# Yapay Zekâ Uygulamalarının Güvenlik, Terörizmle Mücadele ve İstihbarata Katkıları

**Yapay Zekâ Uygulamalarının Güvenlik, Terörizmle Mücadele ve İstihbarata Katkıları[1]**

**Semih SEVİNÇ[2]**

**Giriş**

Terörizm devletlerin kurulduğu ilk yıllardan itibaren devletler için güvenlik sorunu olmuş ve her dönemde terörizmle mücadele kapsamında farklı mücadele teknikleri uygulanmıştır. Günümüzde teknolojinin hızla gelişmesi ile birlikte saldırı ve savunma sistemlerindeki değişim de artarak devam etmektedir. Bu kapsamda terör örgütleri yapay zekâya dayalı silah, mühimmat ve araç sistemleri ile eylemlerini gerçekleştirmeyi hedeflemektedirler.

İstihbarat doğası itibariyle süreklilik arz eden ve meydana gelen her türlü değişime ayak uydurmayı gerektiren, açık, yarı açık ve gizli kaynaklardan toplanan bilgilerin ulusal güvenliği tehdit edecek unsurlara karşı koruma sağlamak amacıyla ulusal menfaatler doğrultusunda sınıflandırılması ve analiz edilmesi sürecidir.

Yapay zekânın temel amacı, insanlar tarafından belirlenen hedef ve amaçları akılcı, insan davranış ile düşüncelerine benzer ve anlaşılır şekilde yerine getiren yapay varlıklar, (bilgisayar programları, robotlar ya da makineler) üretmektir.

Bilgisayar biliminin kurucusu sayılan ve algoritma tanımı ile modern bilgisayarların kavramsal temelini atan İngiliz matematikçi ve kriptolog Alan Turing, Nazi Almanya'sı tarafından gizli mesajların şifrelenmesini sağlayan Enigma makinesinin şifrelerini kırmayı başararak 2'nci Dünya Savaşı'nın daha erken bitmesini, dolayısıyla daha az can kaybı ile sona ermesini sağlamış, aynı zamanda geliştirdiği Turing Testi ile makinelerin ve bilgisayarların düşünme yetisine sahip olup olamayacakları konusunda bir kriter öne sürmüştür.

Bilgi teknolojilerinde özellikle son elli yılda gerçekleşen gelişmeler sonucunda finans ve ekonomiden sağlığa, eğitimden kolluk faaliyetlerine, otomotiv sektöründen güvenliğe ve hatta devletlerin iç ve dış politikalarına kadar birçok alanda değişim ve ilerlemeler kaydedilmiştir. İnsan hayatındaki tüm bu alanlar ile birlikte geçmişte kullanılan istihbarat toplama ve analizindeki teknik, araç ve alanlarda da değişimler hızla devam etmektedir.

İstihbaratın elde edilmesi kapsamında bilginin toplanması, tasnif edilmesi, değerlendirilmesi, analiz edilmesi ve yorumlanması süreci siber istihbarat ve yapay zekâ yöntemleri kullanılarak yapılabilmekte olup, belirtilen süreç klasik yöntemlere göre daha geniş bir alanda ve daha ucuza, insan analistlerden daha hızlı ve daha akılcı bir şekilde yürütülebilmektedir. İstihbarat çarkı olarak ifade edilen bahse konu sürecin gelecekte tamamının (insan öğesi çıkartılarak) yapay zekâ ile donatılmış tam otonom sistemler (robot istihbarat analistleri ve saha uzmanları) tarafından yürütülüp yürütülemeyeceği ve avantaj / dezavantajlarının neler olacağı tartışılmaktadır.

Günümüzde teknoloji ve internet kullanımının yaygınlaşmasıyla yeni bir boyut kazanan güvenlik, istihbarat ve terörizmle mücadele faaliyetleri yapay zekâ ve robotik teknolojisinin gelişimiyle çok farklı bir yapıya dönüşmektedir. Gelecekte yapay zekânın, özellikle devletlerin terörizmle mücadele faaliyetlerinde daha önemli bir yere sahip olacağı öngörülmekte olup, bu çalışmada istihbarat, güvenlik ve terörizmin başta yapay zekâ olmak üzere teknolojik gelişmeler ile ilgili olarak ortaya çıkan risk ve tehditlerden nasıl etkilendiği ve gelecekte nasıl etkileneceği ortaya konulmuştur.

**Güvenlik yaklaşımlarının tarihsel süreçteki yeri**

Uluslararası güvenlik yaklaşımlarının başında güç ve çıkar mücadelesini esas alan realizm gelmektedir. Realizmde temel aktör egemen ulus devletlerdir. Devletler rasyonel karar veren ve bu doğrultuda hareket eden bütüncül yapılardır. Uluslararası sistemin anarşik yapısı güç mücadelesine neden olur. Anarşik yapı ile bahsedilen devletler arasında merkezi bir otoritenin olmayışı ve her devletin kendi çıkarını düşünmesidir. Güç, bir devletin diğerlerini etkileyebilme ve istediği şekilde yönlendirebilmesini sağlar. Askeri, teknolojik ve ekonomik güç bunu sağlamada başlıca etkili olan güç türleridir.

Realizmin kökenleri Tukidides' e (M.Ö.5.yy) kadar dayanır. 16.yy.da Machiavelli "Prens" adlı eserinde devlet adamlarının rasyonel ve çıkarcı hareket etmeleri gerektiğini anlatmıştır. 17.yy.da Hobbes temel amacın güç arttırmak olduğunu savunmuştur. 20.yy.da ise yine realizmi savunan Carr ve Morgenthau liberalizmi (idealizm) ütopik olarak değerlendirerek eleştirmişlerdir. 1970'lerden itibaren ise Kenneth Waltz' un uluslararası politika kuramı ile Neorealizm anlayışı ortaya çıkmıştır. Yapısal realizme göre, uluslararası sistemin anarşik yapısı devletlerin dış politikalarını sınırlamaktadır.

Devletler ile uluslararası sistem arasındaki ilişki önemlidir. Klasik realizm ile Neorealizmi karşılaştırmak gerekirse, klasik realizmde güç ana amaçken, Neorealizmde güç güvenlik için araçtır; klasik realizmde güç mücadelesi insanın bencil ve çıkarcı doğasından kaynaklanırken, Neorealizmde sistemin anarşik yapısı güç mücadelesine neden olur; klasik realizmde öncelik güvenlik konuları iken (yüksek politika), Neorealizmde ekonomik konular da önemli hale gelmiştir (alçak politika). Her iki yaklaşımda da siyasi, askeri ve ekonomik güç dengesi uluslararası politikada belirleyici faktörlerdir.

Diğer bir yaklaşım realizm savunucularına göre ütopik olarak görülen klasik liberalizmdir. Bu yaklaşımda düşünce, eşitlik, rasyonellik, özgürlük ve özel mülkiyet kavramları ön plana çıkmaktadır. Bu yaklaşıma göre tüm insanlar eşittir ve yaşama, özgür olma, mutluluğunu sürdürme, fırsat eşitliği gibi hakları dokunulmaz olmalıdır. J.Locke' un bu konuda "birey haklarını devlet korumalı" fikri mevcuttur. Uluslararası hukukun babası sayılan Hugo Grotius ise devletler arasında barışın sağlanmasının ve işbirliğinin mümkün olduğunu söyler. J.J.Rousseau ve Montesquieu toplumsal yönetim biçimi olarak demokrasiyi savunur. Bir diğer liberalizm temsilcisi Immanuel Kant'ın iyimser olarak görülen fikri de uluslararası ilişkilerin bireylere dayalı olduğudur.

Adam Smith ise özel mülkiyetin önemi ve gerekliliğinden bahsetmiştir. Neoliberalizm akımında ise devletlerin hak ve özgürlükleri yani egemenlikleri temeldir. Savaş devletler arasında istenen bir durum değildir. Maddi ve manevi bedeli bulunur. Ekonomik güç askeri güçten daha önemlidir. Uluslararası örgütlerin kuruluş maksadı barışı ve güvenliği sağlamaktır. İşbirliği için hegemon yani baskın devletin varlığı şart değildir.

Genel olarak yaklaşımları incelediğimizde realizmi savunan Hobbes yaklaşımının en karamsar şekilde savaşların bitmesinin mümkün olmayacağı, tam tersi iyimser bir yaklaşım olarak Kant' ın liberal bakış açısına göre ise bunun bireylerin davranışları ile başarılabileceği anlaşılmaktadır. Kant ve Hobbes' un kötümser ve iyimser yaklaşımlarının arasında bir noktada bulunan Grotiusçu yaklaşım ise hem savaşın hem de barışın mümkün olabileceği, her iki durumun da devletlerin arasındaki işbirliğine dayalı olduğunu savunur.

Güvenlik yaklaşımları devletlerin yapısı, kullanılan silahlar, teknolojik ve siyasi gelişmeler, savaşlar sonucu sınırlardaki tehdit ve fırsatların değişmesi, göç ve nüfus artış/azalışları gibi sebeplerle her dönemde farklılık göstermiştir. Orta Avrupa' da Katolik ve protestanların Otuz Yıl Savaşlarını sona erdiren 1648 yılı Westfalya Anlaşması uluslararası sistemin bir miktar kontrol altına alınmasını sağlaması ve modern devletler mimarisinin temeli olarak görülmesi açısından önemlidir. Bu anlaşma ile devletlerin egemenlik hakkı, devletlerarası yasal eşitlik hakkı ve bir devletin başka bir devlete karışmaması gibi kavramlar ortaya çıkmıştır. Sonucunda ise kilisenin önemi azalmış ve modern Avrupa sınırları oluşmuştur.

19. YY. ise buhar ve sınırlı savaşlar çağı olarak bilinmektedir. 1806' da Napoleon Prusya ordusunu yendiği dönemlerde devletlerin bünyesinde kişiye (lidere) bağlı istihbarat organizasyonları bulunmaktaydı. Bu dönemde askeri istihbarat kavramı ilk defa Moltke tarafından kullanılmıştır. Avrupa savaşlarının sonunu getiren Napoleon'un Waterloo yenilgisiyle ise istihbarat servislerinin, orduların ve toplumların düzeni değişmiştir.

İstihbaratın bürokraside kurumsallaşması ise 20.yy.da gerçekleşen endüstri devrimi ve I'nci Dünya Savaşı ile başlamıştır. Savaşın ana sebebi olarak devletlerin çıkar çatışmaları gösterilebilir. Bu dönemde birçok cephede gerçekleşen savaşta düşmanla mücadelede bilgi toplamanın ve olayların seyrini değiştirmenin yeni yöntemi olarak istihbarat yöntemlerinin önemi anlaşılmıştır. Teknolojik bilgi toplama ve analiz, analitik ürün elde etme ve liderlerin istihbarat bilinci kazanması yeniliklerin başında sayılabilir.

Hız, ateş gücü, zamanlama, telsiz ve keşif uçağının kullanılması, saha izleme ve kontrolü için kablosuz vericilerin kullanılması, denizaltıların ilettiği sinyallerin takibi (sinyal istihbaratındaki gelişmeler) ve düşmanın izlenmesi maksadıyla kripto cihazların kullanılması savaşlardaki önemli faktörler olmuştur. Savaşın başlarında istihbarat çalışmaları, yöntemleri ve dokümanlar sınırlı iken yaşanan acı dolu tecrübelerle istihbarat toplama metotlarında gelişmeler yaşanmıştır. Dünya haritasında Çarlık Rusya'sının 1917 Ekim Devrimi ile yıkılması ve SSCB' nin kurulması gibi önemli değişiklikler meydana gelmiştir.

I'nci Dünya Savaşı sonrasında ise devletlerin güç dengesi ve uluslararası ilişkilerde barışın tam olarak sağlanamamış olması sonucu II'nci Dünya Savaşı'nın da önüne geçilememiştir. Her ne kadar idealizm (liberalizm) çerçevesindeki Wilson İlkeleri uygulanmaya çalışılsa da sorunlar yeterince çözülememiş ve savaş karşıtı düşünceler uygulanamamıştır. Bu da realizmin tekrardan güçlenmesine sebep olmuştur. Fransız ve İngiliz istihbaratları kendi toprakları ile Almanya ve Osmanlılardan kalan topraklarda yoğunlaşmıştır. İngiltere merkezli Fransa, ABD, Baltık ülkeleri ve hatta Almanya arasında istihbarat paylaşımları yapılmıştır.

En önemli işbirliği Almanya'nın şifre makinesine karşı İngiltere, Polonya ve Fransa işbirliğinde enigma projesinde görülmüştür. Bletchley Park' ın sinyal istihbaratı başarılarında büyük bir yeri bulunmaktadır. Sovyet komünizmi ile Alman faşizminde ideolojilerinin yıkılması korkusu ile birbirlerine karşı istihbarat faaliyetleri yürüttükleri görülmüştür. Ayrıca Çin' de Mao liderliğinde Sovyetlerden istihbarat elde etmek maksadıyla istihbarat birimleri oluşturulmuştur. II'nci Dünya Savaşı tanklar (İngilizlerin icadı), uçaklar, keşif uçakları (U-2), U-Boat denizaltıları (Almanlar ABD'nin İngilizlere yardım gemilerini batırmak üzere Atlantik Okyanusunda kullanmışlardır), bombardıman uçakları ve uçak gemileri (Japonların Pearl Harbor baskını) gibi kullanılan araç ve silahlar bakımından oldukça gelişmiş ve farklıdır. Bu savaş modern ordularda askeri istihbarat doktrininin de başlangıcı olmuştur.

Hitler yıldırım harekâtı (Blietzkrieg) ile Polonya ve Fransa' da hızlı şekilde ilerlemiş, Dunkirk' te İngiliz ve Fransız birliklerini çaresiz duruma düşürse de devamındaki Britanya muhaberesinde, Alman Hava Kuvvetleri Komutanı Göring (Luftwaffe) İngiliz TAF (Kraliyet Hava Kuvvetleri)' ne karşı başarısız olmuştur. Buna sebep olan ana etken olarak Almanların İngiliz hava savunma (erken uyarı) sistemlerinden haberlerinin olmaması gösterilebilir (istihbarat başarısızlığı). Churchill liderliğinde İngiliz Gizli İstihbarat Servisi ve SOE, gizli operasyonlar ile görüntü izleme ve tespitlerinde önemli başarılar elde etmiş ve bu konuda ABD' ye de yardım etmişlerdir. Müttefiklerin koordineli istihbarat çalışmaları ve materyal üstünlükleri Nazi Almanyası ve Japonya' nın çöküşüne neden olmuştur. Ayrıca Sovyetlerin Richard Sorge ve Cambridge Beşlisi denilen gizli espiyonaj elemanları ile insan istihbaratı alanında mihver devletlerine göre önemli derecede üstünlük sağladığı söylenebilir. Bilim ve istihbarat bağı ilk olarak I'nci Dünya Savaşında kurulmuş, II'nci Dünya Savaşında ise atom bombasının kullanımı (Hiroşima ve Nagazaki) ile bilim istihbaratın ayrılmaz bir parçası haline gelmiştir.

20'nci YY'da gerçekleşen dünya savaşları, soğuk savaş ve sonrasındaki dönemler incelendiğinde güvenlik yaklaşımlarının bilim ve teknolojideki gelişmeler, devletlerin ekonomik ve siyasi hedefleri ile uluslararası güç dengelerine göre değişiklik gösterdiği fakat günümüzde halen savaş ve çatışmaların sona ermediği düşünüldüğünde realizm düşüncesinin halen ön planda olduğu, istihbarat faaliyetlerinin ise devletlerin ana hedeflerine ulaşmasında elzem olduğu söylenebilir.

**Güvenlik ve İstihbarat**

Güvenlik, tehditlerin bulunmaması, kaygı ve endişelerden uzak olma durumu olarak tanımlanabilir. Latince Securitas kelime kökünden gelmektedir. Türkçede kavramsal olarak bir şeye dayanmak, güç almak, dayanışma anlamlarında da kullanılmaktadır. Örneğin; bir evin güvenliğinden bahsediliyorsa kapı kilidi, güvenlik kameraları, sitenin güvenlik görevlisi, apartmandaki yangın merdivenlerinin durumu, depreme dayanıklılık hali gibi emniyet tedbirlerinden bahsedilmelidir. Yine aynı şekilde evrak ve belge güvenliğinde evrakların numaraları, gizlilik dereceleri, sorumlu personel ya da oda ve çekmece kilitlerinden bahsedilir.

İstihbarat bilme merakı ile ortaya çıkan bir mücadele sahasıdır. İnsanın temel dürtülerinden olan merak, insanı kendisi ve çevresi hakkında bilgi toplamaya yönlendirir. Bu nedenle istihbarat güvenlik ihtiyacına yönelik bir araç olarak tarih boyunca kullanılmıştır. Karar vericilerin gelişen olaylarla ilgili olarak bilgi sahibi olmasında ve strateji geliştirmesinde istihbarat faaliyetleri önemli bir başvuru aracıdır (Treverton,2004:177-184).

Devletlerin güvenlik kaygılarından dolayı yaşanan modern anlamda ilk savaşlar M.Ö.5. YY'daki Atina-Sparta arasındaki mücadelelere kadar dayanır. Milli Güvenlik kavramı ise 1940'lardan itibaren özellikle 2.Dünya Savaşından sonra popüler hale gelerek siyasal literatüre girmiştir. ABD'nin bazı kurum isimlerinde güvenlik kavramını kullanması da bu dönemlerde başlamıştır. Arnold Wolfers'e göre güvenlik somut olgu ve durumlarla anlaşılabilir. Bu sebeple, "Neyin güvenliği?", "Kimin için güvenlik?" gibi sorulara cevap verilebilmelidir. Soğuk Savaşın bittiği dönemden itibaren askeri güvenlik kavramı çeşitlenerek, toplumsal, siyasal, bireysel, çevresel güvenlik kavramları da yazına eklenmiştir. Bilişim ve teknoloji ile birlikte ise ortaya siber güvenlik, bilgi ve dosya güvenliği gibi sanal uzay güvenliklerini kapsayıcı tanımlar ortaya çıkmıştır.

Bilişim sistemlerinde gerekli olan ve son dönemde önemi daha çok artan siber güvenlik kavramı incelendiğinde sızma testleri, bilgisayar şifreleri, sistemdeki hata ve açıklıklar ile veri tabanı ve ağ güvenliği gibi unsurlar öne çıkar. Devletin en önemli işlevi güvenliği sağlamaktır. İç güvenlik ve dış güvenlikte devlet güvenliğin hem öznesi hem de nesnesidir. Yani her devlet güvenliğini kendi imkanları dâhilinde almalıdır. Devletler arasında ise bir devletin kendi güvenliğini sağlamak maksadıyla aldığı tedbirler, diğer devletleri kendini yetersiz hissetme gibi bir duruma sürükleyebilir. Burada ortaya güvenlik ikilemi sorunsalı çıkar. Yani bir devlet kendi güvenliğini sağlamaya yönelik faaliyetlerde bulunurken diğer devletlerin güvenliğini tehlikeye sokmaktadır (Chen,2005:1-5).

Devletler hem kendi çıkarını sağlayacak hem de diğer devletlere zarar vermeyecek şekilde kendine yardım (self-help) ilkesi ile güvenlik sorununu çözmeye çalışır. Sonuç olarak iki devlet arasındaki ilişkinin sürdürülebilmesi için ulus çıkarları birbirleriyle çatışmamalıdır ve ortak bir güvenlik konsensüsü gereklidir. Somut bir örnek olarak 1962'deki ABD ve SSCB arasındaki Küba Krizi (Ekim füzeleri) bu kapsamda tartışılabilir.

Dünya devletlerinin bir güç mücadelesi içinde olduğu düşünüldüğünde istihbaratın gerekliliğinden de bahsedilmelidir. İstihbarat, çok sayıda bilgiyi toplamak, bu bilgilerin arasından ihtiyaç duyuları almak, gerekli verileri işlemek ve karar vericilere dağıtmak, sonuç olarak ise yeni bir bilgi seti (ürün) ortaya çıkarmaktır. İstihbarat stratejik, operatif ve taktik seviyelerde incelenebilir. İstihbaratın hedefi, düşmanın güçlü yanlarından kaçınarak onu daha hassas hale getirmek, hassas taraflarını istismar ederek kendi çıkarı doğrultusunda kullanmak ve zayıf taraflarını kullanarak buralardan saldırmaktır. İstihbarat, bilgi karmaşasını önlemek için tek elden ve gizli olmalı, üstünlük unsuru olarak baskın bir şekilde kullanılmalıdır. Çünkü istihbaratın başarısı bir ülkenin başarısı olabilir. İstihbaratçıların barış zamanında savaş halinde oldukları unutulmamalıdır.

Geçmiş dönem ile günümüzdeki istihbarat anlayışının karşılaştırılması altı temel başlıkta yapılabilir (Agrell,2012:131-132) şartlar ve durumlar günümüz şartlarında daha hızlı değiştiğinden istihbarat süreci uzun vadeli değildir ve sürekli yenilenmelidir, yeni bilgi alanları geliştikçe istihbarat uzmanlığı ve yapısı da şekillendirilmelidir, iletişim teknolojilerinin gelişmesiyle açık kaynak istihbaratı sıklet merkezi haline gelmiş ve önemi artmıştır, özel istihbarat şirketleri gibi istihbarat sağlayan yeni aktörler ortaya çıkmıştır, bilgiye sahip unsurların artışıyla rekabetçi bir ortam meydana gelmiş ve geçmişteki bilgiyi tekelinde bulundurma olanağı ortadan kalkmıştır, günümüzde bilgi kaynaklarının artışı ve bilgi karmaşasının artmasıyla güvenilirliğin de önemi daha çok anlaşılmaya başlanmıştır.

Milli güç unsurları; askeri, coğrafi, biyografik, bilimsel ve teknolojik, ulaştırma ve iletişim, ekonomik, politik ve sosyolojik alanların tümünü kapsamaktadır. Bu anlamda istihbaratçı analiz yaparken tüm bu alanlar hakkında mevcut ve potansiyel durumlar hakkında bilgi sahibi olmalı ve yorumlama kabiliyetine (analiz, çıkarım) sahip olmalıdır. Bu anlamda istihbaratçı, ülkelerin jeopolitik ve jeostratejik konumlarını, liderlerin kişilik yapılarını ve sağlık durumlarını, toplumların din, mezhep, tarikat gibi unsurları ile kamuoyu araştırmalarını, bilim ve teknolojideki yapay zekâ gibi gelişmeleri

göz önünde bulundurarak çıkarımlar yapabilmelidir. Tüm bunlar yapılırken geçmiş, mevcut, gelecek ve potansiyel unsurlar ile fırsat ve tehditlerin birlikte değerlendirilmesi gerekmektedir. Bu sebeple istihbarat, teori ve saha analizinin birleştirilmesi ile kapsamlı bir bilimsel disiplin olarak incelenmelidir. Örnek olarak Türkiye'nin Doğu Akdeniz, Libya, Suriye ve İdlib' teki politikaları istihbarat disiplini çerçevesinden değerlendirildiğinde milli güç ve haklarını savunmak için yapılan hareket tarzları ve güvenlik politikaları olarak görülmelidir.

İstihbarat faaliyetlerinde başarılı olmanın tek kriteri teknolojik imkânlara sahip olmak değildir. Fakat istihbarat faaliyetlerini teknoloji ile desteklemek başarı oranını artırıcı bir etkendir. Bu kapsamda istihbarat elde etme konusu teknolojik imkânlarla birlikte düşünüldüğünde pahalı bir süreçtir. Teknoloji alanındaki gelişmelerin güvenlik alanı ile doğrudan ya da dolaylı şekilde ilişkisi bulunmaktadır. Örneğin askeri alanda kullanılan İHA, SİHA veya keşif uçakları doğrudan askeri anlamda istihbarat sağlamak için kullanılırken fotoğraf makinesi, kamera veya internet gibi teknolojik ürün ve imkanlar hem günlük hayatta hem de istihbarat elde etmek maksadıyla kullanılmaktadır. Bu bakımdan istihbarat temel olarak "gizlilik" ilkesi ile icra edildiğinden devletler teknolojik çalışmalarını özellikle savunma sanayi alanında büyük oranda gizli bir faaliyet olarak yürütmektedirler.

İstihbarat faaliyetleri başlangıcı itibariyle insan faaliyetleri ile başlamışsa da zamanla veri toplama ve istihbarata karşı koyma alanlarında gerçekleşen uydu, gemi, casus uçaklar ve gelişmiş bilgisayarlar ile şifreleme cihazları ile teknik istihbarata dönüşmüştür. Özellikle 2'nci Dünya Savaşı sonrasındaki devrim ile devletler arasında teknoloji yarışı başlamış, bu da uzman personel yetiştirme ihtiyacını doğurmuştur. 1939-1945 yılları arasında gerçekleşen Büyük Savaş İngiltere ve Almanya'nın karşılıklı sinyal istihbaratı çalışmalarına (Enigma) tanık olmuştur. Sonrasında ise Almanya ve ABD'nin dünya devletlerinin diplomatik yazışmalarını dinleme (Rubicon Operasyonu) konuları gündeme gelmiştir.

Benzer şekilde ABD, İngiltere, Kanada, Yeni Zelanda ve Avustralya gibi devletlerin kendi aralarında yaptığı UKUSA anlaşması ile ECHELON ve PRİSMA gibi projelerle kendi aralarında diğ dünya devletleri ile ilgili elde edilen bilgileri paylaştıkları bilinmektedir. Uluslararası alandaki güvenlik dengesi bu anlamda istihbarat örgütlerini birbirleri ile adı konulmamış bir yardımlaşmaya yönlendirmektedir. Günümüzde ise casusluk ve karşı casusluk gibi faaliyetlerde istihbarat çalışanlarının yerine yapay zekânın kullanılması tartışılan konular arasındadır.

Sonuç olarak güvenlik ve istihbarat birbirinden ayrı düşünülmemesi gereken kavramlardır. Her iki kavramın da kesişim bölgesinde sorunsal olarak risk ve belirsizliği ortadan kaldırma çabası ile daha fazla güç elde etmek için atılması gereken adımlar bulunmaktadır.

**Yapay zekâ uygulamalarının istihbarata etkileri**

İstihbarat disiplininin tarihi insanlığın ve devletlerin ilk olarak ortaya çıktığı zamanlara dayanır. İstihbarat toplama yöntemleri Endüstri Devriminden önce temel olarak insan istihbaratına dayanmakta olsa da, 1'nci ve 2'nci Dünya Savaşlarından sonra teknolojik gelişmelerle birlikte sinyal, radar, iletişim, elektronik, görüntü ve siber istihbarat kavramları ile birlikte kullanılmaya başlanmıştır. Bilgisayarın bulunması ve toplumun her alanında kullanılmaya başlamasıyla ortaya çıkan siber uzay kavramı siber istihbarat, yapay zekâ ve siber güvenlik konularının önemini artırmıştır.

Günümüzde büyük devletlerin istihbarat örgütlerinin yapay zeka temelindeki programlarla işbirliği yapacak şekilde çalışmalar yürütmesi istihbarat ve yapay zeka disiplinlerinin gelecekte birbirinden ayrı düşünülemeyeceklerini göstermektedir. "Sosyal İkilem (Netflix, 2020)" adlı belgeselde yapay zekaya dayalı sosyal medya faaliyetlerinde insan istihbaratının nasıl toplandığı anlatılmıştır. Siber güvenlik kapsamında tehdit aktörlerince ve güvenlik uzmanlarınca kullanılan yapay zekâ uygulamaları hem saldırı hem de savunma ve istihbaratta önemli role sahiptir. IBM-DeepLocker isimli yapay zekâ virüsü, kullanıcıları gizlice takip ederek en çok konuştukları konuları tespit etmekte ve buna göre dijital reklamlarda oynamalar yapabilmektedir.

Yapay zekanın siber uzayda geliştirilen makine öğrenmesi, veri bilimi, derin sinir ağları, robotik gibi alanları güvenlik sistemleri için kolaylık ve fırsat olarak değerlendirilse de, kötü niyetli kişilerce kullanıldığında tehdit ve güvenlik problemine dönüşmektedir (Çetin,2018:161-164).

Güvenlik kavramı, bireyden uluslara kadar bütün aktörler için önem arz eden, her seviyede farklı anlam taşıyan ve her dönemde hayati gereklilik ifade eden bir kavram olup, güvenlik ihtiyacı varlığı koruyan ve sürdürme amacı taşıyan davranış biçimlerinin bütünü olarak tanımlanabilir. Güvenlik, yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, tehdit bulunmaması, emniyet gibi anlamlara gelmektedir. Siber uzay kavramı, bilginin tanımlanması, kaydedilmesi, iletilmesi amacıyla ağ merkezli sistemler ve elektromanyetik spektrumun kullanılmasıyla oluşturulan, internet ve benzeri haberleşme ağlarını kapsayan bir sanal ortamdır (Bilişim ve iletişim ağlarını şekillendiren uzay).

Siber savaş kavramı ise ekonomik, politik, askeri veya psikolojik amaçlar için hedef seçilen ülkeye yönelik bilgi ve iletişim sistemleri üzerinden gerçekleştirilen organize saldırılar bütünüdür. Siber tehdit kavramı, siber uzayda bulunan bilginin bozulması, ifşa edilmesi, erişilebilirliğinin kesintiye uğraması gibi istenmeyen durumlara neden olma potansiyelidir. Eğitim, finans, ulaştırma, iletişim, enerji, savunma vb. birçok alanda teknolojik gelişme sağlayan devletlerin siber uzayın bir aktörü haline gelmesi, siber suçların etki alanının genişlemesine ve yarattığı tehdit potansiyelinin artmasına neden olmaktadır. Bilginin ve bilişim sistemlerinin korunması ve tehditlerin ortadan kaldırılması gerekliliği siber güvenlik kavramını ortaya çıkarmıştır. Askeri ve jeopolitik üstünlüğü öne çıkaran taarruz ve savunma stratejileri yerine, bilişim sistemleri üzerinde (siber uzayda) gerçekleştirilen siber savaş teknikleri ile kritik altyapı sistemleri kesintiye uğratılarak çökertilebilmektedir (Zero Day saldırıları). I.ve II. Dünya Savaşı ile Soğuk Savaş sonrasında güvenlik algılamalarının değişmesi ile ulusal güvenliğe yönelik tehditler farklılaşmış, konvansiyonel savaşlardan çok daha etkili olacağı öngörülen siber savaşlar önemli bir tehdit parametresi haline gelmiştir. Konvansiyonel savaş ile siber savaş kavramlarını şu şekilde karşılaştırmak mümkündür (Bayraktar, 2018:77-80)

| KRİTERLER | KLASİK SAVAŞ VE GÜVENLİK | SİBER SAVAŞ VE GÜVENLİK |
|---|---|---|
| **SALDIRI KAYNAĞI VE HASAR TESPİTİ** | Saldırıların nereden kaynaklandığının bulunması ve hasar tespiti (fiziksel) kolaydır. | Saldırı kaynaklarının bulunması ve hasar tespiti zordur (bazen imkansızdır). |
| **HIZ** | Bir füze, helikopter, uçak, top, tank veya başka bir silah sisteminin hızı kadardır. | Işık hızındadır. (Zero Day) |
| **SİLAH SİSTEMLERİ** | İHA/SİHA, tabanca, tüfek, e bombası, hava savunma sistemleri, radar vb. | Çipler, bilgisayarlar, yazılımlar veya bilgi sistemlerinde kullanılan donanımlar. |
| **TEKNOLOJİ İHTİYACI** | Genelde ileri teknoloji sistemi gerekir. | Bilgisayar kullanımı olduğundan yüksek teknik ve teknoloji gerekir. |
| **MALİYET** | Silah sisteminin pahalılığına bağlıdır. | Genelde çok ucuzdur (bilgisayar maliyeti). Fakat kullanım yeteneği gerektirir. |
| **ETKİ** | Fiziksel alanda etkilidir. | Bilgi ve iletişim sistemleri alanında etkilidir. |

Yapay zekâ (Artificial Intelligence), insan gibi akılcı düşünen ve davranan sistemlerle ilgilenen bilimsel bir disiplindir. Başka bir ifadeyle yapay zekâ, hem bilişsel sistemleri simule etmeyi (akılcı/ insan gibi düşünme) hem de akıllı sistemler yapılandırmayı (akılcı/ insan gibi davranma) amaç edinmektedir. Her iki çabanın da ortak yönü bilginin akılcı ve insanda olduğu gibi işlenmesinin ilkelerini araştırıp bulmaktır. Ayrıca yapay zekâ, insan zekâsının yapabileceği görevleri gerçekleştirebilecek sistemleri oluşturmak için dijital teknolojinin kullanılmasını gerektirir. Turing Testi; Alan Turing tarafından geliştirilen test, seçilen şahıslar (C) tarafından bir insan denek (B) ile makine deneğe (A) sorular sorarak hangisinin makine hangisinin insan olduğunu ayırt edebilme başarısına dayanmaktadır. Yapay zeka tarihindeki önemli gelişmeler incelendiğinde Isaac Asimov' un "Ben Robot" isimli romanı yazması, Deep blue isimli bir bilgisayarın satrançta ilk kez bir satranç şampiyonu insanı yenmesi, Google'ın Siri adlı uygulaması ve Go isimli oyunda bir makinenin insanı yenmesi olayları sayılabilir (Say,2018:115-117).

Yapay zekanın istihbarat biliminde de kullanılan başlıca uygulama alanlarından birisi *Yapay Sinir Ağlarıdır - YSA*(Günther ve Bernhard, 2005:31-33) YSA, insan beyninden esinlenerek geliştirilmiş, ağırlıklı bağlantılar aracılığıyla birbirine bağlanan ve her biri kendi belleğine sahip işlem elemanlarından oluşan paralel ve dağıtılmış bilgi işleme yapılarıdır. Biyolojik sinir ağlarını taklit eden bilgisayar programları bilgiler arasında ilişkiler kurma yeteneğine sahiptir. YSA'nın kullanıldığı alanlar; denetim, sistem modelleme, ses tanıma, el yazısı tanıma, parmak izi tanıma, elektrik işareti tanıma, meteorolojik yorumlama, otomatik araç denetimi, fizyolojik işaretleri (kalp fonksiyonları gibi) izleme, tanıma ve yorumlama olarak sayılabilir. Ayrıca, endüstriyel (yer altındaki gaz ve petrol alanlarını tespit etme), ulaştırma ve havacılık (Ford Motor Co.'da fren denetimi, NASA'da uzay mekiği, uçaklarda erken uyarı sistemi, sürücüsüz kara taşıtı seyri, havaalanlarında bagaj geçişlerinde bomba tanıma), finans, borsa ve kredi kartı (Citibank, World Bank mali tahminleri, American Express sahtekarlıkları önlemek için el yazısı ve imza tanımlama, Veratex Corp. Borsa müşteri tahminleri), tıp, bio medikal ve ilaç sanayi(hastaların ilaçlara karşı tepkilerinin incelenmesi ve kanser tanısı) ve iletişim sanayi (belgegeçer ve telefon hatlarının güncellenmesi) alanlarında "Öngörü, Sınıflandırma, Veri birleştirmesi, Veri kavramlaştırılması, Veri süzülmesi, Resim veya görüntü işleme" sınıflandırılmasına göre uygulanır. Bu sıralama istihbarat sürecindeki adımları anımsatmaktadır.

Yapay zekânın diğer bir uygulama alanı olan *Uzman Sistemler*, temelde insan düşüncelerini gerçekleştirmek amacıyla bilgisayar tarafından işlenen yazılımlardır (uzmanların bilgi ve deneyimlerinin bilgisayara aktarılması). *Bulanık mantık* ise, bulanık küme teorisine dayanan bir matematiksel disiplindir (Uzun-kısa, sıcak-soğuk, hızlı-yavaş, siyah-beyaz yerine insan mantığında olduğu gibi; Uzun, ortadan uzun, orta, ortadan kısa, kısa ; Sıcak, ılık, az soğuk, soğuk, çok soğuk vb. ara değerlere göre çalışır).

Başka bir yapay zekâ uygulaması olarak *Genetik Algoritma*, evrimsel hesaplama tekniğinin bir parçasıdır. Darwin' in evrim kuramındaki doğada en iyinin yaşaması kuralından esinlenerek, bir veri öbeğinden özel bir veriyi bulmak için kullanılır (sanal olarak evrimden geçirilmesi). En yaygın uygulamalardan birisi olan *Makine Öğrenmesi (yapay öğrenme),* matematiksel ve istatistiksel

yöntemler kullanarak mevcut verilerden çıkarımlar yapan, bu çıkarımlarla bilinmeyene dair tahminlerde bulunan; yapısal işlev olarak öğrenebilen ve veriler üzerinden tahmin yapabilen algoritmaların çalışma ve inşalarını araştıran bir sistemdir (yüz tanıma, belge tanıma ve spam tespiti gibi uygulamalar). Gözetmenli (sınıflandırma, regresyon), gözetmensiz (kümeleme,boyut azaltımı, anomali tespiti) ve yarışmacı öğrenme olarak üçe ayrılmaktadır. Benzetme yapılacak olursa; bir öğrenci konuya çalışıp ders kitabındaki örnek çözümlü soruları çözer ve öğrenir. Ardından kitapta bulunmayan ama aynı bilgiye dayanan farklı bir test önüne konulur. Öğrenci cevapları bilmeden testi çözer. Sonra değerlendirmeye alınır, ne kadar başarılı olduğu görülür. Eğer ezberci bir öğrenciyse benzeri kitapta olmayan soruları muhtemelen yanlış yanıtlayacaktır. Eğer işin temelini anlayan bir öğrenciyse farklı tarzda soru gelse bile doğru çözebilecektir. Öğrenci test sonucunu ve nerelerde hata yaptığını inceler. Kendisine "Şu soruda şöyle bir genelleme yapmışım ama aslında iş bu kadar basit değilmiş", "Şu etkeni hesaba katmayı düşünemedim" gibi dersler çıkarır. Ardından derslerini almış bir gözle kitabını tekrar çalışır ve tekrar testi çözer. Yeterince iyi sonuç alana kadar hatalarını keşfedip konunun püf noktalarını öğrenmeye çalışır[3].

Günümüzde makine öğrenmesi ile birlikte popüler olan diğer bir uygulama olan *Veri Madenciliği* ise verilerdeki geçmiş ve bilinmeyen özelliklerin keşfedilmesine odaklanır (Jonas ve Harper, 2006: 4-6). Bu veri tabanlarında bilgi keşfi analizinin bir adımıdır. Bilişim teknolojilerinin ve sosyal medya mecralarının yaygın kullanımına bağlı olarak veri miktarı çok büyük boyutlara ulaşmış ve çeşitlenmiştir. Özellikle sosyal medya mecralarında üretilen ses, görüntü ve yazı gibi veri kümeleri inanılmaz boyutlara ulaşmıştır. *Büyük veri (Big data)* olarak adlandırılan bu veri kümelerini işlemek, veriyi bilgiye çevirmek için geleneksel yöntem ve araçlar yetersiz kalmaya başlamıştır (Lim, 2016:621-623).

Büyük veri kümelerinin yanı sıra paralel çalışan Grafiksel İşleme Birimi (GİB,GPU) ve Merkezi İşleme Birimi (MİB,CPU) gibi donanımlarda elde edilen gelişmesiyle birlikte daha fazla sayıda sir ve katmana sahip YSA'nın eğitilmesi ve çalıştırılması mümkün hale gelmiştir. Daha fazla derinliğe ve genişliğe sahip bu ağlar *'Derin Sinir Ağları'*, eğitimleri de *Derin Öğrenme (Deep Learning)* olarak adlandırılmıştır. Derin öğrenme yaklaşımlarının en önemli özellikleri; önişleme, boyutsal indirgeme, öznitelik çıkarma ve sınıflandırma aşamalarının tek ağda birleştirilmiş olmasıdır. DSA, ses işleme ve sınıflandırma için de kullanılmasına rağmen daha çok görüntü işleme, görüntü sınıflama, görüntü içindeki nesnelerin birbiriyle olan ilişkisinin anlamlı bir şekilde ortaya konulması için kullanılmaktadır (Özellikle kriminal araştırmalar ve güvenlik alanında kullanılır). DSA'nın kullanıldığı alanlar: Görüntü ve video işleme, örüntü, nesne, sinyal ve ses tanıma, doğal dil işleme, otomatik araç denetimi, fizyolojik işaretleri izleme, tanıma ve yorumlamadır. Derin öğrenme çalışmalarında Phyton, Java, C++ ve R programlama dilleri kullanılmaktadır. Bahsedilen uygulamalar istihbarat analizleri ve terörizmle mücadelede ihtiyaç duyulan bilgilerin süzme ve kullanımında büyük kolaylıklar sağlamaktadır (Scott ve Hughes,2009:14-21).

İstihbarat, hem bilgi toplayıp analizler yaparak karar vericilerin önünü aydınlatma faaliyeti, hem de karar vericilerin belirlediği politikalar doğrultusunda psikolojik harekât ve propaganda gibi yöntemler kullanarak toplumların algılarını yönetmek olarak ifade edilebilir. İstihbarat disiplini, bir yandan yeni tehditler ile beraber yeni ilgi alanları kazanırken, diğer yandan gelişen teknolojiler sayesinde haber alma yöntem ve vasıtalarına yenileri eklenmiştir. Siber uzayda yaşanan gelişmeler kara, hava ve deniz harekat ortamlarına yeni bir mekan boyutu eklemiş ve siber istihbarat kavramının elde edilen başarılarda kuvvet çarpanı olarak ortaya çıkmasını sağlamıştır[4].

Bilgi teknolojilerindeki gelişmeler, istihbarat faaliyetlerine büyük kolaylıklar sağlarken, diğer taraftan siber uzayın etkin kullanımı büyük güvenlik açıklarını da beraberinde getirmiştir. Bilgi üretebilen, ürettiği bilgiyi teknolojiye, teknolojiyi güce çevirebilen ülkeler bu imkânlar sayesinde küresel haber alma ve kontrol yeteneğine sahip olmaktadır. Teknolojik gelişmeler ile birlikte günümüzde geleneksel istihbarat giderek yerini teknik istihbarat, sinyal istihbaratı, ölçüm ve iz istihbaratı gibi spesifik alanlara bırakmıştır. İnternet ve bilgi sistemleri sayesinde istihbaratın ihtiyaç duyduğu personel ve malzemenin azalmasıyla birlikte bilginin maliyeti düşerken, aynı zamanda kaynaklardaki artış nedeniyle bilgilerin depolanması ve analiz edilmesi için bilgisayarlar istihbarat faaliyetlerinin vazgeçilmez bir parçası haline gelmiştir. Siber istihbarat kavramı, siber uzayda devletin kontrol fonksiyonundan ötürü tehdidin seviyesine göre yakın ve uzak tehlikelerin engellenmesi amacıyla karar vericilere bilgi desteği sağlamak, örtülü operasyon yöntemleri ile olayları yönetmek ve düşmanın istihbarat faaliyetlerini engellemektir.

İstihbarat analizi, çeşitli kaynaklardan toplanan verilerin analizci tarafından süzgeçten geçirilerek gerekli olan kısımlarının işlenmesidir. İstihbarat örgütleri geliştirmekte oldukları yapay zeka projeleri büyük veri akışındaki gerekli kısımların süratle süzülmesini sağlayarak analizciye vakit kazandırmakta ve analizcinin daha fazla düşünebilmesine yardımcı olmaktadır. Oren Etzioni' nin Farecast isimli büyük veri analizine dayalı uçak bileti artış/azalış programını %75 doğrulukla bularak Microsoft Bing arama motoruna entegre etmesi, yolcuların bilet başına 50 dolar tasarruf etmesini sağlamıştır. Amazon'un ideal kitabı önermesi, Google' ın en uygun web sitelerini sıralaması, Facebook'un kullanıcıların beğenilerini bilmesi veya LinkedIn' in tanıdık kişileri tahmin etmesi gibi, gelecekte de aynı teknoloji hastalıkların teşhis ve tedavi önermelerinde ya da suç işlenmeden önce suçlunun tespit edilmesinde uygulanabilir. Önleyici kolluk istihbaratının pre-crime çerçevesinde anlatıldığı "Minority Report (Azınlık Raporu)" filmi bilim kurgu gibi gözükse de gelecekteki istihbaratla ilgili olarak bilgilendirici niteliktedir.

Potansiyel suçluların gözetleme ve yakalama imkânlarının yanında, mahkumların tekrar suç işleme olasılığını değerlendiren COMPAS adlı yapay zeka sistemi ABD'de kullanılmaktadır.Analizde N=Hepsi yöntemini kullanarak anormallikleri tespit etmek fayda getirmektedir. Ayrıca, para transferinde uzman Xoom firmasının yasal olmayan işlemleri tespit etmesi ve Google Flu Trends' in arama motorundaki bölgelere göre grip hastalığına dair aramaların analizi ile alakalı uygulamalar mevcuttur. N=Hepsi veri girişi ile satrançta bilgisayarı hiçbir insanın yenemeyeceği bir durum mevcuttur. Büyük veri sayesinde analiz işleminde 'neden' sorusunda vakit kaybetmeden 'ne' sorusuna hızlı şekilde cevaplar bulabiliriz. Örneğin, bir bakkal gün sonu karını kendi hesaplayabilir fakat bir ülkenin yıllık gayrisafi milli hasılatını günümüz dünyasında bilgisayar kullanmadan hesaplamak imkânsızdır. Verileştirilen algoritmalarla bir kişinin konumu (ne ile ilgileniyor?), bir motorun titreşimleri(ne zaman bozulacak?), bir insanın sağlık durumu (kalp krizi geçirme zaman aralığı), bir köprünün gerilimi(dayanıklılığı ve ömrü ne kadar?) , sosyal medyada ve telefon görüşmelerinde insan ilişkileri (yakın, hısım, ortak veya hasımları kimler?), piyasaların durumu (borsa düşüş/yükselişi vb.), toplumun yapısı (genel ahlaki, eğitim, moral, ekonomik durumları ile olaylara bakış açısında oluşan genel algı) gibi hayatın tüm alanları ile ilgili elde edilen bilgiler grafikleştirilerek bilginin gizli değerine erişilmektedir.

Sonuçta çeşitli alanlarda elde edilen bu değerler, verileştirmeyle ve ölçülebilir hale getirilmektedir. Veri öğütme teknikleri önceden yalnızca casusluk büroları ve araştırma laboratuvarlarında kullanılmaktayken, bunu sağlık, perakende satış ve banka sektöründe dünya çapında iyi kullanan 23AndMe (Steve Jobs' a ait genetik kodlama programı), Walmart ve Capital One gibi şirketler endüstri anlayışına da değişim ve yenilik getirmişlerdir. Tüm bu örnekler kapsamında yapay zekanın güvenlik ihtiyaçları doğrultusunda istihbarat biliminde kullanıldığı temel sınıflandırma şu şekilde yapılabilir (Mayer-Schönberger ve Cukier,2013:80-101):

- *Doğal dil işleme ve çeviri sistemleri:* Soğuk Savaş döneminde ABD' nin Rus mesajlarını IBM701 makinesi ile anlaşılır hale getirmesi, Candidade projesi ile Kanada parlamentosundaki deşifre edilen metinler, Google translate çevirilerindeki yüksek başarı (yapay zeka mimarı Peter Norwig)

- *Yüz tanıma, ses tanıma ve görüntü işleme:* ABD'de havaalanları güvenliğinde ve Çin'de vatandaşların puanlanmasında (ödül-ceza sistemi) yüz tanıma sistemleri uygulanmakta. Ayrıca Wuhan'da yüz, ses ve görüntü işleyen yapay zeka destekli bir polis merkezi bulunmaktadır.

- *Veri toplama ve veri analizi:* Öngörücü polislik (predictive policing) uygulamaları ve suç aydınlatmaları kapsamında kullanılan PTS/mobil PTS/JETTON/JEMUS gibi uygulamalar, salgı sürecinde maske takmayan vatandaşların drone ile tespiti.

- *Akıllı istihbarat araç gereçleri ve akıllı sistemler:* MilSoft sürü İHA projesi, Kuzey ve Güney Kore arasında yer alan askerleştirilmiş bölgede kullanılan Samsung SGR-A1 platformları.

- *Robotik ve istihbarat:* Güney Kore şirketi DoDAAM' ın Super aEgis II robotları, birden fazla SİHA' nın telefon sinyalleri veya yüz tanıma etmenlerini kullanarak saldırı amaçlı kullanımı, Yeni Zelanda yapay zekâ polisi Ella.

**Terörizmle mücadelede yapay zekâ uygulamaları**

20'nci YY özellikle Avrupa ve Kuzey Amerika tarihinde silahlı çatışmaların siyasetteki rolüne, savaş araçlarındaki dönüşüme sahne olmuştur. Ayrıca ideoloji, endüstriyel teknoloji ve Clausewitz'in savaş kavramı ile beslenmiş yıkıcı bir dönemdir. Kurumsal yapılar bu dönemde yükselişe geçmiş, istihbaratın da kurumsallaşmaya dönüşü bu dönemlerde sağlanmıştır. Özellikle İkinci Dünya Savaşı ve Soğuk Savaş döneminde orduların askeri istihbarat ihtiyacını karşılamak üzere hızlanan teknolojik değişimler ile askeri araştırma ve geliştirme projeleri alışılagelmiş konvansiyonel savaşların yapısını değiştirmiştir. Teknolojik değişimin diğer bir etkisi istihbarat toplama vasıtaları ve iletişim üzerinde olmuştur.

Birinci dünya savaşı döneminde telgraf ve benzeri düşük teknolojili cihazlar kullanılırken, İkinci Dünya Savaşı döneminde ise şifreleme makineleri ve keşif uçakları gibi sinyal istihbaratı elde etmeye yönelik araçlar kullanılmıştır. Alman şifreleme makinesi Enigma' nın şifreleri İngilizler tarafından Bletcley Park'taki çalışmalarla çözülmüştür. Ayrıca ABD' ye ait savaş gemilerinin Alman U-Boat'larının konumlarını tespit etmeye yönelik sensör ve sinyal alıcı cihazları da bu dönemde kullanılmıştır. Hem kod çözme makineleri hem de sensörlü cihazlar karşı istihbarat faaliyetleri bakımından etkili olmuş ve sinyal istihbaratının önemini ortaya koymuştur.

Terörizmle mücadelede kuvvet çarpanı olarak akla gelen en önemli uygulama silahlı ve silahsız İHA'lardır. Birçok terör örgütü ise hâlihazırda gelişimi devam eden droneları kullanarak imkânlarını geliştirme çabasındadır. İnsansız hava araçlarının günümüz şartlarında Dördüncü Sanayi Devrimi' nin bir parçası olarak görülmesi gerekmektedir. Bu durum hükümetler için de hem avantaj hem de dezavantaj olarak değerlendirilerek ekonomi, teknoloji, dijital ve fiziki güvenlik kapsamında tedarik, düzenleme ve kısıtlamalar kapsamında stratejik planlamalara dâhil edilmektedir (McKendrick,2019:3-8).

SİHA ve İHA'lar hem düzensiz ve gayrinizami harplerde hem de klasik savaşlar da kuvvet çarpanı olarak dengelere etki etmektedir. Yine yapay zekâya dayalı silahlarla öldürüldüğü düşünülen İranlı nükleer fizikçi Muhsin Fahrizade suikastında da teknolojik imkanların kullanımının ne kadar etkili bir konuma ulaştığı görülmüştür. Ayrıca ABD ve Almanya istihbarat örgütlerinin 1950' li yıllardan itibaren dünya devletlerini dinlemek için kullandığı Rubicon yönteminin, günümüzde geçmiştekinden farklı olarak üretilen akıllı telefonlar, internete sahip her türlü cihaz veya sosyal medya

hesapları üzerinden kişilere ve devletlere yönelik istihbarat toplama şekillerine dönüştüğü düşünülmektedir. Bu konuda bir dönem CIA için çalışan teknoloj uzmanı Edward Snowden' ın da ifşaatları da aydınlatıcı olmuştur. 20.yy istihbaratı ayrıca, güvenlik alanındaki talepler ve yayılmalar ile devletlere yönelik iç ve dış tehditler etrafında şekillenmiştir. İstihbaratın geleceği hakkında fikir sahibi olabilmek için güvenliğin gelişen doğasını ve tehditlerin dinamiklerini incelemek gerekmektedir (Brantly,2018:564-566).

Düşman kuvvetlerin hamle yapacakları bölgeleri önceden öğrenme, sahip oldukları teknik araçları ve kapasiteyi belirleme, konumlandıkları stratejik bölgeleri tespit etme ve kendi aralarındaki iletişimi analiz edip dinleme gibi kabiliyetler muharebe sahasında üstünlük sağlayacaktır (Ganor,2021:606-607).

Türkiye'de özellikle son dönemde savunma sanayiinde yaşanan sıçrama SIGINT faaliyetlerinde de etkisini göstermektedir. Bazı resmi ve sivil kuruluşlar bu alanda çalışmalarına hız vermiştir. TÜBİTAK, Elektronik İstihbarat Çözümleri kapsamında IF Dönüştürücü Sistemler, Spektrum Gözetleme Sistemleri, Mikrodalga Frekans Genişletici, Yarı-İletken Tespit Sistemi gibi ürünk geliştirmiş, üretmiş ve bu alanda yeni çalışmalara hız vermiştir. BAYKAR, sinyal istihbarat sistemleri kapsamında gerçek zamanlı istihbarat, keşif ve gözetleme gerçekleştirebilen, geniş frekans aralığında çalışabilen, taşınabilir, yüksek performanslı BS-101 Sinyal İstihbarat Sistemini üretmiş ve hâlihazırda kullanılan Bayraktar TB-2 İHA üzerinden denemelerine başlamıştır. Bu cihazla İHA'lar üzerinden telsiz ve radar tespitine ek olarak dinleme yapma kabiliyeti de kazanılmıştır. ASELSAN, radar ve elektronik harp kapsamında geliştirdiği KORAL ED ve KORAL E sistemlerini askeri araçlar üzerine entegre ederek yerli bir taarruz sistemi üretmiştir. KORAL ED sistemi tespit, teşhis ve yön bulma kapsamında ELINT faaliyetleri gerçekleştirirken; KORAL E sistemi çoklu hedef karıştırma, tehdit karıştırma ve aldatma yeteneğiyle SIGINT faaliyetleri gerçekleştirmektedir.

Bu gelişmeler Türk Silahlı Kuvvetleri'nin harekât kabiliyetini büyük ölçüde artırarak Türkiye' nin bölgesel çapta rekabet gücünü artırmaktadır. Türkiye, bölgesinde stratejik olarak önemli bir konuma sahip olması sebebiyle, savunma sektöründe kazanmış olduğu bu bilinci artırarak devam ettirmeli ve gelişme sürecini akademik, teknik ve taktik kabiliyetlere sahip öğelerin işbirliğiyle sürdürmelidir.

**Sonuç**

Terörizmle mücadelede yapay zeka uygulama, yazılım ve modelleri devletlerin askeri imkan ve kabiliyetlerini artırma kapsamında içinde bulunulan çağın yeni ve vazgeçilmez alanlarından biri olarak görülmektedir. Ülkeler rakipleri karşısında üstünlük sağlamak, vatandaşlarını ve sınırlarını korumak için teknoloji ile askeri sistemlerin kullanılmasına ciddi yatırımlar yapmaktadır. Teknolojik güce sahip ülkeler bu güç ile hem ihtiyaç duydukları ülkeleri yanlarına çekerek yeni müttefikler kazanmakta hem de ciddi ekonomik kazanımlar elde etmektedirler. 21'inci yüzyıl dünyasında durağan bir dış politika ile milli birlik ve bütünlüğü daim kılmak mümkün değildir. Özellikle Türkiye'nin bulunduğu coğrafyada hüküm süren siyasi karmaşa göz önünde bulundurulduğunda sorunları yalnızca diplomasiyle çözmeye çalışmak bazen karmaşık ve zor bir hal alabilmektedir.

Yapay zekâ her geçen gün kendini geliştiren bir bilim dalıdır. Bu sebeple hayatın her alanındaki teknolojik gelişmelerle birlikte varlığını daha çok hissettirmektedir. Sistem ve faaliyetlerin bilgisayarlar yolu ile yürütülmesinin insan faktörünün de nicelik ve niteliğine etki edeceği kaçınılmaz bir gerçektir. Özellikle istihbarat bilimi ile ilgili olarak analiz konusuna yapay zekanın büyük katkısının olacağı öngörülmektedir. Bu bağlamda ülkeler karar alma mekanizmalarını bağımsız işletebilmek için yapay zeka sistemlerine dayalı Sinyal İstihbaratı (SIGINT) ana başlığında değerlendirilen Elektronik İstihbarat (ELINT), İletişim İstihbaratı (COMINT) ve Görüntü İstihbaratı (IMINT) faaliyetlerini yürütmek durumundadır.

Günümüzde başta internete sahip cihazlar (IoT), web siteleri, sanal uygulamalar ve sosyal medya bağlantıları olmak üzere veri akışı artışı geçmişe göre katlanarak artmaya devam etmektedir. Mevcut bilgi miktarı incelendiğinde kaynakların yaklaşık olarak %95' inin açık kaynak, %5' inin ise gizli kaynak olduğu değerlendirilmektedir. Bu büyük veri okyanusunda açık kaynaklarda ihtiyaç duyulan bilgiyi süzerek analiz etme aşamasında yapay zeka uygulamalarının gelecekte analizciye daha çok yardım edeceği tahmin edilmektedir. Her ne kadar yapay zekânın analize bir çok katkısı olacaksa da, insan zihninin ve duygularının tamamına sahip olamayacağı açıktır. İstihbarat biliminde yapay zekâ uygulamaları insan unsurunun yerini almaktan ziyade, nitelikli ve yapay zekayı kullanabilecek insan gereksinimini ortaya çıkaracaktır.

Sonuç olarak, büyük veri çağında güvenlik sistemleri, terörizmle mücadele, iklim değişiklikleri, hastalıklara çözüm bulma, iyi yönetim ve ekonomik kalkınma gibi global problemlere yeni çözüm önerileri aranmakta olsa da, bu yeni dönemle birlikte gelen değişime kurumlar ve toplum bireyleri olarak hazır olunması gerekmektedir. Bu anlamda sadece istihbarat biliminde mevcut olan toplama araç ve yöntemlerinin değil diğer bilimlerdeki çalışmaların da yapay zeka uygulamaları etkisi altına girmesi kaçınılmazdır. Gelecekte başta güvenlik, saldırı ve savunma sistemleri ile istihbarat ve terörizmle mücadele faaliyetleri olmak üzere her alanda yapay zeka - insan rekabetinden ziyade insan - makine ortaklığına ihtiyaç duyulacağı değerlendirilmektedir.

**KAYNAKÇA:**


Agrell, W., (2012), The Next 100 Years? Reflections on the Future of Intelligence, Intelligence And National Security.

Bayraktar, G., (2018), Siber Savaş ve Ulusal Güvenlik Stratejisi, Yeniyüzyıl Yayınları, İstanbul.

Brantly, A.F., (2018), When Everything Becomes Intelligence: Machine Learning and The Connected World, Intelligence And National Security.

Chen, H., (2005), Artificial Intelligence for Homeland Security, University of Arizona,Lauder School of Government, Diplomacy & Strategy and International Institute for Counter-Terrorism (ICT), IDC Herzliya, Israel

Çetin, E., (2018), Yapay Zeka Uygulamaları, Seçkin Yayınları, Ankara.

Ganor, B., (2021), Artificial or Human: A New Era of Counterterrorism Intelligence?

Günther, G. ve Bernhard, N.,(2005), Yapay Zeka, İnkılap Yayınları, İstanbul.

Jonas, J. ve Harper J. (2006), Effective Counterterrorism and the Limited Role of Predictive Data Mining, Policy Analysis

Lim, K.,(2016), Big Data And Strategic Intelligence, Intelligence And National Security.

Mayer-Schönberger, V. ve Cukier, K., (2013), Büyük Veri, Paloma Yayınevi, İstanbul.

McKendrick, K.,(2019), Artificial Intelligence Prediction and Counterterrorism, Research Paper.

Say, C., (2018), 50 Soruda Yapay Zeka, Bilim ve Gelecek Kitapçılığı, İstanbul.

Scott, L. ve Hughes,R.G., (2009), Intelligence in the Twenty-First Century, Intelligence And National Security.

Treverton, G. F. (2004). Reshaping national intelligence for an age of information. Cambridge: Cambridge University Press.


---

[1] Atıf için: Sevinç, S. (2021). Yapay Zekâ Uygulamalarının Güvenlik, Terörizmle Mücadele ve İstihbarata Katkıları. Erişim adresi: https://www.teram.org/Icerik/yapay-zek-uygulamalarinin-guvenlik-terorizmle-mucadele-ve-istihbarata-katkilari-165

[2] Jandarma ve Sahil Güvenlik Akademisi Güvenlik Araştırmaları Merkezi Müdürlüğü Öğt.Üyesi

[3] Microsoft edge sesli okuma programı bu mantığa göre çalışmaktadır.

[4] SİHA'ların terörle mücadeledeki etkisi örnek olarak verilebilir.

Semih SEVİNÇ