



International
SOCIAL SCIENCES
STUDIES JOURNAL



SSSjournal (ISSN:2587-1587)

Economics and Administration, Tourism and Tourism Management, History, Culture, Religion, Psychology, Sociology, Fine Arts, Engineering, Architecture, Language, Literature, Educational Sciences, Pedagogy & Other Disciplines in Social Sciences

Vol:5, Issue:41
sssjournal.com

pp.4224-4234
ISSN:2587-1587

2019
sssjournal.info@gmail.com

Article Arrival Date (Makale Geliş Tarihi) 02/07/2019 | The Published Rel. Date (Makale Yayın Kabul Tarihi) 23/08/2019
Published Date (Makale Yayın Tarihi) 23.08.2019

İSTİHBARAT VE YAPAY ZEKÂ İLİŞKİSİ¹

RELATIONSHIP BETWEEN INTELLIGENCE AND ARTIFICIAL INTELLIGENCE

Yüksek Lisans Öğrencisi. Mehmet Akif ORUÇ

İstanbul Aydın Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler ve İstihbarat İncelemeleri Bölümü, İstanbul/TÜRKİYE



Article Type : Research Article/ Araştırma Makalesi

Doi Number : <http://dx.doi.org/10.26449/sssj.1680>

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

ÖZ

Gelişen teknoloji ve internet kullanımının yaygınlaşmasıyla yeni bir boyut kazanan istihbarat ve güvenlik faaliyetleri yapay zekâ ve robotik teknolojisinin gelişimiyle çok farklı bir yapıya dönüşmektedir. Yapay zekâ, istihbarat ve güvenliğin geleceğinde önemli bir yere sahip olacaktır. Bu çalışmada, istihbaratın; başta yapay zekâ olmak üzere teknolojik gelişmelerden nasıl etkilendiği ve gelecekte nasıl etkileneceği ortaya konulmuştur. Günümüzde istihbarat amacıyla bilginin, toplanması, tasnif edilmesi, değerlendirilmesi, analiz edilmesi ve yorumlanması sürecinin tamamı siber istihbarat ve yapay zekâ yöntemleriyle yapılabilmektedir. Üstelik bu süreç klasik yöntemlerden daha geniş bir alanda ve daha ucuz, insan analistlerden daha hızlı ve daha rasyonel bir şekilde yürütülmektedir. Bu çalışma istihbarat çarkı olarak ifade edilen bahsi geçen sürecin gelecekte yapay zekâ ile donatılmış tam otonom sistemler (robot istihbarat analistleri ve saha uzmanları) tarafından yürütülebileceğinin olabirliğini ortaya koymaktadır.

Anahtar Kelimeler: İstihbarat, Yapay Zekâ, Siber İstihbarat, Siber Uzay, Espiyonaj

ABSTRACT

Intelligence and security activities, which gained a new dimension with the development of technology and widespread use of the Internet, are turned into very different structure with the development of artificial intelligence and robotic technology. Artificial intelligence will have an important place in the future of intelligence and security. This paper is examined how intelligence especially artificial intelligence is affected by technological developments, and how it will be affected in the future. Today, the whole process of collecting, classifying, evaluating, analyzing and interpreting information for intelligence purposes can be done by cyber intelligence and artificial intelligence methods. Moreover, this process is carried out by artificial intelligence wider and cheaper than classical methods, faster and more rationally than human analysts. This paper points out the possibility that the so-called intelligence cycle can be carried out by fully autonomous systems which equipped with artificial intelligence (robotic intelligence analysts and robotic field experts) in the future.

Key Words: Intelligence, Artificial Intelligence, Cyber Intelligence, Cyber Space, Espionage.

1. GİRİŞ

Bu çalışma istihbarat faaliyetlerinin yapay zekâ ile nasıl daha etkili, daha ucuz ve daha hızlı yapılabileceğini, istihbaratta, nesnelere interneti, veri madenciliği, makine öğrenmesi, veri bilimi ve yapay zekâ kavram ve disiplinlerinden nasıl faydalanılabileceğini ve tüm bu kavramlar çerçevesinde gelecekte istihbaratın ne şekilde yapılacağını ortaya koymak için hazırlanmıştır. Çalışmada literatür taraması yapılarak tarama yöntemi kullanılmıştır.

¹ Bu makale Mehmet Akif ORUÇ'un "İstihbaratın Geleceği: Siber Uzayda İstihbarat ve Karşı İstihbarat Faaliyetlerinde Yapay Zekâ ve Veri Bilimi Kullanımı" başlıklı yüksek lisans tezinden türetilmiştir.

İstihbarat, siber istihbarat ve yapay zekânın tarihi gelişimi incelenerek, istihbaratın, bugünkü haline nasıl dönüştüğü, gelecekte nasıl dönüşebileceği ile ilgili çıkarımlar yapılabilmektedir. Siber istihbaratın bilim ve teknolojinin gelişmesi ile nasıl ortaya çıktığı, siber uzay diye adlandırılan, bilişim altyapı ve hizmetlerini, interneti, gerçek uzayı ve insanı kapsayan alanın, nasıl meydana geldiği ve bu alanın ne tür risk ve avantajlar barındırdığı soruları incelenmiştir.

İstihbarat ve yapay zekâ hakkında neredeyse hiç akademik çalışma bulunmaması literatür taraması açısından bazı zorluklara neden olsada, her bir disiplin ile ilgili geniş literatür taraması yapılarak disiplinler arası bağlantı kurulmuştur. Ayrıca istihbarat teşkilatlarının ve devletlerin yöneticilerinin yapay zekâ ve siber uzay hakkındaki söylemlerinin analizi yapılarak istihbaratın, gelecekte yapay zekâyı çok yoğun bir şekilde kullanacağı sonucuna varılmıştır.

Günümüzde istihbarat amacıyla bilginin, toplanması, tasnif edilmesi, değerlendirilmesi, analiz edilmesi ve yorumlanması sürecinin tamamı siber istihbarat ve yapay zekâ yöntemleriyle yapılabilmektedir. Üstelik bu süreç klasik yöntemlerden daha geniş bir alanda ve daha ucuza, insan analistlerden daha hızlı ve daha rasyonel bir şekilde yürütülmektedir. Bu çalışma istihbarat çarkı olarak ifade edilen bahsi geçen sürecin gelecekte yapay zekâ ile donatılmış tam otonom sistemler (robot istihbarat analistleri ve saha uzmanları) tarafından yürütülebileceğinin bilim kurgu olmaktan, nasıl bilimsel bir gerçeğe dönüştüğünü ortaya koymaktadır.

Dünyadaki küresel veri miktarı son yıllarda bilgi işlem gücü olan nesnelere artışına paralel olarak çok hızlı bir şekilde artmıştır. Öyleki içinde bulunduğumuz zaman dilimi veri ve bilgi çağı olarak adlandırılmaktadır. Veri çağı beraberinde yeni bilimsel disiplinleride getirmiştir. Büyük Veri (Big Data), Veri Madenciliği (Data Mining), Veri Bilimi (Data Science), Makine Öğrenmesi (Machine Learning), Derin Öğrenme (Deep Learning) ve Yapay Zekâ (Artificial Intelligence) bu yeni disiplinlerden birkaçıdır. Gelecek ve yeni dünya düzeni bu yeni kavramlar üzerinden şekillenmektedir. Tüm bu disiplinlerin tarihi gelişimleri incelendiğinde, aslında en eski olanın varlığının bile birkaç onyılda uzun süre olmadığı görülmektedir. Bu çalışmada Yapay Zekâ kavramı diğer tüm bahsi geçen kavramları kapsayacak şekilde kullanılmıştır.

Dördüncü endüstri devrimi ve bilgi çağının getirdiği teknoloji ve büyük miktardaki verilere birde eşyanın interneti ve robotik gelişmeler eklenince siber uzayın sınırları gerçek uzay ve insanı da içine alan ve insanın hayal gücü sınırlarını aşan bir genişliğe ulaşmaktadır. Böyle bir alan istihbarat açısından birçok zorlukla beraber sayısız kolaylığı da beraberinde getirmektedir. Eskiden ufak bir istihbaratı elde edebilmek için onlarca personel, büyük miktarlarda para ve çok uzun sürelere ihtiyaç duyulmakta iken, şimdi siber uzay ve siber istihbaratın imkânlarıyla terabaytlarca bilgiye dakikalar içerisinde ve sadece bir bilgisayar aracılığı ile ulaşılabilmektedir. Gelecekte ise veri bilimi ve yapay zekânın imkanları ile istihbarat çok daha farklı bir boyut kazanacaktır.

2. İSTİHBARAT, SİBER UZAY VE SİBER İSTİHBARAT

2.1. İstihbarat:

İstihbarat, Arapça kökenli bir kelime olup, “bilgi toplama ve haber alma” anlamlarına gelmektedir (TDK, 2019). İstihbarat kelimesinin İngilizce karşılığı olan “Intelligence” kelimesi ise “zekâ ve akıl” anlamlarına gelir (Cambridge Dictionary, 2019). Intelligence kelimesi İngilizce literatüre köken olarak Latince “anlamak, kavramak ve idrak” anlamlarına gelen “intelligere” ve “intelligentia” kelimelerinden geçmiştir.

İstihbarat kelimesinin anlamındaki bu etimolojik farklılık aslında kavramın tanımlanmasının, farklı toplumlar açısından algılanışını ifade etmek adına oldukça manidardır (Özdağ, 2018:19-20). İstihbaratın Türkçe ve Arapça anlamları bu toplumların, istihbarata dair bilginin edinilmesi, toplanması ve derlenmesi üzerinde yoğunlaştıklarını gösterir. Buna karşın, istihbaratın batı dillerindeki anlamı, batı toplumlarının, istihbarat sürecinde elde edilen bilgiyi akıl ve idrak yoluyla değerlendirme ve analiz etmeye odaklandıklarını gösterir.

Benzer şekilde farklı devletlerin resmi kaynaklarından edinilen istihbarat tanımları incelendiği zaman, hukuki, siyasal ve kültürel farklılıkların istihbarat üzerindeki etkileri görülebilir. İstihbarat kelimesinin etimolojik farklılığı aynı zamanda istihbarat faaliyetlerinin tarihsel süreç içerisindeki evrimine de işaret etmektedir. Başlangıçta insanoğlunun en temel duygularından olan korku ve merakını gidermek için “bilgi toplamak, haber almak” olarak başlayan, istihbarat eylemi günümüzde, “elde edilen bilginin, akıl ve zekâ yardımıyla değerlendirilip, yorumlanması ve analizi” şeklinde gerçekleşmektedir.

İstihbaratın tarihi insanlık tarihi kadar eski olmasına rağmen bilimsel bir disiplin olarak istihbarat incelemeleri yaklaşık olarak yarım yüzyıl gibi nisbeten çok kısa bir geçmişe sahiptir (Kahn, 2002) Birçok yeni akademik disiplinde olduğu gibi istihbaratın kavramsal çerçevesi ve tanımı konusunda da farklı bakış açılarından kaynaklı birçok tanıma rastlamak mümkündür.

Örneğin David Kahn, istihbaratı en geniş anlamıyla yani bilgi olarak tanımlar (Kahn, 2002). Sherman Kent ise istihbarata üç ayrı açıdan bakar. Kent'e göre istihbarat, bir tür bilgi, bilgi üreten bir tür örgüt ve istihbarat örgütü tarafından yürütülen bir faaliyettir (Kent, 1968). Warner'ın istihbarat tanımında, rakip güçlerin karşılaştıkları tehditlere karşı tedbir alabilmeleri için özel yöntemlerle yardım edilen bir ilişki ve hizmettir. Pratik anlamda, istihbarat karar alıcıları bilgilendirir ve kararları yönlendirir (Warner, 2009:19). Muzazzez Şenel ve Turhan Şenel'e göre istihbarat hasım veya hasım olması muhtemel devletlerin, planlarını ve planlarını gerçekleştirebilecek güç unsurları hakkında malumat toplamaktır. Sims'e göre istihbarat, rekabetçi bir ortamdaki karar vericiler için bilginin toplanması, analizi ve yayımıdır. NATO istihbaratı ham bilgilerin işlenmesinin neticesi olarak tanımlar (Clark, 2019). Milli İstihbarat Teşkilatı'nın tanımı, NATO'nun tanımına bilginin işlenmesi bakımından benzerlik göstermesine ek olarak bilginin işlenme sürecine yani istihbarat çarkına işaret eder. MİT'e göre "İstihbarat haberlerin (ham bilgilerin) işlenmesi (tasnif, kıymetlendirme, yorum) sonucu üretilen bir ürün veya bilgidir (MİT, 2019). 2004 yılı ABD 'İstihbarat Reformu ve Terörizmin Önlenmesi Yasası'nda ise "ABD içinden ve dışından toplanan ve ulusal güvenliğe yönelik tüm bilgiler kaynağına bakılmaksızın istihbarat olarak tanımlanır" (IRTPA, 2019).

İstihbarat ile ilgili tanımların sayısı arttırılabilir. Ancak yukarıdaki tüm tanımlar ışığında genel olarak "İstihbarat; karar vericilerin, karar verme süreçlerine yardımcı olmak için, toplanılan bilginin, tasnif edilip, değerlendirilmesi, analiz edilip, yorumlanması süreci (İstihbarat Çarkı) sonucunda ortaya çıkan üründür." denilebilir.

2.2. Siber İstihbarat:

Siber istihbarat, bilişim ağ ve sistemleri, internet, bilgisayar ve diğer akıllı makineler ve benzeri siber uzayın imkân ve kabiliyetlerinden faydalanarak gerçekleştirilen istihbarat türüdür.

İstihbarat türleri, istihbaratın zaman içindeki seyriyle şekillenmiştir. Zamanın gerekleri değişip geliştikçe istihbarat alanı ve buna bağlı olarak istihbarat türleri de değişip gelişir. Standart istihbarat kitaplarına bakıldığında, istihbarat alanları arasında siber istihbaratın ya hiç yer almadığı ya da birkaç paragrafta geçiştirildiği görülür. Oysa günümüzde gelişen teknoloji ve bilişim altyapı ve sistemleri, yukarıda saydığımız tüm alanları siber istihbaratın konusu ve alanı haline getirmiştir. Siber istihbarat diğer tüm istihbarat alanlarını kapsar şeklinde bir yaklaşım abartılı olmakla beraber, tüm istihbarat alanlarının siber istihbaratın imkân ve kabiliyetinden faydalanabileceği ve hepsinin siber istihbaratla kesişen bir yanı olduğu da kaçınılmaz bir durumdur.

Fransız ihtilali ve Sanayi devrimi ile modern dünyanın temelleri atıldığında istihbarat içinde yeni bir kapı aralanmıştır. O döneme kadar istihbarata olan ihtiyaç hep sınırlı olmuştur. Siyasal ve endüstriyel devrimler sonrası dünyada ulus-devletlerin sınırları, imkân ve kabiliyetleri ve sahip oldukları güç unsurları hızla gelişmeye başlamıştır. Bu durum savaşta ve bilhassa barışta istihbarata olan ihtiyacı artırmıştır. Sanayideki gelişmeler yeni ve daha etkili silah yapabilmeye imkanını ve silahlanma yarışını başlatmıştır. Dünyada askerî açıdan niceliksel bir büyüme hızla devam ederken, savaşlarda başarıya götürecek şey eskisi gibi nicel büyüklük olmayacaktır. Artık savaşta galibiyet nitelikli bilgiye ve istihbarata dayanmaktadır.

Birinci ve İkinci Dünya Savaşları dünyanın, o döneme kadar gördüğü en büyük yıkımlardır. Bu savaşlar süresince bir taraftan sanayi ve teknolojideki gelişim hız kazanmış, bir taraftan da yeni gelişen teknolojik imkanlar yıkımı artırmıştır. Bilim ve teknoloji neredeyse tamamen savaşa odaklanmış ve savaş kazanmaya yönelik gelişim sergilemiştir. Bu dönemde kriptografi makinaları, uçaklar, denizaltılar, fotoğraf makinaları, telsizler vb. birçok teknolojik araç gereç yapılmış ve geliştirilmeye devam edilmiştir. Bu araç ve gereçlerin en dikkat çekici özellikleri birçoğunun doğrudan savaş aracı ve silah olmanın dışında, doğrudan istihbarat toplama amaçlı veya istihbarata karşı koyma amaçlı geliştirilmiş olmasıdır. İstihbarat toplama araç ve teknolojisi geliştikçe istihbaratın savaşın seyrine olan etkisi ve buna paralel olarak da istihbarat ve istihbarata karşı koymanın önemi artmıştır. Savaş dönemi gelişmeler bilim, teknik, sinyal, ses ve görüntü istihbaratı gibi kavramlarında doğmasına vesile olmuştur.

İkinci dünya savaşı sonrası savaş döneminde edinilen tecrübelerinde büyük etkisi ile kriptoloji, istatistik, şifre çözme gibi alanlarda gelişmeler devam etmiştir. 1960'larda olası bir nükleer saldırı sırasında ordu içi iletişimin kesilmemesi amacıyla internetin geliştirilmesi istihbarata yepyeni bir boyut kazandırmıştır. 1990'lara kadar önemli oranda gelişme yaşayan internet 90'larda ciddi bir sivilleşme ve yaygınlaşma sürecine girmiştir. Artık dünya sıcak ve soğuk savaş dönemlerini geçmiş, topyekün savaşların korkunç yıkımları insanlığı dehşete düşürmüştür. Bunun yerine bölgesel çatışmalar, devlet dışı unsurlar ve terör hareketleri geçmiştir. Bir yandan internet ve kitle iletişim araçları hızla gelişip dünyayı global bir köye dönüştürürken, bir taraftan da uluslararası arenadaki aktörlerin sayısı artmıştır. Devlet dışı aktörlerin de devletler kadar istihbarata ulaşabilme imkânı doğmuştur. Teknolojinin gelişmesi, internet ve kitle iletişim cihazlarının yaygınlaşması, terör örgütleri ve benzeri grupların istihbarat ve karşı istihbarat faaliyetlerinde bulunmasını kolaylaştırmıştır. Bu gelişmeler hiç kuşkusuz siber istihbarat alanını doğurmuştur.

2.3. Siber Uzay:

Siber uzayın, fiziksel altyapı, mantıksal yapı, bilgi ve insandan oluşan dört temel unsuru olduğunu söyleyebiliriz (Clemente, 2015: 163-164). Fiziki sistemlere, haberleşme ağları, iletişim kabloları, bilgisayar ve tüm işlem gücüne sahip cihazların oluşturduğu ağ ve sistemler, uydular, akıllı telefon ve diğer akıllı cihazlar ve benzeri birçok örnek verilebilir. Mantıksal yapılar ise yukarıda saymış olduğumuz fiziki sistemlerin çalışmasını ve birbirleri ile iletişim halinde olmasını sağlayan yazılımları ifade eder. Fiziki altyapılar üzerindeki mantıksal yapılar aracılığı ile elde edilen siber uzayın ürünü olan bilgi ise siber uzayın üçüncü unsurudur. İnternet ve bilişim sistemleri aracılığıyla depolanan ve paylaşılan resim, video, e-posta, vb. birçok veri bilgi unsuru kapsamında değerlendirilmektedir. Siber uzayın dördüncü ve en önemli unsuru ise insandır. İnsan kendisi dışındaki unsurların tasarlayıcısıdır. Siber uzayı meydana getiren fiziki altyapıları kurup, bu yapılar üzerine mantıksal yapıları inşa eden insan, kurduğu bu sistem üzerinde veriyi depolayıp, işleyip, iletimini sağlayıp, kendi yararına kullanan unsurdur.

Siber uzay, endüstriyel üretim tesislerinden, sağlık, ekonomi ve finans sistemlerine, askeri sistemlerden uzay ve istihbarat sistemlerine kadar çok geniş ve kritik bir alanı kapsamaktadır.

Bu kadar geniş ve kritik bir alan istihbarat açısından değerlendirildiğinde birçok tehdit ve tehlikeyi barındırmakla beraber birçok fırsat ve kolaylığı da sağlayabilmektedir. Böyle bir tezatlık oluşması siber uzayın yapısından kaynaklı birtakım parametrelere sahip olmasına bağlıdır. Siber uzayda meydana gelecek güvenlik problemleri ve istihbarat faaliyetlerinin önemini anlayabilmek için zaman, uzay, denksizlik, bilinmezlik ve verimlilik parametrelerini incelemek faydalı olacaktır.

Siber uzayda zaman, gerçek uzaya göre farklı değerlendirilmelidir. Gerçek hayatta aylar süren bir eylem siber uzayda saniyeler içinde gerçekleşebilmektedir. Örneğin gerçek hayatta bir kütüphanenin bir yerden başka bir yere taşınması aylar alırken, siber uzayda bir kütüphane dolusu verinin başka bir yere aktarılması dakikalar içinde gerçekleşebilir. Güvenlik perspektifinden bakılacak olursa, gerçek dünyada, iki ülke arasında çatışma yaşanması ve savaş durumu meydana gelmesi, çeşitli hazırlıkların yapıldığı ve birçok belirtinin olduğu uzun bir süreçtir. Buna karşın siber alandaki çatışma ve savaş çok kısa bir zaman diliminde ve ansızın gerçekleşebilmektedir.

Siber uzaydaki, uzay parametresi gerçek uzayda olduğu gibi sonsuzlukla ifade edilebilecek bir mekandır. Zaman kavramına bağlı olarak sınırlarında daralma ve genişleme olabilmesi, uzayın belirsizliği, siber uzayın boyutlarını ortaya koymaktadır. Siber uzayın sınırları hayal gücünün sınırlarını aşmaktadır.

Siber uzay asimetrik ve bilinmezliklerle dolu bir alandır. Bu alanın asimetrik yapısından kaynaklanan bir denksizlik söz konusudur. Gerçek dünyada birbirine denk olmayan kuvvetlerden genellikle nicel olarak büyük olan kazançlı çıkmaktadır. Siber uzay ise asimetrik çatışma ve savaş alanıdır. Birkaç bilgisayar korsanı büyük bir devlete ciddi anlamda zarar verebilir. Üstelik bu saldırganları tespit edebilmek gerçek dünyaya oranla çok daha zordur. Siber uzayı bu anlamda değerlendirdiğimizde saldırganlar açısından oldukça verimli bir alan olduğu söylenebilir. Gerçek dünyada kara, hava, deniz ve uzay kuvvetleriyle ve çok yüksek maliyetler neticesinde bile elde etmenin mümkün olmayacağı başarı siber uzayda birkaç kişi ve çok düşük maliyetle elde edilebilir. Bu durum siber uzayın güvenlik ve istihbarat açısından önemini bariz bir şekilde ortaya koymaktadır.

3. İSTİHBARAT VE YAPAY ZEKÂ:

3.1. Yapay Zekâ:

Binlerce yıldır filozoflar ve bilim insanları, insan zihninin nasıl çalıştığı ve insan dışı varlıkların zihinlerinin olup olamayacağı sorularına yanıt aramaktadır. Ancak her iki soruya da net cevaplar bulunabilmiş değildir. Bununla beraber bazı bilim insanları, son yıllarda akıllı bilgisayar ve işlem gücü olan diğer akıllı eşyalarda meydana gelen gelişmelerden etkilenerek, makinelerin insanın yapabileceği her şeyi yapabileceğine ve insan üstü bir zihne sahip olabileceğine inanmışlardır (Yılmaz, 2017:4-7). Diğer taraftan karşıt görüşün savunucuları ise, sevgi, saygı, hoşgörü, ahlaki seçimler ve yaratıcı keşifler gibi son derece karmaşık yetilerin hiçbir zaman bir makinenin yapabilecekleri kapsamında olamayacağını dile getirerek, bir önceki görüşe açıkça karşı çıkmışlardır. Her iki bakış açısının da hiç kuşkusuz doğru ve yanlış yanları vardır. Burada önemli olan şey insan-makine rekabetinden ziyade, insan-makine uyumu olmalıdır.

1940'ların sonuna doğru makinelerin düşünüp, düşünemeyeceği veya zekaya sahip olup, olamayacakları sorusu gündeme gelmiştir. Ancak bu sorunun cevabı basitçe 'evet' veya 'hayır' değil bulanık ve belirli olmayan bir cevaptir. Bu noktada yapay zekânın bir disiplin olarak görevi, insanlar tarafından yapıldığında zekâ gerektiren işleri makinelerin yapabilmesini sağlamaktır.

İnsanlar farklı durumlar karşısında farklı yetenekler sergileyebilir. Bir insan bir diğerinden zeki olabilir. Kimi insan matematik ve mühendislikte çok başarılıken kimisi sosyal bilimlerde daha başarılı olabilir. Zekâ insandan insana farklılık gösterebileceği gibi bazen de bir insanda zamana bağlı olarak farklılık gösterir. Yani bazen matematik ve mühendislikle ilgili bir problemi başarıyla çözebilen insan bazen de benzer bir problem karşısında başarısız olabilir. İnsan beynini modelleme temelinde geliştirilen makinelerde benzer şekilde biri diğerinden akıllı olabilecektir.

Zeki makineler ile ilgili ilk makale 1950 yılında ünlü İngiliz matematikçi Alan Turing tarafından yazılmıştır. İkinci dünya savaşı sırasında Alman kriptoloji cihazı Enigma'nın şifrelerinin çözülmesinde kilit rol oynayan Turing, makineler düşünebilir mi gibi klasik anlamsal tartışmalara girmek yerine, başka makinelerin yaptıklarını taklit edebilen Turing makinelerini geliştirerek düşünebilen makinelerin temelini atmıştır. Ayrıca Alan Turing literatüre Turing testi olarak geçen ve geçerliliğini bugünde koruyan bir yapay zekâ testini geliştirmiştir. Turing testi aynı zamanda yapay zekâ çalışmalarında, zeki bir makine geliştirildiğine dair ulaşılmak istenen hedef ve bir referans noktasıdır.

Turing testi iki aşamadan oluşmaktadır. Birinci aşamada bir sorgulayıcı, bir kadın ve bir erkekle farklı odalara konularak sadece yazılı olarak aralarında iletişim kurular. Sorgulayıcı soracağı sorulara alacağı cevaplara göre kimin kadın kimin erkek olduğunu bulmalıdır. İkinci aşamada ise sorgulayıcı benzer şekilde kendisiyle aynı ortamda bulunmayan, bir makine ve bir insana sorular sorar. Sorgulayıcı sorduğu sorulara karşılık aldığı cevaplar neticesinde cevaplayanlardan hangisinin makine hangisinin insan olduğunu anlamaya çalışır (Russell, Norving, 2003:2). Sorgulayıcı makineyi tespit edebilmek için insanın çözmesinin uzun zaman alacağı karmaşık matematiksel sorular soracağı gibi insanı tespit etmek içinde duygusal ağırlıklı sorular sorabilir. Burada matematiksel soru karşısında, makinenin ne zaman gecikmeli cevap vereceğini ve ne zaman hata yapması gerektiğini bilmesi gerekir. Benzer şekilde duygusal sorular karşısında da makinenin insanın duygusal tepkilerini simule edebilmesi beklenir (Negnevitsky, 2005:2). Testin sonunda sorgulayıcı makineyi tespit etmede ne kadar zorlandıysa makine o kadar zekidir. Alan Turing 20. yüzyılda testini geçebilecek bir bilgisayarın programlanabileceğine inanmaktaydı. Bugün hala Turing testi sayesinde bazı özel uzmanlık alanlarında geliştirilen zeki makinelerin performansı bir uzman insan ile kıyaslanarak ölçülebilmektedir.

3.2. İstihbaratta Yapay Zekânın Kullanım Alanları:

İstihbarat ve güvenlik alanında yapay zekâ, veri bilimi, makine öğrenmesi gibi disiplinler son yıllarda yaygın olarak kullanılmaya başlanmıştır. Söz konusu teknolojilerin istihbaratta belli başlı kullanımları aşağıdaki şekilde sıralanabilir.

3.2.1. Doğal Dil İşleme ve Çeviri Sistemleri:

Özellikle soğuk savaş döneminde ABD istihbarat servisleri Rusların konuşmalarını deşifre edebilmek için İngilizce-Rusça çeviri yapabilecek yapay zekâ projelerine ağırlık vermiştir. Böylece doğal dil işleme ve çeviri sistemlerinin istihbaratta kullanımı başlamıştır. Bir dilden başka bir dile çeviri yapmak sadece metin içindeki bütün kelimeleri çevirerek gerçekleşemez. Anamlı bir sonucun çıkması için her iki dile ve bu dilleri konuşan toplumların sosyolojik ve kültürel durumlarına da hâkim olmak gerekir. Bu nedenle çeviri

programları başlangıçta hayal kırıklıklarına sebep olmuştur. Ancak istihbarat teşkilatları için dilbilimci istihdamı önemli bir yere sahip olduğu için çeviride yapay zekâ kullanımı sürekli olarak geliştirilmeye devam etmiştir. Günümüzde yapay zekâ alanındaki gelişmelere paralel olarak çeviri programları da nispeten daha başarılı sonuçlar üretmektedir.

İstihbarat teşkilatları çeviri sistemleri sayesinde yüzlerce dil arasında kısa sürede uzun metinleri çevirebilmektedir. Dolayısıyla yüzlerce dil için ayrı ayrı dilbilimci istihdamı etme gerekliliği ve zaman kaybı bu sistemler sayesinde ortadan kalkacaktır. Bunun yerine insan kaynağı çok daha verimli bir şekilde kullanılabilir. Çeviri sistemleri çok mesafe almış olmasına rağmen henüz istenen seviyelere ulaşamamıştır. Çeviri sistemlerinin yaptığı çeviriler hala insan dil analistlerinin kontrolünden geçmeye muhtaçtır. Hedeflenen ise her dilde hem metin hem ses çevirilerini yüzde yüzlük bir başarıyla gerçekleştirebilmektir.

3.2.2. Yüz Tanıma, Ses Tanıma ve Görüntü İşleme:

Yapay zekâ, veri bilimi, makine öğrenmesi ve bilhassa derin öğrenmede meydana gelen gelişmeler neticesinde yüz ve ses tanıma ile görüntü işleme konularında oldukça başarılı çalışmalar meydana gelmiştir. Uydularda, dronlarda, sokaklarda, hava alanlarında, kamu kurumlarında bulunan güvenlik kameralarında ve hatta cep telefonlarında bulunan yüz ve ses tanıma sistemleri aracılığıyla istihbarat toplanabilmekte ve güvenlik önlemleri alınabilmektedir. Yüz ve ses tanıma sistemleri çeşitli istihbarat ve güvenlik veri tabanlarıyla eş zamanlı entegrasyona sahip olduklarından hedef bir kişiyi anında tespit ederek mevcut dosyasına erişebilmek mümkündür. Bu sistemler adeta istihbarat teşkilatlarının her yerdeki gözü ve kulağı olmuştur.

3.2.3. Veri Toplama ve Veri Analizi:

İstihbarat veri toplanması, tasnifi, analizi ve anlamlandırılması sürecidir. Veri toplama, tasnif ve analiz gelişen teknolojik imkanlar sayesinde hızlı ve güvenilir bir şekilde yapılabilmektedir. İstihbarat analistleri üzerinde oluşan veri toplama ve analizi yükü veri bilimi ve yapay zekâ yöntemleri ile azaltılmaktadır. Bu sayede istihbarat analistleri, analizi yapılmış bilgiden sonuç üretme, anlamlandırma ve karar verme kısmına odaklanma imkânı bulabilmektedir.

Son yıllarda verinin her geçen yıl bir önceki yıla göre katlanarak arttığı gözlenmektedir. Böylesine büyük bir veri yığını arasında boğulma riski her zaman mevcuttur. İstihbarat açısından doğru güvenilir ve anlamlı bilgiye ulaşmak hayati önem taşıdığından, akıllı cihazlar, kameralar, uydular, telefonlar vb. yollarla adeta sel gibi akan verinin analizi de yine aynı teknolojik gelişmeler ve yapay zekâ yöntemleriyle mümkün olacaktır.

Veri toplama ve analizinde yapay zekâ ve veri bilimi yöntemlerini kullanma istihbarat analistlerine hız ve güvenilirlik imkânı vermekle beraber, analistlerin zamanlarını daha verimli kullanabilmelerini sağlamaktadır.

3.2.4. Akıllı İstihbarat Araç Gereçleri ve Akıllı Silah Sistemleri:

Bilgisayar bilimleri ve teknolojik gelişmelerin, savunma ve istihbarat alanına uyarlanması ile akıllı istihbarat araç gereçleri ve akıllı silah sistemleri geliştirilmektedir. İzleme, dinleme, takip ve tarassut eylemleri klasik yöntemler yerine akıllı sistemlerle gerçekleştirilmekte, imha ve etkisiz hale getirme ise akıllı silahlarla yapılmaktadır. İnternetin yaygınlaşması ile uydu, drone, zeplin, şehir içi kamera sistemleri, termal görüntüleme sistemleri, akıllı telefon, akıllı araç ve hatta akıllı ev aletleri aracılığıyla istihbarat toplanabileceği gibi özel olarak istihbarat toplama amacıyla geliştirilen gözlük, kulaklık, dinleme-izleme cihazlarıyla da istihbarat toplama yapılabilmektedir.

3.2.5. Robotik ve İstihbarat:

Geniş anlamıyla herhangi bir iş veya işlemi otomatik bir şekilde gerçekleştirme kabiliyetine sahip mekanik, elektronik veya mekatronik sistemlere robot sistemler denilebilir. Robot sistemlerin geçmişi 12.yy'da yaşamış Ebû'l İzz İsmail İbni Rezzaz El Cezeri ye kadar uzanmakla beraber, son yıllarda yapay zekâ alanındaki gelişmeler ile beraber akıllı robot kavramı ortaya çıkmıştır.

Robot sistemler, ilk olarak mekanik olarak geliştirilmiş ardından elektronik robotlara ve son olarak da yazılım destekli elektro-mekanik bilgisayar sistemlerine dönüşmüştür. Robot denilince akla insana benzeyen sistemler gelse de mutfakta kullanılan elektrikli meyve sıkacağı da otomotiv sektöründe insan eli değmeden otomobil üretimini sağlayan robotik sistemlerde genel anlamda birer robottur. Yapay zekâ

çalışmalarının hız kazanması özellikle savunma ve askeri alanda insana benzeyen, insan gibi hareket edebilen ve aynı zamanda insan bilinç seviyesine sahip akıllı robot askerler yapılması hedefini gündeme getirmiş, kısmen başarılı projeler de gerçekleştirilmiştir. Gelecek birkaç on yılda muhtemelen bu çalışmaların sayısı ve başarı oranı önemli ölçüde artış gösterecektir.

Robot sistemler istihbarat alanında da veri toplama, veri sınıflandırma, veri analizi ve anlamlandırması gibi konularda yaygın bir şekilde kullanılmaktadır. Bu işlemleri akla ilk geldiği şekliyle insansı robotlarla (insan benzeri) olmasa da çeviri robotlarıyla, akıllı kameralarla ve benzeri sistemlerle gerçekleştirmektedirler. Robotik teknoloji, makine öğrenmesi, veri bilimi ve yapay zekâ teknolojilerinin gelişmesi ve birbirleriyle entegre kullanılması halinde robot askerlerde olduğu gibi insansı robot istihbaratçıları da hayatımızın bir parçası haline getirecektir. Kulağa bilim kurgu gibi gelmesine karşın bu durum, bahsi geçen disiplinlerin mevcut hali göz önüne alındığında gerçekleştirilmesi kuvvetle muhtemel bir bilimsel gerçekliktir.

4. İSTİHBARAT VE GÜVENLİKTE YAPAY ZEKÂ KULLANIMININ ÖNEMİ:

İstihbarat analiz süreci bilgi toplama, sınıflandırma, anlamlandırma, analiz etme ve karar verme gibi adımlardan oluşur. İçinde bulunduğumuz bilgi çağında, çok yüksek miktarlarda veri oluşması, bu verilerden istihbarat açısından faydalı bilgiler elde etmek bakımından veri bilimi, makine öğrenmesi, yapay zekâ ve robotik alanlarından farklı aşamalarda ve farklı boyutlarda yararlanılabilmektedir. Verinin toplanması aşamasında robotik cihazlar, nesnelere interneti kapsamındaki tüm akıllı makinelerden faydalanılabilecekken, verinin depolanması, tasnifi ve analizi sürecinde veri bilimi, veri madenciliği, yapay zekâ ve makine öğrenmesinden faydalanılır. Benzer şekilde bir istihbarat verisine göre karar verip aksiyon alabilecek yapay zekâlı robotlardan da bahsedebiliriz. Görüldüğü üzere istihbarat sürecinin farklı aşamalarında farklı disiplinlerden yararlanılabildiği gibi aynı disiplin sürecin birden fazla aşamasına katkıda bulunabilmektedir.

Teknolojinin gelişmesi ve bilgi işlem yeteneği olan cihazların yaygınlaşması istihbaratın geleceğini git gide yapay zekanın eksenine yaklaştırmaktadır.

İstihbarat teşkilatlarının yapay zekâ ile tanışması ve bu alanda çalışmalar yapması, yapay zekanın ortaya çıktığı ilk dönemlerde başlayıp, yapay zekânın popülerlik kazandığı 1980'li yıllarda iyice belirginleşmiştir. Bu bağlamda CIA tarafından 1980'lerin başında bir yapay zekâ yönlendirme grubu kurularak, yapay zekâdan istihbarat, savunma ve diğer devlet kuruluşlarının katılımıyla nasıl fayda sağlanacağı üzerinde çalışmalar yapılmıştır (CIA, 2019).

Günümüzde de istihbarat teşkilatları yüzlerce yapay zekâ projesi yürütmekte ve birçok ülke karşılıklı olarak yapay zekâ ve teknolojik imkanlarla birbirlerinin ajanlarını takip ettirmektedir. CIA Bilim ve Teknoloji Bölümü direktör yardımcısı Dawn Meyerriecks'e göre yaklaşık 30 ülkede dijital gözetim, fiziki takibe gerek kalmayacak kadar gelişmiş durumdadır. Meyerriecks, CIA'nın yürüttüğü 140 yapay zekâ projesinden birine, kolay erişemedikleri büyük başkentlerden birindeki kameraların haritasını çıkarmada makine öğrenmesi ve yapay zekâ algoritmalarından yararlandıklarını örnek göstermektedir. Bu sayede ajanları kameralara yakalanmadan hareket edebilecekler (MCLAughlin, 2019).

Yapay zekanın istihbarata en büyük katkısı zaman ve kapasite bakımından olmuştur. Dronelardan, uydulardan ve diğer cihazlardan ses ve görüntü toplayarak tüm bu verileri analiz edip yorumlamak, istihbarat analistlerine ciddi bir yük getirmektedir. Bu yük yapay zekâ tarafından alınarak istihbarat analistleri mesailerini rutin veri toplama gibi işlemlere ayırmak yerine, yorumlama ve karar süreçlerine ayırabilirler. Yapay zekâ sayesinde istihbaratçılar daha fazla düşünmeye vakit bulabilecekler.

2016 yılında ABD başkanı Barack Obama hükümeti Beyaz Sarayın yapay zekâ kullanımını artırmak için stratejik öneriler içeren bir bildiri yayınlamıştır (Whitehouse, 2019). Bunun üzerine 2017 yılında ve sonrasında CIA, FBI ve NSA başta olmak üzere Amerikan istihbarat topluluğunun bütün kurumları yapay zekâ projeleri geliştirme veya satın almaya hız vermiştir.

Yapay zekanın bir bilim olarak ortaya çıktığı yıllarda kurulan Savunma İleri Araştırma Projeleri Ajansı (Defence Advanced Research Project Agency-DARPA) ilk yıllarından beri istihbaratta yapay zekâyı desteklemiştir. Özellikle Sovyetlere karşı dil çevirisi konusunda önemli yatırımlar yapılmıştır. DARPA kurulduğu 1958 yılından bu yana siber istihbarat ve istihbaratta yapay zekâdan faydalanılması gibi birçok proje gerçekleştirmiştir (DARPA, 2019). 2006 yılında DARPA tarafından İstihbarat Topluluğu (Intelligence Community) kurumları arasında koordineli olarak ileri teknoloji

arařtırmaları yapmak üzere kurulmuř olan, (İstihbarat İleri Arařtırma Projeleri Etkinliđi-Intelligence Advanced Research Projects Activity) IARPA'nın grevleri arasında siber gvenlik ve yapay zekadan nemli bir yer kaplar (IARPA, 2019).

Çin, Rusya ve ABD savunma bakanlıkları savunma ve silah teknolojilerinde yapay zekâ kullanımına yatırımlar yaparak, yapay zekâ alanında lider olma konusunda birbirleriyle rekabet halindedirler (Congressional Research Service, 2019). Rusya devlet başkanı Vladimir Putin'in 2017 yılında niversite đrencilerine yaptıđı konuřmasında, yapay zekâya hâkim olanın dnyanın hâkimi olacađını soylemesi bu rekabetin birinci ađızdan dile getirilmesidir (Pecotic, 2019). Putin'in bu szleri savunma ve istihbaratın geleceđinin yapay zekâ ile řekilleneceđi gerçeđini kanıtlar niteliktedir.

Savunma ve istihbarat amacıyla yapay zekadan faydalanılması son yıllarda artıř gstermektedir (Allen, Chan, 2017). Kuzey ve Gney Kore arasındaki silahsızlandırılmıř gvenlik blgesinin korunmasında Gney Kore gvenlik gçlerine yardımcı olmak amacıyla Samsung tarafından geliřtirilen SGR A1 yapay zekanın savunma ve istihbaratta kullanımı ile ilgili nemli bir rnektir (Say,2019:143). SGR-A1, ses ve grnt tanıma, gzetleme, izleme ve ateř etme zelliklerinin tamamını tek bir nitelerde barındıran akıllı bir istihbarat ve gvenlik robotudur (Kee, 2019). Bu robot istihbaratın gelecekte yapay zekâyı nasıl kullanacađı konusunda nemli bir ip ucu vermektedir.

Yapay zekânın, istihbarat toplama ve analizde birok kullanımı vardır. Akıllı cihazlar, nesnelerin interneti ve sosyal medya kullanımından kaynaklı ok yksek miktarda veri retilmektedir. İnsandan kat kat fazla veri reten cihazların verilerini aynı hızlarda toplamak, iřlemek ve analiz etmek de aynı řekilde akıllı cihazlarla mmkn olmaktadır. Bu nedenle yapay zekâ ađırlıklı olarak veri analiz srecini hızlandırma amacıyla kullanılır. Bunun dıřında ses ve grnt tanıma, bařta olmak zere gzlem ve tarassut amacıyla da sıklıkla kullanılmaktadır (Horowitz ve diđerleri, 2018). Mevcut geliřmeler gelecekte yapay zekânın tm zelliklerinin robotik teknolojiyle birleřerek tam otonom istihbarat sistemlerinin ortaya ıkabileceđini gstermektedir.

İnsana dair yorulma, acıkma, yaralanma ve lme gibi zellikleri olmayan bunun yanı sıra insana oranla daha hızlı ve daha rasyonel karar alabilen akıllı robotlar gelecekte her alanda olacađı gibi askeri alanda ve istihbarat alanında da istihdam edilecektir. Yarım yzyıl nce bilim kurgu olarak grlen bu durum bu gnk bilimsel geliřmelerle rasyonelliđini kanıtlamıřtır.

Trkiye de yapay zekâyı savunma ve istihbarat alanlarında kullanmaya bařlamıřtır. Trkiye Cumhuriyeti Cumhurbaşkanı Recep Tayyip Erdoğan, ODT Teknopark aılıřında yaptıđı konuřmada dnyanın yapay zekâ alıřmalarıyla yeni bir teknoloji dzeyine gittiđini ve Trkiye'nin de bu dzende yerini alacađını soylemiřtir (Cumhurbaşkanlıđı, 2019). Aselsan, Havelsan, STM gibi kurumların zellikle savunma sanayine ynelik bir takım yapay zekâ alıřmaları bulunmaktadır. Bu alıřmalar ođunlukla insansız savunma ve saldırı aralarıyla ilgilidir. Diđer yandan TBMM'de olduđu gibi gvenlik ve istihbarat amacıyla ses ve yz tanınması yapabilen ve eř zamanlı olarak bazı ulusal veri tabanlarında kimlik arařtırması yapan sistemlerde kullanılmaktadır. Ancak Trkiye bir takım bařarılı projelere rađmen henz yapay zekâ konusunun ok bařında olup, tketiciler konumundadır. Veri ađı, yapay zekâ ve siber uzay bilginin bir anlamda zgrleřmesine neden olmuřtur. Bilgi bir veya birka lkenin tekeline dkp insanlıđa mal olacak imkânı bulmuřtur. Bu nedenle her lke siber uzayın hız, uygun maliyet ve kolay eriřilebilirlik zelliklerinden faydalanarak kendi siber uzayının gvenliđini sađlayabilir ve kendi istihbarat faaliyetlerinde yapay zekâ gibi teknolojileri tketen konumdan reten konuma geebilir.

Devletler bir yandan kendi yapay zekâ alıřmalarını ve siber istihbarat faaliyetlerini yrtrken, bir yandan da zel sektr zerinden bu faaliyetlerini yrtmektedir. zellikle son dnemde global lekli teknoloji řirketlerinin, bađlı buldukları devletin istihbarat servisine hizmet ettiđine dair iddialar sıklıkla gndeme gelmektedir. Eski NSA analisti Edward Snowden Facebook'un CIA'e hizmet eden ve insanların mahrem bilgilerini satarak para kazanan bir řirket olduđunu iddia ederken (Chaitin, 2019), CIA Huawei 'i Çin gizli servisi tarafından finanse edilmekle suçlamaktadır (Fisher, 2019). Benzer řekilde Yandex'in Rus gizli servisi tarafından istihbarat elde etmek amacıyla finanse edildiđi iddia edilmektedir. Buna sebep olarak da mail ve navigasyon gibi yksek maliyetli hizmetleri cretsiz olarak sunması gsterilmektedir.

Sonuç olarak, dnyanın geleceđinin, bařta yapay zekâ olmak zere, veri bilimi, makine đrenmesi ve robotik gibi konular erevesinde siber uzayda řekilleneceđi ařıkardır. Dolayısıyla istihbarat ve gvenlik

alanlarının da bu gelişmeler ışığında yapay zekâyı ve söz konusu diğer bilimsel disiplinleri çok daha yaygın ve etkin bir şekilde kullanması gerekmektedir.

5. SONUÇ VE ÖNERİLER

Ünlü İngiliz düşünür Francis Bacon'un "bilgi güçtür" sözüne ilaveten "bilgi, elde edilmesi için yoğun bir çaba gerektiren ve korunması gereken bir güçtür" denilebilir. Bir yandan bilgisayar ve bilgi işlem yeteneği olan makinelerin gelişmesi, diğer yandan internet kullanımının yaygınlaşması, bilgiye erişimi kolaylaştırırken, bilginin korunmasını zorlaştırmaktadır. İnsanlar doğa ile iç içe yaşadıkları ve her türlü dış etkiye karşı savunmasız oldukları dönemlerde hayatta kalabilmek için bilgiye ihtiyaç duymuştur. Başlangıçta hayatta kalmalarını sağlayan bilgi bir süre sonra birbirleriyle ve doğayla rekabet etmelerini sağlayan bir güç haline gelmiştir. İnsanlık çoğalıp geliştikçe bilgi ve bilginin kaynağı olan veri her geçen gün biraz daha artmıştır. Ancak veri miktarındaki bu artış son birkaç yılda insanlık tarihi boyunca oluşan toplam veriden daha fazla olmuştur. Bunun sebebi bilgi işlem sistemleri, işlem gücü ve internet bağlantısı olan nesnelerin yaygın kullanımı ve dünya nüfusunun yarısından fazlasının internet kullanıyor olmasıdır. Aynı nedenlerden ötürü bilgiye erişmek insanlık tarihinin hiçbir döneminde bugünkü kadar kolay olmamıştır. Bu çalışmada ısrarla üzerinde durulan, bilgiye ulaşmayı kolay, hızlı ve ekonomik kılan siber uzay, aynı zamanda bilginin korunmasındaki zorlukları da doğurmuştur.

Bilgiye kolay ulaşılabilmesi istihbarat ve güvenlik açısından son derece önemli bir sonuçtur. İstihbarat teşkilatları, siber uzayda, açık kaynaklardan veya çeşitli araç ve yöntemlerle gizli bir şekilde bilgi toplayabilmektedir. Bugün neredeyse dünya nüfusunun yarısı sosyal medya hesapları üzerinden kendileriyle ilgili her tür bilgiyi paylaşmaktadır. Böylece dünyanın öteki ucundaki bir insan hakkında sadece bilgisayar başında oturarak istihbarat elde edilebilmektedir. Yarım yüzyıl önce aynı şekilde dünyanın uzak bir bölgesindeki biriyle ilgili bilgi edinmek için o bölgeyi tanıyan ve dilini bilen bir ekip görevlendirilerek bölgeye gönderilmesi gerekirdi. Görevlerini büyük bir gizlilikle yapması beklenen bu ekip için ciddi bir para kaynağı gerekirken, başarı garantisi olmayan uzun bir süreç başlatılmış olacaktır.

Siber uzay, gerçek dünyadaki hemen hemen tüm tehdit ve risklerin sanal ortamda yapılmasına olanak vermektedir. Siber uzayda; suçlular suç işleyip, haksız kazanç ve çıkar elde ederek masum insanları mağdur edebilir, terör örgütleri dehşet ve korku yayma amacıyla propaganda yapabilir, mal ve can kayıplarına sebep olan eylemlerini gerçekleştirebilir. Dahası kötü niyetli kullanıcılar tüm eylemlerini kimliklerini gizleyerek, hızlı ve ekonomik bir şekilde yapabilir. Bu nedenle siber uzay güvenlik güçleri ve istihbarat teşkilatlarının kontrolü altında olmalıdır.

Teknolojik ve bilimsel gelişmelerle birlikte güvenlik ve istihbaratın yeni alanı, siber uzay olmuştur. Siber istihbarat siber uzayın imkanlarını kullanarak ekonomik, siyasi, coğrafi, biyografik, bilim ve teknoloji, iletişim ve ulaşım, askeri ve siyasi istihbarat alanlarının tamamıyla ilgili bilgi edinmeyi sağlayabilir. Bu nedenle stratejik istihbarat açısından siber istihbarat ve siber uzay çok önemli hale gelmiştir.

Son 20-30 yılda yapay zekâ alanında büyük gelişmeler yaşanmıştır. Uzman sistemler, doğal dil işleme, makine öğrenmesi ve derin öğrenme modelleri sayesinde dünyanın en karmaşık oyunlarında dünya şampiyonlarını yenmekten, kendi kendine gidebilen arabalara kadar geniş bir alanda yapay zekâ başarılarına örnekler verilebilir. Hayatın her alanında kullanılmaya başlayan ve devletlerin yeni rekabet aracı olan bu yeni nesil teknoloji istihbarat alanında da kendini göstermektedir. Özellikle savunma ve güvenlik alanlarında, ses ve görüntü taraması yapabilen, gözetleme, izleme ve ateş etme yeteneği bulunan tam otonom robot sistemler gibi çok başarılı projelerle karşılaşmak mümkündür.

İstihbaratta yapay zekâdan, alan bilgisi dahilinde birçok şekilde faydalanabilmekle beraber günümüzde ağırlıklı olarak istihbarat toplama ve analiz işlemlerinde faydalanılmaktadır. Akıllı cihazlar, nesnelerin interneti, uydu sistemleri, ses ve görüntü tanıma, doğal dil işleme istihbaratın toplanmasına önemli katkı sağlamaktadır. Toplanan istihbarat makine öğrenmesi, veri bilimi, yapay zekâ vb. yöntemlerle insan analistlerden daha hızlı ve daha rasyonel bir şekilde değerlendirilmektedir.

Yapay zekâ destekli makinelerin uzman sistemlerdeki başarısı, tam otonom robotların insan çalışanların işini elinden alacağı gibi bir kaygıyı doğurmuştur. Klasik yapay zekâ tartışmalarında olan insan-makine rekabeti, yani makine insanın yaptığı her şeyi yapabilir mi tartışması yeni bir boyut kazanmış bir istihdam meselesi haline gelmiştir. Bir otomobilin hiç insan eli değmeden üretilmesi, akıllı bir makinenin bir yargıçtan daha rasyonel yargılama yapabilmesi ve dünya şampiyonlarının dünyanın en karmaşık oyunlarında yapay zekâ karşısında yenik düşmesi, makinelerin, insanların işini elinden alacağı kaygısına neden olmuştur. Yapay zekâ çok büyük başarılarla imza atmasına rağmen bu başarılar belirli konulara

odaklanıldığı durumlarda mümkündür. Diğer bir deyişle henüz Turing testini geçebilen ve geniş açıdan bir insanın yaptığı her işi yapabilen bir makine mevcut değildir. Yani bir makine dünyadaki bütün hukuk sistemlerini öğrenebilir, tüm yaşanmış vakıaları kaydedebilir ve buna göre çok başarılı bir yargılama yapabilir. Ancak bu makinenin başarısı hukukla ilgilidir. Aynı makine ressam ve yüzücü bir yargıcın yetenekleri konusunda başarılı olamayabilir. Tabi ki bu sadece bugünün teknolojisiyle ilgilidir ve gelecekte tüm bunları yapabilen bir makine yapılabilir. Bu çalışmada yapay zekâ makinenin, bir gün, bir insanın yaptığı her şeyi yapabileceğinin mümkün olduğu fikriyle beraber, önemli olanın insan-makine rekabetinden çok insan-makine uyumu olması gerektiği kanaati hakimdir. Dolayısıyla yapay zekâ insan istihbarat analistleri tarafından etkili ve verimli bir şekilde kullanılmalıdır. Gelecekte tam otonom saha robotları ve istihbarat analistlerinin olması, insan istihbaratçıları işsiz bırakmak yerine daha fazla düşünmeye vakti olan karar verici konumuna yükseltebilir. Her iki durumdan hangisinin olacağı tamamen sürecin nasıl yönetildiğine bağlı olacaktır.

İstihbarat, hakkında açık kaynaklardan çok fazla bilgi edinilebilen bir disiplin değildir. Yapay zekâ ise birçok noktada henüz birçok bilinmeyi bulan bir disiplindir. Her ikisi de yaklaşık yarım yüzyıldır akademik birer disiplin olan yapay zekâ ve istihbarat ile ilgili yeterli literatür bulunmamaktadır. Bu nedenle bu çalışmada iki disiplini ayrı ayrı ele alarak belirli bir uzmanlık bilgisi dahilinde harmanlamak gerekmiştir. Çalışmanın diğer bir kısıtı ise her iki konunun da manipülasyona yatkın bir popülerliğinin olmasıdır. Özellikle son dönemlerde yapay zekâ kavramının teknolojik ve bilimsel alt yapısı yok sayılarak, bilim kurgu nevi bir popülerlik kazanması bilgi kirliliğine neden olmaktadır. Yapay zekâ birçok başarılı projeye rağmen henüz çok mesafe kat etmesi gereken bir disiplindir. Önümüzdeki on yıllarda dünya yapay zekâ eksenine doğru kaymaya devam edecek ve yeni dünya düzeninde yeni rekabet sahası yapay zekâ ve istihbarat olacaktır.

Bu çalışmanın kendinden sonraki çalışmalara ön ayak olması ve birbirleriyle sıkı ilişkisi olan istihbarat, siber uzay ve siber istihbarat, veri bilimi, makine öğrenmesi ve yapay zekâ çalışmalarında akademik bir bakış açısı koyması hedeflenmiştir. Bundan sonra yapılacak çalışmalarda da bilimsel gerçeklik ile bilim kurgu arasındaki ince çizgiye dikkat edilmesi gerektiği önerilmektedir.

KAYNAKÇA

- Allen, G, Chan, T. (2017). Artificial Intelligence and National Security. Cambridge: Belfer Center. Cambridge Dictionary, (2019, Mayıs 18). Intelligence, <https://dictionary.cambridge.org/tr/s%C3%B6zl%C3%BCk/ingilizce-t%C3%BCrk%C3%A7e/intelligence>
- Chaitin, D. (2019, Mayıs 18). Edward Snowden: Facebook İis A Surveillance Company Rebranded As Social Media, <https://www.washingtonexaminer.com/news/edward-snowden-facebook-is-a-surveillance-company-rebranded-as-social-media> adresinden alındı.
- CIA (2019, Mayıs 18). The Intelligence Research and Development Council, <https://www.cia.gov/library/readingroom/docs/CIA-RDP87B00305R000801500020-3.pdf> adresinden alındı.
- Clark, J.R. (2019, Mayıs 18). What is Intelligence, http://intellit.muskingum.edu/whatis_folder/whatisintelintro.html adresinden alındı
- Clemente, D. (2015). 'Fundamentals of Cyber Security', A biennial collection of analysis on international agreements for security and development, Vertic (Verification, Research, Training and Information Centre), Chapter 10, <http://www.vertic.org/media/assets/Publications/Verification%20and%20Implementation%202015.pdf> adresinden alındı.
- Congressional Research Service (2019, Mayıs 18). Artificial Intelligence and National Security, <https://fas.org/sgp/crs/natsec/R45178.pdf> adresinden alındı.
- Cumhurbaşkanlığı. (2019, Mayıs 18). ODTÜ Teknokent Açılışında Yaptıkları Konuşma, <https://www.tccb.gov.tr/konusmalar/353/102215/odtu-teknokent-acilisinda-yaptiklari-konusma> adresinden alındı.
- DARPA (2019, Mayıs 18). 60 Years 1958-2018, https://www.darpa.mil/attachments/DARAPA60_publication-no-ads.pdf adresinden alındı.

Fisher, L. (2019, Mayıs 18). CIA Warning Over Huawei, https://www.thetimes.co.uk/edition/news/cia-warning-over-huawei-rz6xc8kzk?wgu=270525_54264_15579525598831_3633d25741&wgexpiry=1565728559&utm_source=planit&utm_medium=affiliate&utm_content=22278 adresinden alındı.

Horowitz, M.C, Allen, G.C, Saravealle, E., Cho, A, Frederick, K, Scharre, P. (2018). Artificial Intelligence and International Security, <https://www.cnas.org/publications/reports/artificial-intelligence-and-international-security> adresinden alındı.

IARPA (2019, Mayıs 18). Research Programs, <https://www.iarpa.gov/index.php/research-programs> adresinden alındı.

IRTPA (2019 Mayıs 18). The Intelligence Reform and Terrorism Prevention Act of 2004, <https://it.ojp.gov/PrivacyLiberty/authorities/statutes/1282> adresinden alındı.

Kahn, D, 2002, '*İstihbaratın Tarihsel Teorisi*', Avrasya Dosyası, Cilt.8, Sayı. 2, ss.5-20.

Kee, E. (2019, Mayıs 18). Samsung SGR-A1 Robot Sentry is One Cold Machine, <https://www.ubergizmo.com/2014/09/samsung-sgr-a1-robot-sentry-is-one-cold-machine/> adresinden alındı.

Kent, S. (1968). Stratejik İstihbarat. İzmir: Endüstri Basım ve Yayımevi.

MCLAughlin, J. (2019, Mayıs 18). CIA Agents in About 30 Countries Being Tracked by Technology, Top Official Says, <https://edition.cnn.com/2018/04/22/politics/cia-technology-tracking/index.html> adresinden alındı.

MİT (2019, Mayıs 18). İstihbaratın tanımı, <http://www.mit.gov.tr/tarihce/giris.html> adresinden alındı.

Negnevitsky, M. (2005). Artificial Intelligence: A Guide Intelligent Systems. Essex, England: Addison-Wesley.

Özdağ, Ü. (2018). İstihbarat Teorisi. Ankara: Kripto Basım YayımDağıtım.

Pecotic, A. (2019, Mayıs 18). Whoever Predicts The Future Will Win The AI Arms Race, <https://foreignpolicy.com/2019/03/05/whoever-predicts-the-future-correctly-will-win-the-ai-arms-race-russia-china-united-states-artificial-intelligence-defense/> adresinden alındı.

Russell, S, Norving, P. (2003). Artificial Intelligence – A Modern Approach. New Jersey, USA: Prentice Hall.

Say, C. (2019). 50 Soruda Yapay Zekâ. İstanbul: 7 Renk Basım Yayım.

TDK, (2019, Mayıs 18). Güncel Türkçe Sözlük, "İstihbarat", http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c894e4f166307.32122960

Warner, M, 2009, 'Intelligence as Risk Shifting', Studies in Intelligence, Vol. 53, No.2.

Whitehouse, (2019, Mayıs 18). Preparing for The Future of Artificial Intelligence, https://obamawhitehouse.archives.gov/sites/default/files/whitehouse_files/microsites/ostp/NSTC/preparing_for_the_future_of_ai.pdf adresinden alındı.

Yılmaz, A. (2017). Yapay Zekâ. İstanbul: Kodlab Yayınları.