

# YAPAY ZEKÂNIN MİLLİ GÜVENLİK POLİTİKALARINA ETKİLERİ

TREND ANALİZİ MART 2019



İşbu eserde yer alan veriler/bilgiler, yalnızca bilgi amaçlı olup, bu eserde bulunan veriler/bilgiler tavsiye, reklam ya da iş geliştirme amacına yönelik değildir. STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş. işbu eserde sunulan verilerin/ bilgilerin içeriği, güncelliği ya da doğruluğu konusunda herhangi bir taahhüde girmemekte, kullanıcı veya üçüncü kişilerin bu eserde yer alan verilere/bilgilere dayanarak gerçekleştirecekleri eylemlerden ötürü sorumluluk kabul etmemektedir. Bu eserde yer alan bilgilerin her türlü hakkı STM Savunma Teknolojileri Mühendislik ve Ticaret A.Ş.'ye aittir. Yazılı izin olmaksızın işbu eserde yer alan bilgi, yazı, ifadenin bir kısmı veya tamamı, herhangi bir ortamda hiçbir şekilde yayımlanamaz, çoğaltılamaz, işlenemez.

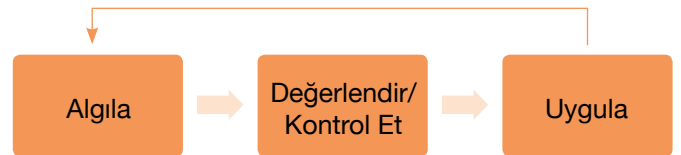
 Alper KENDİ

## 1. GİRİŞ: YAPAY ZEKÂ VE DERİN ÖĞRENME HAKKINDA

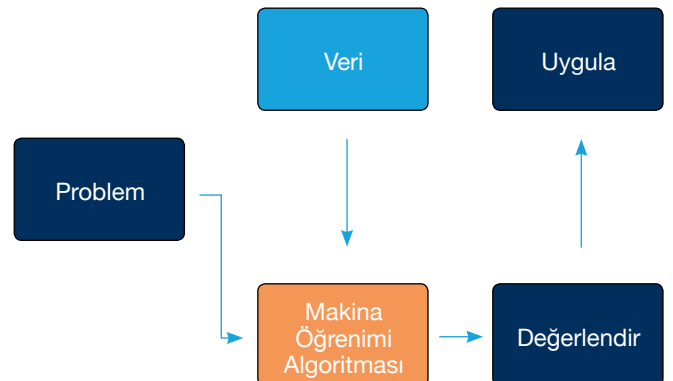
Yapay zekânın milli güvenlik politikalarına olası etkilerini değerlendirmeden önce yapay zekânın işleyiş mekanizmasını ve yeteneklerini bilmek ve olası stratejik etkilerini buradan yola çıkarak değerlendirmek doğru olacaktır.

Geleneksel yöntemler olarak sınıflandırabileceğimiz kural tabanlı algoritmalar İngilizce if-then-else örgüsü ile kodlanan giriş ve çıkış durumları ön tanımlı olarak belirlenmiş sistemlerdir. Örneğin karadan havaya atılan bir füzenin ön kısımda bulunan arayıcı başlığı ve buradaki algılayıcılardan gelen veriyi işleyen yazılımı ele alacak olursak; füzenin ateşlenmesinden hedefe ulaşılmasına kadar geçen süre zarfında sonsuz bir döngü içerisinde yazılım sürekli olarak belirli bir alanda ön tanımlı izleri (örneğin ısı izlerini) arar ve füze kontrol yüzeylerini oluşturan kanatçıkları bu bilgiye (ize) yaklaşmak için yönlendirir. İnsansız hava aracı seyrüsefer sistemi benzer şekilde kural tabanlı olarak tanımlı coğrafi haritalar üzerinde, GPS verilerini değerlendirir ve İHA konumunu hesaplar. Özetle, günümüzde otonom sistemlerin yaptıkları iş, tanımlı veri setleri çerçevesinde yine tanımlı koşullar içinde sonuca ulaşmaktır. (Bkz: Şekil 1)

Makine öğrenmesi teknikleriyle geliştirilen bir program ise sürekli tekrar eden (iteratif) öğrenme işlemi gerçekleştirir. Geleneksel programlama yöntemlerinde yazılıma veri kümesinde nereye bakması gerektiğini programcı söyler. Örneğin telefon rehberinde bir isim aratılacağında algoritma yaklaşık olarak şu şekilde çalışır. Rehber verilerini belleğe yükle -> verinin başlangıcından sonuna



Şekil 1: Günümüzde otonom sistemlerin fonksiyon akışı

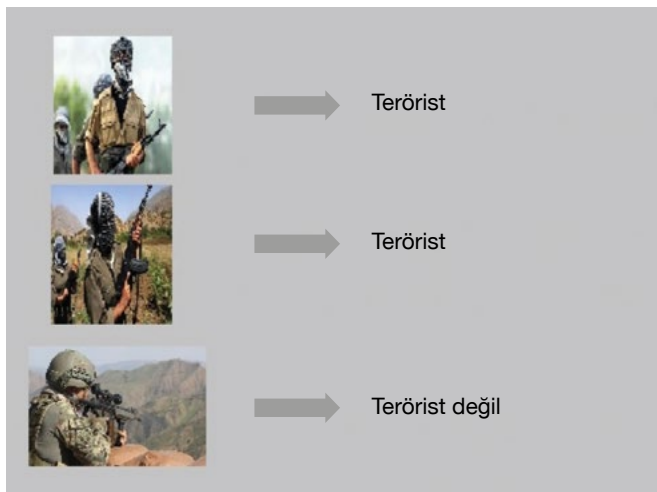


Şekil 2: Makine öğrenmesi kullanan sistemlerin fonksiyon akışı

kadar kullanıcı tarafından girilen ismi ara -> eşleşen isim bilgilerini ekranda göster. Burada aratılan isim “Osman” ise Osman kelimesini oluşturan karakterler ile eşleşen tüm isimler ekranda gösterilecektir.

Aynı uygulama makine öğrenmesi yöntemleri kullanılarak yapıldığında uygulama veriler arasında kendi başına bağlantı kuracaktır. Örneğin “Osman” kelimesini arattığınızda daha sık telefonla görüştüğünüz erkek kardeşiniz Osman’ın telefon numarasını ilk sırada gösterecektir. Klasik programlama yöntemlerinde programın takip edeceği kurallar bir kez oluşturulur ve program kullanımdan kaldırılıncaya veya sürüm yükseltinceye kadar bu kurallar değişmez. Makine öğrenmesinde ise bu kurallar programın kullanılması esnasında birtakım özel yöntemlerle değiştirilir. Program gelişir ve öğrenme sağlanır. Yapay zekâyı kural tabanlı programlardan ayıran, yapay zekânın öğrenerek yeni kurallar oluşturma yeteneğidir. Yapay zekâ öğrenmesinin değişik türleri vardır:

- **Gözetimli öğrenme:** Her bir verinin bir etiketi vardır. Yapay zekâ algoritması bu verileri kullanarak öğrenme gerçekleştirir. Örneğin binlerce hayvan fotoğrafının olduğu bir veritabanını düşünebiliriz. Her bir fotoğrafın altında fotoğraftaki hayvanın hangi türe ait olduğunu belirten Kedi, Köpek, İnek vb. etiketleri olur. Bu şekilde yapay zekâ bir sürücüsüz araç, yolda karşısına yapay zekâ programcısı tarafından ona öğretilmemiş insan dışında bir canlı çıktığında veritabanındaki fotoğraflardan yola çıkarak karşısındaki nesnenin ne olduğunu anlayabilir ve ona göre davranır.
- **Gözetimsiz öğrenme:** Verilerin etiketi yoktur. Algoritma ilgili veriler arasında kendisi bir bağlantı kurar, gruplara ayırır.
- **Yarı gözetimli öğrenme:** Gözetimli öğrenme ile gözetimsiz öğrenme arasında kalan bir yapay zekâ öğrenmesi türüdür. Etiketlenmiş küçük miktarda veri ile etiketlenmemiş büyük miktarda veri bir arada bulunur. Yapay zekâ modelimiz ne kadar çok veriyle beslenirse



Şekil 3: Gözetimli öğrenme verisi

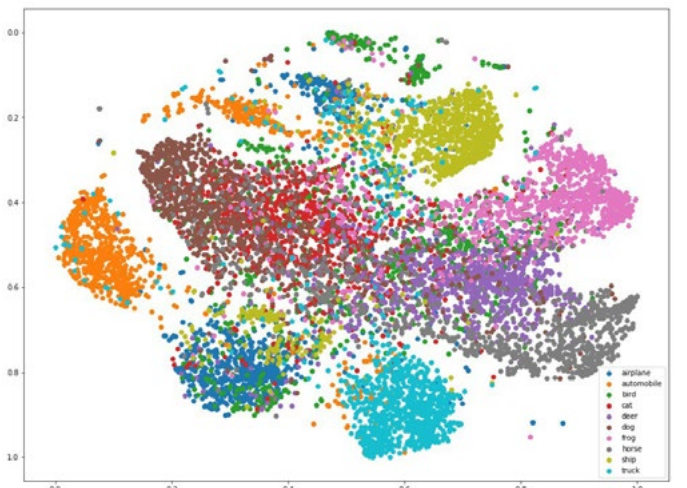
yapay zekâ o oranda daha doğru tahminler yapabilir. Şekil 4’te CIFAR-10 veri kümesini t-SNE algoritmasıyla görselleştirerek oluşturulmuş bir grafik görülüyor. CIFAR-10 veri kümesinde 10 farklı sınıftan 60.000 adet resim vardır. Görüldüğü gibi, kullanılan yapay zekâ algoritması kamyonlar, kurbağalar, otomobiller gibi farklı sınıftan fotoğrafları kendi aralarında toparlayabiliyor. Algoritmanın kedi ve köpekleri birbirinden ayırt etme yeteneğinin biraz daha güçlendirilmesi gerektiği yine bahse konu görselde kahverengi ve kırmızı noktaların birbirleri içindeki yoğun dağılımından anlaşılıyor.

Otonom sistemlerin kullandıkları algoritmalar ile yapay zekâ algoritmaları arasındaki en büyük fark tahmin yeteneğidir ve bu yetenek yapay zekânın öğrenme kabiliyeti sayesinde kazanılmaktadır. Yapay zekâ öğrenmesi de yapay zekâ uygulamasına sunulan veri kalitesiyle doğru orantılıdır.

## 2. YAPAY ZEKÂ NELER YAPABİLİR?

Askeri alanda yapay zekânın harp silahlarının birçoğunda kullanılarak bu silahları daha akıllı hale getireceği kesin. Bu durum askeri operasyonlarda insan müdahalesinin asgariye inmesine de yol açacaktır. Hız ve enformasyon gereken birçok operasyonu insandan daha doğru ve hızlı gerçekleştirebilen yapay zekâli silahlar piyade tüfeğinden, hava savunma sistemlerine kadar geniş bir uygulama alanı bulacaktır.

Evrimsel sinir ağları (CNN) kullanan Silahlı İnsansız Hava Araçları’nın nesnelere, dost ve düşman unsurları kendi başlarına ayırt etmesi mümkündür. Piyade silahları benzer uygulamalarla ateş açılan noktalardan gelecek—insanın tespit etmesi mümkün olmayan—ses ve görüntü verilerini işleyerek silah operatörüne düşman ateşinin açıldığı noktayı kolaylıkla gösterebilir. Anti-tank mühimmat ise ateşlendikten itibaren hedef tankın tipine göre en zayıf bölgesine saldırarak onu imha ihtimali en yüksek noktadan vurmaya ve aktif/pasif tank koruma sistemlerini bertaraf etmeye çalışacaktır.



Şekil 4: CIFAR<sup>[1]</sup> Makine öğrenmesinde kullanılan CIFAR resim veri kümesi



Bugüne kadar savaşlarda henüz aktif olarak kullanılmamış olsa bile yapay zekâyla birlikte sahneye çıkması daha olası silahlar da vardır - robot askerler! Elektromekanik sistemlerdeki gelişmelerle robotların birçok alanda olduğu gibi muharebe alanlarında da yaygınlaşacağı görülebiliyor. Otonom tanklar ve robot askerler gibi kara unsurları milli güvenlik stratejilerini ciddi olarak değiştirecek etkenlerdir.

### 3. MİLLİ GÜVENLİK POLİTİKALARI BAĞLAMINDA YAPAY ZEKÂ

Günümüzde veri insanlık tarihi boyunca hiç olmadığı kadar önem taşımaktadır. Veriden 21'inci yüzyılın petrolü olarak söz ediliyor. 2013'de dünyada üretilen toplam verinin 4 zetabyte'dan fazla olduğu düşünülmektedir<sup>[2]</sup>. Bunun en önemli sebebi artık her türlü verinin çok hızlı üretiliyor, paylaşılabilir ve depolanabiliyor olmasıdır. Veri dijital ve analog olmak üzere iki farklı şekilde ortaya çıkar. Dijital bilgi e-posta, GPS, kamera, sensör, uydu vb. teknolojilerle elde edilir. Analog veri ise, ses, görüntü ve fiziksel aktiviteler gibi (örneğin insan kalbinin hızı) daha çok insan ve çevre kaynaklıdır. Ancak analog veriler dijital veri haline de getirebilir.

Yapay zekânın ülke güvenliğine olası etkilerini incelerken verinin tanım ve öneminden bahsetmemizin sebebi yapay zekânın üretim araçları olarak kabul edebileceğimiz algoritmalarının hammadde olarak veriyi kullanmasıdır. O nedenle milli güvenliğimizi etkileyecek

yapay zekâ unsurlarının geliştirilmesinde tehdit algımızın ve bertaraf yöntemlerimizin esasına uygun veriler kullanılması gerekir. Dünyanın en hızlı ve en kesin sonuç veren yapay zekâ algoritmasını yazsanız dahi onun öğrenme fonksiyonunu besleyecek veri kümesini uygun şekilde sağlayamazsanız sıradan bir programdan farkı kalmayacaktır.

Yapay zekânın eğitilmesi bir problemdir ancak bunun başarılabilmesi uluslar için önemli bir kazanımdır. Özellikle harp görmüş ulusların bu tecrübelerini aktarmayı başardıkları yapay zekâ uygulamaları gerçek bir savaşta fark yaratır. Örneğin ülkemizin gayri nizami harp konusundaki tecrübeleri internette bulunamaz. Bu alanda 40 sene boyunca elde edilen tecrübe başka bir ulusun geliştireceği yapay zekâ tarafından da kullanılamaz. Bu tecrübe bilgisinin dijitalleştirilerek yapay zekâ öğrenmesinde kullanılabilir hale getirilmesi önemlidir.

Dünyamızın doğal kaynakları kısıtlıdır. Son yapılan araştırmalara göre dünyamızın kaynaklarını 1,7 oranında kullanıyoruz<sup>[3]</sup>, yani dünya kaynaklarını iki dünya varmış gibi tüketiyoruz. Üstelik ülkeler bu tüketimi maalesef adil olmayan bir biçimde, coğrafi konumları ve askeri güçleriyle orantılı şekilde gerçekleştiriyor. O nedenle, milli güvenlik politikaları kısıtlı olan dünya kaynaklarını kullanmak isteyen devletlerin birbirlerine karşı oluşturduğu tehditlere karşı önlem almak üzere geliştiriliyor.

Yapay zekâ teknolojilerinde ileri ulusların yaratabileceği tehditlere bakacak olursak;

Ulusların savaşması için aşılması gereken bir fayda/zarar denkleminin varlığından söz edebiliriz. Bu denklem, savaşa girildiğinde elde edilecek kazanımlar ile verilecek kayıplar arasındaki fayda zarar oranını ifade eder. Ülkeler çıkarlarını korumak için giriştikleri savaşın bedelini para ve insan olarak öderler. Ülke ordularının asker kaynağı halktır, bu yüzden hükümetler savaşa girmek için kamuoyu desteği ararlar. En modern ordulara dahi sahip olsanız, günümüzde arkanızda, aldığınız savaş kararını destekleyen bir halk yoksa savaşı sürdüremezsiniz. Hatırlarsak Irak harekâtında ABD hükümetinin Amerikan kamuoyunu ikna etme yöntemi “kimyasal silahlar ulusumuz için bir tehdittir” tezi olmuştur. Yapay zekâ ve robot teknolojilerindeki gelişmeyle birlikte sözü geçen savaşma eşiğinin düşeceği beklenmelidir. Olası bir savaşın bedelini para ve robot olarak ödeyecek hükümetler, kamuoyu desteğini aramayacaktır. Bunun sonucu, yapay zekâ ve robot teknolojileri konusunda ileri ülkelerin çıkarları doğrultusunda daha kolay savaş ilan edebilir hale gelmeleri olacaktır. Küresel savaşma eşiğinin düşmesinden kaynaklı tehditler, milli güvenlik politikalarımızda ifadesini bulan tehdit algımızın da değişmesini gerektirecektir. Teknolojik gelişmeler neticesinde, örneğin Yunanistan gibi az nüfuslu bir ülkenin Türkiye gibi bir ülkeye Akdeniz gazı için rahatlıkla savaş açabildiği veya Çin gibi bir ayda on binlerce dron üretebilecek bir ülkenin çıkarları uğruna her türlü küresel çılgınlığı göze aldığı bir noktaya gelinebilir.

Yapay zekâ ve robot teknolojilerindeki gelişmeler gayri nizami harp konusunda da tehdit algılarımızın değişmesini gerektirebilir. Bugün örneğin teröristlerin kullandığı AK-47 veya AR-15 model silahların menşei konusunda, üreticiler ve araçlar dahil hiçbir ülke sorumluluk kabul etmemektedir. Silahlar üretilir ve bir şekilde terörist eylemlerde kullanılır. Benzer şekilde öldürme kabiliyeti olan otonom sistemlerin de bir şekilde teröristlerin eline geçmesi beklenmelidir. Yapay zekâlı robotların kullanılmasıyla terör olaylarında menşei bilinen/bilinmeyen robotlarla eylem yapılabilmesinin önü açıldığında, terörü maşa olarak kullanan bir takım odakların emelleri yurdumuz için bugünkünden daha büyük bir risk oluşturacaktır. Bunun da ötesinde CIFAR-10 örneğinde görülebileceği üzere kediye, köpeği, uçağı, arabayı ayırt edebilen yapay zekâyâ sahip kitle imha silahları, doğal kaynaklara, alt yapılara zarar vermeden, nükleer, kimyasal, biyolojik izler bırakmadan sadece hedef coğrafyadaki insan

varlığını yok edebilir. Bu şekilde insandan temizlenen bölgelerde işgalci devlet/gruplar için yeni bir vatan yaratılabilir. Bugün DAEŞ vb. örgütleri kullanarak etnik temizlik yapan, bölgesel çıkarları uğruna yapay devletçikler oluşturmaya çabalayan odakların, sözü geçen akıllı silahları kullanmakta tereddüt etmeyeceği öngörülmelidir.

Henüz bahsettiğimiz otonomi (zekâ) seviyesine sahip, insan müdahalesi gerektirmeden aktif olarak kullanılan otonom unsurlar yoktur. Mevcut otonomi seviyesi sahada askerlerin kullandığı mikro/mini İHA'lar, insansız personel taşıyıcıları ve insansız hava araçları düzeyindedir. Enerji ve işlem gücü gibi kısıtlar henüz yapay zekâ sistemleri insan müdahalesine muhtaç bırakmaktadır.

Ancak unutmamak gerekir ki taş devri dünyada taş kalmadığı için bitmemiştir, insan askerli orduların çağı da dünyada insan kalmadığı için bitmeyecektir. Yapay zekâlı silahların önünü kesmek ve onlara mukavemet edebilmek için insan zaafına sahip olmayan araçlar geliştirilmesi zorurudur. Daha önce belirttiğimiz üzere yapay zekâ sadece yazılım kodlarından oluşan bir teknoloji değildir, yapay zekâ öğrenmesi için veri kümeleri gerekmektedir ve askeri konuları içeren veri kümelerinin dijital olarak oluşturulup depolanması hususu milli güvenlik politikalarına girmesi gereken önemli bir konudur.

## 4. SONUÇ

Yapay zekâ geniş bir uygulama alanına sahiptir. Hızla gelişmekte olan yapay zekâ teknolojilerinin askeri alanda kullanılmasıyla ülkelerin milli güvenlik politikalarının tarihte görülmemiş şekilde değişeceğini söylemek yanlış olmaz. Yapay zekânın Türkiye'ye milli güvenlik dâhil tüm alanlardaki etkilerini sağlıklı analiz edebilmek ve geleceğini planlamak için bir yapay zekâ teknolojileri ofisinin kurulması, ülkemizin yapay zekâ teknolojilerinde dünya ile rekabet edebilmesine yardımcı olacaktır.

## KAYNAKÇA

- [1] CIFAR foto <https://medium.com/@pslinge144/representation-learning-cifar-10-23b0d9833c40>
- [2] Industrial Research Institute (2016), '2016 Global R&D Funding Forecast', supplement to R&D Magazine, Winter 2016.
- [3] Worldwatch Institute <http://www.worldwatch.org/node/810>



**thinktech**  
**STM** Teknolojik Düşünce Merkezi  
<http://thinktech.stm.com.tr>

