SAVAŞ NESNELERİNİN İNTERNETİ

TREND ANALİZİ KASIM 2018

thinktech
STM Teknolojik Düşünce Merkezi

STM ThinkTech

1. GİRİŞ

Savaş tarihinde, hatta belki de insanlık tarihinde yepyeni bir döneme giriyoruz. Makinelerin cephede ve cephe gerisinde insanlarla yan yana çarpıştığı savaşlar çağına.

Aslına bakarsanız, bilim kurgu filmlerinde askeri robotlar çoğu zaman "kötü adam" rolündeydi[1]. Terminator'den, Matrix'e tüm filmlerde güçlü makineler kontrolden çıkıyor ve silahlarını kendilerini yaratanlara çeviriyorlardı. Hatta robot kelimesinin isim babası Karel Capek de 1920'lerde yazdığı RUR adlı oyunda insan ırkının sonunun yapay zekâ sahibi varlıklardan geleceği uyarısı yapıyordu.

Ancak bu uyarılara rağmen robotlar, bilim kurgudan gerçeğe fırlayarak ordudaki yerini aldı. Artık karada, havada ve denizde daha fazla robotik sistem ama daha az insan çarpışıyor. Bu robotlar uçabiliyor, yüzebiliyor; sadece bir dakikada 550 yüksek patlayıcı içeren mermi atabiliyor. Bu da şu çarpıcı gerçeği önümüze koyuyor: Geleceğin savaşları asker, drone ve yapay zekâ temelli sistemlerin kombinasyonuyla yapılacak. "Internet of Battle Things (Savaş Nesnelerinin İnterneti)" adı verilen bu kavram, makine ve insanlardan oluşan geniş bir savaş ağından oluşuyor.

Günümüzde "sivil hayatta" kullanımı gittikçe yaygınlaşmaya başlayan nesnelerin interneti kavramı, 1970'lerde askeri laboratuvarlarda askeri amaçlarla ortaya atılmıştı. ABD Savunma Bakanlığı İleri Araştırma Projeleri Kurumu'nun (DARPA) 1970'lerin sonlarında başlayan ve 1980'lerde devam eden dağıtık sensör ağları araştırma programı kapsamında geliştirilen ayakkabı kutusu boyutlarındaki sensörler, savaş meydanındaki tehditlerin tespiti amacıyla kullanılmıştı. Bu program çerçevesinde geliştirilen teknolojiler, sivil uygulama alanları bularak günümüzde kullanılan nesnelerin interneti ekosistemini oluşturmuştu[2]. Şimdi bu çalışmalar orijinal amacına dönüyor ve nesnelerin interneti bir kez daha savaş alanına taşınıyor. Savaş Nesnelerinin İnterneti teknolojisiyle birlikte ortaya çıkan Ağ Merkezli Savaş (Network-Centric Warfare / NCW) paradigması, üç farklı alanı entegre ediyor:

- Operasyonların gerçekleştiği, verilerin üretildiği **"fiziksel alan"**;
- Verilerin aktarıldığı ve depolandığı **"veri alanı";**
- Verilerin işlendiği, analiz edildiği, karar süreçlerine destek amacıyla kullanıldığı **"bilişsel alan"**[3].

ABD Ordusu Araştırma Laboratuvarından Alexander Kott'un hazırladığı "*Challenges and Characteristics of Intelligent Autonomy for Internet of Battle Things in Highly Adversarial Environments*" adlı raporda[4] "Savaş Nesnelerinin İnterneti" kavramı şöyle tanımlanıyor:

> *"Nesnelerin internetinin hızla ortaya çıkması, karşı konulamaz iki teknolojik argümanın mantığıyla ilerliyor: Makine zekâsı ve ağ iletişimi. Nesneler daha akıllı olduklarında ve birbirleriyle konuştuklarında, daha da faydalı ve etkilidirler. Tam olarak aynı mantık, askeri savaşların dünyasına yerleştirilen nesnelere uygulanır. Onlar da daha fazla istihbarat ve kendi aralarında eylemlerini koordine etmenin daha fazla yollarına sahip olduklarında insan savaşçılara daha iyi hizmet edebilirler. Buna '**Internet of Battle Things – IoBT**' diyoruz. Bazı yönlerden, Savaş Nesnelerinin İnterneti hâlihazırda*

bir gerçeklik haline geliyor ama 20-30 yıl sonra savaşta hâkim bir varlık haline gelmesi muhtemel."

Rapor[4], Savaş Nesnelerinin İnterneti'nin kullanılacağı savaşları şöyle tanımlıyor:

"*Bu tür akıllı 'nesne'lerin çoğu, bugün savaş alanlarında gördüğümüz sistemlerden çok farklı olmayacak. Mesela bağımsız yer sensörleri, güdümlü füzeler (özellikle at ve unut tipi kendinden güdümlü füzeler) ve tabi ki insansız hava araçları bulunacak. Bunlar muhtemelen boyutları çok küçük (böcek boyutunda mobil sensörler gibi) robotlardan askeri birlik ve malzeme taşıyabilecek kadar büyük araçlara kadar çeşitlilik gösterecek. Bunlardan bazıları uçabilecek, bazıları yerde sürünebilecek veya yürüyebilecek.*"

Şekil 1: Geniş çeşitlilikte sistemler ve diğer "nesneler" savaş alanında iletişim kuracak ve işbirliği yapacak.
Kaynak: Evan Jensen, ABD Ordusu Araştırma Laboratuvarı[5]

Şekil 2: Ağ bağlantılı akıllı nesneler ve insanlardan oluşan ekipler, son derece karmaşık zorlayıcı koşullarda -yapılandırılmamış, istikrarsız, hızla değişen, kaotik, düşman- operasyonlar yürütecek.
Kaynak: Evan Jensen, ABD Ordusu Araştırma Laboratuvarı[5]

Akıllı savunma cihazları, ABD'nin Avustralya gibi müttefiklerinin ordularında da yerini alacak[6]. Ayrıca, cephaneler de akıllanacak, düşmana fiziksel zararın yanı sıra siber zararlar da verecek. Cephede akıllı fiziksel sistemler savaşırken, cephe gerisinde ise "siber robotlar" görev yapacak. Bilgisayar ağlarında üslenen bu robotlar, siber uzayda operasyonlar gerçekleştirecek. Tıpkı fiziksel robotlar gibi, siber robotlar da çok önemli işlevler üstlenecek. Kimileri bilişim ve haberleşme sistemlerini koruyacak, kimileri elektronik cihazları savunacak. Sadece savunmakla da kalmayacak, düşman sistemlere de siber saldırılar düzenleyecek, bu yolla enerji, iletişim ve ulaşım altyapılarını çökertecekler.

Savaş Nesnelerinin İnterneti sistemlerinin belki de en önemli katkıları; yapay zekâ sistemleri ve veri analiz becerileriyle, insanlara ve cephedeki robotlara danışmanlık yapmak olacak.

2. ROBOTLAR SAHNEDE

Savaşların şeklini değiştiren bu çarpıcı süreç; 2001 yılında, tüm dünyayı şok eden 11 Eylül saldırılarının hemen sonrasında başladı. 11 Eylül'den sonra uzaktan kontrol edebilen on binlerce robot, ABD ordusunun operasyonlarında aktif rol almaya başladı. İnsansız hava araçları, Ortadoğu'daki operasyonların sıradan unsurları halini aldı. İnsansız kara araçları Irak ve Afganistan'da yollara döşenen bombaların imhasında kullanıldı. Su altı robotları da istihbarat ve veri toplamanın yanı sıra, su altı mayınlarının imhası için kullanılmaya başlandı[1].

Bu konudaki dönüm noktası 7 Ekim 2001 tarihi oldu. Bu tarihte 3034 kuyruk numaralı MQ-1 Predator drone'u, insansız bir araçla gerçekleştirilen ilk ölümcül hava saldırısına imza atarak robotların savaşlarda ne kadar yararlı olabileceğini kanıtlamış oldu[1]. Bu drone, şu anda Washington'daki Ulusal Hava ve Uzay Müzesi'nde sergileniyor[7]. Bu ilk başarının ardından, Predator ve daha iri Reaper drone'larının kullanımı hızlanarak arttı.

Havadaki Robotlar

Drone'lar savaş uçaklarına göre daha düşük taşıma kapasitesine sahip olmalarına rağmen; ses hızına ulaşan süratleri, yüksek manevra yetenekleri, yüksek isabet oranları, radara yakalanma ihtimallerinin ve operasyon maliyetlerinin düşük olması, askeri zayiatın azaltılmasına katkıda bulunmaları nedenleriyle birçok görevde uçaklara göre daha çok tercih edilmeye başlandı. ABD Dış İlişkiler Konseyi üyesi Micah Zenko'nun tahminlerine göre; Bush döneminde 50 olan drone saldırısı sayısı, Obama döneminde 506'ya ulaştı[8]. ABD Başkanı Donald Trump da 2016 sonunda göreve gelir gelmez drone kullanımının yaygınlaştırılması, sınır güvenliğinde drone'lardan yararlanılması talimatını verdi[1].

Senatör Lindsey Graham, 2013 yılı itibarıyla drone saldırılarında 4.700 insanın öldürüldüğünü açıkladı[9]. Bu yüksek rakam, tartışmaları da beraberinde getiriyor. Tartışmanın bir tarafında binlerce kilometre ötedeki operatörler tarafından yönetilen drone'ların hata yapmaya

müsait olduğunu savunanlar bulunuyor. Düşman birlikler yerine düğün yapan sivillerin bombalanması benzeri olaylar da bu eleştirileri haklı çıkarıyor[10].

Karadaki Robotlar

Robotlar sadece havada değil; karada da savaşa katılıyor[1]. Bunun ilk örneğini, Irak ve Afganistan'da binlerce ABD askerinin ölümüne yol açan bombaların imhasında kullanılan insansız araçlar oluşturuyor[11]. "*Wired for War: The Robotics Revolution and Conflict in the 21st Century"* kitabının yazarı Peter W. Singer, 2004 yılında Irak'ta kullanılan kara robotlarının sayısının 150 kadar olduğunu, 2008 sonunda ise bu sayının 12 bine ulaştığını belirtiyor[12].

PackBot adı verilen mini tank görünümlü uzaktan kumandalı araçlar ise mağara benzeri tehlikeli yerlerde keşif görevi üstlenerek gizli bombaları ve bubi tuzaklarını tespit ediyor[13]. PackBot'un üreticisi iRobot şirketi, 2012 yılı itibarıyla orduya ve polise 5.000'i aşkın robot sattığını açıkladı. Satılan robotlar arasında 75 kilo taşıyabilen PackBot'un yanı sıra, 2,5 kilo ağırlığındaki FirstLook gibi modeller de bulunuyor[14]. FirstLook "atılabilir" robotlar sınıfına giriyor. Çünkü gerçek anlamda potansiyel tehditlerin bulunduğu binalara, araçların altına vb. fırlatılıyor[1].

Bu konuda ABD yalnız değil. Eski düşman Rusya da bu alandaki çalışmalarını sürdürüyor. Bu çalışmaların ürünlerinden biri, Kalashnikov şirketinin geliştirdiği yeni bir taarruz modülü. 7,62 mm makineli tüfek ile bilgisayar sistemine bağlı bir kameradan oluşan bu sistem, bir insanın kontrolü olmaksızın kendi hedeflerini belirleyebiliyor. Rusya'nın resmi haber ajansı TASS'a göre, bu sistem, "hedefleri belirlemek ve vurma kararını alabilmek için sinir ağı teknolojileri" kullanıyor[15].

Rusya'da bu alanda farklı çalışmalar da yürütülüyor. İnsansız bir kara harp aracı olan Uran-9, makineli tüfeğe ve 30 mm'lik havan topuna sahip. 10 kilometreye varan uzaklıklardan kontrol edilebiliyor. Platform-M savaş robotları aşırı sıcak ve soğuklarda çalışma kabiliyetine sahip. Armata T-14 "süper tank" ise savaş meydanında tam otonom tankların yolunu açacak bir çalışma[16].

Denizdeki Robotlar

Benzer şekilde ABD donanması da denizlerdeki mayınların tespiti için robotlardan yararlanıyor[1]. 2003 yılında REMUS (Remote Environmental Monitoring Units)[17] adı verilen torpido şeklindeki insansız denizaltılar Irak'ın liman kenti Umm Kasr'da mayın aramak amacıyla kullanılmaya başlandı. Ancak şu ana dek mayınla mücadele robotları beklentileri karşılayamadı. Senato Silahlı Kuvvetler Komitesi Başkanı John McCain'in, sistemin harcanan 706 milyon dolar ve 16 yıla rağmen istenilen sonuçları vermediğini ortaya koyan raporunun ardından, geçen yıl projeye nokta konuldu[18]. McCain şöyle demişti: "Başta planlanandan daha fazla para harcamamıza rağmen planlananın yarısı kadar sistemi, planlananın iki katı sürede üretebildik. Bir de, çalışmıyorlar…[19]"

Henüz Alınacak Çok Yol Var

Savaşçı robotların istenilen seviyeye gelmesinin önünde birçok engel bulunuyor. Bunların ilki, robotların aralarında hızlı ve etkin bir şekilde iletişim kuramaması ve savaş ortamındaki değişen koşullara ayak uyduramaması. Bunun için çok sayıda dinamik varlığı (cihazı ve kanalı), değişen ortama uyum gösterecek esnekliğe sahip olacak şekilde düzenlemek ve yönetmek gerekiyor. Bu uyumun tamamen otonom bir şekilde sağlanması gerekiyor. Aksi halde robotların insanlara destek değil; yük olması söz konusu olabilir.

İkinci güçlük, Savaş Nesnelerinin İnterneti'nin üreteceği devasa miktarda verinin zaten fiziksel ve psikolojik baskı altındaki insanlara ağır bir yük daha getirecek olması. Bunu aşmanın yolu devasa, karmaşık, kafa karıştırıcı ve bazı durumlarda yanıltıcı verilerin, insanların emrine düzenli ve rahatça yorumlanabilir şekilde sunulmasından geçiyor. Bunu gerçekleştirirken hızla değişen koşullar ve insanların toplumsal, bilişsel, fiziksel ihtiyaçları da dikkate alınmalı. Savaş sırasındaki öncelikler, hedefler her an değişebiliyor. Akıllı sistemlerin de bu değişimleri algılaması, en doğru davranışa hızla karar vermesi ve uygulaması gerekiyor.

Savaş Nesnelerinin İnterneti sistemlerinin ürettiği veriler Komuta, Kontrol, Haberleşme, Bilgisayar, İstihbarat, Gözetleme ve Keşif (C4ISR) sistemlerinde toplanıyor. Bu verilerin yorumlanması ve düzenlenmesi amacıyla aralarında Lockheed Martin'in de bulunduğu birçok şirket makine öğrenmesi sistemleri geliştiriyor[20].

Üçüncü güçlük de savaşın yok sayılamayacak unsuru olan düşman. Bu süreçte düşman sistemler de sürekli gelişiyor. Düşman birlikleri de boş durmayacak ve Savaş Nesnelerinin İnterneti sistemlerini etkisiz hale getirmek, şaşırtmak ve yanıltmak için elinden geleni yapacak. Böylesine bir ortamda robotların hızla artan ve değişen riskleri hesaba katması, sağlıklı kararlar vermesi daha da güçleşecek. Yani, akıllı makinelerin kendilerini aldatmayı ve yenmeyi hedefleyen düşman sistemlerini de anlayacak ve yorumlayacak kadar akıllı olması gerekiyor.

Lockheed Martin şirketi, bu tehditlere hazırlanmak amacıyla uluslararası bir siber korsan ekibiyle çalışıyor. Bu siber korsanların sisteme sızma ve saldırı girişimleriyle ortaya çıkan açıklar, teker teker kapatılarak sistem daha da güçlendiriliyor. Bunun yanında düşman sistemler üzerinde veri toplama çalışmaları da sürdürülüyor[20].

Bir diğer pratik engel de enerji sorunu. Sensörlerin çok düşük düzeyde enerji tüketmesi, hatta kendi enerjilerini kendilerinin üretmesi gerekiyor. Aksi halde savaş alanına bataryaların taşınması, ordu açısından Savaş Nesnelerinin İnterneti sistemlerini bir avantaj olmaktan çıkararak bir yüke dönüştürebilecek[21].

Yapay zekânın önündeki daha büyük bir engel ise birlikte savaştıkları insanları anlamayı başarmaktır. Bazen diğer insanların ve hatta kendilerinin bile anlamadığı kararlar veren insanlar, yapay zekâ açısından da büyük bir gizem oluşturma potansiyeli taşıyor.

3. YOL HARİTASI

Etkin ve güvenli robotların üretimine yönelik çalışmalar kararlılıkla sürdürülüyor. Örneğin, ABD Ordusu Araştırma Laboratuvarı gündemdeki sorunlara çözüm getirmek adına sektörden, akademik çevrelerden ve ordudan uzmanları bir araya getirdi. ABD ordusunun amacı; sektördeki farklı araştırmaları ve teknolojileri tek bir merkezde toplayarak, entegre ve çok daha hızlı bir şekilde ilerlemesini sağlamak[1].

Uzmanlara göre öncelikle yapılması gereken; yeni teoriler, modeller ve teknolojik yaklaşımlar geliştirmek. Çünkü ordunun savaş alanındaki ihtiyaçları, mevcut nesnelerin interneti sistemlerinden çok daha farklı olacak. Bu nedenle, günümüzde sanayide ve gündelik yaşamda kullanılan sistemlerden çok daha farklı ve büyük sistemler kurulacak.

ABD Füze Savunma Ajansının, 81.000 kilometrelik askeri iletişim ağını kullanan Komuta, Kontrol, Savaş İdaresi ve İletişim Sistemi (C2BMC), gelecekteki devasa Savaş Nesnelerinin İnterneti sistemlerinin örneklerinden birisidir. Sistem, ABD ordusunun Balistik Füze Savunma Sistemi'nin (BMDS) farklı unsurlarını tek bir sistem altında bir araya getiriyor. Sistem bünyesinde binlerce sensör, radar ve uydudan gelen veri ortak bir dile çevriliyor ve sistemlerin birbiriyle iletişimi sayesinde, dünya genelindeki tehditler gerçek zamanlı olarak tespit ediliyor[20].

Bu askeri sistemlere mevcut sivil sistemler de eklenecek. Örneğin NATO, kurduğu akıllı üslerde akıllı kent teknolojilerini kullanıyor. Akıllı trafik kontrol sistemleri benzeri sivil sistemlerin de gerektiğinde askeri amaçlarla kullanılması NATO'nun gündeminde. Tabii bunun için öncelikle farklı sistemlerin birbirleriyle sağlıklı bir şekilde iletişim kurması gerekiyor[1].

Avrupa Savunma Ajansı da (EDA) Savaş Nesnelerinin İnterneti'ni kent savaşlarında kullanmaya odaklanmış durumda. WINLAS (Wireless Sensor Networks for Urban Local Areas Survillance) projesi kapsamında kentlerdeki mevcut milyonlarca sensörün ürettiği verilerin, orduya durumsal farkındalık ve istihbarat sağlaması üzerinde çalışmalar sürüyor[22]. Nesnelerin internetini daha çok savunma ve istihbarat amacıyla kullanma eğiliminde olan EDA, nesnelerin internetinin çok farklı ortamlarda durumsal farkındalık sağlayacağı inancında[23]. EDA örneğinden de görüleceği gibi yapay zekâ sistemlerinin ağırlık kazandığı robotların yanı sıra birçok sivil nesnelerin internet sistemi de lojistikten enerji verimliliğine dek birçok alanda kullanılıyor.

Verimlilik ve Etkinlik Artırıcı Sistemler

Sensörlerin yanı sıra, sivil ve ticari sistemler de askeri amaçlarla etkin bir şekilde kullanılarak ordunun verimliliği ve etkinliği artırılacak. Hâlihazırda kullanılan ve ordunun emrine sunulan sistemlerden bazıları şunlar:

- General Motors'un geliştirdiği, motorların performansını izlemeye yönelik Telogis sistemi yakıt tüketimini yüzde 25 azaltırken, filo kullanımını yüzde 25 ve işgücü verimliliğini yüzde 15 artırıyor[24] .
- Nesnelerin interneti temelli enerji yönetim sistemleri, ofislerdeki enerji kullanımını yüzde 20 azaltıyor. Akıllı termostatlar ve HVAC sistemleri, ısıtma ve soğutma masraflarını yüzde 10-15 azaltıyor[25].
- USTRANSCOM'un Küresel Ulaşım Ağı (Global Transportation Network/GTN) ve Savunma Lojistik Ajansı, kurdukları ortak bilgi platformuyla askeri lojistik operasyonlarının görünürlüğünü ve verimini artırmış durumda[26].
- Ticari nesnelerin interneti sistemlerinin kullanımıyla kurulacak akıllı üsler. Bu teknolojiler akıllı üslerin güvenliğini pekiştirmekten öte, personelin sağlık durumunun takibinden enerji kullanımının optimizasyonuna kadar birçok amaçla kullanılabilir.
- Kentlerdeki sensörler ve nesnelerin interneti ağları, bir saldırı durumunda arama, yardım ve kurtarma çalışmalarını kolaylaştırabilir. Nesnelerin internetinin cephede en yaygın şekilde kullanılacağı alanlardan biri de taktik istihbarat çalışmaları olabilir. CSIS tarafından hazırlanan bir rapora göre, nesnelerin interneti cihazları çok daha fazla veri toplayabilir, çok daha karmaşık analizler gerçekleştirebilir, çok daha hızlı tepki verilmesine olanak tanıyabilir[27].
- Nesnelerin internetiyle entegre halde çalışan yapay zekâ sistemleri elde edilen istihbaratın anlamlı bilgiler haline gelmesini sağlayabilir[28].
- Nesnelerin internetinin bir diğer etkisi de lojistik alanında görülecek. Sensörler ve analiz sistemleri askeri birliklerin ihtiyaç duyduğu malzeme ve mühimmatın anında tespit edilmesini ve kısa sürede temin edilmesini sağlayabilir[29].

NATO İletişim ve Bilişim Ajansı tarafından geçen yıl başlatılan ve 2018'in Aralık ayında tamamlanması planlanan çalışma kapsamında da sivil sensörlerin ve akıllı kent sistemlerinin lojistik ve sağlık amacıyla kullanılması olanakları araştırılıyor[30].

ABD ordusunun 2013 yılında yayınladığı 25 yıllık yol haritası, gelecekteki robotların birbirleriyle veri paylaşabileceğini ve bir ekip halinde çalışabileceğini vurguluyor[31]. Plan kapsamında robotların standart arayüzler kullanması planlanıyor. Böylece farklı şirketler tarafından üretilen robotlar, sensörler ve diğer donanımlar birlikte sorunsuz bir şekilde kullanılabilecek. Bu doğrultuda, ABD ordusu 2017 yılında iki standart modüler robot platformu satın alma çalışmalarına başladı. İlk aşamada

bu türden 4400 cihaz satın alınacak. Sonrasında da alınacak donanımların bu platformlarla uyumlu olması sağlanacak.

Yatırım yapılan bir diğer alan ise, düşman drone'ları tespit ve imha edecek teknolojiler. Uzmanlar drone'lar aracılığıyla ABD topraklarında terör saldırıları düzenlenebileceğini, bu araçlara kimyasal silahlar yüklenebileceğini belirtiyor[32]. Bunlara karşı savunma sistemleri geliştirmek gerektiğinden; radyo sinyallerini karıştırmaktan, düşman drone'un "beynini" hack'lemeye ve ağ fırlatarak drone'u esir almaya kadar çeşitli teknolojiler geliştiriliyor[33].

Robotlara Verilecek Yetki Tartışması

Bu tür sistemler daha önce karşılaşmadıkları bir tehditle karşılaşırlar ve onlara karar verme yetkisi tanınırsa ne olur? Böyle bir durumda yapılacak hatalar; masum sivillerin hayatını kaybetmesi, askeri olmayan hedeflerin vurulması ve dost ateşi gibi çok ciddi sonuçları da beraberinde getirebilir.

Bu konuda Vatikan dâhil birçok kesimden itirazlar yükseliyor[34]. En az 19 ülke ve aralarında Uluslararası Af Örgütünün de bulunduğu birçok uluslararası örgüt, otonom katil robotların yasaklanması çağrısı yapmış durumda. Konu BM gündemine taşındı[35]. İnsan Hakları İzleme Örgütü (HRW) ve Harvard Üniversitesi Hukuk Fakültesi'nin Uluslararası İnsan Hakları bölümü tarafından hazırlanan "*Mind the Gap: The Lack of Accountability for Killer Robots*" isimli çalışmada da yapay zekâya sahip robotların insanların kontrolü dışında hedef seçip güç kullanacağı ve bu durumun ahlaki ve yasal endişeleri beraberinde getireceği uyarısında bulunuluyor[36]. Askeri yöneticiler de hedefini kendi seçen, nişan alan ve insanların müdahalesi olmaksızın ateş eden sistemlere çok sıcak bakmıyor[37].

Bu endişeler pek yersiz sayılmaz. Zira 2008 yılında Güney Afrika'da yaşanan bir olay hafızalarda tazeliğini koruyor. İki devasa 35 milimetrelik bombardıman silahına sahip MK5 uçaksavarı, büyük bir robotik silah ve bilgisayar tarafından kontrol ediliyor. Ancak dizüstü bilgisayarınız kilitlendiğinde, eğer bu bilgisayar 550 yüksek patlayıcılı mermi içeren bir şarjörü kontrol ediyorsa, olayın boyutu değişebiliyor. Böyle bir durumla karşılaşan Güney Afrikalı askerler bir şeyin yanlış gittiğini fark etti. Sistem kilitlenmişti; ancak daha sonra yaşananlar tam anlamıyla tüyler ürperticiydi. Robotun otomatik silahtan saçtığı mermiler, kapatmak için koşan kadın askere isabet etti ve asker yere yığıldı. Robotun şarjörü boşalana kadar 8 asker daha öldü. 14 asker de ciddi bir şekilde yaralandı. Katliamın sorumlusu "yazılım hatası" olarak belirlendi[38].

Kontrol Hâlâ İnsanlarda

Kararı robotlara bırakma konusunda üç farklı yaklaşım bulunuyor: İlki, insanların devrede olduğu sistemler. Burada hedefler insanlar tarafından belirleniyor, komutlar insanlar tarafından veriliyor. İkincisi, insanların kontrolde olduğu sistemler. Burada robotlar otonom bir şekilde hedefi belirleyerek ateş edebiliyor ancak insanların bunu dilediği an durdurma, engelleme yetkisi bulunuyor. Üçüncüsü ise, insanların tamamen devre dışı olduğu sistemler. ABD'li askeri yetkililer, şu an itibarıyla insanların devrede olduğu sistemleri tercih ediyor. Bu yaklaşım, 2012 yılında, dönemin ABD Savunma Bakanı Ash

Carter'ın ilan ettiği otonom silahlara yönelik kurallarla uyum içinde görünüyor[39]. Carter, o dönemde robotların siber korsan saldırılarına karşı katı bir şekilde test edilmesi ve yarı otonom robotların, hedeflerini insanların denetimi olmaksızın belirlememesi talimatını vermişti. İnsanların denetimindeki robotlar, sadece yaklaşan füzeler ya da diğer robotlar gibi insan olmayan hedefleri kendileri belirleyecekti. Tamamen otonom sistemler ise insanlar karşısında sadece "ölümcül olmayan" silahlar kullanabilecekti.

Kimi uzmanlar ise, kararın robotlara bırakılmasının daha sağlıklı ve güvenli olacağı görüşünde. Örneğin, Georgia Teknoloji Enstitüsü Mobil Robot Laboratuvarı Direktörü Ronald Arkin'e göre, robotlar riski insanlardan daha iyi ölçebilir ve duygusal kararlar vermekten, stres kaynaklı hatalar yapmaktan kaçınabilir[40].

Ayrıca, Cincinnati Üniversitesi doktora öğrencileri tarafından geliştirilen bir yapay zekâ pilotu, sadece diğer yapay zekâya sahip pilotları yenmekle kalmıyor; onlarca yıllık deneyime ve geçmişe sahip insan pilotları da alt edebiliyor. ALPHA adı verilen sistemin süper-insan uçuş yetenekleri, genetik bulanık ağaç (genetic fuzzy tree) adı verilen bir çeşit bulanık mantık (fuzzy logic) algoritmasından kaynaklanıyor. Sistem, karmaşık sorunlara tıpkı bir insanın yaklaştığı gibi yaklaşıyor. Büyük görevleri daha küçük parçalara ayırıyor ki bu, üst düzey taktik, ateşleme, kaçma ve savunma gibi stratejileri içeriyor. Sadece en önemli değişkenleri hesaba katarak, aşırı yüksek bir hızda son derece karmaşık kararlar alabiliyor. Buna bağlı olarak da yapay zekâ; karmaşık, dinamik çevrelerde manevra kararları alabiliyor. Yapay zekâ bu kararları o kadar kısa bir sürede alıyor ki insanın göz kırpma süresi bunun 250 katından fazla bir süreye tekabül ediyor[41]. Arkin, düzenlemelere itiraz etmese de otonom robotların tamamen yasaklanmasına karşı çıkıyor ve uluslararası kurallara insanlardan daha başarılı bir şekilde uyum gösterdikleri kanıtlandıktan sonra cepheye gönderilebileceklerini söylüyor.

Destek Kuvvet Olarak Yararlı

Robotların tetiği çekmesi konusundaki tartışmalar sürse de, destek görevi üstlenen robotların otonom hareket etmesi konusunda pek bir engel bulunmuyor. Karada malzeme taşıyan otonom araçlara gideceği yeri bildirmek yetecek. Otonom gemiler ve denizaltılar da giderek daha karmaşık manevralar yapabilecek ve birbirleriyle iletişim kurabilecek hale geliyor. ABD Deniz Araştırmaları Bürosu'nun geçtiğimiz günlerde düzenlediği tatbikat, otonom gemilerin kolektif bir şekilde hareket ederek düşman hedeflerini kuşatabildiğini gösterdi. Bu sistemler yakın zamanda limanların savunulabilmesi amacıyla kullanılabilecek[42].

Ülke sınırlarına yakın gemilere ve denizaltılara, çeşitli silahlarla yapılan sürpriz saldırıların yol açtığı tehditler karşısında yapay zekâ sistemlerinin hızlı karar verme yeteneklerinden yararlanmak, karşı saldırıların başlatılması da dâhil olmak üzere çeşitli kendini savunma taktiklerinin yapay zekâya emanet edilmesi mümkün. Otonom drone'lar geniş sürüler halinde uçabiliyor ve grup halinde karar vererek, ortam koşulları doğrultusunda formasyon değişimini, insan operatörlerden çok daha hızlı bir şekilde gerçekleştirebiliyor.

4. SONUÇ

Makinelerin cephede ve cephe gerisinde insanlarla yan yana çarpıştığı yeni bir çağa adım atıyoruz. "Internet of Battle Things (Savaş Nesnelerinin İnterneti)" adı verilen bu kavram, makine ve insanlardan oluşan geniş bir savaş ağından oluşuyor. Bu tür akıllı "nesne"lerin en heyecan verici ve en göz önünde olan kısmını robotlar oluşturacak. Bunlar muhtemelen boyutları çok küçük robotlardan askeri birlik ve malzeme taşıyabilecek kadar büyük araçlara kadar çeşitlilik gösterecek.

Cephede akıllı fiziksel sistemler savaşırken, cephe gerisinde ise "siber robotlar" görev yapacak. Bilgisayar ağlarında üslenen bu robotlar, siber uzayda operasyonlar gerçekleştirecek. Tıpkı fiziksel robotlar gibi, siber robotlar da çok önemli işlevler üstlenecek. Ayrıca, cephaneler de akıllanacak, düşmana fiziksel zararın yanı sıra siber zararlar da verecek.

Savaşçı robotların istenilen seviyeye gelmesinin önünde birçok engel bulunuyor. Bunların ilki, robotların aralarında hızlı ve etkin bir şekilde iletişim kuramaması ve savaş ortamındaki değişen koşullara ayak uyduramaması. Bununla birlikte etkin ve güvenli robotların üretimine yönelik çalışmalar kararlılıkla sürdürülüyor. ABD ordusunun yayınladığı yol haritası, gelecekteki robotların birbirleriyle veri paylaşabileceğini ve bir ekip halinde çalışabileceğini vurguluyor. Uzmanlara göre öncelikle yapılması gereken; yeni teoriler, modeller ve teknolojik yaklaşımlar geliştirmek. Çünkü ordunun savaş alanındaki ihtiyaçları, mevcut nesnelerin interneti sistemlerinden çok daha farklı olacak. Bu nedenle, günümüzde sanayide ve gündelik yaşamda kullanılan sistemlerden çok daha farklı ve büyük sistemler kurulacak.

Robotların yanı sıra sivil ve ticari nesnelerin interneti sistemleri de askeri amaçlarla etkin bir şekilde kullanılarak ordunun verimliliği ve etkinliği artırılacak. Nesnelerin interneti, ordulara lojistik, enerji verimliliği, envanter yönetimi gibi alanlarda hizmet vererek daha etkin ve verimli operasyon olanağı sunacak.

KAYNAKÇA

[1] Steven Melendez, "The Rise Of The Robots: What The Future Holds For The World's Armies", *Fast Company*, 06 December 2017, https://www.fastcompany.com/3069048/where-are-military-robots-headed.

[2] Cian O Flaherty, "The Internet of Battlefield Things – Issue #13", *The Convex Lens*, 12 June 2017, https://www.theconvexlens.co/2017/06/12/internet-battlefield-things-iot-war/.

[3] Fraga-Lamas, P., Fernández-Caramés, T.M., Suárez-Albela, M., Castedo, L. and González-López, M., "A Review on Internet of Things for Defense and Public Safety", *Sensors,* Vol. 16, No. 10, October 2016, pp. 1-44.

[4] Alexander Kott, "Challenges and Characteristics of Intelligent Autonomy for Internet of Battle Things in Highly Adversarial Environments", *CoRR*, 2018, https://arxiv.org/ftp/arxiv/papers/1803/1803.11256.pdf.

[5] Alexander Kott, Ananthram Swami and Bruce J. West, "The Internet of Battle Things", *IEEE Computer*, Vol. 49, No. 12, 2016, pp. 70-75, https://arxiv.org/ftp/arxiv/papers/1712/1712.08980.pdf.

[6] Kathryn Toohey, "Robotics and Autonomous Systems: Smart Machines", Defence and Security Equipment International, Australian Army, September 2017, https://www.army.gov.au/sites/g/files/net1846/f/speeches/170906_ras_speech_for_hlc_final_for_publish__0.pdf.

[7] Arthur Holland Michel, "Drones in the National Air & Space Museum", *Center for The Study of Drone*, 02 April 2015, http://dronecenter.bard.edu/drones-in-the-national-air-space-museum/.

[8] Micah Zenko, "Obama's Embrace of Drone Strikes Will Be a Lasting Legacy", *New York Times*, 12 January 2016, https://www.nytimes.com/roomfordebate/2016/01/12/reflecting-on-obamas-presidency/obamas-embrace-of-drone-strikes-will-be-a-lasting-legacy.

[9] Scott Neuman, "Sen. Graham Says 4,700 Killed In U.S. Drone Strikes", *NPR*, 02 February 2013, https://www.npr.org/sections/thetwo-way/2013/02/21/172598593/sen-graham-says-4-700-killed-in-u-s-drone-strikes.

[10] Lucy Draper, "The Weddıng That Became A Funeral: U.S. Still Silent One Year On From Deadly Yemen Drone Strike", *Newsweek*, 12 December 2014, http://www.newsweek.com/wedding-became-funeral-us-still-silent-one-year-deadly-yemen-drone-strike-291403.

[11] Gregg Zoroya, "How the IED changed the U.S. military", *USA Today*, 19 December 2013, https://www.usatoday.com/story/news/nation/2013/12/18/ied-10-years-blast-wounds-amputations/3803017/.

[12] P. W. Singer, "Robots At War: The New Battlefield", *The Wilson Quarterly*, 2009, https://wilsonquarterly.com/quarterly/winter-2009-robots-at-war/robots-at-war-the-new-battlefield/.

[13] "New Robots Well Trained for War: Next Generations Learn Lessons Of Afghanistan", *NBC News*, 14 January 2003, http://www.nbcnews.com/id/3078710/ns/technology_and_science-science/t/new-robots-well-trained-war/#.WvmZzYiFPIV.

[14] "iRobot First Look", http://media.irobot.com/download/iRobot-110-First-Look-Spec.pdf.

[15] William McKinney, "Russia is Building War Robots: a Fully-Automated Kalashnikov Neural Network Gun", *Edgy Labs*, 07 July 2017, https://edgylabs.com/war-robots-automated-kalashnikov-neural-network-gun.

[16] Mark Smith, "Is 'killer robot' warfare closer than we think?", *BBC*, 25 August 2017, http://www.bbc.com/news/business-41035201.

[17] "REMUS and Mine Countermeasures", Office of Naval Research, https://www.onr.navy.mil/en/About-ONR/History/tales-of-discovery/remus.

[18] Indefensible: $706 Million And 16 Years Developing A Navy Minehunting System That Doesn't Really Work", The Office of Senator John McCain, https://www.mccain.senate.gov/public/_cache/files/1807ea90-50bf-4816-91fe-67b3b74701cb/americas-most-wasted-presents-indefensible---remote-minehunting-system-9-3-15.pdf.

[19] Lance M. Bacon, "McCain slams Remote Minehunting System as a failure", *Navy Times*, 14 September 2015, https://www.navytimes.com/news/pentagon-congress/2015/09/14/mccain-slams-remote-minehunting-system-as-a-failure/.

[20] "IOT Is Transforming Modern Warfare", *Lockheed Martin*, https://www.lockheedmartin.com/en-us/news/features/2017/internet-of-things-transofrming-modern-warfare.html.

[21] Niranjan Suri, Mauro Tortonesi, James Michaelis, Peter Budulas, Giacomo Benincasa, Stephen Russell, Cesare Stefanelli and Robert Winkler, Analyzing the Applicability of Internet of Things to the Battlefield Environment", International Conference on Military Communications and Information Systems (ICMCIS), 2016, https://www.researchgate.net/publication/303839381_Analyzing_the_Applicability_of_Internet_of_Things_to_the_Battlefield_Environment

[22] Ignacio Montiel-Sánchez, "Defence Internet Of Things (DIOT)", *European Defence Matters (EDA)*, https://www.eda.europa.eu/webzine/issue14/cover-story/defence-internet-of-things-(diot)

[23] Ignacio Montiel-Sánchez, "Defence Internet Of Things (DIOT)", *European Defence Matters (EDA)*, https://www.eda.europa.eu/webzine/issue14/cover-story/defence-internet-of-things-(diot)

[24] "Telogis has become Verizon Connect", *Verizon Connect*, https://www.verizonconnect.com/telogis/

[25] Denise E. Zheng and William A. Carter, "Leveraging the Internet of Things for a More Efficient and Effective Military", *CSIS*, September 2015, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150915_Zheng_LeveragingInternet_WEB.pdf.

[26] "Global Transportation Network (GTN)", The Office of the Director Operational Test and Evaluation (DOT&E), http://www.dote.osd.mil/pub/reports/FY1999/pdf/af/99gtn.pdf

[27] Denise E. Zheng and William A. Carter, "Leveraging the Internet of Things for a More Efficient and Effective Military", *CSIS*, September 2015, https://csis-prod.s3.amazonaws.com/s3fs-public/legacy_files/files/publication/150915_Zheng_LeveragingInternet_WEB.pdf.

[28] "SpS2 – Military Applications of IoT", *IEEE*, http://wfiot2018.iot.ieee.org/sps2-military-applications-iot/.

[29] "3 Military Applications of The Internet of Things", *Augmate*, 27 August 2018, https://www.augmate.io/3-military-applications-of-the-internet-of-things/.

[30] George I. Seffers, "NATO Studying Military IoT Applications", *AFCEA*, 01 March 2017, https://www.afcea.org/content/Article-nato-studying-military-iot-applications.

[31] "Unmanned Systems Integrated Roadmap: FY2013-2038", U.S. Department of Defense (DoD), p. 32,37.http://archive.defense.gov/pubs/DOD-USRM-2013.pdf.

[32] Fred Byus and Matthew Shaw, " To counter weaponized drones, US needs joint public-private solutions", *Defence News Commentary*, 07 November 2017, https://www.defensenews.com/opinion/commentary/2017/11/07/to-counter-weaponized-drones-us-needs-joint-public-private-solutions-commentary/.

[33] Matthew Humphries, "US Air Force orders anti-drone net-filled shotgun shells", *Fox News*, 14 March 2017, http://www.foxnews.com/tech/2017/03/14/us-air-force-orders-anti-drone-net-filled-shotgun-shells.html.

[34] Carol Glatz, "Killer robots will make war even more inhumane, Vatican official says", *Catholic Herald*, 13 April 2018, http://www.catholicherald.co.uk/news/2018/04/13/killer-robots-will-make-war-even-more-inhumane-vatican-official-says/.

[35] "Ban support grows, process goes slow", *Campaign to Stop Killer Robots*, 15 April 2016, https://www.stopkillerrobots.org/2016/04/thirdmtg/.

[36] "Mind the Gap The Lack of Accountability for Killer Robots", *HRW*, 09 April 2015, https://www.hrw.org/report/2015/04/09/mind-gap/lack-accountability-killer-robots.

[37] Simon Parkin, "Killer Robots: The Soldiers That Never Sleep", *BBC*, 16 July 2015, http://www.bbc.com/future/story/20150715-killer-robots-the-soldiers-that-never-sleep.

[38] Graeme Hosken, "Army blames gun's maker for Lohatla", *IOL*, 26 January 2008, https://www.iol.co.za/news/south-africa/army-blames-guns-maker-for-lohatla-387027.

[39] "Autonomy in Weapon Systems", U.S. Department of Defense, 21 November 2012, https://cryptome.org/dodi/dodd-3000-09.pdf.

[40] Ronald C. Arkin, "Ethical Robots in Warfare", *Georgia Tech*, https://www.cc.gatech.edu/ai/robot-lab/online-publications/arkin-rev.pdf.

[41] M.B. Reilly, "Beyond video games: New artificial intelligence beats tactical experts in combat simulation", *UC Magazine*, 27 June 2016, http://magazine.uc.edu/editors_picks/recent_features/alpha.html.

[42] David Smalley, "Autonomous Swarmboats: New Missions, Safe Harbors", Office of Naval Research Corporate Strategic Communications, 14 December 2016, https://www.onr.navy.mil/Media-Center/Press-Releases/2016/Autonomous-Swarmboats.

thinktech

STM Teknolojik Düşünce Merkezi

http://thinktech.stm.com.tr