun, M. (2017, Ocak 17). *Cybermag*. Aralık 31, 2019 tarihinde <https://www.cybermagonline.com/rus-siber-ordusu-suarilerini-nasil-topluyor> adresinden alındı

Seldin, J. (2020, Ocak 11). *Voice of America*. Ocak 16, 2020 tarihinde <https://www.amerikaninsesi.com/a/iranin-siber-saldirilar%C4%B1na-karsi-abd-alarmda/5241558.html> adresinden alındı

Sözen, M. (2019, Eylül 2). *Siber Bülten*. Aralık 31, 2019 tarihinde <https://siberbulten.com/uluslararasi-iliskiler/abd-siber-saldiriyla-iranin-kritik-veri-tabanini-sildi/> adresinden alındı

*Sputnik News*. (2019, Haziran 2). Ocak 16, 2020 tarihinde <https://tr.sputniknews.com/rusya/201906021039225374-rus-egitim-denetim-kurumu-na-siber-saldiri/> adresinden alındı

T.C. Savunma Sanayii Başkanlığı. (2016, Temmuz 24). <https://www.ssb.gov.tr/Website/contentlist.aspx?PageID=1083&LangID=1> adresinden alındı

Tolga Yanık, M. T. (2019, Nisan 27). *Anadolu Ajansı*. Ocak 31, 2020 tarihinde <https://www.aa.com.tr/tr/bilim-teknoloji/canim-sikildi-nasayi-hackledim/1463872> adresinden alındı

Uslu,S. (2016, Haziran 4). *Anadolu Ajansı*. Ocak 17, 2020 tarihinde <https://www.aa.com.tr/tr/turkiye/turk-ordusunun-yeni-kuvveti-siber-savunma/584061> adresinden alındı

Yayla, M. (2013). HUKUKİ BİR TERİM OLARAK "SİBER SAVAŞ". *TBB Dergisi*, 178-202.

Yazıcı, M. (2015, Mayıs 23). *TUIC Akademi*. Aralık 31, 2019 tarihinde <http://www.tuicakademi.org/stuxnet-virusu-iran-a-nasil-etki-etti/> adresinden alındı

Yinanç, B. (2019, Temmuz 8). *Hürriyet*. Aralık 31, 2019 tarihinde <http://www.hurriyet.com.tr/teknoloji/iranli-hacker-grubu-outlook-uzerinden-kurbanlarini-vuruyor-41267003> adresinden alındı



## DERGİNİN AMAÇ VE KAPSAMI

Yirminci yüzyılda hızla gelişen bilgi ve iletişim teknolojileri alanı başta akademik araştırmacılardan başlayarak uygulamacılara doğru ilgi odağı haline gelmiştir. Bu kapsamda yayın hayatına atılan dergimizin amacı, Kamu Yönetimi ve Teknoloji konusunda çalışan akademisyen ve uygulamacıları paylaşım yapacağı ve bu alanda geleceğin dünyasını inşa etmeye yardımcı olacak bir akademik dergi oluşturmaktır. Binaenaleyh, kamu yönetimi ve teknoloji alanı başta olmak üzere, ilgili sosyal bilimler çalışmalarının alanyazına kazandırılması amaçlanmaktadır. Ek olarak bu dergi ile İktisadi ve İdari Bilimler, Siyaset Bilimi ve Uluslararası İlişkiler vb. beşeri bilimler bünyesindeki farklı disiplinlerden ortak bir akademik platform oluşturulmak istenmektedir. Bilgi ve değer üretilmesine katkı vermek; akademik yayıncılıkta referans kaynağı olmak; bilgi ve iletişim teknolojileri, kamu yönetimi ve sosyal alanda sürdürülebilirliği incelemek ve kamu yönetiminde kullanılan teknolojiler, kamu yönetiminin daha etkin, verimli ve hızlı olmasını sağlayacak yeni teknolojileri içeren çalışmaları gündeme getirmek derginin hedefidir. Kamu Yönetimi Teknoloji Dergisi (KAYTEK) editör kurulu, yayın hayatına başladığı günden bu yana hedeflerin ancak ilkeli yayıncılık politikası, bilim ve ifade özgürlüğüne saygı, bilim ve araştırma etiği ilkelerine koşulsuz bağlılık ile gerçekleşeceğine inanmaktadır.

1. Kamu Yönetimi ve Teknoloji (KAYTEK), Haziran ve Aralık ayları olmak üzere yılda iki kez yayınlanan ulusal hakemli bilimsel bir dergidir. Dergi gerektiğinde özel sayılar çıkarabilecektir.
2. Yayınlanmak üzere gönderilen çalışmaların başka bir yerde yayınlanmamış veya yayınlanmak üzere gönderilmemiş olması gerekmektedir. Derginin yayım dili Türkçe ve İngilizce'dir.
3. Dergide, sosyal bilimler alanındaki tüm konu başlıklarına sahip bilimsel makaleler kabul edilmektedir. Dergimizde belirtilen sosyal bilim dallarında teorik ve deneysel dayalı çalışmalar, kitap incelemeleri, açıklamalı bibliyografiler ve derleme makaleler de yer alabilecektir.

4. Kamu Yönetimi ve Teknoloji Dergisi, açık erişim politikasını benimsemiş ve akademik özgürlüğü savunan bir yayım alanıdır. Yayın öncesinde, sürecinde ya da sonrasında yazarlardan ücret talep edilmez. Yazarlara bir telif ücreti ödenmez.
5. Yayınlanmak üzere dergiye gönderilen yazılar, yayın kurulu tarafından ilk değerlendirilmesi yapıldıktan sonra hakemlere gönderilir. Yayın kurulu hakemlerden gelecek rapor doğrultusunda yazının basılmasına, yazardan makalesinde düzeltme istenmesine ya da basılmamasına karar verir. Yayım kararı yazar(lar)a bildirilir.
6. Yazarlar makalelerinin başlığını, ad, soyadı, unvan, bağlı oldukları kurum adı, posta adresi, telefon ve e-posta adreslerini ayrı bir kâğıda yazarak bir kapak sayfası hazırlayıp makaleleri ile birlikte göndermelidir. Hakemlere gönderilecek metinde makalenin başlığı, makale metni, Türkçe ve İngilizce özetler bulunmalı, kimlik bilgileri yer almamalıdır.
7. Sisteme yüklenen her bir makalenin iThenticate, Turnitin gibi intihal tarama programı aracılığı ile taranarak sisteme yüklenmesi gerekmektedir. Tarama sonucu %20'nin üzerinde olan makaleler RET edilmektedir. Makaleler en az iki hakem tarafından kör hakemlik uygulamasıyla değerlendirilmektedir.
8. Dergide yayımlanması istenilen metinlerin, word veya open office gibi döküman biçiminde ve DergiPark sistemi üzerinden (<https://dergipark.org.tr/tr/pub/kaytek>) başvurusu yapılmalıdır.
9. ULAKBİM/TR Dizin'in 2020 yılında zorunlu kıldığı "etik kurul kararı gerektiren klinik ve deneysel insan ve hayvanlar üzerindeki çalışmalar için ayrı ayrı etik kurul onayı alınmış olmalı, bu onay makalede belirtilmeli ve belgelendirilmelidir." kriteri çerçevesinde insan ve hayvan örnekleme olan nitel ve nicel saha araştırmaları için etik kurul onayı makaleye ek olarak verilmeli ve makalenin yöntem kısmında belge tarih ve sayısı belirtilerek etik kurallara uyulduğu ifade edilmelidir.
10. Dergiye gönderilen çalışmaların Araştırma ve Yayın Etiğine uygunluğuna dikkat edilmektedir. ICMJE (International Committee of Medical Journal Editors) tavsiyeleri ile COPE (Comittee on Publication Ethics)'nin editör ve yazarlar için uluslararası standartlara uygunluk aranmaktadır.
11. Yazım ve biçim kurallarına uygun olmayan makaleler hakeme gönderilmez ve basılmaz.
12. Düzeltme metnini 30 gün içerisinde göndermeyen yazarların metinleri reddedilir.

## ETİK İLKELER VE YAYIN POLİTİKASI

Kamu Yönetimi ve Teknoloji Dergisi (KAYTEK) kamu yönetimi ve bilgi ve iletişim teknolojileri başta olmak üzere, ilgili sosyal bilimler çalışmalarını yayımlamak amacıyla kurulmuştur. Kamu Yönetimi ve Teknoloji Dergisinde yer alan etik görev ve sorumluluklar oluşturulurken açık erişim olarak Committee on Publication Ethics (COPE) tarafından yayınlanan rehberler ve politikalar dikkate alınmıştır. Aşağıda yazar, hakem ve editörlerin uyması gereken etik ilke ve kurallara yer verilmiştir.

### Yazarlara İlişkin Etik İlke ve Kurallar

- Kamu Yönetimi ve Teknoloji Dergisi'ne gönderilen makalelerin kamu yönetimi ve bilgi ve iletişim teknolojileri başta olmak üzere ilgili sosyal bilimler alanlarında özgün çalışmalar olması gerekmektedir.
- Makalelerde yararlanılan tüm kaynaklara ilişkin doğru ve uygun bir şekilde kaynak gösterimi gerekmektedir.
- Dergiye gönderilen makalelerin başka bir dergiye gönderilmemiş olması ve KAYTEK Telif Hakkı Devir Formu doldurulması gerekmektedir.
- Makaleye fikren katkıda bulunmayan kişilere yazar olarak yer verilmemelidir.
- Gönderilen makaleye ilişkin çıkar çatışmaları belirtilerek nedeni açıklanmalıdır.
- Yazarların, hakem sürecindeyken çalışmalarına ilişkin ham verileri editörler kuruluna iletmesi istenebilir, bu durumda yazarların ham verilerini editörler kuruluyla paylaşmaları beklenebilir. Yazarlar, yayımlanan bir makaleye ilişkin verileri 5 yıl süreyle saklamakla yükümlüdürler.
- Yazarlar çalışmalarında bir hata tespit ettiklerinde editörü ve editörler kurulunu bilgilendirmelidir. Düzeltme veya geri çekme süreçlerini editörler ile iş birliği içerisinde gerçekleştirmelidirler.

## Hakemlere İlişkin Etik İlke ve Kurallar

Kamu Yönetimi ve Teknoloji Dergisi'ne gönderilen tüm makaleler çift taraflı kör hakemlik süreci ile değerlendirilmektedir. Çift taraflı kör hakemlik, yansız, nesnel ve bağımsız bir değerlendirme sürecinin sağlanabilmesi için yazarların hakemlerden, hakemlerin de yazarlardan gizli tutulması anlamına gelmektedir. Hakemlere makaleler değerlendirilmek üzere Dergipark sistemi üzerinden iletilmektedir. Hakemler, değerlendirdikleri makalenin KAYTEK'in temel yayın alanlarına katkısını ve makalenin yayımlanabilir olup olmadığına ilişkin kararlarını kendilerine sistem üzerinden iletilen formu doldurmak suretiyle gerçekleştirmektedirler. Kamu Yönetimi ve Teknoloji Dergisi'nde hakem olarak görev yapan akademisyenlerin etik sorumlulukları şunlardır:

- Hakemlerin uzmanlık alanlarına ilişkin makalelere hakemlik yapmaya özen göstermeleri gerekmektedir.
- Hakemler çıkar çatışması olabilecek çalışmalarını değerlendiremeyeceklerini editörlere iletmelidirler.
- Hakemler makaleleri tarafsız olarak değerlendirmelidirler.
- Hakemlerin değerlendirdikleri makalelere ilişkin çevrimiçi Makale Değerlendirme Formunu doldurmaları gerekmektedir. Hakemler değerlendirdikleri makaleye ilişkin görüşlerini makale değerlendirme formunda gerekçeli olarak ifade etmelidirler.
- Hakemler makale değerlendirmelerinde yazarları rencide edecek bir dil kullanmaktan kaçınmalı, aksine önerilerinde kullandıkları üslubun bilimsel olması gerekmektedir. Olumsuz bir durum ile karşılaşılması halinde editörler hakem ile iletişime geçerek yorumlarını yeniden gözden geçirmeleri ve düzeltmelerini talep edebilirler.
- Hakemlerin kendilerine verilen süre içerisinde etik sorumluluklara uyarak değerlendirmelerini tamamlamaları gerekmektedir.

## Editör(ler)e İlişkin Etik İlke ve Kurallar

- Editörlerin Committee on Publication Ethics (COPE) tarafından yayınlanan olduğu 'COPE Dergi Editörleri için Etik Davranışlar ve En İyi Uygulamalar Kılavuzu'nda yer alan etik sorumlulukları yerine getirmekle yükümlüdürler. Editörlerin etik görevleri ve sorumlulukları aşağıdaki gibidir:
- Editör derginin niteliğinin artırılması ve gelişimine katkıda bulunmak için çaba sarf etmekle yükümlüdür.
- Editörün, yazarların ifade özgürlüğünü desteklemesi gerekmektedir.
- Editörün, dergide hakem değerlendirmesinin gerekli olmadığı bölümlerin (editö-

re mektup, davetli yazılar, konferans duyuruları vb.) açıkça belirtildiğinden emin olması gerekmektedir.

- Editörün yayımlanan makalelerin dergi okuyucularının bilgi ve becerileriyle uyumlu olabilmesi için çaba sarf etmesi gerekmektedir.
- Editör, hakemlerin bilgi ve uzmanlıklarına uygun makaleleri değerlendirmelerini istemelidir. Böylece makalelerin alanında uzman kişilerce uygun bir şekilde değerlendirilmesi sağlanmalıdır.
- Editör, hakemlerin bir makaleyi değerlendirmeden önce makaleye ilişkin çıkar çatışmaları bulunmadığını belirtmelerini talep etmekte yükümlüdür.
- Editörün hakem değerlendirme sürecine ilişkin gerekli tüm bilgileri ve hakemlerden yapması beklenenleri hakemlere iletmesi gerekmektedir.
- Editör, hakem değerlendirme sürecinin çift taraflı kör hakemlik ile sürdürüldüğünden emin olmalı ve yazarlara hakemleri, hakemlere de yazarları ifşa etmemelidir.
- Editör, hakemleri zamanlama ve performanslarına göre değerlendirmelidir.
- Editör, hakemlere ilişkin bir veri tabanı oluşturmalı ve hakemlerin performansına göre veri tabanını güncellemelidir.
- Editör, kaba ve kırıcı yorumlarda bulunan ya da geç dönen hakemleri hakem listesinden çıkarmalıdır.
- Editör, hakem listesini hakemlerin uzmanlık alanlarına göre sürekli yenilemeli ve genişletmelidir.
- Editör, yazarlara kendilerinden ne beklendiğine ilişkin yayım ve yazım kuralları ile örnek şablonu sürekli güncellemelidir.
- Editör dergiye gönderilen makaleleri dergi yazım kuralları, çalışmanın önemi, özgünlüğü açısından değerlendirmeli ve makaleyi ilk gönderim sürecinde reddetme kararı alırsa, yazarlara bunun nedenini açık ve yansız bir şekilde iletmelidir. Bu süreçte, makalenin dilbilgisi, noktalama ve/veya yazım kuralları (kenar boşlukları, uygun şekilde referans gösterme, vb.) açısından tekrar gözden geçirilmesi gerektiğine karar verilirse, yazarlar bu konuda bilgilendirilmeli ve gerekli düzeltmeleri yapabilmeleri için kendilerine zaman tanınmalıdır.
- Makalelerde gönderim ve yayıma kabul tarihleri yer almalıdır.
- Yazarların makalelerinin durumuna ilişkin bilgi talebi olduğunda çift taraflı kör hakemlik sürecini bozmayacak şekilde yazarlara makalelerinin durumuna ilişkin bilgi verilmelidir.

- Dergiye yayınlanmak üzere gönderilen makalelerde son karar editör kuruluna aittir. Editör kurulu objektif ve akademik kriterler dahilinde dergide yayınlanacak makaleleri belirlemekle yükümlüdür.
- Editör, editörler kurulu üyelerine yayım ve yazım kurallarını iletmeli ve kendilerinden beklenenleri açıklamalıdır.
- Editör, editörler kurulu üyelerine yayım ve yazım kurallarının en güncel halini iletmelidir.
- Editör, editörler kurulu üyelerini değerlendirmeli ve derginin gelişimine aktif olarak katılım gösterecek üyeleri editörler kuruluna seçmelidir.
- Editör, editörler kurulu üyelerini aşağıda yer alan rolleri ve sorumluluklarına ilişkin bilgilendirmelidir
  - Derginin gelişimini desteklemek
  - Kendilerinden istendiğinde uzmanlık alanlarına ilişkin derlemeler yazmak
  - Yayım ve yazım kurallarını gözden geçirmek ve iyileştirmek
  - Derginin işletiminde gerekli sorumlulukları yerine getirmek

### **İntihal ve Etik Dışı Davranışlar**

Kamu Yönetimi ve Teknoloji Dergisi'ne gönderilen tüm makaleler basılmadan önce herhangi bir intihal yazılım programı ile taranmaktadır. Benzerlik oranı %20 ve altında olan makaleler yayına kabul edilir. Bu oranı aşan makaleler ayrıntılı olarak incelenir ve gerekli görülürse gözden geçirilmesi ya da düzeltilmesi için yazarlara geri gönderilir, intihal ya da etik dışı davranışlar tespit edilirse yayımlanması reddedilir.

Aşağıda etik dışı bazı davranışlar listelenmiştir:

- Çalışmaya fikren katkıda bulunmayan kişilerin yazar olarak belirtilmesi,
- Çalışmaya fikren katkıda bulunan kişilerin yazar olarak belirtilmemesi,
- Makalenin yüksek lisans/doktora tezinden ya da bir projeden üretilmişse bunun belirtilmemesi,
- Dilimleme yapılması yani, tek bir çalışmadan birden fazla makale yayımlanması,
- Gönderilen makalelere ilişkin çıkar çatışmalarının bildirilmemesi,
- Çift taraflı kör hakemlik sürecinin deşifre edilmesi.

## YAZARLAR İÇİN NOTLAR

1. KAYTEK hakemli bir dergidir ve Haziran ve Aralık aylarında olmak üzere yılda iki kez yayımlanır. KAYTEK Dergisinde yayınlanacak çalışmalar “Kamu Yönetimi ve Teknoloji” temalı olmalıdır.
2. Derginin yayım dili Türkçe ve İngilizcedir.
3. KAYTEK Dergisinde yayınlanan tüm yazıların yayım hakları Kamu Bilişimcileri Derneğine devredilmiş olur.
4. Gönderilen yazılar özgün olmalı, başka bir yerde yayımlanmamış ya da yayımlanmak üzere başka bir yere gönderilmemiş olmalıdır.
5. Yayımlanmak üzere dergiye gönderilen yazılar, yayım kurulu tarafından ilk değerlendirmesi yapıldıktan sonra hakemlere gönderilir. Hakemlerden gelecek rapor doğrultusunda yazının basılmasına, yazardan makalesinde düzeltme istenmesine ya da basılmamasına yayım kurulu karar verir. Yayım kararı yazar(tar)la bildirilir.
6. Yazarlar makalelerinin başlığını, ad, soyadı, unvan, bağlı oldukları kurum adı, posta adresi, telefon ve e-posta adreslerini ayrı bir kâğıda yazarak bir kapak sayfası hazırlayıp makaleleri ile birlikte göndermelidir. Hakemlere gönderilecek metinde makalenin başlığı, makale metni, Türkçe ve İngilizce özetler bulunmalı, kimlik bilgileri yer almamalıdır.
7. Makaleler MS Word veya Open Office belgesi olarak gönderilmelidir. Makaleler yalnızca derginin <https://dergipark.org.tr/tr/pub/kaytek> adresinde bulunan DergiPark gönderme sistemi üzerinden gönderilmelidir. Başka bir mecradan gönderilen yazılar değerlendirmeye alınmayacaktır.
8. Yazım ve biçim kurallarına uygun olmayan makaleler hakeme gönderilmez ve basılmaz.
9. Her makalede, ana başlığın hemen altında, makalenin amacı ve önemini içeren biri Türkçe biri İngilizce olmak üzere 150-200 kelimeyi aşmayan öz/abstract yer almalıdır. “Öz”lerin altında, beş kelimeyi aşmayan anahtar sözcükler/keywords bulunmalıdır. Kısacası makaleler, Ana Başlık, Öz, Anahtar Sözcükler, Abstract, Keywords, Makale Metni, Notlar ve Kaynakça sırası ile kaleme alınmış olmalıdırlar.
10. Makaleler 8.000 kelimeyi geçmemeli, A4 ebadındaki Microsoft Office Word dosyasına 1.5 aralıklı, soldan 3.5 cm, sağdan 3 cm, üstten 3.5 cm ve alttan 3 cm olacak şekilde düzenlenmelidir.
11. Metin 10 punto büyüklükte DIN Pro yazı tipi ile yazılmalıdır. Makale başlığı 16 punto, DIN Pro yazı tipi, kalın ve ana metinden ayrı olmalıdır. Alt başlıklar 12 punto, DIN Pro, kalın ve metinden ayrı olmalıdır. İkincil alt başlıkların altındaki alt başlıklar 10 punto, DIN Pro, kalın ve italik olmalı ve paragrafın ilk cümlesinin başında yer almalı ve bir nokta ile sonlanmalıdır.

12. Bütün izelge, grafik ve diyagramlara Őekil denilmeli ve birbirini izleyen numaralar verilmelidir. Her Őekil ve tabloya bir numara verilmeli ve numaradan sonra baŐlıđı yazılmalıdır.
13. Kaynaklara gnderiler dipnot biiminde olmamalı, ilgili kaynak(lar) metinde ayrıca iine alınarak (yazar soyadı, yayım yılı: sayfa numarası) biiminde gsterilmelidir.
14. Kaynaklara gndermeler, metin iinde aılacak aralarla yapılmalıdır. Ara iin-deki sıra Őyle olmalıdır:  
.....Őeklinde zetlenmiŐtir (Ergun, 2004).  
.....belirtilmiŐtir (Leblebici, 2004: 210-215).  
.....Babaođlu (2017a: 15-20) ileri srmektedir.  
.....(Yıldız vd., 2012: 126-153).  
.....(Babaoglu ve Demirciođlu, 2011: 399-432).
15. Metin iindeki gnderiler ve metne iliŐkin ek aıklamalar dipnotlarda gsterilebilir.
16. Metinde gnderme yapılan bütün kaynaklar, kaynakada belirtilmeli; gnderme ya-pılmayan kaynaklar, kaynakaya konmamalıdır. Kaynaklar, ayrı bir sayfada alfabetik sırayla yazılmalıdır. Dergi ve derlemelerdeki makalelerin sayfa numaraları kesinlikle belirtilmelidir. Kaynakada, aŐađdaki rneklenen biim kurallarına uyulmalıdır:

#### **Kitaplar:**

MıŐıođlu, C. (1988) Trkiye’de ađdaŐ Kamu Ynetimi đretiminin BaŐlangı Yılları, Ankara: Ankara niversitesi SBF.

#### **Dergiler:**

Yıldız, M.; Babaođlu, C. & Őahin, B. (2016) “Kamu Politikasını Trk İdare Tarihi zerin-den alıŐmak”, Hacettepe niversitesi IIBF Dergisi, 34(2), s. 133-158.

#### **Derlemeler:**

Allison, G. (2006) “Emergence of Schools of Public Policy: Reflections by a Founding Dean”, i. The Oxford Handbook of Public Policy, (Ed.) Robert E. Goodin, Michael Moran, and Martin Rein, Oxford: OUP Oxford. s. 58-79.

#### **Elektronik Kaynaklar:**

Trkiye Cumhuriyet Merkez Bankası (2014), Kredi Kartı İŐlemlerinde Uygulanacak Aza-mi Faiz Oranları, <http://www.tcmb.gov.tr/>, EriŐim Tarihi/Access Date: 15.09.2014.



## NOTES FOR CONTRIBUTORS

1. KAYTEK is a refereed journal published twice a year, June and December. Studies which will be published in the Journal of KAYTEK must be related to "Public Administration and Technology".
2. Manuscripts should be written in Turkish or English.
3. Copyrights of the articles appearing in the KAYTEK Journal belong to the Kamu Bilişimcileri Derneği.
4. Articles submitted should be original contributions and should not be published elsewhere or should not be under consideration for any publication at the same time.
5. Manuscripts submitted to the journal will first be viewed by the Editorial Board then forwarded to the referees. In line with the evaluation of the referees, Editorial Board will make the final decision, either in favor or against publication, or return the manuscript back to the author for any revision required by the referees. Author(s) will be informed of the publication decision.
6. Authors should include a separate title page with their name, institutional affiliation, full address and other detailed contact information. The title of the article alone should appear on the top of the first page of the manuscript.
7. Complete manuscripts should be submitted as an MS Word or Open Office document. Manuscripts can only be submitted through the journal's DergiPark submission system, available at <https://dergipark.org.tr/tr/pub/kaytek>. Manuscripts submitted via any other medium will not be evaluated.
8. Authors are responsible for ensuring that their manuscripts conform to the journal style. The editors will not undertake retyping of manuscripts before publication.
9. After the manuscript title, a concise (150-250 words) abstract, including the aim and significance of the manuscript, the methodology followed, the main findings both in Turkish and English is required. Maximum of five keywords should be stated following the abstracts. Shortly, the manuscript should be submitted in the following order: manuscript title, abstract, keywords, body text, notes and references.
10. Manuscript should not exceed 8,000 words, typed on A4 page with 1.5-line spacing, leaving margins 3.5 cm at the left, 3 cm at the right, 4.5 cm at the top and 3 cm at the bottom of the page.
11. Main text should be written 10 point, DIN Pro font. Article title and principal subheads should be 16-point DIN Pro type, bold and set on a line separate from the text. Secondary subheads should be 10-point DIN Pro, bold and set on a line separate from the text. Sub-subheads 10-point DIN Pro type, bold and italic, run-in at the beginning of the paragraph, and followed by a period.

12. All diagrams, charts and graphs should be referred as figures and consecutively numbered. Tables should be kept to a minimum and contain only essential data. Each figure and table must be given an Arabic numeral, followed by a heading, and be referred to in the text.
13. To cite the works you used in developing your article, use the author-date system. For each work to which you refer, give the author's last (family) name, date of publication of the work cited, a page number(s) if needed.
14. Every reference cited in the text should be in parentheses. Reference in parentheses should be at the following order: Surname(s) of author (s), publication year and page number(s). Examples are as follows:  
.....is stated (Ergun, 2004).  
.....is indicated (Leblebici, 2004: 210-215).  
.....Babaoğlu (2017a: 15-20) ileri sürmektedir.  
.....(Yıldız vd., 2012: 126-153).  
.....(Babaoglu ve Demircioğlu, 2011: 399-432)
15. Please use footnotes to elaborate or comment on material in the text.
16. Only reference cited in the text should be included in the reference section. The references should be listed in an alphabetical order in a separate page. Page numbers of articles in periodicals or edited books should be indicated. The examples given below should be followed strictly:

#### **Books:**

Mıhçıoğlu, C. (1988) Türkiye'de Çağdaş Kamu Yönetimi Öğretiminin Başlangıç Yılları, Ankara: Ankara Üniversitesi SBF.

#### **Periodicals:**

Yıldız, M.; Babaoğlu, C. & Şahin, B. (2016) "Kamu Politikasını Türk İdare Tarihi Üzerinden Çamak", Hacettepe Üniversitesi IIBF Dergisi, 34(2), pp. 133-158.

#### **Edited Books:**

Allison, G. (2006) "Emergence of Schools of Public Policy: Reflections by a Founding Dean", in: The Oxford Handbook of Public Policy, (Ed.) Robert E. Goodin, Michael Moran, and Martin Rein, Oxford: OUP Oxford. pp. 58-79.

#### **E-Sources:**

Türkiye Cumhuriyet Merkez Bankası (2014), Kredi Kartı İşlemlerinde Uygulanacak Aza-mi Faiz Oranları, <http://www.tcmb.gov.tr/>, Access Date: 13.08.2017.

