



ORGANİZASYON ÖZETİ VE SONUÇ RAPORU

GELECEĞİN ASKERİ 2024 FUTURE SOLDIER 2024

ORGANİZASYON ÖZETİ VE SONUÇ RAPORU



Telefon: 0312 426 22 55

Faks: 0312 426 22 56

E-Posta: sasad@sasad.org.tr

İnternet Sitesi: www.sasad.org.tr

Adres: Ankara Sanayi Odası Binası, Atatürk Bulvarı.
No: 193, Kat: 6, Kavaklıdere, Ankara, Türkiye

© **SASAD**

Savunma ve Havacılık Sanayii İmalatçıları Derneği – 2025

Proje Koordinatörü:

Türkünaz ÜNLÜ

turkunaz.unlu@sasad.org.tr

Editör:

Dr. Oğuz HAMŞİOĞLU

Türkünaz ÜNLÜ

Selahaddin KOYUNCU

ISBN: 978-625-95822-0-7 (Basılı Materyal)

ISBN: 978-625-95822-1-4 (Elektronik Türkçe)

ISBN: 978-625-95822-2-1 (Elektronik İngilizce)

Proje, İçerik ve Etkinlik Ajansı:

AJANSBK

AjansBK Medya ve İletişim Teknolojileri Ltd. Şti.

Kavaklıdere Mah. Büklüm Cad. No: 22/6 Çankaya – ANKARA

0312 417 03 30 & 0534 321 46 55

Baskı

Tek Ses Ofset Matbaacılık Yayıncılık Organizasyon Hayvancılık Otomotiv
Sanayi ve Ticaret Limited Şirketi

Adres: Kazımkarabekir Caddesi Kültür İş Hanı
No: 7/60 Altındağ Ankara

Sertifika No: 44186

Bu tespit ve önerileri kapsayan değerlendirme, Millî Savunma Bakanlığı (MSB), Savunma Sanayi Başkanlığı (SSB) ve Türk Savunma ve Havacılık Sanayi İmalatçılar Derneği (SASAD) tarafından düzenlenen Geleceğin Askeri - Future Soldier 2024 organizasyonunun çıktılarından oluşmaktadır.

Organizasyon, 26-27 Kasım 2024 tarihlerinde Ankara Uzay ve Havacılık İhtisas Organize Sanayi Bölgesi (HAB) Konferans Salonu'nda "Yeni Dünya, Yeni Savaş ve Yeni Savaşçı" ana temasıyla düzenlenmiştir.

Panel formatında düzenlenen organizasyonda Türkiye'den ve dünyanın farklı ülkelerinden uzmanlar bir araya gelerek, 10 farklı oturumda geleceğin askeri kavramını ve teknolojileri konusundaki önerilerini sunmuşlardır. Birinci gün uluslararası perspektif ve ikinci gün ise Millî perspektiften geleceğin askeri teknolojileri gelişmeleri ele alınmıştır.

Panelistlerin konuşma metinleri, sunumlarından çözümlenmiş (deşifre edilmiş) şekilde yer almaktadır. Bu raporda yer alan değerlendirmeler konuşmacılara ait olup kurumların ve temsilcilerinin görüşü ile önerilerini yansıtmaktadır.

Bu raporun içeriğinin telif hakları SASAD'a ait olup kaynak gösterilerek, kısmen yapılacak makul alıntılar ve yararlanma dışında önceden izin alınmaksızın kullanılamaz, yeniden yayınlanamaz.

SASAD Genel Sekreterliği 2025

TAKDİM	1-3
YÖNETİCİ ÖZETİ	4-5
AÇILIŞ KONUŞMALARI	6-13
SATIR ARALARINDAN	14-47
1. OTURUM Rusya-Ukrayna Savaşı ve Savaşın Teknolojik Boyutu	48-76
2. OTURUM Savaşta Modernizm: Teknolojik Aktörler	77-104
3. OTURUM İnsan-Makine Organizması: TEK-ER	105-123
4. OTURUM Yenilikçi Dönüşüm: Hibrit Teknolojiler ve Çok Alanlı Operasyonlar	124-141
5. OTURUM Teknolojinin Paradoksal Sınırları	142-167
6. OTURUM Rusya-Ukrayna Savaşı ve Savaşın Teknolojik Boyutu	168-198
7. OTURUM Müttefik Teknoloji ve Ulusal Uyum	199-222
8. OTURUM Teknolojinin Temeli: Eğitim, Öğretme ve Öğrenme	223-240
9. OTURUM Müttefik Teknoloji ve Ulusal Uyum	241-266
10. OTURUM Güvenli Teknoloji ve Ulusal Hassasiyetler	267-289
CENGAVER SUNUMU	290-296
KAPANIŞ KONUŞMASI	297
DEĞERLENDİRME VE SEKTÖREL BİLGİLER	298-324
SONUÇ	325-328

TAKDİM

Savaş alanının ve askeri doktrinlerin köklü bir dönüşümüne tanıklık ediyoruz. Savaşlar sadece fiziksel alanda değil, dijital ve siber ortamlara da taşınmış durumda. Dolayısıyla, hava, kara, deniz, uzay ve siber alanda top yekûn bir mücadeleden ve ona uygun bir asker ve harp teknolojileri kurgulamaktan bahsediyoruz.

Millî Savunma Bakanlığımız ve Savunma Sanayi Başkanlığımız ile işbirliğiyle düzenlediğimiz 'Future Soldier, Geleceğin Askeri 2024' organizasyonu, çok farklı teknolojilerin geleceğin muharebe ortamını belirleyeceğinin en net ipuçlarına ulaştığımız günümüzden geleceğe bir rehber olacaktır.

İki gün yoğun bir gündemle gerçekleşen organizasyonda ülkemizdeki ve dünyadaki gelişmeler değerlendirilirken, otonom sistemler, robotik sistemler, yapay zekâ, uydu ve haberleşme, giyilebilir askeri teknolojiler, büyük veri, insan-makine entegrasyonu gibi çok sayıda başlıkta 'Yeni Dünya, Yeni Savaş ve Yeni Savaşçı' vurgusuyla geleceğin savaş ortamına yönelik stratejiler tartışıldı.

Yurt dışından ve yurt içinden alanında uzman çok sayıda ismin katkı sağladığı organizasyonumuz, teknolojik dönüşüme öncülük eden ülkemizin, dünyadaki yakın ve uzak gelecekteki rekabette konumlanmasına da katkı sağlayacaktır.

Kamu paydaşları, özel sektör firmaları ve temsilcileri, akademisyenler ile endüstrinin tüm bileşenlerini bir araya getiren organizasyonun sonuç raporunun sektörümüze yön vermesi ve geleceğe yönelik stratejilerin şekillendirilmesine, Ar-Ge ve Ür-Ge süreçlerinin yönetimine büyük değer sağlayacağına inanıyoruz.

Osman OKYAY
Türk Savunma ve Havacılık Sanayii
İmalatçılar Derneği (SASAD) Yönetim Kurulu Başkanı



10

**OTURUM
ANA TEMA
MODERATÖR**

29

KONUŞMACI

700

**DAVETLİ
KATILIMCI**

17

**SAAT
OTURUM
SÜRESİ**

**26-27
KASIM
2024**

Ankara
Uzay ve
Havacılık
İhtisas
Organize
Sanayi
Bölgesi

SAVUNMA Teknolojileri

Üretiminin temellerini oluşturan
BİLİM, TEKNOLOJİ, MÜHENDİSLİK VE MATEMATİK (STEM)
alanında, askeri bilimleri de kapsayan

104

OLOJİ

disiplinler arası içerikte sunum ve paylaşımlar.

AEROLOJİ, ASKİYOLOJİ, ALERJİLOJİ, ALGOLOJİ, ANDROLJÖİ, ANESTEZİYOLOJİ,
ANJİYOLOJİ, ANTROPOLOJİ, ATMOLOJİ, ATOMOLOJİ, BAKTERİYOLOJİ,
BİYOJEOMORFOLOJİ, BİYOKLİMATOLOJİ, BİYOLOJİ, BİYOMETEOROLOJİ,
BİYOSEOLOJİ, DOSOLOJİ, EKOİDROLOJİ, EKOLOJİ, ELEKTROFİZYOLOJİ,
EDİPEMİOLOJİ, ESKATOLOJİ, ETYOLOJİ, FİZYOLOJİ, GENOKOLOJİ, HİSTOLOJİ,
HİSTOPATOLOJİ, HİDROLOJİ, İMMÜNOLOJİ, JEObİYOLOJİ, JEOLOJİ, KARYOLOJİ,
KİLLOLOJİ, KLİMATOLOJİ, KİNEŞİYOLOJİ, KONYOLOJİ, KOROLOJİ, KRİPTOLOJİ,
LUDOLOJİ, MERELOJİ, METEOROLOJİ, METROLOJİ, METHODOLOJİ,
MİKROBİYOLOJİ, MİKROLOJİ, MİNERALOJİ, MİYOLOJİ, NANOTEKNOLOJİ,
NEPHOLOJİ, NÖROLOJİ, NÖROPATOLOJİ, NUMEROLOJİ, ODOLOJİ, OFTALMOLOJİ,
OKSOLOJİ, ONTOLOJİ, ONKOLOJİ, OROLOJİ, OSTEOLOJİ, OTOLARİNGOLOJİ,
OŞİNOGRAFI, OTORİNOLOJİ, PARAZİTOLOJİ, PATOLOJİ, PEDOLOJİ,
PENOLOJİ, PERSONOLOJİ, PETROLOJİ, PİROLOJİ, PNÖMOLOJİ, POSOLOJİ,
PATOMOLOJİ, PSİKOBİYOLOJİ, PSİKOFİZYOLOJİ, PSİKOLOJİ,
PSİKONÖROENDOKRİNOLOJİ, PSİKONÖROİMMÜNOLOJİ, PULMONOLOJİ,
RADYOLOJİ, REFLEKSOLOJİ, REOLOJİ, RİNOLOJİ, ROMATOLOJİ, SEMBOLOJİ,
SEMİOLOJİ, SEROLOJİ, SOSYOLOJİ, SOMNOLOJİ, SİTİOLOJİ, SPLANKOLOJİ,
STOMATOLOJİ, TANATOLOJİ, TERATOLOJİ, THERMOLOJİ, TİPOLOJİ, TOPOLOJİ,
TOKSİNOLOJİ, TRAVMOTOLOJİ, TRIBOLOJİ, TRİKOLOJİ, VAKSİNOLOJİ, VİSSEROLOJİ,
VİROLOJİ, ZİMOLOJİ

EN ÇOK KULLANILAN KELİMELELER

#yapay zekâ	#robotik
#insansız hava aracı	#güvenlik
#bakım	#strateji
#sürdürülebilirlik	#lojistik
#gerçek zamanlı	#dijitalizasyon
#otonom sistemler	#sensör
#siber	#işbirliği
#müşterek	#elektronik harp
#komuta kontrol	#makine öğrenimi
#insan	#veri yönetimi
#uyum	#enerji
#teknoloji	#müttefik
#bilişim	#karar
#analiz	#tasarım
#hız	#psikoloji

YÖNETİCİ ÖZETİ

Geleceğin Askeri 2024 – Future Soldier organizasyonu, yurt içi ve yurt dışındaki üniversiteler, araştırma kurumları, üretici firmalar ve savunma sanayi danışmanları ile ülkemizde faaliyet gösteren firmaların temsilcilerinin katılımıyla gerçekleştirilmiştir.

26-27 Kasım 2024 tarihlerinde gerçekleştirilen ‘Future Soldier-Geleceğin Askeri 2024’ organizasyonunun sonuç raporu ‘Teknoloji’ ve ‘Tek-Er’ olarak iki bölüm halinde sunulmuştur.

Yapay Zekâ, Nesnelerin İnterneti (IoT), Büyük Veri, İnsan-Makine Öğrenimi, Otonom ve Robotik Sistemler, Siber Güvenlik, Sensörler ve Elektronik Harp, Taşınabilir ve Giyilebilir Sistemler, Uydu ve Uzay, Kuantum Alt Yapısı gibi konu başlıkları ‘teknoloji’, insan odaklı yaklaşımlar ise ‘Tek-Er’ özelinde arz edilmiştir.

Askeri teknolojilerdeki gelişmelerin incelenmesinde Ukrayna-Rusya, Karabağ Savaşı, İsrail-Filistin çatışmaları, Çin-ABD teknoloji rekabeti, NATO ve Avrupa Birliği çalışmaları gibi güncel olaylardan örnekler, çıkarılan dersler ve geleceğe yönelik öngörüler de alanında uzman isimlerin görüşleriyle paylaşılmıştır.

Yeni teknolojilerin üretimi ve kullanım süreçleri için, risk ve fırsatların yakın, orta ve uzun vadeli süreler içinde ele alınmasının önemi vurgulanmıştır. Örneğin, yapay zekâ konusunda Millî bir yapay zekâ dilinin hızla kurulmasının Millî güvenlik, savunma ve istihbarat alanlarında büyük önem arz ettiği belirtilmiştir. Yapay zekânın oluşturabileceği etik süreçlerde ulusal ve uluslararası alanda etkin rol oynanmasının gerekliliği, yapay zekânın doğurabileceği risklere karşı erken önlemler geliştirilmesinin ‘ulusal’ bir strateji olarak ele alınması gerekliliği kaydedilmiştir.

Büyük verilerin faydalı veriye çevrilmesinin en büyük kuvvet çarpanları alanında olacağı, kuantum teknolojileri ve blokchain teknolojilerinin de büyük verinin işlenmesinde büyük avantajlar sunacağına dikkat çekilmiştir.

Yeni teknolojilerin gelişiminde ‘veri’ paylaşımının özellikle yapay zekâ eğitimi ve otonom sistemlerdeki algoritmaların geliştirilmesinde önem arz ettiği, kamu ve özel sektör arasında yazılım ve teknoloji üretimi için bir veri paylaşım yönteminin belirlenmesinin faydalı olacağı görüşüne varılmıştır.

Askeri Savunma Teknolojilerinde Elektronik Harp, siber saldırılar, otonom teknolojiler, robotik teknolojiler gibi alanlarda hava, kara, deniz, siber ve uzay platformlarının ‘müşterek kuvvet’ olarak kullanımının artacağı, hız faktörünün belirleyici olacağı ifade edilirken, birlikte çalışabilirlik, kullanıcının hareket yeteneğini kısıtlamayan, bilişsel yükü artırmayan, modüler ve taşınması kolay sistemlerin giderek artacağı kaydedilmiştir.

Haberleşme sistemlerinin, uydu ve iletişim teknolojilerinin, savunma ve saldırı sistemlerinde önemini daha da artıracaklarını vurgu yapılırken, mühimmat, sürü kullanımı ve lazer teknolojilerinin de kuvvet çarpanı etkisinde belirleyici rol oynayacağı dile getirilmiştir. Aldatma teknolojileri ve dijital ikiz gibi kavramların savaş doktrinlerini değiştirecek potansiyel barındırdığı, bu noktada komuta ve kontrol sistemlerindeki veri güvenliğine yönelik çalışmaların artırılması gerektiği paylaşılmıştır. Özellikle siber güvenlik kavramının kurumsal bir kültür haline getirilmesi gerektiğine de dikkat çekilmiştir.

Her teknolojinin odağında insanın olduğu vurgusunu yapan katılımcılar, eğitim ve yetenekli personel konusunun da giderek önem kazanacağına vurgu yapmışlardır.

Oturumlarda ön plana çıkan konular ‘özet’ bölümünde, konuşmacıların ön plana çıkan cümleleri ise ‘satır aralarından’ bölümünde paylaşılmıştır. Paneldeki tüm konular için özet sonuç ve değerlendirme raporu da takdirlerinize arz edilmiştir.

Saygılarımla,

Dr. Oğuz HAMŞİOĞLU

SASAD Genel Sekreteri



AÇILIŞ KONUŞMALARI

Saygıdeğer Komutanlarım, kamu kurum ve kuruluşlarımızın ve sektör şirketlerimizin çok değerli temsilcileri, tüm değerli konuşmacılar ve katılımcılar, hepinizi saygıyla selamlıyorum.

Bugün burada küresel savunma teknolojilerinde trendlerini değerlendirmek üzere düzenlenen etkinliğimizde bir araya geldik. Bu organizasyon sadece teknolojik çözümlerin sergilendiği bir etkinlik olmanın ötesinde günümüzün hızla değişen güvenlik ortamında stratejik planlamanın ve savunma inovasyonunun önemi hakkında düşünme fırsatı da sunan önemli bir platformdur.

Silahlı kuvvetlerimizin ve müttefiklerimizin yeni nesil muharebe kabiliyetini artırma vizyonuyla bir araya geldiğimiz vizyonumuz, ümit ediyorum ki savunma ve havacılık sanayimiz için bir rehber niteliği taşıyacaktır. İlkinin 2008’de, ikincisini pandeminin zorlu koşullarına rağmen yüksek bir katılımıla 2021’de gerçekleştirdiğimiz organizasyonumuzun üçüncüsünde siz değerli paydaşlarımızla olmaktan mutluluk duyuyor ve sizleri tekrar saygıyla selamlıyorum.

Geleceğin Askeri’ni ve savaşlarını tanımlayabilmek ve stratejilerimizi bu doğrultuda inşa edebilmemiz için öncelikle içinde bulunduğumuz zorlu konjonktürü iyi anlamamız gerekiyor. Günümüz dünyasında uluslararası sistemin çok kutuplu bir mücadeleye doğru hızla evrildiğini ve büyük güçlerin ekonomik, askeri ve dijital alanlardaki rekabetlerinin yoğunlaştığını görmekteyiz. Çok kutuplu dengelerle beraber bu durumun sadece başat güçler değil, orta büyüklükte devletler olarak da tanımladığımız etki alanı geniş ülkeler için de geçerli olduğu ortaya çıkmıştır.

Avrupa’nın doğusunda süregelen Rusya-Ukrayna savaşı jeopolitik dengeleri her geçen gün sarstığı gibi Pasifik Sahnesinde Çin’in artan askeri ve ekonomik nüfuzu, buna karşılık olarak da ABD’nin bölgeye yönelik güvenlik stratejileri küresel arenada yeni gerilimlerin habercisi olmaktadır.



Osman OKYAY

**SASAD Yönetim
Kurulu Başkanı**

Ortadoğu'da insani yıkımı ve vicdani yükü her geçen gün büyüyen çatışma ortamı, bölgesel güvenlik parametrelerinin ötesine geçme ve daha büyük güvenlik tehditlerini beraberinde getirme potansiyeline sahiptir. Bir yandan büyük sivil kayıplarına rağmen İsrail'in sorumsuzca büyüttüğü ve genişlettiği hareket, diğer yandan da İran'ın artan askeri kabiliyet ve agresyonu Ortadoğu'daki iki büyük temel güvenlik sorununa işaret etmektedir. Ekonomik alanda ticaret savaşları ve artan korumacı politikalar, özellikle yüksek teknoloji, enerji ve hammadde alanlarında ülkelere ciddi regülatif ve finansal belirsizlikler dayatmaktadır. Bu durum sadece devletler arası ilişkileri değil, aynı zamanda başta küresel tedarik zinciri risklerine hassas, ihracat odaklı üreticileri ve sanayicileri de derinden etkilemektedir.

Siber güvenlik ve askeri hareketlerin bir boyutu olarak siber harp ve bilgi operasyonları da giderek daha tehlikeli hale gelen küresel güvenlik ortamında ciddi bir yer tutmaktadır. Siber alan, devlet dışı aktörlerin ve devlet destekli grupların, güvenlik zafiyetlerini istismar edebilecekleri bir saha haline gelirken, bilgi operasyonlarının hızla yayılması, ülkelerin hem iç hem de dış politikada güvenlik risklerini artırmaktadır. Buna ek olarak iklim değişikliği kaynaklı güvenlik sorunları, afetlere karşı direncin azaltılması ve bu durumun ekonomik yapıları zayıflatması gibi faktörler güvenlik kavramının boyutlarını genişletmektedir. Tüm bu belirsizlikler ışığında, Türkiye savunma sanayii alanında kendi ürünlerini üreterek ve yüksek teknolojiye dayalı bir alt yapı inşa ederek stratejik etki alanını genişletmek ve Millî güvenliğini tahkim etmek yolunda kararlı adımlar atmaktadır ve atmaya devam edecektir. Bu bağlamda, hem savunma sanayiimizin müttefik ülkelerle oluşturduğu işbirliğini güçlendirmek hem de küresel arenada Türkiye'nin stratejik rolünü pekiştirmek adına buradaki çabalarımızın büyük bir değeri olduğuna inanıyorum.

Uluslararası sistemdeki stratejik manevra alanımızın genişletilmesi hedefi, bu rotanın Kuzey Yıldızı'dır. Müttefiklerimize de muhtelif diplomatik, askeri ve ticari araçlarla katkıda bulunarak pekiştireceğimiz savunma sanayii eko sistemimiz küresel belirsizlikler çağında Türkiye'yi bölgesel bir güç olmanın ötesinde bir çok küresel ajandaya liderlik eden aktör konumuna getirecektir.

Etkinliğimiz yalnızca yenilikçi teknolojilerin sergilenmesi değil, aynı zamanda bu teknolojilerin jeopolitik anlamının değerlendirilmek açısından da büyük önem taşımaktadır. Burada yapacağımız tartışmalar ve tanıtılan çözümlerle geleceğin savaş ortamını şekillendiren teknolojik trendler üzerinde duracak ve Türkiye'nin bu alanlardaki liderlik hedeflerini de ele alacağız.

Etkinlik boyunca savunma sanayii eko sistemimizin farklı paydaşlarıyla birlikte ülkemizin küresel güvenlikteki rolünü daha da güçlendirmeye yönelik adımlarımızı gözden geçirme fırsatına sahip olacağız. Otonom ve robotik sistemlerden giyilebilir teknolojilere, yapay zekâ ve siber güvenlikten enerji güvenliğine uzanan geniş bir yelpazede konuları ele alırken, eko sistemimize kıymetli girdiler sağlayacağımıza dair hiç şüphem yoktur.

Belirtmek gerekir ki, savunma sanayiimizdeki atılımlar Türkiye'nin caydırıcılık kapasitesini güçlendirirken, aynı zamanda küresel savunma ekosistemine de entegre olma sürecimizi hızlandırmaktadır. Bu kapsamda Türk sanayicilerin geliştirdiği ileri teknolojilerin sadece operasyonel üstünlük sağlamasını değil, aynı zamanda çift kullanım potansiyeli taşıyan çözümlerle sivil ve askeri alanları buluşturan bir inovasyon platformu haline geldiğini görüyoruz. Bu teknolojilerin etkin kullanımı, ülkemizin sadece bölgesel değil, küresel güvenlik mimarisinde de stratejik bir konum elde etmesini destekleyecektir.

Bugün burada sergilediğimiz vizyon ve işbirliği, Türkiye'nin savunma sanayiinde yükselen başarısının temel taşlarını oluşturmaktadır. Sizlerin katkıları, ülkemizi sadece üretim gücüyle değil stratejik liderliğiyle de küresel arenada öne çıkarmaktadır. Etkinliğimizin ilham verici ve işbirliğine açık bir platform olacağına yürekten inanıyorum.

Tüm katılımcı paydaşlarımıza tekrar teşekkür ediyorum, faydalı bir etkinlik geçirmenizi diliyorum.

Saygılarımla.

Sayın başkanım, değerli silah arkadaşlarım, kamu kurumları ile sanayimizin kıymetli temsilcileri, yurt içi ve yurt dışından gelen değerli katılımcılar,

Sözlerime 23 Ekim 2024 tarihinde Türk Savunma Sanayii'nin gözbebeği olan TUSAŞ'a yönelik hain terör saldırısında şehit olan vatandaşlarımıza Allah'tan rahmet ve TUSAŞ'ımızın fedakar çalışanlarına geçmiş olsun dileklerimle başlamak istiyorum.

SASAD tarafından düzenlenen kullanıcı, tedarik makamı, üretici ve araştırma kurumlarının bir araya geldiği 'Uluslararası Geleceğin Askeri' konferansında sizlerle birlikte olmaktan mutluluk duyuyorum.

Türk Silahlı Kuvvetleri'nin kamu kurumları ve yerli-yabancı sanayi kuruluşları ile bir araya getiren bu tür faaliyetlerin geleceğin güvenlik ortamının şekillendirilmesine ve uluslararası işbirliğinin artırılmasına yönelik önemli adımlar atılmasına katkı sağlayacağına inanıyorum.

Saygıdeğer konuklar, değerli katılımcılar,

Saygınlığın yanı sıra güçlü, caydırıcı ve etkin bir ordu haline gelebilmek için sadece teknolojiyi takip edebilmek değil, bunun bir adım ötesine geçerek modern teknolojiye öncülük edebilmeyi hedeflemek ve bu hedefe ulaşmak için vizyonunu sağlam ve bilimsel konseptlere dayandırmak, diğer dünya ordularının sahip olmadığı yeni silah sistemlerini üretmek son derece önemlidir.

Gelişen teknoloji ve ortaya çıkan yenilikler, özellikle yapay zekâ, otonom sistemler, hipersonik sistemler, kuantum sensörler ve biyoteknoloji gibi nanoteknoloji gibi alanlarda yaşanan hızlı gelişmeler, muharebe şekilleriyle konsept ve doktrinleri de etkileyerek değişmesine sebep olmaktadır. Dahası, bu gelişmeler savunma ve güvenlik sektöründe köklü değişimleri de beraberinde getirmektedir.



**Korgeneral Zorlu
TOPALOĞLU**

**Kara Kuvvetleri
Komutanlığı Eğitim
ve Doktrin (EDOK)
Komutanı**

Geleceğin muharebe ortamında yapay zekâ destekli analiz ve karar sistemleri anında ve doğru karar alınmasını sağlayacak, otonom sistemler ise insan faktörünü en aza indirerek riskleri azaltacak ve etkinliği artıracaktır.

Teknolojik ilerlemenin yanı sıra etik sorumluluk ve sürdürülebilirlik te geleceğin askeri yapısının temel taşlarını oluşturacak diğer faktörlerdir. Silah sistemlerinin askeri operasyonların çevresel etkileri göz önünde bulundurularak sürdürülebilir çevre ve çevre dostu çözümler geliştirmelidir.

Ayrıca, yapay zekânın muharebe alanında kullanımıyla ilgili etik ve yasal düzenlemelerin yapılması insan haklarının korunması açısından kritik öneme haizdir. Bu kapsamdaki adımlar, proaktif bir tutum ve anlayış çerçevesinde atılmalıdır. Küresel tehditler ve güvenlik problemleri, tek bir ülkenin üstesinden gelebileceği sorunlar değildir. Bu nedenle ülkeler arası işbirliği, bilgi ve teknoloji paylaşımı, ortak eğitim ve tatbikatlar ile müşterek çalışabilirliği sağlamak, güç birliği yapmak ortak güvenlik ve barışın teminatı olacaktır.

Diğer taraftan teknoloji ne kadar ilerlerle ilerlesin insan faktörü her zaman en önemli unsur olarak kalmaya devam edecektir. Geleceğin askerlerinin teknolojinin sunduğu olanaklarla donatılacağı, muharebelerde kesin sonucun geçmişte ve günümüzde olduğu gibi gelecekte de eğitimli insan faktörü ile elde edileceği muhakkaktır. Geleceğin askerleri, ileri teknolojiye uyum sağlayabilecek bilgi ve beceriye sahip olmalı, aynı zamanda etik ve liderlik vasıflarını da geliştirmelidir. Bu doğrultuda eğitim sistemimizin yenilenmesi, askeri personelimizin sürekli kendini geliştirmesi hayati önem taşımaktadır. Çünkü askerin silah ve teçhizatı ne kadar gelişirse gelişsin, geleceğin hareketi ortamında karar verici yine insan olacaktır. Bu gerçek göz önünde bulundurularak geleceğin askerlerinin teknoloji ve siber güvenlik, hibrit hareket, insansız hava kara deniz araçları ve otonom sistemler, simülasyon ve sanal gerçeklik, zeka ve analitik beceriler, psikolojik dayanıklılık, hızlı ve doğru karar verebilme, yeterlilik ve insan yönetimi konularında çok iyi yetiştirilmesi kaçınılmaz bir ihtiyaçtır.

Gelişen teknoloji ile muharebe sahasında tehditlerin çeşitliliği ve etkisi her geçen gün çoğalmaktadır. Bu nedenle, askerlerin icra ettiği görevler artmakta, etki alanı genişlemektedir.

Bu kapsamda, hem beka tedbirlerinin hem de icra edilen görevlerin etkinliğini artırmak amacıyla askerin kullanmış olduğu teçhizatın da icra edilen görevlere uyum sağlayacak şekilde geliştirilmesi gerekmektedir. Geleceğin askerinin sahip olması gereken teçhizatın çeşitleri şu şeklide sıralamak ve özetlemek mümkündür:

Bunlar; kişisel koruma ekipmanları, iletişim ve bilgi sistemleri, siber ve elektronik savaş ekipmanları, silah sistemleri, manevra kabiliyeti ve lojistiği etkileyen araç ve sistemler, bunların düşman tarafından tespitini engelleyen yeni nesil gizleme ve örtü sağlayacak teknolojiler, aldatma teknolojisi bunların önem arz edenleridir. Söz konusu teknolojilerin tasarımı, askerin zihni ve fiziksel açıdan, muharebe ortamında ihtiyacını karşılayabilecek yeterlilikte olmalıdır. Askerin, karar vermesini gerektirmeyen, özellikle beka tedbirlerine yönelik durumlarda alınacak önlemlerin otonom olarak gerçekleştirilmesi sağlanmalıdır.

Personelin eğitimi kapsamında, operasyon fasılaları dahil, Tek-Er'in bulunduğu her ortamda, eğitimine devam edebilmesine imkan sağlayacak sanal ve artırılmış gerçeklik teknolojileri ile gerçek ortamda hareket ediyormuşçasına destek sağlayacak yazılım ve donanımlar kullanmalıdır. Büyük verinin görselleştirilmesi yoluyla, durumsal farkındalık artırılmalıdır. Bu uygulamalar aynı zamanda muharebe ve bilişim sistemleriyle kullanılacak, diğer karar ve destek sistemlerinin kontrolünü de kolaylaştıracaktır.

Bilgisayar teknolojilerindeki gelişmeler, görevleri ve tehditlere yönelik muhtemel hareket tarzlarını belirleyebilmeli, askerin durum muhakemesi yapmasına, karar vermesine ve verdiği kararların sistemde kimliği tanımlanmış personele eş zamanlı olarak iletilmesine imkan sağlamalıdır. Sistemler, kendi personeli için tanımlanan dost kriterlerini tanımalı, düşmanın eline geçmesi halinde ise otomatik olarak devre dışı kalabilmelidir. Bu maksatla askerin, şartlara uyum sağlayabilmesi için hafif, pratik ve ergonomik, hareket ve manevra kabiliyetini artıracak ve koruma sağlayabilecek teçhizatın geliştirilmesi önem arz etmektedir. Dolayısıyla muharebe sahasında her geçen gün artan tehditler karşısında beka tedbirlerinin de geliştirilmesi büyük önem arz etmektedir.

Her asker, her türlü muharebe ve iklim şartlarından etkilenmeden, göreve devam etmek zorundadır. Atalarımızın Orta Asya'dan başlayan ve Türk tarihini süsleyen zaferlerinde en önemli unsurlardan biri, askerlerin çevik ve süratli hareket etme kabiliyeti olmuştur.

Tek-Er'in muharebe ve beka kabiliyetini muhafaza edebilmesi için de bu sistemlere yönelik lojistik sistemin ve teçhizatın ihtiyacı olan enerjinin de pratik ve süratli ve kesintisiz olması gerektiği unutulmamalıdır. İnsansız sistemlerin komuta ve kontrolünde en önemli faktörlerden biri de insan-makine arabirimi olacaktır. Komutanın hareket tasarısı, konuşmadan insansız sistemlere aktarılabilmelidir. Bu noktadaki bir güvenlik açığı, elektronik olarak ele geçirilebilecek insansız sistemlerin birliklerimize karşı kullanılabileceğinden, koruma ve güvenlik faktörü öne çıkmaktadır. Bu kapsamda, durumsal farkındalığı, beka, ateş ve manevra kabiliyeti yüksek, gerek birlik bütünlüğü içinde gerekse tek başına bir sistem olarak geleceğin muharebe sahasında görevler üstlenebilecek Tek-Er sistemlerinin geliştirilmesine, bu sistemlerin muharebe sahasındaki diğer sistemlerle entegrasyonunun sağlanmasına yönelik değerlendirmelerin yapılmasına da ihtiyaç duyulmaktadır.

Değerli katılımcılar, iki gün süreyle icra edilecek 'Uluslararası Geleceğin Askeri' Konferansı'nın bu alanda yürütülen çalışmaların, teknolojik gelişmelerin ve gelecek öngörülerinin takip edilmesi, savunma sanayiinin kabiliyetlerinin ortaya konulması ve farkındalığın artırılması bakımından faydalı olacağını değerlendiriyorum. Bizler, ebedi başkomutan Gazi Mustafa Kemal Atatürk'ün ifade ettiği gibi 'Yurtta Barış, Cihanda Barış' ilkesi kapsamında komşularımızın toprak bütünlüğüne saygılıyız ve diyalogdan yanayız. Ancak, ülkemizin hak, hukuk ve menfaatlerini korumakta da kararlıyız. Terörle mücadelede büyük yetenek ve tecrübe kazanan Türk Silahlı Kuvvetleri'nin etkinliği, caydırıcılığı ve saygınlığı dostlarımız için de büyük bir kazanımdır. Türk Silahlı Kuvvetleri'nin imkan ve kabiliyetlerinin geliştirilmesinde, ihtiyaç duyulacak her türlü bilgi ihtiyacına ve ortak çalışma taleplerine mevzuat çerçevesinde hazır olduğumuzu belirtmek istiyorum.

Konferansın tüm katılımcılar için verimli geçmesini temenni ediyorum, saygılarımla sunuyorum.



SATIR ARALARINDAN

**GÜNÜMÜZ
ÇATIŞMALARINDA
TEKNOLOJİ**

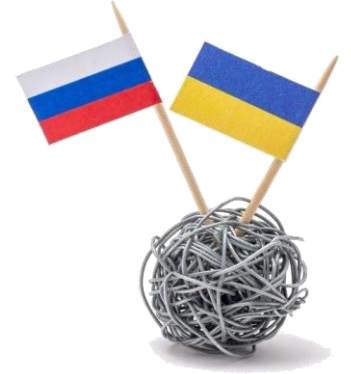
Otonom Sistemler ve İnsansız Hava Araçları, düşman savunma hatlarını hedef alarak stratejik üstünlük sağlamada, savaşın seyrini belirleyici şekilde etkilere sahiptir.



Ukrayna, savaşın ilk dönemlerinde TB2 Bayraktar ile Rusya'ya karşı büyük bir avantaj elde etti. Ancak Rusların çok kısa sürede buna uyum sağladığını gördük. Burada asıl önemli olan, yenilik hızındaki süreklilik. Özel sektör ve yeni girişimler sayesinde, savaş alanında baş döndürücü bir yenilik hızı var.



Ukrayna-Rusya çatışmasında bir kez daha görülmüştür ki, savaş konsepti düşmanlarınızın neyin peşinde olduğunu anladığımız anlardan oluşur. İnsansız Hava Araçları'nın (İHA) bu noktada size tepeden sağladığı bakış açısı, detaylara ulaşma ve savaş stratejilerinin değişimi noktasında çok önemlidir.



Baykar TB2 ile başlayan, ülkelerin kendi üretim ve teknoloji zinciriyle başlattığı benzersiz an 'parlama, kıvılcım veya kıvılcımlar' olarak adlandırılabilir.

Bu kıvılcımın kendi döngüsünü oluşturabilmesi, devam edip ateşe dönüşebilmesi, daha ileriye gidebilmesi ve kalıcılığı başarabilmesi, kendi bağımsız askeri sanayisini inşa etmesi ülkelerin ve ulusların kaderinde dönüm noktasıdır.



Ukrayna-Rusya çatışmasında TB2 Bayraktar, teknoloji tekellerinin değişimi, geleneksel güçlülerin benzersiz üretim yeteneğinin kırıldığını, başka ülkelerin de jeoekonomik ve jeopolitik yapılara müdahale edebildiğine dair önemli bir dönemi işaret etmiştir.



Ukrayna Rusya Savaşı, teknoloji şirketlerinin gelişim ve deneme laboratuvarı olmuştur. Kara, Hava, Deniz, Siber ve Uzay alanlarındaki testlerin yanı sıra, teknolojik rekabet, kaynak ve hammadde temini, alçak dünya yörüngesi teknolojilerinin kullanımı, entegre iletişim sistemleri, endüstriyel teknolojiler gibi her alanda ekonomiden komuta kontrol merkezine, sahadan teknolojiye yön verenlere strateji ve doktrinleri değiştiren, farkındalık, taktik, bilgi kontrol ve yönetimi ile asker koordinasyonuna kadar süreçlerin gözden geçirilmesini sağlayan dersler içermektedir.

Ukrayna'nın insan kaynağı, endüstriyel kapasitesi ve NATO ülkelerinin ekonomik destekleri Ukrayna'nın sürdürülebilir bir ilerleme kaydetmesini ve ön cephe savaşlarında etkili olmasını engelliyor. İnsansız Hava Araçları'nın topçu silahlarının yerini alabileceği, konumsal savaşta Rusları imha edebilecekleri kendi konseptlerini geliştiriyorlar. Örneğin, fiber dronlar ile de elektronik harbe karşı durmaya çalışıyorlar.

Ukrayna-Rusya Savaşı'nda Milattan Önce 2000'li yıllarda Asurlulardan kalma bir tekniğin 21. Yüzyıla taşınarak tanklarını FPV insansız hava araçlarından korumaya yönelik tedbirleri, güçlü bir savunma ve daha az zayıf için basit ama akıllıca yöntemlerin önemini göstermektedir. Bu aynı zamanda, güçlü zırhlı tanklar yapılması veya rakibimizin bunu yapması halinde bunun nasıl delinebileceği yönündeki güçlü mühimmatlar yönünden de düşündürmeli. Klasik savaş ortamı için hazırlanan tankların, hızlı savaş alanında nasıl yok olduğunu ya da nasıl basit bir akılla korunduğunu da düşünmeliyiz.



Ukrayna-Rusya Savaşı'nda Rusların '**Noktasal Vuruş Noktası ve Krank Konsepti**' olarak adlandırılan taktik, Amerikalılar dahil tüm savaş uzmanlarında hayranlık uyandırıyor. Zira Rusların rezervlerinin, lojistik ve ikmal konusunda sıkıntı yaşamalarının beklendiği Orikhiv, Kurakhov, Kurshcyna hatlarında ilerlemeleri herkesi şaşırttı. Havadan elde edilen görüntülerle ve elektronik savaş verileriyle çok etkili önlemler aldıklarını, yeni teknolojileri sadece öldürmek değil, sürdürülebilir savaş noktasında da etkili kullandıklarını, ikmal güçlerini kullanım noktasında da bu teknolojileri seferber ettiklerini görüyoruz. Kendi operasyonlarını yürütmede bağımsızlık ve özerkliğe sahip ve yaklaşık 300 kilometrekareden sorumlu birlik, savaşı istediği gibi yönlendirip Ukraynalı askerleri istedikleri bölgelere çekiyor ve bu bölgelerde noktasal vuruşlar yapıyorlar.



Polonyalı ve Avrupalı savaş uzmanları, Rusların oluşturdukları özel birliklerle 30 kilometrelik hatları enlemesine ve boylamasına, noktasal vuruşlarla ilerlediğini düşünüyor. 'Krank' gibi dairesel bir devinim oluşturan Ruslar, bir tür makine ilerlemesini topçu bataryası, elektronik savaş ve insansız savaş aracı ile yönetiyorlar. Büyük akıllı bombaları da ilerlemeye yardımcı oluyor.

Ordudaki en küçük topçu birliği olan 'Batarya' birimlerinin de Rus ilerlemesindeki etkisini görüyoruz. Özellikle Güney'de Rusların ilerlemesinde insansız hava araçlarını ve özellikle de FPV dronları kullanarak 10'ar kilometrelik bölümler halinde ilerlediklerini görüyoruz. 'Batarya Birliklerini Yeni Taarruz için, her 10 kilometrede bir hazırladıklarını, uydu ve insansız keşif araçlarıyla gözetlemenin ardından FPV dronlar ve topçu atışı desteğiyle ilerlediklerini görüyoruz.

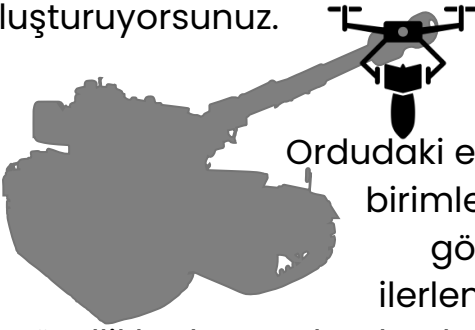


Savaşlarda lojistiğin de yeni teknolojilere göre ve bu teknolojilerin gelişimine göre periyodlara ayrılarak dizayn edilmesi zorunludur.



Azerbaycan'ın etkin İHA ve SİHA kullanımı düşman savunma hatlarını hedef alarak stratejik üstünlük sağlaması, modern teknolojilerin askeri operasyonlardaki önemi ortaya koyarken, daha güvenli ve koordineli çalışmanın etkisini ortaya çıkarmıştır.

Savaş alanına giren yeni bir teknoloji, önceki dinamiklerin ortadan kalktığı anlamına gelmez. Avrupalılar açısından, 10 yıl önceki dinamiklerde Ukrayna ile Rusya arasında Dünya Savaşı'na benzeyen bir savaş olacağını söyleseydiniz kimse inanmazdı. Peki ne oldu, I. Dünya Savaşı'na benzer siper savaşları görüyorsunuz. Dronlar piyade askeri için savaş alanını görünür hale getirir, ön cepheyi temizler. Ama yine de mühimmata ihtiyacınız var. Bunu gelişen teknolojilerle birleştirerek savaş sahasında yeni dinamikler oluşturunuz.



Ordudaki en küçük topçu birliği olan 'Batarya' birimlerinin de Rus ilerlemesindeki etkisini görüyoruz. Özellikle Güney'de Rusların ilerlemesinde insansız hava araçlarını ve özellikle de FPV dronları kullanarak 10'ar kilometrelik bölümler halinde ilerlediklerini görüyoruz. 'Batarya Birliklerini Yeni Taarruz için, her 10 kilometrede bir hazırladıklarını, uydu ve insansız keşif araçlarıyla gözetlemenin ardından FPV dronlar ve topçu atışı desteğiyle ilerlediklerini görüyoruz.

Ukrayna ve Gazze, yapay zekâ ve otonom teknolojilerin kullanımı için inanılmaz bir test laboratuvarı. Günümüzde sivil hayat için geliştirilen teknolojilerin, savaş ortamında nasıl kullanıldığını gösteren önemli örnekler mevcut. Örneğin müşteriyle taksiyi buluşturan uygulamalar, herhangi bir Ukrayna vatandaşının topçu saldırısı veya dron istihbaratının koordinesine destek vermek için kullanıldı.

AElde edilen açık kaynaklı ve masum görünümlü teknolojilerle elde edilen verilerin, yapay zekâ ile şehirlerin elektrik dağıtım merkezlerinin, mühimmat sevkiyat veya merkezinin bombalanmasıyla sonuçlandığını görüyoruz. Elektronik karıştırma sistemleri ve elektronik harp, FPV'lerde GPS sistemlerinden fiber sistemlere dönüşümü ya da yapay zekâ desteğiyle otonom görev tamamlamayı beraberinde getirdi.



Çatışma ortamlarında robot savaşlarının ilk bulgularını insansız kara ve deniz sistemleriyle görüyoruz.

Ve daha önce küçük robot kullanımından artık büyük robot kullanımlarına geçiliyor.

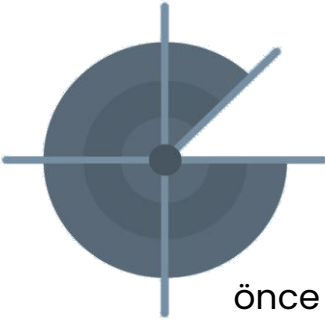
2017'de DAESH terör örgütünün piyasada bulunabilen dronlara AK-47 ile haftada 30 kadar Irak askerinin ölümüne sebep olması ve şimdi akıllı mühimmatlar veya intihar dronlarına dönüşüm, savaşlardaki hızlı teknolojik dönüşüm ve yeni savaş ortamlarına dair önemli bir bulgudur.

Rusya'nın Shaid 36 insansız Hava Araçları ile termobarik yükleri (vakum bombası) taşıması, Odessa'da sığınakları hedeflemesi yeni teknolojilerin öldürücü ve çarpan etkisi boyutuyla ders niteliğindedir.



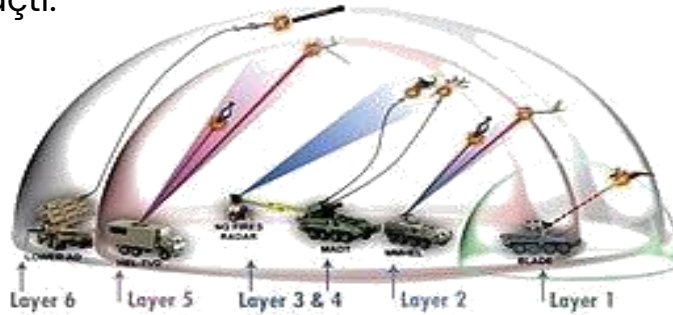
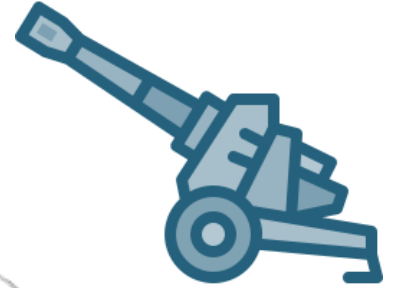
Rusya-Ukrayna çatışması, teknolojik çatışma ortamının geldiği noktanın en güncel örneği. Aynı zamanda savaşların nasıl yapıldığı, kayıp veya kazanımı yeniden tanımlamaktadır.

Silahlı insansız hava araçlarını sahte insansız hava araçlarıyla karıştıran hedef yanıltıcı sistemler, silahlı hava araçlarının radar imzasını taklit etmek için tasarlanmış ve hava savunma sistemini etkilemek için hazırlanan silahsız yem dronların kullanımı, farklı tehdit türlerinin ayırt edilmesini zorlaştırma gibi bir çok yeni taktiği sahada görüyoruz.



Yapay zekâ sisteminin çatışma ortamında analiz ve hızlı karar döngüsüne dahil edilmesinde Ukrayna-Rusya savaşı taze örnek olmuştur. Uydu ve keşif araçlarının görüntüleriyle gözlemlene, yönlendirme, karar verme ve düşman harekete geçmeden önce önlem almak için yapay zekâdan yararlanıldı.

Hipersonik füzeler, anti-teknoloji füzeler akıllı teknolojilerle nokta atışı atış yapma yeteneği, uzun vuruş menzili, etkili hasarlarla topçulukta devrime yol açtı.



Ukrayna'daki çatışmalar, hava üstünlüğünün sağlanamaması ve kara operasyonlarının etkinliğinin sınırlı kalması arasında kaldığı için taraflar birbirine üstünlük sağlayamamıştır. Tarafların birbirlerine füze ve roketler atmasına rağmen bu üstünlük kurulamadığı için savaşta bariz üstünlük olmadığı öngörülmektedir.



SATIR ARALARINDAN

**YAPAY
ZEKÂ**



Yapay zekânın temel aracı ve gerçekten en iyi olduğu şey, veriyi parçalayabilmesi ve verileri analiz edebilmesi. Günümüzdeki dönemde hayatımıza ve askeriye en büyük katkısı analitik bir kolaylaştırıcı olması.

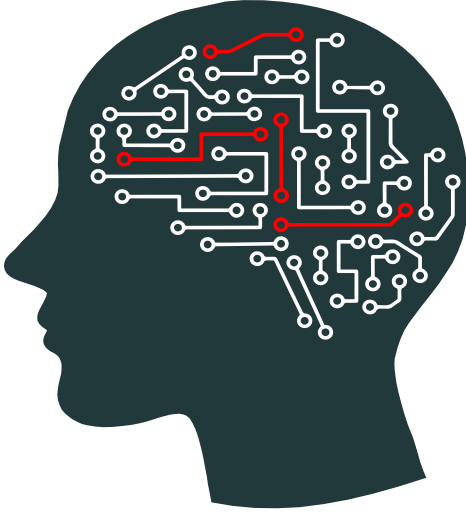
Bilgi operasyonu yıkımı yeni değil. Roma İmparatorluğu'ndan bu yana devam ediyor ve değişen sadece araçlar. Yapay zekâyı da bu yüzden yıkıcı olarak düşünürken, artık ölçeklenebilir ve ölçülebilir olduğunu düşünmeliyiz.

Endişelere ve risklere rağmen yapay zekâ konusunda çok sayıda fırsat bulunmakta. Sivil ve askeri boyutuyla kullanılan teknolojilerde kısa, orta ve uzun vadeli fırsat ve risklere göre bir Ar-Ge ve Ür-Ge yapılanması emek, değer ve zaman planlamalarının sağlıklı yönetilmesini sağlayacaktır.

Yapay zekâ ile ilgili trendler, olasılık, etkiler, belirsizlik dönemi, olası eylem planları ile askeri yapay zekâ ekosistemi, dost ve rakip sistemler ayırımı gibi çalışmaların yetkili merkezler tarafından farklı gruplar halinde çalıştırılması, merkezi veri oluşturulmadan da verilerin önem kategorilerine ayrılması için iyi bir planlama yapılması stratejik önem taşımaktadır.

Yapay zekâ, üretimden eğitime her alanda etkili olacak. Doğrusal gelişimden sarma gelişime bir geçiş eğrisi bekleniyor.





Yapay zekâ destekli askeri platformlar yakın vadede, insan makine ekiplerinin ve alt yapı gücünden yararlanmaya odaklı olacak.

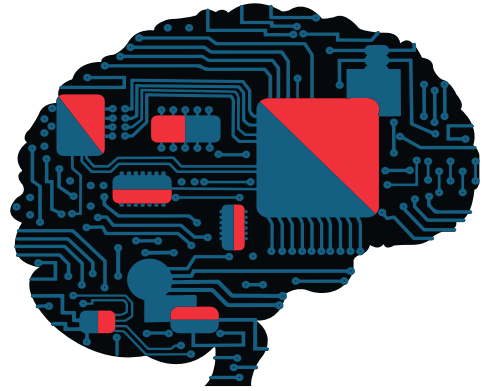
Askeri yapay zekâ, giderek artan bir kuvvet çarpanı olacak.

Askeri yapay zekâ ile, düşmana yönelik Komuta, Kontrol, İletişim, Bilgisayar ve İstihbarat Sistemleri (C4I) altındaki yetenekler için fırsat ve hedeftir. Yapay zekânın savunmanın tüm alanlarında sayısız potansiyel etkisi vardır. İstihbarat analizi, karar destek araçları, savaş oyunları, simülasyon, elektronik harp, insansız, robotik ve sürü sistemler, genel ve saha lojistiğinin optimizasyonu gibi askeri kabiliyetlerin hazırlanması, operasyonel kullanımı ve sürdürülebilir ekonominin oluşturulması gibi konularda yapay zekâ teknolojilerinin kullanılması kaçınılmaz olacaktır.

Askeri yapay zekâ üzerindeki rekabette yeni mekanizmalar getirilmezse, ABD ve Çin arasındaki süper rekabet istikrarsızlaşabilir ve bu diğer ulusları tehdit edecek hale gelebilir.

Yapay zekâ ve askeri kullanımı, demokratik ve otoriter rejimler için farklı üretim ve ürünsel kapasitelerin gelişimini ve potansiyelini sağlıyor.

Askeri yapay zekânın küresel yönetimi, küçük devletleri daha büyük oyuncular tarafından geride bırakılma riskiyle karşı karşıya bırakmaktadır.

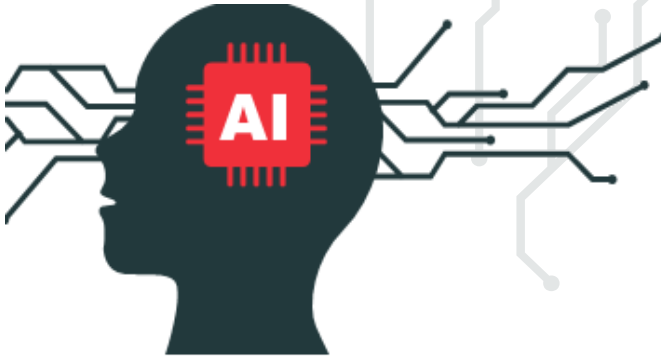


NATO ve Batı, Rusya ve Çin gibi ülkelerin yapay zekâ programlarını yakından takip ederek, modern savaş ve istihbaratta kullanımıyla mücadele edebilecek programlar geliştirmelidir.



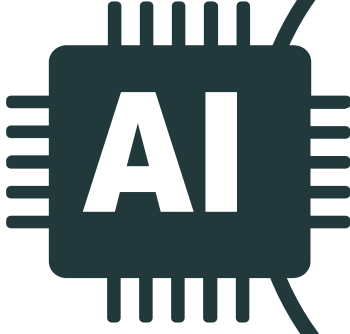
‘Bilgilendirilmiş ve yapay akıllı boyutta savaş’ askeri literatürde yeni terimler arasında yer alabilir.

Yapay zekâ gelişiminde birçok kaldıraç, NATO’nun ve Batı’nın kontrolü dışındadır. Müttefikler, ortak uluslar, sanayi, akademi, sivil toplum ile entegre bir yaklaşım özellikle askeri yapay zekâ alanında geniş bir katılım gerektirmektedir.



Yapay zekâ, hükümet dışı kuruluşlar (NGO) için de yeni ve farklı tehditlere fırsat sunmaktadır.

Çin, yapay zekâ merkezli harp istihbaratı sistemleri ve karşı sistem imhası, bilişsel alanın yıkımı ve benzeri alanlara odaklandılar. Bilişsel savaş yoluyla karar verme ve sistemin felcini tetikleyerek savaşmadan kazanabilme odaklı çalışmalar yapmaya çalışıyor.

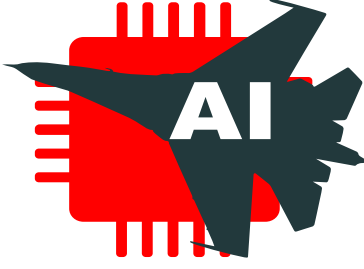


Akıllı, otonom ve yarı robotik sistemlerin kullanımıyla birlikte dünyanın dört bir yanındaki askeri ve siyasi dengelerde değişim görülmektedir. Özellikle ülkelerin nüfuzunda bu sistemler önemli yer tutmaktadır.

Yapay zekâ, düşmanın algılarını etkilemek, bilgi alanına erişim ve düşünmenin yanı sıra, düzensizlik, karşı sistemlerin bozulması ve komuta-kontrol sistemlerinin alt yapılarını felç etme alanlarında çok ciddi imkan ve riskler sunuyor.

Yapay zekâ sistemleri, kullanacağı alt teknolojilerle birlikte veri analizi, hız, konum ve öldürücü boyutuyla savaş kabiliyetlerinde çarpan etkisini belirleyecektir.

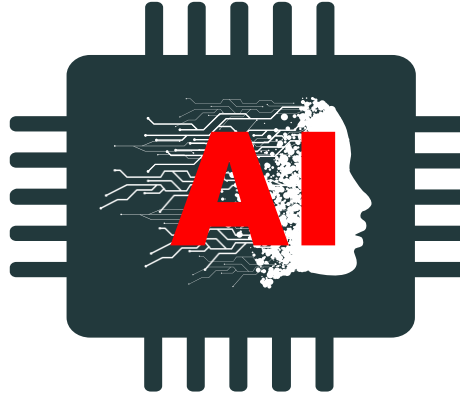
Yapay zekâ sistemlerinin çökmesi halinde, yapay zekâya bağlı olmayan sistemlere geri dönebilme sürekliliği en önemli avantajlar arasında olacaktır. Dünya genelindeki orduların dayanıklılık ve acil durum hazırlığı açısından da bu bir örnek olarak kabul edilmektedir.



ABD Ordusu Hava Kuvvetleri, bir yapay zekâ algoritmasının jeti uçurabildiğini, özerk olarak 8 farklı görevi yerine getirebildiğini açıkladı.

Yapay zekânın bizden daha hızlı çalışması dolayısıyla bu tür bir teknoloji ile büyüyen özerkliğin, endüstriye ve insan kaynağına nasıl entegre edileceğini düşünmeliyiz.

Otonom, robotik ve yapay zekâ sistemleri üzerine yeni askeri yapılanmalar kaçınılmazdır.



Dünya ordularında otonom sistemler ve insansız hava araçları yeni komutanlıklar oluşturmaktadır.

Derin sahtecilik, bilgi ve manipülasyon, siyasi, ekonomik ve sosyal bozulma ile çarpık askeri karar alma süreçleri günümüzde yapay zekâ teknolojilerinin kullanımının ve oluşturabileceği tehdit boyutlarının en yeni örnekleridir.



Bilişsel Savaş'ın da etkili olacağı dönemler başlamaktadır. Bilişsel Savaş'ta beyniniz sizi aslında bir bilgi ortamına kilitleyerek, ilk önce savaş alanı haline getirir ve algıladığınız yeri yeniden tanımlayacak bilgiden fazlasıdır. Bilişsel Savaş, neyi ve nasıl düşündüğünüzü kontrol etme yeteneği, nasıl düşündüğünüzü kontrol etmek için yapılandır.

Derin sahtecilik, 2014 yılında gündemimize girdi, iki resim veya görüntü eşleştirme veya değiştirme yoluyla. Bir savaşta kullanımı ise 2022 Mart ayında Zelenski'nin vatandaşlarına silah bırakma çağrısı şeklinde oldu. Ve Putin'in sıkı yönetim ilan etmesiyle devam etti. Bu paniklere yol açtı. 2013 yılında bir askeri analist olarak bana bu bilginin 10 yıl sonra kitleleri nasıl yöneteceğini veya savaşta neyi etkileyeceğini soracak olsanız bunu ön göremezdik. Bilimsel olarak olmayan bir teknolojinin savaş ortamında nasıl çalıştığını anlamamız ve nasıl kullanacağınızı bilmeniz gerekecek. Bu katlanarak büyüme ve savaş alanında da bir büyümedir.



Derin sahtecilik, yapısal olarak hepimizin psikolojik ön yargılarını asimetric olarak daha etkili kullanımını sağlamaktadır.





Çoğu ülkenin yapay zekâ ile insansız sistemler bir arada kullanma ve birleştirme isteğini açıkça görebiliyoruz; 'savaşçıysa vur ya da sivilse vurma!'.

DARPA, yapay zekâ için iki ayırım yapıyor. Birinci yapay zekâ dalgası makinelerin insanların kodladıklarını uygulaması. İkinci yapay zekâ dalgasında ise makinelerin bu verileri anlamlandırmasını istemek. Üçüncü dalga ise kendi kendine en iyi şekilde yapay zekânın nasıl öğreneceğini öğrenmek. Birbirlerini faaliyet gösterdikleri bağlamda anlayan, kendi eylemlerinin sonuçlarına karar veren ve sonuçlarını anlayan sistemler olacak. Askeri açıdan daha önemlisi, düşmanca eylemlerin sonuçlarını anlayan sistemler olacak. Burada karar verme yetkisinin tamamen makinelere devredildiği dönemler yaşanabilir.

Savaş alanında yapay zekâ kullanımının ilk dönemleri, insanları yeniden tasarlayan, gelişmiş savaş araçlarının yeniden tasarlandığı bir dönem olacak. İnsan kontrolünün içinde ama insanın kontrolünün karar döngüleri içerisinde devreden çıkabileceği bir döneme evrilecek. İnsanın, teknolojik olarak güçlendirilmiş bir çatışmaya ayak uydurma ve ayak uydurmanın aşılacağı dönemler orta ve uzun vadeli savaş stratejileri ve ortamları olabilir.



Yapay zekâ her zaman hizmetkardır, insan efendisidir ama sen ne yapmak istiyorsun, yapay zekâ neyi yapmalı?



SATIR ARALARINDAN

**VERİ YÖNETİMİ
VE
BLOK ZİNCİRİ**



Günümüz savaşlarında üretilen çok ciddi bir iletişim ve veri akışı söz konusudur ve teknolojik planlamalarında alınan verinin faydalı bilgiye çevrilmesi en kritik konular arasındadır.



Blockchain teknolojisi, dağıtık yapısı ve girilen verinin değiştirilemez özelliği ile güvenli veri akışına katkı sunabilir. Gizli ve kritik bilgilerin depolanması ve korunması, haberleşmenin bütünlüğü ile gizliliği, şebeke merkezli muharebe gibi alanlarda gelecekte büyük potansiyel sunmaktadır.



Askeri teknolojilerin etkisi, güvenli iletişim, karar alma ve güvenli veri paylaşımına bağlıdır. Blockchain teknolojisi, dağıtık, merkezi olmayan, değiştirilemez ve şeffaf yapısı, güvenli iletişim, etkili koordinasyon özellikleriyle otonom hava gücü sistemlerinin karşılaştığı güvenlik ve koordinasyon sorunlarına katkı sağlayabilir.



İHA ve benzeri sistemlerin savaş alanındaki verileri toplaması, analiz etmesi, güvenli bir şekilde saklanması, kaydedilmesi ve iletilmesi alanında blockchain operasyonel güvenlik imkanları barındırmaktadır.

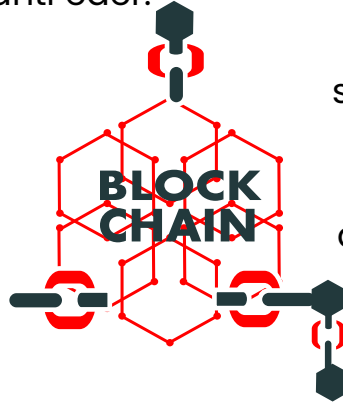
BLOCK CHAIN

Çin, manipülasyona dayalı kimlik yönetimine karşı askeri robotları blockchain tabanlı kimlik yönetme ve donatma ile ilgili projeler yürütmektedir. Her robot veya insansız sistem, yalnızca yetkilendirilmiş parametreler içinde çalışmasını garanti eden benzersiz bir blockchain kimliğine sahip olacağından, sistemlerin yalnızca yetkilendirilmiş kullanıcılar tarafından kontrol edilmesini garanti eder.

Güney Kore, sınırlarında otonom robotik savunma sistemlerini blockchain ile destekleyerek daha güvenilir hale getireceği projeler üzerinde çalışmaktadır.

Yapay zekâ, büyük veri, kuantum ve blockchain entegrasyonu büyük değişimleri beraberinde getirerek bilişsel güç tanımını değiştirebilir.

Otonom sistemler, ortak bir blockchain üzerinde hızlıca istihbarat paylaşabilir ve dinamik savaş ortamlarında stratejilerin belirlenmesini sağlayabilir. ABD Hava Kuvvetleri, otonom dron sürülerinin Blockchain üzerinde gerçek zamanlı olarak bilgi paylaşımını test etmektedir. Bu sistemler, sürü içinde koordinasyonu artırarak hedeflere daha etkili bir şekilde saldırabilir.



Blockchain, hava gücünü uzay, siber uzay, kara, hava ve deniz gibi diğer alanlarla birleştirerek güvenlik doktrinlerini yeniden şekillendirme ve jeopolitik stratejileri yeniden tanımlama gücüne sahip bir sistemdir. Bu yönüyle koalisyon operasyonları ve siber güvenlik önceliğinde büyük katkı potansiyeli bulunmaktadır.

Blokchain teknolojisi, askeri teknolojilerin çok sayıda farklı alanında özellikle büyük verinin işlenmesinde büyük fırsatlar sunabilir.



SATIR ARALARINDAN

**SİBER, UZAY
VE
ELEKTRONİK HARP**



Rusya, Ukrayna navigasyon ve hedefleme sistemlerini bozmak için GPS sinyallerini karıştırdı. Ukrayna'nın dron Karşıtı Elektronik Harp Sistemleri, Rus İHA'larını uçuş ortasında devre dışı bırakabilmesini sağladı. Her saldırı için yeni bir savunma teknolojisi döngüsünü de yakından gördük.

Spektrum teknolojisinde yeni yeteneklere karşı güvenlik açıklarının bulunmasını, zayıf noktalarının tespit edilmesini ve karşı teknoloji uygulanmasını beraberinde getirdi.

Rus devlet destekli bilgisayar korsanları, elektrik şebekeleri ve finansal sistemler de dahil olmak üzere Ukrayna'nın kritik altyapısını hedef alan siber saldırılar başlattı. Ukrayna'nın elektrik şebekesine yapılan saldırı özellikle önemliydi.



Siber dünyada çok şey oluyor ve siber savaş alanındaki operasyonlar oldukça kritik önem taşıyor.

Tüm bunlar bize dijital ve fiziksel dünyanın kusursuz entegrasyonunun ve sonuçlarını göstermektedir.

Demek oluyor ki, siber savaşın yaygınlaşması, küçük bir devletin çok daha büyük bir düşman üzerinde önemli bir yıkıma yol açmasına sebep olabiliyor.



Teknolojik gelişmeler, elektronik harbin önemini giderek en önemli kuvvet çarpanı haline getirmektedir. Elektromanyetik spektrum üzerinden kör olabilirsiniz, uzay ve siber alandaki savaş bu açıdan önemini açık ara artırmaktadır.



Harekat sahaları, fiziki alandan bilgi alanına, bilgi alanından bilişsel alana doğru genişleyecektir. Harpte Komuta, Kontrol, İletişim ve Bilgisayar (C4) harpteki önemini geçmişte olmadığı kadar fazla artıracaktır.



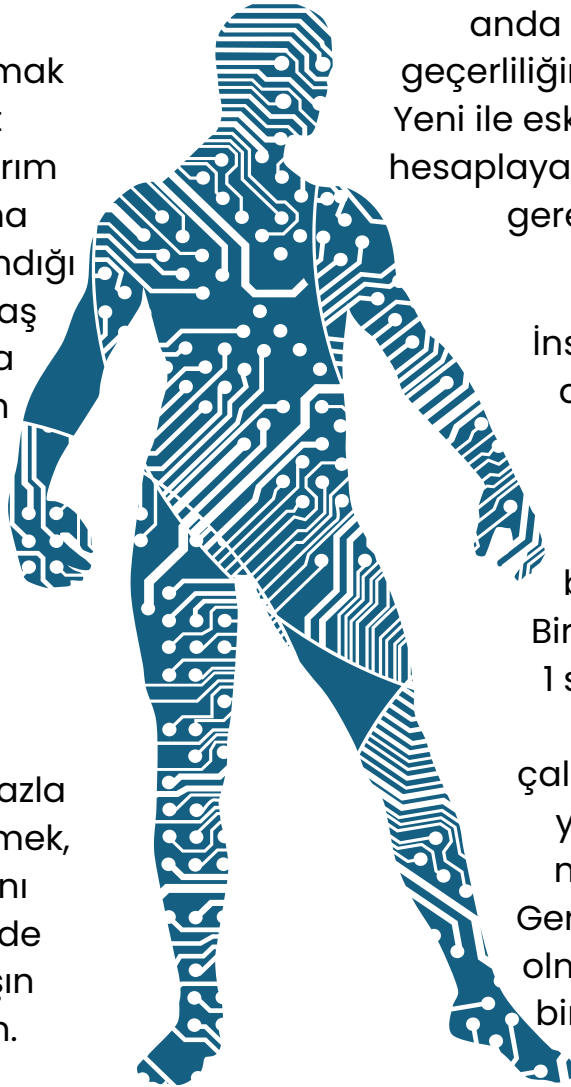
SATIR ARALARINDAN

**GELECEĞİN ASKERİ
İNSAN VE EĞİTİM**

Akıllı kasklar, artırılmış gerçeklik içeren ve veri erişimi sağlayan ekranlar kullanıyorlar. Bu teknolojilerle donatılmış askerler gerçek zamanlı savaş alanı bilgilerine erişiyorlar. Çok daha az iletişimle harita, tehdit ve görev hedefleri dahil çok daha fazla veriye ulaşıyorlar. Bu onlara savaşın durumsal farkındalığına anında sahip olmalarını ve daha hızlı karar alabilmelerini sağlıyor. Amerika Ordusu, örneğin görsel güçlendirme sistemleri gibi programlara çok önem veriyor.

Uluslar yorgunluğu
azaltmak ve
dayanıklılığı artırmak
için dış iskelet
teknolojisine yatırım
yapıyor. Ukrayna
ihtilafında kanıtlandığı
gibi kentsel savaş
senaryolarında
bu teknolojinin
hayati
öneme
sahip
olduğu da
ortaya çıktı.

Yeniliklere daha fazla
insanı entegre etmek,
makine ile insanı
bütünleştirmek de
yeni nesil savaşın
zaruretlerinden.



Yeni teknolojiler, bir
anda eskilerin
geçerliliğini bitirmiyor.
Yeni ile eskiyi bir arada
hesaplayarak ilerlemek
gerekiyor.

İnsan-makine
aracılığıyla
ortaklık
kurmanın
yolunu
bulmalıyız.
Bir yarım veya
1 saniye zeka
hızıyla
çalışıyoruz ama
yapay zekâ
nano hızda.
Gerçekten ortak
olmanın, yolları
birleştirmenin
yolunu
bulmalıyız.

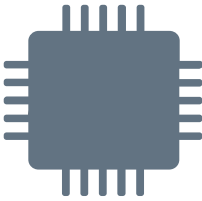
Robotik sistemlerin savaş alanlarında özellikle insan kayıplarında bir devrim oluşturacağını sinyallerini kara, deniz ve hava araçları performansıyla görüyoruz.

Teknolojinin günlük hayattaki olumlu ve olumsuz yönlerinin askere etkisinin doğru yönetilmesi gerekiyor. Savaş alanında, muharebe sahasında performansı etkileyen ortamlar için fiziksel ve besinsel takviyelerin geliştirilmesi, eğitim programlarının buna göre hazırlanması büyük önem arz etmektedir.



Askerin sahadaki hareket kabiliyeti, çeviklik ve verimliliğini artıracak her teknoloji üretiminin kullanımı ve pratik hayata uygunluğu temel şart olmalıdır. Asker için en önemli nokta, reaksiyondaki süratliliktir.

NATO, Multi-Domain operasyonunu çok ciddi ele alıyor. Yakın zamanda insan biraz daha temel kararlar anlamında geri plana itiliyor, otonom ve makinalar tarafından basit kararlar verilebiliyor olacak ama katma değeri daha yüksek, daha sonuç odaklı kararlar yine insan odaklı olacak. Dolayısıyla tam dediğiniz konu da otonom karar alma, süre yapılarını kullanma, insanla insansız sistem entegrasyonu gibi seviyeler de NATO'da da çok ciddi tartışılıyor. İnsan yükünü azaltacak küçük kararlar makinalara bırakılacak. Kara -deniz-hava gibi sistemlerin birlikte çalışması sırasında insanların teknik detaya girmesinin yükünü almak izin bu ortak entegrasyonlarda cihazlar karar verecek gibi gözüküyor.



Yeni teknolojiler daha çevik, daha güçlü insanlarla çalıştırmayı gerektirmektedir. Özellikle yeni ve eski teknolojiler geçmiş ile bugün arasında ciddi bir koordinasyon gerektirecek.

Gelecek veya geleceğin askeri hakkında düşünmek, belki de aşına olduğumuz şeyleri bırakmak, aşına olduğumuz araç ve yöntemleri bir kenara bırakıp yeni düşünce yolları ve önlemler hakkında düşündürmektir.



SATIR ARALARINDAN

**ETİK, ULUSAL
VE
ULUSLARARASI İŞ BİRLİĞİ**



Bir sürü saldırısı riski
durumunda ilk önce saldırmak,
Birleşmiş Milletler'in (BM)
2.4'üncü maddesinin ihlalidir.
BM sözleşmesi buna önleme
demiyor, örneğin potansiyel
olarak bu teknolojinin
uluslararası BM şartını
tamamen tersine çevirme
potansiyeli var.

NATO ve Türkiye, güçlü yapay zekâ endüstrisine ve akademik
araştırma tabanına sahip ve önemli oyuncular.
Bu da NATO müttefiklerinin yapay zekânın erken dönemindeki
avantajından yararlanıp bu süreci sağlamlaştırma fırsatı
olduğu anlamına gelmektedir.

Makinelerin akıllanması çok fazla
etik kaygı uyandırıyor.
Çok fazla can kaybına veya can
kurtarabilmesine hizmet
ederken, hesap verilebilirlik
açısından da endişeler
oluşturuyor.

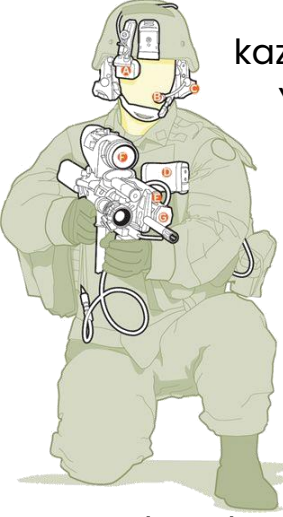


Teknolojiye erişimin demokratikleşmesi ve artan teknolojik
özerklik, ortaya çıkan teknolojilerin kullanımları,
kötüye kullanımları ve kötü niyetli kullanımları hakkında
derin etik kaygılar doğurmaktadır.

İnsan ve makinenin kaynaşması, insan-makine birleşimi, insan
olmanın ne anlama geldiğiyle ilgili dikenli felsefi sorulara da yol
açacaktır.



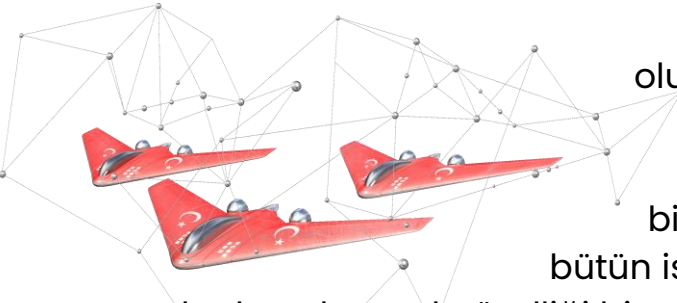
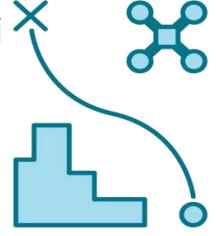
SATIR ARALARINDAN GENEL GÖRÜŞLER VE ÖNERİLER



Geleceğin Savaşları'nı, Geleceğin Savaşçıları ile kazanmak için de gerçekten akıllı olmanız gerekiyor. Yapay zekâ, bulut teknolojileri, otonom makineler, gerçek zamanlı strateji Simülasyonları çok işe yarayacak ama yine de sonucu akıl belirleyecek. Savaşı komuta edenlerin ellerindeki tüm imkanları doğru anlarda ve doğru kullanımı sonuçları belirleyecek.

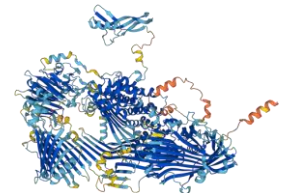
Yeni teknolojiler, tekniği, taktiği ve öldürme zincirini değiştiriyor. 'Düşmanı bul, bastırıcı ateşle onları sıkıştır, düşmanı kuşat, askeri düşmanın yakınına gönder ve tüm düşman savaşçılarını yok et' şeklindeki binlerce yıllık savaş taktikleri muazzam bir şekilde değişiyor.

Günlük hayatta kullandığımız birçok teknoloji bizleri sensör ve veri kaynağı haline getirdi. Hepimiz veri üretiyoruz. Bu veri Rusya'da da kullanılabilir, istihbarat elde etmek amacıyla da kullanılabilir, savaşta da kullanılabilir. Askeri teknolojilerin gelişiminde sivil kullanım artık çok önemli bir parçadır.



Kuş sürülerinde hiçbir kuş oluşturdukları şeklin farkında değil, dev bir bulut gibi. Tek tek birimlerin bir araya getirdiği bütün ise farklı bir şey oluşturuyor ve aslında çok sayıda özelliği bir arada farklı kullanma fırsatı sunuyor. 'Transformers' filmi de sürü fikrinin ana temasıdır. Birkaç şeyi birbirine bağlayarak farklı bir şey oluşturup, birçok özelliği bir arada kullanabilirsiniz. Daha üstün, daha kaliteli ve etkili bir şeye ulaşırsınız.

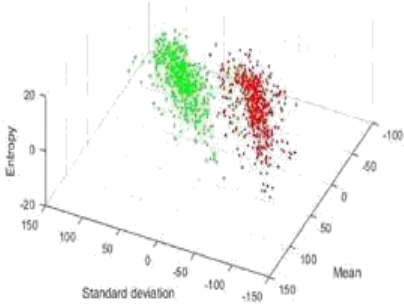
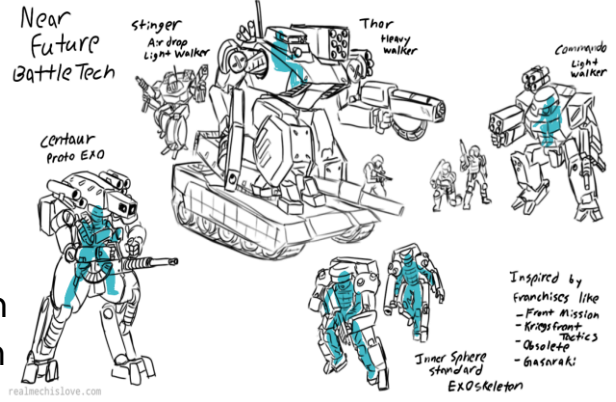
Savaş, çift kullanımlı teknolojilerin yetenekleri için bir «test laboratuvarı» olarak anlaşılır.





istenmeyen şekillerde nasıl kullanılacağını ve kötüye kullanılacağını tahmin etmek zor.

Teknolojideki her türlü gelişmeye rağmen, geleneksel silahlar ile savaşma yolları baskın ve başarının temel belirleyicileri olmaya devam ediyor. Personel ve silahların Kalitesi ve miktarı hayati öneme sahip olmaya devam ediyor, endüstriyel savaş geride değil, gelecekte.



Geleceğin hava gücü ve savaş sistemleri yenilikçi teknolojiler üzerinde inşa edilmeye devam edecektir.

Bu teknolojilerin askeri sistemlerle entegrasyonunda temel bilimlerin öneminin,

matematik, fizik, kimya ve biyoloji alanlarının gelişiminin ve bu alanlarla askeri alanda işbirliği Millî güvenlik meselesi kadar önemlidir. Gelecekte askeriye, gelecekte düşmanınızın hangi gerçeğiyle başa çıkmak zorunda kalacağınızı bilerek

hazırlanmalısınız. Bulacağınız bir teknik çözümle çok dinamik olabilirsiniz, uyum sağlama ve tepki verme konusunda saatlerce tartışabilirsiniz. Çünkü bir önceki teknolojik yenilik, düşmanın yararlandığı bir şeye de sebep olabilir.

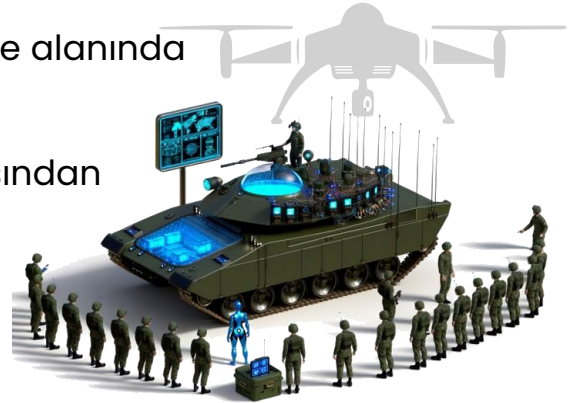




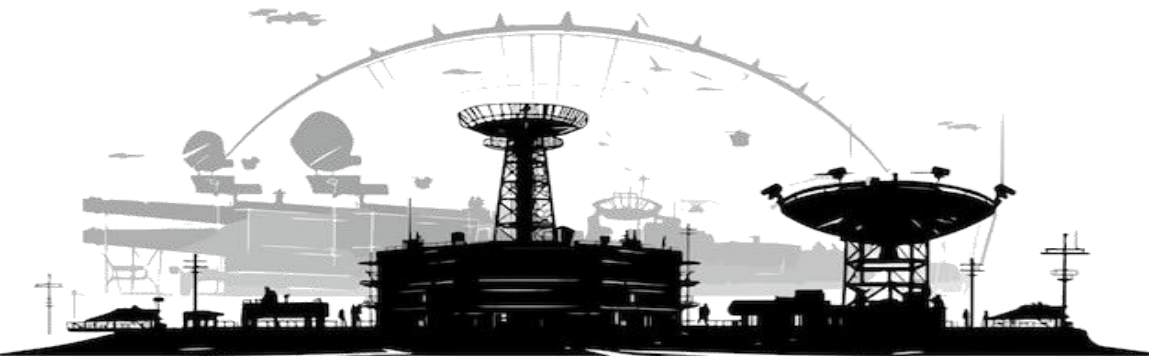
Geleceğin muharebe ortamında yapay karar sistemleri anında ve doğru karar alınmasını sağlayacak, otonom sistemler ise insan faktörünü en aza indirerek riskleri azaltacak ve etkinliği artıracaktır.

Teknolojik ilerlemenin yanı sıra etik sorumluluk ve sürdürülebilirlik te geleceğin askeri yapısının temel taşlarını oluşturacak diğer faktörlerdir. Silah sistemlerinin askeri operasyonların çevresel etkileri göz önünde bulundurularak sürdürülebilir çevre ve çevre dostu çözümler geliştirmelidir.

Ayrıca, yapay zekânın muharebe alanında kullanımıyla ilgili etik ve yasal düzenlemelerin yapılması insan haklarının korunması açısından kritik öneme haizdir. Bu kapsamdaki adımlar, proaktif bir tutum ve anlayış çerçevesinde atılmalıdır. Küresel tehditler ve güvenlik problemleri, tek bir ülkenin üstesinden gelebileceği sorunlar değildir. Bu nedenle ülkeler arası işbirliği, bilgi ve teknoloji paylaşımı, ortak eğitim ve tatbikatlar ile müşterek çalışabilirliği sağlamak, güç birliği yapmak ortak güvenlik ve barışın teminatı olacaktır.



Gelişen teknoloji ile muharebe sahasında tehditlerin çeşitliliği ve etkisi her geçen gün çoğalmaktadır. Bu nedenle, askerlerin icra ettiği görevler artmakta, etki alanı genişlemektedir.



Saldırmanın taktiksel avantajı stratejik bir seviyeye geçerse, sistem saldırının savunmaya göre daha avantajlı olduğu anlamına gelecektir. Hücum ve savunma dengesinde sürü teknolojileri savaş doktrinlerini ve sonuçları değiştiren bir faktör olacak. Bir sürüyü etkileyecek ve vuruş yapacak bir sisteminiz yoksa ne yapacaksınız?

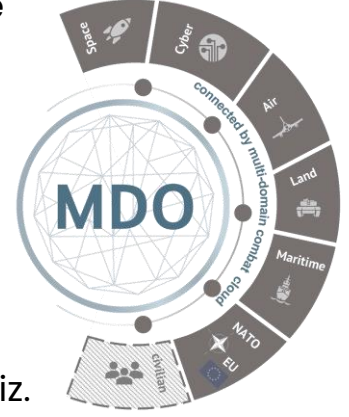


Geleceğin Askerleri, ileri teknolojiye uyum sağlayabilecek bilgi ve beceriye sahip olmalı, aynı zamanda etik ve liderlik vasıflarını da geliştirmelidir. Bu doğrultuda eğitim sistemimizin yenilenmesi, askeri personelimizin sürekli kendini geliştirmesi hayati önem taşımaktadır. Çünkü askerin silah ve teçhizatı ne kadar gelişirse gelişsin, geleceğin hareketi ortamında karar verici yine insan olacaktır. Bu gerçek göz önünde bulundurularak geleceğin askerlerinin teknoloji ve siber güvenlik, hibrit hareket, insansız hava kara deniz araçları ve otonom sistemler, simülasyon ve sanal gerçeklik, zeka ve analitik beceriler, psikolojik dayanıklılık, hızlı ve doğru karar verebilme, yeterlilik ve insan yönetimi konularında çok iyi yetiştirilmesi kaçınılmaz bir ihtiyaçtır.

Sürü halinde hareket kavramının temelinde, sürünün genel liderinin davranışlarını takip ettiği gerçeğiyle başlamak gerekir.

Çok sayıda farklı savaş aracı ve teknolojisine sahip olduğunuz savaş ortamında, en farklı neyi başarabileceğiniz başarıyı getirecek. Bu araçlara erişiminiz olmasıyla çok şey yapabilirsiniz ama bu onları en verimli, zamanında veya orijinal olarak kullanacağını bildiğiniz anlamına gelmez. Yani yapılanmanız için her şeyi kontrol ederek en iyiyi yapabilecek hale getirmelisiniz.

İster Pentagon olun, ister uyuşturucu karteli olun en önemlisi bu olacak. Üreticilik, orijinallik, iyi insan kaynağına sahip olmak ve en iyiyi yapabilmek mücadelesi, yeni savaş teknolojilerinde de en önemli mücadele olacak.



Geleceğin askerlerinin teknolojinin sunduğu olanaklarla donatılacağı, muharebelerde kesin sonucun geçmişte ve günümüzde olduğu gibi gelecekte de eğitilmiş insan faktörü ile elde edileceği muhakkaktır.

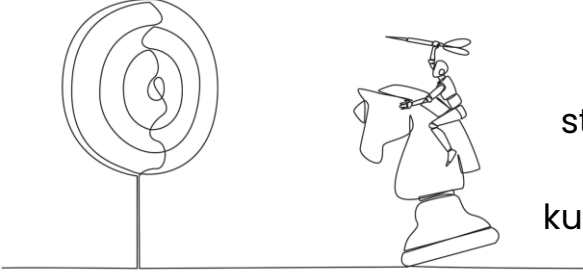
Teknoloji ancak taktik ve doktrine başarılı entegrasyonu kadar faydalıdır. Teknolojik bir avantaj, yalnızca düşman adapte olmadığı sürece sürer.



Geleceğin savaşları eski ile yeni savaş zamanlarının zorluklarıyla denenmiş ve denenmemiş zorlukların bir karışımı olacak.

Sonunda sahip olduğunuz beklentileri karşılayan çözümler geliştirmek son derece önemlidir. Asimetrik muharebelerde asimetrik mukabele paketleri geliştirmek zorundayız.

Genetik değişiklikler ve biyoteknolojiler, insan vücuduna dair geliştirme programları askeri daha fazla korumak, kollamak, daha aktif kılma merkezli programlar ve buna da hazırlanılmalıdır. Bu teknolojiler özellikle yakın cephe ve kentsel savaş ortamlarında askeri daha hazır kılmaya çalışmaktadır.



Yapay zekâ bir kutudur.
Yöntemlerle doludur ve
stratejik hedefinize ulaşmak için
hangi yöntemi en iyi şekilde
kullanacağınızı anlamamız gerekir.

Amerika, Tayvan ile
Çin arasındaki
olası bir
çatışmada,
otonom sürü
yeteneğine yönelik
çalışmalar yapıyor.
Yani büyük oyuncu
bunun üzerinde
çalışıyor.
Bizim de büyük
ihtimalle buna
hazır olmamız
gerekecek, gelecek
savaş alanında bu
sorunla
karşılaşmamız çok
olası.



Gen ve bilişsel
iyileştirmeler çok
önem kazanıyor.
Genlerle veya
takviye
teknolojilerle
insanların fiziksel
ve bilişsel
yeteneklerini
geliştirmek ve
durumsal
farkındalığını
artırmak
yönünde
çalışmalar var.
Operasyonel
yetenekleri
yükseltmek için
biyoteknoloji de
popüler.

Her teknolojik
gelişme, geçirdiği
olgunlaşma
döneminin
ardından günlük
hayatın bir
parçası haline
geliyor ve hayata
nüfuz edici bir
şekilde insanla
bütünleşiyor. Bu
inovasyon değil,
penetrasyon
olarak
adlandırılabilir.
Çünkü, insanı da
yeniden
şekillendiriyor



Yapay zekâ destekli tanımlama yapan teknolojiler, operasyonel verimliliği artırırken, istihbarat toplama ve teknik dağıtım arasındaki süreyi kısaltırken savaş ve kişisel güvenlik arasındaki çizgileri belirsizleştiriyor.

Yapay zekâ veya otonom sistemler gibi ulusal askeri teknolojilerin geliştirilmesinde ortak ve güvenilir bir çalışma ağı zorunluluktur. Örneğin 'askerler verilerin korunası' taraftarı ama mühendisler ise gelişim süreçleri için verilere ihtiyaç duyuyor. Güvenlik mi, çalışma kolaylığı mı? Katmanlı, şifrelemeli güvenlik sistemleriyle ortak bir çalışma havuzu şart!



AI ARMY



Deepmind, derin robot bilimi yeni teknolojiler üzerine çalışıyor. Yani robot ve insansız sistemlerin giderek artan etkisini ve bunu sürüler halinde yaptıklarını göreceğiz.

Çoğu AB ve NATO ülkesinde ortak operasyonel tabloyu yapay zekâda gizlilik dolayısıyla oluşturamayacağımızı unutuyorlar. Veriler farklı hizmetleri birimler arasında, ülkeler arasında paylaşamazsınız.



Sürü fikri, düşman sisteminizi doyurmaktır. Örneğin İsrail'in Hava Savunma Sistemi gerçekten iyi ama o sistemi doyurursanız o zaman bazıları hava sisteminin etkisinden çıkacak ve sürü başarıya ulaşacak.

I. GÜN BİRİNCİ OTURUM – YENİ DÜNYA

TEMA:
Küresel Dengesizlikler ve Yeni Düzen Arayışı

OTURUM KONUSU:
Rusya-Ukrayna Savaşı ve Savaşın Teknolojik Boyutu

OTURUM TEMALARI:
Günümüz Çatışmalarında Yıkıcı Teknolojilerin Boyutu
Küresel Arenada Geleceğin Askeri ve Askeri Teknoloji
Programlarına Genel Bakış
Otonom Teknolojiler
Bütünsel Omurga ve Entegre Operasyon Kavramı

I. OTURUM ÖZETİ

Yapay zekâ hızlı bir gelişim sergilemektedir ve henüz internetin hayatımıza ilk girdiği dönemlerdeki gibi henüz yolun başındadır. Tüm dünya ülkeleri, yapay zekânın askeri sistemlerde kullanımına yönelik çalışmalar yapmaktadır. Bilişsel seviyelerle insana ilişkin görevleri yerine getirebilen ölümcül otonom sistemler konusunda dünyada çok sayıda ülke rekabet halindedir. Küresel anlamda, küçük devletlerin yapay zekânın kullanıldığı sistemler ve karşı önlemler karşısında geride kalma riski bulunmaktadır. Bu da dünyadaki küresel dengelerin değişiminde önemli rol oynayabilir. Özellikle elektronik harp ve kontrol sistemleri konusunda yapay zekânın sistemlerin ele geçirilmesi noktasındaki etkilerinde güç savaşı ve teknoloji savaşı yaşanacaktır. Özellikle Büyük Dil Modelleri'nin (LLM) gelişmesi sonrasında ve makinelerin birbiriyle konuştukları dönemlerde otonom sistemlerin vereceği kararlar endişe uyandırmakta, ancak özellikle çatışmalarda belirleyici olacaktır. NATO ve Avrupa Birliği gibi yapıların özellikle Çin, Rusya ve ABD'nin bu alandaki hedefleri doğrultusunda gelişmeleri yakından takip edip teknoloji gelişiminde işbirliği yapması önerilebilir.

Yakın temastaki askerin kıyafet ve ekipmanlarının özellikle insansız sistemlerde kullanılabilecek kimyasal, biyolojik, radyolojik ve nükleer tehditler (KBRN) karşısında geliştirilmesi önem arz etmektedir. Ayrıca, otonom ve robotik sistemlerle yapılabilecek bu tarz saldırılar yeni oluşan risk faktörleri arasındadır. Günümüz çatışmalarında kullanılan teknolojiler, geleceğin harp ortamlarına dair fikirler vermekte, çatışmaların uydular ve yapay zekâ destekli komuta ve kontrol sistemleri alanına taşınacağı öngörülmektedir.

Gelişen teknolojilere karşı tedbir hızı da günümüz çatışmalarının getirdiği önemli mesajlar arasında görülmektedir. Eski ile yeni teknolojiler arasındaki adaptasyon döneminde savaş doktrinleri açısından da önemli gelişmeler yaşanmaktadır. Özellikle sürü sistemlerin gelişmesiyle savaş taktiklerinin boyut değiştirmesi kaçınılmazdır.

Yapay zekâ artan bir şekilde kuvvet çarpanı olarak savaş ortamında etkisini göstermektedir.

Ukrayna ve Gazze konvansiyonel savaş, siber savaş, akıllı robotik sistemler ve insansız sistemlerin deney alanı olarak görülmektedir.

Kısa vadede büyük robotların da savaş ortamlarında yer alması hızlanacaktır. Orta ve uzun vadede, otonom ve robotik çatışmaları besleyen bilişsel savaş, yani sosyal medya, artırılmış gerçeklik, sanal gerçeklik metotlarıyla, düşünce okumaya yönelik çalışmalarla savaşların dönüşüm geçirmesi ön görülmektedir



Dr. Erol YÜCEL
HAVELSAN
MODERATÖR

Değerli misafirlerimiz, Future Soldier Geleceğin Askeri organizasyonumuza hoş geldiniz. İlk panelimizin oturum teması 'Küresel Dengesizlikler ve Yeni Düzen Arayışı'. Bu panelde çok değerli uzmanlarımız 'Günümüz Çatışmalarında Yıkıcı Teknolojilerin Boyutu, Küresel Alanda Geleceğin Askerleri ve Askeri Teknolojiler Programlarına Bakış, Otonom Teknolojiler ile Bütünsel Omurga, Entegre Operasyon Konsepti' konularını bizimle paylaşacaklar. Ve Rusya-Ukrayna Savaşı'nın teknolojik boyutundaki tespitlerini paylaşacaklar.

Beni davet ettiğiniz için teşekkür ederim. Türkiye Millî Savunma Bakanlığı'na ve SASAD'a teşekkür ederim. Bu benim ilk Türkiye ziyaretim oldu ve bana soyadımın aslında bir Türk soyadı olduğu söylendi. Ve küçük bir itirafta bulunmam gerekiyor. Birkaç yıl öncesine kadar bunu bilmiyordum. Soyadımın garip görülmediği bir ülke olduğu için çok mutlu oldum. Beni kabul ettiğiniz için teşekkürler, kendimi buraya ait hissediyorum.



Dr. Mattias EKEN
RAND
İNGİLTERE

Bir nevi önce yapay zekânın stratejik çıkarımları, riskler ve fırsatlar ve sanırım nereye gidebileceğimize dair genel bir bakış sunmak istiyorum. Yapay zekâ hızlı bir tempoda ilerliyor, toplum, ekonomi ve tüm hükümet genelinde kapsamlı sonuçlar doğuruyor. Türkiye ve diğer NATO ülkeleri güçlü bir yapay zekâ endüstrisine ve akademik araştırma tabanına sahip ve önemli oyuncular. Bununla birlikte, diğer ülkelerde bu alana yoğun yatırım yapıyor ve onları geçme tehdidinde bulunuyor. Bu da NATO müttefiklerinin yapay zekânın erken dönemindeki avantajından yararlanıp sağlamlaştırma fırsatına sahip olduğu anlamına geliyor. Yapay zekâ büyük potansiyel faydalara sahipken, güvenlik önyargısı etrafında artan endişeler var ve aksaklıktan kaynaklanabilecek sonuçları tartışılıyor

Yapay zekânın dünya çapındaki ordular tarafından giderek daha fazla uyarlanması riskleri ve fırsatları hakkında çok fazla abartılı anlaşmazlık ve belirsizlik var. Ben yapay zekâ üzerindeki bu tartışmaların stratejik düzeyde etkilerinin ikinci ve üçüncü dereceden olduğunu düşünüyorum.

Yapay zekâ bir boşlukta var olamaz ve boşlukta değildir. Bence riskten çok fırsatlar var. En iyisi yapay zekânın, önemli bir insan bileşenine sahip karmaşık, uyarlanabilir bir kurum teknik sistemi olarak anlaşılmasıdır. Çeşitli engeller nedeniyle teknolojinin kendisine çok fazla kapılmamak önemlidir. Çeşitli engeller nedeniyle teknolojinin kendisine çok fazla kapılmamak önemlidir. Çünkü çeşitli engeller ve kolaylaştırıcılar, yeni yapay zekâ teknolojilerinin savunma organizasyonlarına ne kadar hızlı ve ne şekilde dahil edileceğini şekillendirecek.

Her türlü teknolojinin savunma konusunda önemli olduğunu ve kullanım yaygınlığını biliyoruz. Yapay zekâ, çift kullanımlı genel amaçlı teknolojiler ailesinin bir üyesidir, motor, elektrik ve internet gibi. Yapay zekâ teknolojileri yazılım tabanlıdır ancak geleneksel askeri teknolojilerden farklı olarak onları oldukça yüksek kılar ve donanım desteklidir, donanım etkindir. Hızla yaygınlaşan Yapay zekâ, bir teknolojiden çok daha fazlası için oradadır; örneğin sohbet amaçlı Chat GPT gibi büyük bir dil modeli gibi. Ayrıca yenilik; hükümet veya savunma tarafından değil, ticari kullanımlar için özel sektör tarafından yönlendirilir. Askeri alanda yapay zekânın uygulamalarının ve sonuçlarının kolektif olarak anlaşılması gerekir. Yapay zekânın uygulama alanları ve etkileri geliyor ama oldukça düşük bir temelden yola çıkarak tartışmanın çoğu yüksek profilli konular etrafında toplanıyor, buna öncelik veriliyor. Görevleri insana ilişkin bilişsel seviyelerle yerine getirebilen Tam Yapay Zekâ veya Yapay Genel Zekâ (AGI) gibi, ölümcül otonom silahlar ölümcül özerklik gibi. Diğer konuların aksine tartışma, taktik, stratejik risk veya fırsatlar yerine uzun vadede etkili olabilecek ikinci veya üçüncü dereceden yapay zekânın sonuçlarına ve etkileri yerine acil sonuçlara odaklanıyor. Genel amaçlı teknolojinin birçok sektörde, savunmada dahil üretkenliği önemli ölçüde etkileme potansiyeli vardır.

Ayrıca sosyal yapıları ve bireysel yaşam tarzlarını da önemli ölçüde dönüştürüyor. Yapay zekâ, makinelerin normalde insan veya biyolojik zekâ gerektiren görevleri, özellikle de makine verilerden öğrendiğinde ve bu görevlerin bağımsız olarak nasıl yapılacağını öğrendiğinde bağımsız olarak gerçekleştirmesine olanak tanıyor. Bu anlamda Yapay zekânın savunmanın tüm alanlarında sayısız potansiyel etkisi vardır; örneğin istihbarat analizi, karar destek araçları, savaş oyunları, simülasyon, elektronik harp, lojistiğinin optimizasyonu ve benzeri.

Sonuç olarak yapay zekâ, strateji oluşturma, düzenleme ve tamamlama orkestrasyonunu dönüştürecek, savunma teşebbüsünün üretkenliğini dönüştürecek. Savunmanın hatları dediğimiz tüm kavramları, tüm gücün verimliliği ve uygulanmasını da etkileyecek. Askeri kabiliyetleri, hazırlığı ve Operasyonel Sapma Şekillerini (ODS) etkileyecek.

Yapay Zekâ Geliştirme (AI-D) etkisi hakkında biraz daha ayrıntıya gireceğim. Özellikle vurgulamak istediğim sonuç, yapay zekânın ve avantajın en iyi uyum sağlayanlara gideceğidir. Ayrıca, askeri yapay zekânın ve genel olarak yapay zekânın yaygınlaştırılması farklı uluslararası aktörleri de farklı etkileyecektir. Stratejik düzeyde Askeri yapay zekâ üzerindeki rekabet, yeni mekanizmalar getirilmezse ABD ve Çin arasındaki süper rekabeti istikrarsızlaştırabilir ve diğer ulusları tehdit edebilir. İngiltere gibi orta güçler, asimetric güç ve etki alanlarını nasıl şekillendirecekleri konusunda üssün kaynaklara nasıl odaklanılacağı konusunda zor seçimlerle karşı karşıyadır.

Askeri yapay zekânın küresel yönetimi küçük devletleri daha büyük oyuncular tarafından geride bırakılma riski taşıyor ama bazıları askeri yapay zekâyı olduğu gibi benimsemeye daha çevik olduklarını kanıtlarsa, stratejik düzeyde olağanüstü bir etkiye sahip olabilirler. Singapur, Finlandiya ve Hollanda gibi bazı ülkelerin dış gücüne de bu yansımıştır. Yapay zekâyı etik bir şekilde kullananlar ile bunu daha az kısıtlamayla yapanlar arasında önemli bir ayrım ve çizgi var. Demokrasilerin yapay zekâ yeteneklerini çekme ve inovasyonu besleme konusunda avantajlı olduğunu düşünüyorum. Ancak yapay zekâ Çin ve Rusya gibi ülkelere otoriterliği sağlamlaştırmak ve ihraç etmek için yeni araçlar sunuyor.

Ve zaten gördüğümüz düşman kuvvetlerin yapay zekâ ve akıllı sistemler gibi yetenekleri ihraç etmeye çalıştıkları. Akıllı Sistemlerin askeriyede kullanımıyla birlikte dünyanın dört bir yanındaki ülkelere nüfuzun kesinleştirilmesi için dağıldığını görüyoruz. Bu sistemlerin askeriyedeki gelişimiyle de özel sektör gibi farklı türden devlet dışı aktörlerle ilgili yeni riskler ve fırsatlar da ortaya çıkıyor, ancak aynı zamanda durum karmaşılaşıyor. Yapay zekânın egemenliği, eylem özgürlüğü ve yapay zekâ yönetişiminin meşruiyetini sağlamaya yönelik.

Yapay zekânın meşruiyeti, aşırılıkçı örgütlerin ya da vekil aktörlerin yapay zekâ araçlarını kullanmasına izin verebilir, örneğin militan temin etmek gibi alanlarda veya Birleşik Ortak Kimyasal, Biyolojik, Radyolojik ve Nükleer (KBRN) ve terörist eylemler de dahil olmak üzere daha karmaşık hale gelen saldırıların finans planlaması ve yürütülmesi gibi. Daha önce de gördüğümüz gibi halihazırda saldırganlar, Kızıldeniz'de de görüldüğü gibi vekil aktörler halihazırda akıllı robotik sistemleri kapsamlı bir şekilde kullanıyorlar.

Yapay zekâ ile bu eğilimi daha da şiddetlendirecek şekilde ciddi ve organize suç grupları da benzer şekilde giderek daha fazla güç elde edebilir. Yapay zekâ uluslararası güvenliğe, devlet dışı aktörlere yönelik yeni tehditler oluşturabilir, daha karmaşık yapay zekâ yetenekleri elde edebilir. Yapay zekâ kullanan bir hükümet dışı kuruluş (NGO), Türkiye veya diğer NATO müttefikleri için doğrudan bir askeri tehdit oluşturmaya da yine de harekete geçebilirler, dikkatli bir şekilde ele alınmazlarsa istenmeyen sonuçlara yol açabilirler. Yapay zekâ sadece savunmanın sağlaması gereken askeri görev güçleri ve askeri yetenekleri üzerinde değil, aynı zamanda bazı durumlarda derin etkilere sahip olabilir. Bazı durumlarda genel olarak göz ardı edilen ofis işlevleri de var. Savunma Bakanlıklarının ve kuvvetlerin üretkenlik, verimlilik ve esnekliğini, harcamaların karşılığını değiştirebilir. Ya da bunların daha çevik ve yenilikçi rakipler tarafından geride bırakıldığını da hızla görebilir. Askeri ve stratejik rekabet üzerindeki etkileri etkileyebilir. Askeri yeteneklerin nasıl kullanılacağını da etkilemek için kullanılır. Ve bütünü oluşturan tüm parçalarda bu etkilerin nasıl görülebileceğini de etkileyebilir. Yapay zekâ üretimden eğitime her alanda etkili olacak. Doğrusal gelişimden sarma gelişime bir geçiş göreceğiz ve platformlar sunarken yazılım merkezli modellere odaklanacağız.

Platformlarımız, insan makine ekiplerinin ve alt yapı gücünden yararlanmaya yönelik olacak. Avantaj nasıl avantaja dönecek, NATO'nun avantaj elde etme konusundaki düşüncelerinin de merkezinde bu fikirler manevra yaklaşımı üzerine inşa edilmiştir. NATO içindeki görev komutanlığı, düşmanın eylem tekrarının gözlemi ve eylem döngüsünün analiziyle onlardan daha iyi düşünmek için bir hareket eylemine karar veriyor, bir eylem döngüsüyle onları alt etmek için ve sonra düşmanları çoklu ikilemlere sokmak için, NATO çıkarlarını destekleyecek şekilde davranışlarını şekillendirmek için çalışıyor.

Rusların ve Çinlilerin doktrinleri de kendi kültürleri ve tarihsel deneyimlerinin merceğinden çerçevelenirse onların da benzer kavramları vurguladığını da belirtmek önemlidir. Rusya Silahlı Kuvvetleri de yapay zekânın kullanımı ve kontrol refleksi gibi kavramların işlevsel hale getirilmesini ve operasyonelleştirilmesini vurguluyor. Düşmanın algılarını etkilemek, bilgi alanına erişim ve düşünmenin yanı sıra düzensizlik, yapay zekâ temeli sistemlerin bozulmaya çalışılması, özellikle de savaşın başlangıç döneminde düşman komuta ve kontrol yapılarını felç etmek isteniyor. Özellikle Çin, sistem yıkımı, sistemlerin imhası olarak adlandırdığı savaşa hazırlık olarak hızla modernleşiyor. Yapay zekâ ile avantaj, düşmanın kuvvetlerini ayrıntılı olarak yok etmekten değil, onların kilit noktalarını ve bağlantılarını hedef almaktan, komutasındaki gücü hedef almaktan ve zayıflatmaktan ya da yok etmekten gelir. Yapay zekâda kafa karışıklığı komuta ve kontrol sistemlerini şaşırtmak, felç etmek ve nihayetinde düşmanı alt etmek için kullanılır. Ve 'Bilgilendirilmiş veya Akıllı Boyutta Savaş', literatürde yer alan terimlerden biri olabilir. Bu rekabetin anlamı, karşıt yapay zekâ destekli sistemler arasında bir avantaj rekabetidir.

Askeri haberleşme, çağrılar, komuta kontrolü, iletişim bilgisayarları, istihbarat, gözetim, keşif, hedef tespiti gibi yaygın adıyla komuta, kontrol, iletişim, bilgisayar, istihbarat sistemleri (C4I) alanındaki yetenekler hem avantaj hem de hedef haline gelir. Örneğin her bir tarafın rakibin yapay zekâ Algoritması için eğitim verilerinin zehirlenmesi veya yapay zekâ sistemlerinin sınırlamalarından yararlanmak için, yapay zekâ desteği gibi savunma amaçlı bir yardım olarak da kullanılabilir.

Örneğin yapay zekâ, otomatik siber savunmaları desteklemenin yanı sıra, kinetik veya kinetik olmayan etkilerin karıştırılması gibi bir yöntemle saldırıyı destekleyen bir araç veya savunma yardımcısı olarak da kullanılabilir.

Elektronik harpte gizli düşman iletişim ve bilgisayar sistemlerinin çözümlenmelerinin yapılması ve hedeflenmesi gibi amaçla da kullanılabilir. Mobil merkezler uzun menzilli atışlarla saldırıya uğrayabilir ve burada hedeflerin tespitinde yapay zekânın entegrasyonu ile hızına ihtiyaç duyulabilir. Düşmanın yapay zekâ sistemini kötüye kullanabileceği veya bozabileceği olası tehdit vektörlerini dikkate almak için yapay zekânın stratejik karar alma süreçlerine dahil edilmesi aynı zamanda teknik ve prosedürel fazlalıklara ve geriye dönük revizyonlara sahip olmak anlamına da gelir.

Yapay zekâ sistemleri çökerse, düşmanın yapay zekâ sistemini kötüye kullanması veya bozması, uğranmasa durumunda Yapay Zekâya bağımlı olmayan sistemlere geri dönebilme sürekliliği de bir avantaj olacaktır. Dünya genelindeki orduların dayanıklılık ve acil durum hazırlığı açısından bu da bir örnektir. Örneğin, insani krizler, afet müdahale operasyonları gibi insani yardım ve afet müdahale operasyonları yürütmeye yönelik artan taleplerle karşı karşıyayız. Yapay Zekâ, iklim değişikliği, doğal afetler gibi konularda erken uyarı sistemlerini iyileştirerek, kriz müdahalesini ve kaynak tahsisini planlama, kritik varlıkların en çok ihtiyaç duyulduğu anla konuşlandırılması ve kullanılmasını sağlayarak da bizlere yardımcı olabilir. Sivil kuruluşların savunma üzerindeki baskıyı azaltması için de bir yöntem olarak kullanılabilir. NATO operasyonlarına katkıda bulunmak gibi diğer askeri görevler için yapay zekâ kullanılır ama yeni şeyler de üretir.

Ve beraberinde bağımlılıklar ya da dayanıklılık riskleri de oluşturabilir. Örneğin siber saldırılar yapay zekâ sistemlerini zayıflatabilir. Yapay zekâ sistemleri etkinlik, algoritmik, hatalar, etkileri ile önyargılar, halkta güven eksikliğine yol açabilir. Askeri yapay zekâ, düşman devletler veya devlet dışı aktörler tarafından kritik ulusal alt yapıya saldırılar düzenlemek için silah olarak kullanılabilir. Tedarik zincirleri veya sivillere saldırılar düzenlemek için silah haline getirilebilir.

Yapay zekânın askeri kullanımı geleneksel nükleer ve konvansiyonel caydırıcılıkla ilgili konularda potansiyel faydalar sunar, gelişmiş analizler sağlar.

Ancak aynı zamanda nükleer komuta ve kontrol sistemlerinin yapay zekâ tarafından kazara hedeflenmesi gibi riskler ve yeni belirsizleri de beraberinde getirir. Bunların kazara hedef alınması gerilimi tırmandırabilir.

Geleneksel savaşta askeri yapay zekâ destekli askeri yetenekler, hız, konum ve öldürücülüğü artırabilir. Bunun yanı sıra insan personelini tehlikeye maruz bırakmaya gerek duymadan yardım odaklı veri analizi de yapabilir. Askeri komutanların savaş alanı hakkında daha doğru, kapsamlı bir anlayış geliştirmelerine yardımcı olabilir ve onların daha bilgili olmalarını sağlayabilir. Güçlerini nasıl konuşlandıracakları konusunda bilinçli karar almalarını sağlayabilirler, yapay zekâ ile uzun menzilli pozisyonları hedeflemeyi başarabilirler. Düşman hatlarını ve füze savunmalarını bastırmaya yardımcı olmak için otonom sistemlerin kullanımıyla desteklenen uzun menzilli pozisyon ateşlerinin hedeflenmesini geliştirebilir.

Savaş hasarının değerlendirilmesi, istihbarat topluluğu ve bilgi savaşı, siber savaş, lojistik destek ve ikmalin yanı sıra farklı alanlarda bu teknolojinin değerini kanıtladığını gördük. Özellikle Ukrayna ve Rusya savaşında uzaktan yönetilen otonom sistemler çok sayıda konuşlandırıldılar ve kullanıldılar giderek artan yapay zekâ ve özerklik özellikleriyle birlikte. Ukrayna, otonom robotik ve yapay zekâ sistemleri üzerine yeni bir askeri şube ve birlik bile kurdu. Ancak mevcut durum göz önüne alındığında, bu tür taktiksel etkilerin, stratejik sonuçları nasıl etkileyeceği yönünde açık bir şekilde belirsizliğini koruduğunu düşünüyorum.

Yapay zekâ, barışın inşası, gerginliği azaltma, çatışmaların sona erdirilmesi ve sonrasında güvenlik koşullarının oluşturulması, güvenlik istikrarı, refah ve güvenlik koşullarının sağlanması konusunda da yardımcı olabilir. Örneğin çevrimiçi nefret söylemi, propaganda veya çatışmalar etkilenen bir bölgede herhangi bir barış görüşmesini veya kırılğan ateşkesin altını oyabilecek kamuoyu duyarlılığındaki değişiklikleri gerçek zamanlı olarak izlemeye ve tamamlamaya yardımcı olabilir.

Yapay zekâ benzer şekilde otonom sistemlerle birlikte barışı koruma, barış uygulama operasyonunun yanı sıra, mayın temizleme, silahlı grupların silahsızlandırılması, yıkılan ve tahrip edilen alt yapı ve hizmetlerin yeniden hazırlanması ve uygulanmasında da kullanılabilir.

Yapay Zekâ ile ilgili en acil tehditler nelerdir?

Birkaç belirli konu derin sahtecilik (deepfake), bilgi ve manipülasyonu, siyasi, ekonomik ve sosyal bozulma ile çarpık askeri karar alma sürecini çarpıtan yapay zekâ manipülasyonlarını içeriyor yaptığımız araştırmalar. İkinci olarak NATO ordularına meydan okumak için asimetrik yeteneklere sahip devlet dışı aktörlerin güçlendirilmesi. Biyolojik ve kimyasal silahlar ile ilgili de çalışmalar var ama büyük dil modellerinin mevcut nesli, bu alandaki boşluğu kapatma yeteneğine sahip görünmüyor. Yine de bu bir rehabet anlamına gelmemeli. Gelecekte Büyük Dil Modelleri'nin (LLM) ne yapacağını bilmiyoruz, bilemiyoruz. Gelecekte anlama ve üretme yeteneğinin hangi alanı kapsayacağını düşünerek hareket etmeliyiz.

Üçüncüsü yapay zekânın interlink etkileri. Konvansiyonel savaşta hücum savunma dengesi, gerilme dinamikleri, nükleer caydırıcılığın istikrarsızlığı üzerine mücadele, özellikle halihazırda güvensizliğin diğer etkenleriyle boğuşan çok kutuplu bir dünyada süper güç rekabetlerinin yoğunlaşması konseptinde uzun vadede güvensizliğin diğer itici güçleriyle boğuşmak ve tartışmayı çarpıtmak ve yapay zekânın gelecekteki potansiyel ortaya çıkışıyla ilişkili tartışmaya odaklanmak istememek.

Elbette yapay zekâ ile ilgili güvenlik riskleri de olduğunu düşünüyorum. Türk savunması riskleri azaltmak ve stratejik çıkarları en üs düzeye çıkarmak için politika müdahalelerine öncelik vermek için yapay zekâyı kullanabilir. Yapay zekâ ile ilişkili stratejik fırsatları en üst düzeye çıkarmak için müdahaleleri önceliklendirmek için kullanılabilecek çeşitli yöntemler var: Genel anlamda yapay zekâ ile ilişkili fırsatlar geniş anlamda risk tabanlı yöntemlerle gruplandırılabilir. Belirli yapay zekâ ile ilgili trendlerin hem olasılığı hem de etkisine yönelik projeksiyonlarda yüksek düzeyde güven var mı? Belirli senaryolara karşı en iyi duruma odaklanmaktır birinci yöntem. İkincisi ise belirsizliğe dayalı yöntem.

Olasılık ve etki tahminlerine olan güven, mümkün olan en geniş senaryo yelpazesinde pişmanlığı en aza indirmeye odaklanmaya yol açar. Sağlam karar vermedir. Daha ayrıntılı risk analizi yapma amacı ile en fazla ilk vaatleri taşıyabilir. Yapay zekânın teknik düzeyde neler yapabileceğinin ve gerçek dünyada nasıl kullanıldığının anlaşılmasıyla birlikte daha ayrıntılı risk modellemesine girme isteği çeşitli diğer analitik faaliyetlerle beslenebilir.

Müttefiklerin yapay zekâyâ uyumu da büyük fırsatlar oluşturacaktır ve askeri yapay zekâ için yerel bir ekosistem inşa etmek, küresel ruh yönetişim düzenlemelerini şekillendiren bir ekosistem oluşturmak için düzenlemeler yapmak avantaj fırsatlarını en üst düzeye çıkaracaktır. Gerilim risklerini azaltmak için rakiplerle çalışma da buna dahildir. İleriye dönük ana çaba, yapay zekânın benimsenmesini artırma çabalarından oluşan bir araç setini içermelidir. . Aynı zamanda devlet dışı ve terörist aktörler veya düşman haydut devletler tarafından benimsenmesini sınırlamak ve aynı zamanda yapay zekâyı empoze etmek için savunma çabalarına faydalarını en üst düzeyde çıkarmak için çabalar içermelidir. Bu mücadele aynı zamanda maliyetler de yüklemektedir.

Yapay zekânın gelişim sürecinde NATO'nun müttefikleri arasında entegre ve bütünlük bir yaklaşım gerekiyor. Bu alanda ortak bir endüstri ve akademi, sivil toplumu oluşturulması için uzay, nükleer, biyolojik ve kimyasal silahlar gibi. Ancak yapay zekâ genel amaçlı teknolojilere oranla özel bir yaklaşım gerektiren ayırt edici özelliklere de sahip. Askeri yapay zekânın davranışlarını göreceli güç konumundan şekillendirmesine yardımcı olmak için bir kombinasyon gerekiyor. Askeri yapay zekâ açısından güç ve sınırlamalarının net değerlendirmelerle daha net anlaşılmasını sağlamak amacıyla, farklı düşmanların algıları, hedefleri ve sınırlamaları hakkında daha net bir anlayış, rakiplere maliyeti sınırlamak veya artmasını engellemek için önlemler, fikri mülkiyet, veri hesaplama, alt yapı, caydırma, zorlama, ikna ve şekillendirmeye yönelik birtakım önlemler kapsamında küresel yapay zekânın haritalanmasını geliştirmek için başlatılan yeni girişimler gibi önlemler. 50'den fazla aktif düzenleme var, bazıları keşifsel diyaloga, bazıları da gönüllü ilkelere ve kapsam belirlemeye odaklanıyor. Diğerleri yeni düzenlemeler veya politika yönergeleri için daha iddialı teklifler geliştirmeye çalışıyor.

BM Genel Sekreteri'nin AI Yüksek Düzeyli Danışma Kurulu, AB AI Yasası gibi. Bundan dolayı Türkiye ve NATO müttefikleri yapay zekâ yönetim mimarisinin şekillendirilmesi için proaktif bir strateji geliştirmelidir. Nükleer caydırıcılıkta olduğu gibi sağlam bir yapının nihai konsolidasyonlarına doğru güven ve ivme oluşturulması gerekmektedir.

Beni dinlediğiniz için teşekkür ederim.

SUNUMUNDAN NOTLAR:

- Yapay zekânın yaygın kullanımıyla, askeri yapay zekâ savunmanın Strateji oluşturma, düzenleme ve uygulama alanlarını da kapsayan askeri yetenek ile hazırlığı etkileyen 'Savunma Geliştirme Hattı'nı etkileyecektir. Avantaj, en iyi uyum sağlayanlara gidecektir.
- Farklı asimetrik güç bu durumu telafi edebilir mi, nasıl edebilir bu konuda kesin bir cevabım yok. Ancak, Çin bazı sınırlamalarını ve endişelerini telafi etmek için bizden daha fazla buna odaklanıyor ve bence NATO ve Batı olarak bununla mücadele etmenin bir yolunu bulmalıyız. Aynı zamanda başka bir asimetrik avantaj elde etmek için bir şeyler yapmak da gerekebilir.



Dr. Ridvan Bari URCOSTA
VARŞOVA ÜNİVERSİTESİ
POLONYA

Merhaba, aranızda bulunmaktan dolayı büyük mutluluk ve onur duyuyorum. Türk kökenlerini tanıtmak iyi bir gelenek. Ben bir Kırım Türküyüm ama 10 yıldır Polonya'da yaşıyorum. Jeopolitik gelecekler için çalışıyorum ve işimin temel amacı tam olarak Rusya-Ukrayna Savaşı'nda neler olup bittiğini analiz etmektir. Jeopolitik gelecekler için çalışıyorum.

İşimin temel amacı tam olarak Rusya-Ukrayna Savaşı'nda neler olup bittiğini analiz etmektir. Bugün temel spesifik kavramlarla doğrudan savaşa gideceğim. 1959 yılında Robert A. Heinlein tarafından yazılan Yıldız Gemisi Askerleri (Starship Troopers) kitabını hepimiz hatırlıyoruz, filmi de yapılmıştı. 1999 yılında yeni versiyonları da yazılmış. Kitapta, askeri hayatı ve geleceğin askerini tasvir ederken, örneğin giyilen kıyafetlere 'güçlü takım elbise' adı veriliyordu. Ukrayna'daki savaşta ve dronlar nedeniyle kayıplarda da gördüğüm şey şuydu; FPV dronlar gerçekten çok farklı ve öldürücü. 1959 yılında bahsedilen şey günümüzün gerçeği ve bize askerler için yeni kıyafetler hazırlanması gerektiğini, özellikle Çin ve benzeri yapımı bu ucuz öldürme araçlarına karşı tedbir alınması gerektiğini gerçekten acı bir şekilde gösterdi. Hem Ruslar hem de Rusyalılar için oldukça tehlikeliler. Bakın kitapta ne yazıyor; «Elbiselerimiz bize daha iyi gözler, daha iyi kulaklar ve daha güçlü sırtlar verir. Daha fazla silah ve cephane taşımak için güçlü bacaklar. Daha fazla ateş gücü, daha fazla dayanıklılık, daha az kırılganlık». Aslında burada geleceğin askerinden ve yapay zekâdan bahsettiğini söyleyebiliriz, bu atıflar bize yapay zekânın ipuçlarını veriyor. Neredeyse, 70 yıl önce bu konu yazılmıştı. Geleceğin Askeri için insan vücuduna yapılacak ek yerleştirmeler, bir çeşit makine öğrenimi bile entegre edilmeli gerektiği ve bunların askerin savaşma yetenekleri üzerinde ciddi etkiye sahip olacakları belirtilmişti. Ancak diğer taraftan hiçbir şeyin değişmediğini hesaba katmalıyız. Tarihten bu yana askerin kendini savunmasının ek unsurlarını incelediğimizde, dış iskeletler evrimleşiyor, koruma ekipmanları gelişiyor ve uzay savaşçısı gibi tanımladığımız fütüristik askerin geleceğini göz ardı etmemeliyiz.

Tarih boyu gelinen noktada bize bunu gösteriyor. Belki de bugün Elon Musk'ın ya da Çin Savunma Endüstrisi'nin neler yaptığına, bugün ne noktada olduğuna bakarsak bunun on yılın sonunda bir olabileceğini düşünebiliriz.

Özetle nereye yaklaştığımızı bilmiyoruz, o yüzden teori olarak açıklayabiliriz. Tanık olduğumuz bilimsel devrim Neolitik Devrim'le açıklanabilir veya Ray Kurzweil'in 'Yaklaşan Teknolojik Tekillik' kitabındaki insanların biyolojiyi aştığı varsayımını esas alabiliriz. Ve bu tekillik bu on yılın sonunda, yani 2030'lu yıllarda olmalı. Veya Endüstri 4.0 devrimi. Neolitik devrimde bahsedilen sosyal ütopya, anti-ütopya, siber, yüksek teknoloji-düşük yaşam (cyberpunk) ya da Endüstri 4.0 devrimindeki yapay zekâ, uzay teknolojileri, robotik teknolojiler gibi kavramlar ve 'son' kavramını işleyen eskatoloji ile biyolojik olmayan sistemlerin evrimi (non-biological revolution) kavramları 100 yıl, 70 yıl önce hayatımıza girdi ve bugün rutinimiz olmaya başlıyorlar. Günlük hayatımızın bir parçası haline geliyorlar ve nüfuz edici bir şekilde bizimle bütünleşiyorlar. Bunu tanımlamak için doğru kelime inovasyon bile değil, bir şekilde virüsün hücre içine girmesi ya da bir bilgi sistemi ya da ağa yetkisiz bir şekilde erişme girişimi tanımlı olan penetrasyon olabilir. Çünkü bizi yeniden şekillendiriyorlar. Bunlar çok ciddi olaylar ve dünün geçmişinin bugünün gerçekçi olduğunu görüyoruz. Endüstri 4.0'ın halen daha neleri değiştireceğini ve ne anlama geldiğini bile bilmiyoruz, Kurzweil dahi varsayımlarda bulunurken tam olarak açıklayamadı. Özetle yeni toplum inşa edilirken, savaşların şekli de yeniden inşa ediliyor.

Ukrayna-Rusya Savaşı'nın yanı sıra Karabağ'daki savaştan da örnek vermek istiyorum savaşın teknolojik dönüşümünü anlatırken; özellikle teknolojinin son örneklerinde Türkiye'ye de tanık oluyoruz burada. Son birkaç yüz yıldır teknolojinin tekelsinin, liderliğinin Batı'da olduğunu söyleyebiliriz. 20. Yüzyılda teknoloji konusunda meydan okuyan Sovyetler Birliği'ydi ama bu tam doğru olmazdı çünkü Sovyetler Birliği de bir bakıma Batı'nın parçasıydı. Şu anda Karabağ Savaşı'nın başlangıcından bu yana bu alanda da değişimler görüyoruz. Çünkü Karabağ Savaşı'ndan bu yana biz bazı tekel güçlerin, lider güçlerin tekelleşme listesinden çıktığını, geleneksel güçlüler listesinden ayrıldığını görüyoruz. Genelde teknolojik güçler benzersiz bir şeyler üretir ve yeni jeoekonomik ile jeopolitik yapısına hükmederler, dünya pazarına sunarlar.

Bunu kendi üretim zincirleriyle, teknoloji zincirleriyle yaparlar. Bu benzersiz bir şeydir ve ülkelerin, bizlerin yönünü değiştirebilir. Bu genelde küresel bir dinamik gibidir ama bu noktada dikkate almamız gereken, çok özel bir an var. Ben bunlara 'kıvılcım ya da kıvılcımlar' diyorum.

Örneğin Türkiye'nin kendi bağımsız askeri sanayisini inşa etmesi gibi. Evet ama bu kıvılcım ne kadar sürecek, ne kadar kıvılcımlar sürecek ve ateşe dönüşecek? Gelecekte bir nevi kendi döngüsünü oluşturabilecek mi, kendisini koruyabilecek mi, bu kıvılcımı devam ettirebilecek mi ve ateşe çevirebilecek mi? Şu anda iyi ama bu daha ileriye gidebilecek mi? Gelecekte kalıcı olacak mı? Tüm bu tespitler benim Ukrayna Savaşı'ndaki analizlerimden de geliyor.

Hepimiz biliyoruz ki savaş konsepti, düşmanlarınızın neyin peşinde olduğunu anladığımız zamandır. Clausewitz'in dediği gibi 'Savaş belirsizlik alanıdır, savaştaki eylemin dayandığı faktörlerin dörtte üçü az ya daha çok belirsizlik sisine sarılır. En iyi örnek satranç veya gerçek zamanlı strateji (RTS) oyunlarıdır. Hamle yapabileceğiniz alanı satrançtaki savaş alanı gibi görünmese de yine de savaşlarda da arka planı göremiyorsunuz. Düşmanınızın ne hazırladığını anlamıyorsunuz, bu da düşmanın ne olduğunu anlamadığının anlamına geliyor. Ama insansız hava araçlarının bu noktada size tepeden bir bakış sağladığını, bazı detaylara ulaşabildiğinizi görebiliyorsunuz, özellikle alçak yörüngede kullanılanlarla. Elbette geri dönebilmesi, elektronik savaş, sinyal bozucu ve benzeri teknolojilerle engellemeler oluyor ama artık oyunun stratejilerinin, savaşın kurallarının değiştiğini görebiliyoruz.

Rusların Ukrayna'nın (Kupyansk) bazı kesimlerindeki kötü hava şartlarını bile kurnazca kullanarak avantaja çevirip istihbarat alanında da bu sistemleri kullandığını, durumu kendi için istikrara kavuşturduğu ve savaş alanındaki durumu karmaşıktırdıklarını görebiliyoruz. Ve bununla 5-7 kilometrelik ilerleme kaydedebildiler. Ve burada Alçak Dünya Yörüngesi (leo) alanında Yapay Zekâ, jeo-uzaysal zeka bağlantısının da kullanıldığını söyleyebilirim. Savunma hatlarını zayıflattılar veya yok ettiler. Ve tüm bunlarda komutanın, tıpkı bir satranç oyuncusu gibi, sanal gerçeklik veya anlık veri yoluyla da stratejiyi anında kontrol edip değiştirebildiğini, oyunu değiştirebildiğini anlayabiliyoruz.

Savaş Katmanları ve Uzay Faktörü'nü oluşturan uzay yarışı, teknolojik rekabet, kaynaklar ve hammaddeler, endüstriyel teknoloji seçkinleri, komuta ve kontrol odasında strateji, tüm birimler arasında entegre iletişim sistemleri (dikey ve yatay), kapsamlı jeo-uzamsal zeka oluşturma yeteneği, operasyonel sanat, durumsallığın yeniden tanımlanan farkındalık boyutu, taktikler, bilgi kontrolü ve askerin eyleminin koordinasyonuna yönelik taktik birimler yeniden gözden geçiriliyor, doktrinler değişiyor.

Savaşın sahadaki sürtünmeleri yani temasları değiştirken, sisi artıyor. İşte tam bu noktada, yine bir şey satranç ile benzerlik gösteriyor. Düşmanınızın her hareketini görebilirsiniz ama yenilebilir veya kazanabilirsiniz, yani mantığınızı, Yapay Zekâyı, dron ve uzay teknolojilerini kullanıyorsunuz ama beyniniz hala en geçerli silah. Yani gelecekteki savaş, önceki savaşlara göre farklı da olsa; ciddi entelektüel yeteneklere sahip komutanların stratejisi sonuçları belirleyecek. Kapasitelerini iyi bilen ve bu kapasitelerini yerinde ve zamanında kullanabilenler kazanacak. Geleceğin Savaşları'nı geleceğin savaşçıları ile kazanmak için de gerçekten akıllı olmanız gerekiyor. Yapay Zekâ, Bulut Teknolojileri, Otonom Makineler, Gerçek Zamanlı Strateji Simülasyonları evet çok işe yarayacak ama yine de akıllı olmalısın. Geçmişte bize savaşı komuta edenlerin akıllı olması gerektiğine işaret ediyor. İnsansız Hava Araçları, Bayraktar ve benzerleri savaş alanının görme yeteneğini, işitselliğini hissettiriyor. Tıpkı geçmişteki bir Napolyon'un 'Savaş Alanının Tamamını Görme' isteği gibi. Evet, teknolojiler eski konseptleri yeniden şekillendiriyor. Uzay Teknolojileri, İnsansız Hava Araçları ve Yapay Zekâ, taktik savaş felsefesi ve 'cephe gerisi' kavramındaki devrimi yoğunlaştırıyor. Tekniği, taktığı, öldürme zincirini değiştiriyor. Düşmanı bul, bastırıcı ateşle onları sıkıştır, düşmanı kuşat, askeri düşmanın yakınına gönder ve tüm düşman savaşçılarını yok edin şeklindeki zincir muazzam bir şekilde değişiyor. Ama Rusya-Ukrayna Savaşı'nda, Milattan Önce 2000'li yıllarda yaşayan Asurlulardan 21. Yüzyıla taşınan bir örnekte bize akıllı kullanmanın önemini gösteriyor.

Ruslar, 'mangal' ismini verdikleri ve Asurluların kabartmalarında yer alan üçgen şeklinde, bir evi andıran silah koruma aparatını FPV insansız hava araçlarına karşı kullandılar.

Rusların güvenli ve korunaklı olarak nasıl ilerlediklerine bakarsak ve Ukraynalıların da bu yöntemi kullandığına dikkat edersek, güçlü bir savunma ve daha az zayıflık için basit ama akıllı bir yöntem kullandıklarını anlıyoruz. Pahalı bir tank için güçlü bir savunma ama ucuz da bir yöntem. Ve bu bize geleceğin savaşlarında insansız hava araçları dolayısıyla, güçlü zırhlı tanklar yapılması veya bunun nasıl delinebileceği yönündeki güçlü mühimmatlar yönünden de düşündürmeli. Klasik savaşlarda FPV dronlar için hazırlanmamış bir tank, hızla savaş alanında basit bir akılla dönüşüm geçiriyor, bu da düşündürücü.

Ukrayna'daki ve Karabağ'daki savaş, bazı güçlere küresel pazara giriş için de fırsatlar verdi. Örneğin FPV dronlar ucuz ve sonuç odaklı ürünler olarak hızlı bir Pazar elde etti ve kısa sürede büyüdü. Yeniden Rusya-Ukrayna Savaşı'na dönecek olursak ve somut örneklerle ilerlersek, Rusların birkaç fikir entegrasyonu ile sahada olduklarını görüyoruz benim gözlemim ve teorime göre. Krank kavramı birkaç fikrin birleşmesinden oluşan derin bir kavram ve bir nevi 'Vuruş Noktası Krank Konsepti' uyguluyorlar. Derin operasyon ve savaş cephesi, bunun iki anlamı var. Bir anlamı sadece bir cephe, ön cephe. Diğer anlamı ise cephede birkaç ordu olduğu anlamına gelir. Örneğin, yaklaşık 300 kilometrekareden sorumlu olan belirli bir birim veya birlik. Ve bu özel birim kendi operasyonlarını yürütmede bir çeşit bağımsızlığa ve özerkliğe sahip. Bundan dolayı o an ki şartlara göre kendi kararlarını uyguluyor ve eski Sovyetler Birliği konseptini modernize edilmiş bir şekilde derin operasyon olarak bölgesel alanda ve cephede uyguluyorlar. Ve ağ merkezli savaş alanındaki bu örneğe Amerikalılar da hayranlık duyuyor.

Erişimin reddedildiği bir yöntemle, uzay istihbaratı gibi mümkün uygulamalara yoğunlaşarak noktasal vuruş gerçekleştiriyor ve ilerlemeyi noktasal kaydediyor. Dron istihbaratı, elektronik savaş gibi yöntemlerle Orikhiv, Kurakhov, Kurshchyna hatlarındaki ilerlemeler, Rusların iki yıldız bir takım rezervlerinin tükenmesi şeklinde yorumları bile tersine çevirdi. Özellikle tüm bu süreç boyunca ikmal ve lojistik konusunda da etkili önlemler aldıklarını ve yeni teknolojileri sadece öldürmek değil, sürdürülebilir savaş noktasında da etkili kullandıklarını, seferber ettikleri ikmal gücünde de kullandıklarını görüyoruz..

Ayrıca, bir şekilde savaşı istedikleri şekilde yönlendirebiliyorlar ve Ukraynalı askerleri istedikleri bölgelere çekmeyi başarıyorlar ve kendilerini rahat hissettikleri bölgelerde de noktasal vuruşlar yapıyorlar. Polonya'daki savaş uzmanları da bu görüş birliğine sahip. 30 kilometrelik bir hattı enlemesine ve boylamasına kontrol ederek ilerliyorlar. Ukrayna'nın bu ilerlemeye nasıl tepki verebileceğini konuşursak da 'Krank' gibi dairesel bir devinim oluşturan bu bir tür makine gibi ilerleme karşı topçu bataryası, elektronik savaş, insansız hava aracı kullanıyorlar. Hatta şimdi fiber dronlar kullanıyorlar.

Rusya'nın ilerleyişine karşı duruş Ukraynalıların insan kaynağı, endüstriyel kapasiteleri ve NATO ülkelerinin ekonomik destekleriyle de ilgili ama Ruslar bölgelere ayırdıkları güçlerin küçük alanlarda ilerlemeleri, kuvvetlerin belirli bir alanda yoğunlaşması ve bunu adım adım yapmalarıyla gerçekleştiriyor Batıya doğru adım adım ilerliyorlar. Ve büyük akıllı bombaların da Ruslara yardımcı olduğunu söylemeliyiz. Ve ordudaki en küçük topçu birliği olan 'Batarya' birimlerinin etkisini göz önüne almalıyız. Rus topçularının ortalama menzili yaklaşık 25-30 kilometre. Özellikle Güney'de Rusların ilerlemeleri bu güçlerin de etkisiyle oldu. Her 10 kilometre de ilerleme kaydedip durdular ve yeniden 10 kilometre için hazırlandılar. Yani topçu atışlarının ardından askerler ilerleyip yerleşirken, yeni 10 kilometrelik alan için hazırlandılar. Neden ilerleme kaydedilmiyor sorusunun cevabı buydu; 'Batarya Birliklerimiz Yeni Taarruz İçin Hazır Olmalı.' Ve topçu atışını insansız hava araçlarıyla da desteklediklerini görüyoruz, özellikle FPV dronlar. Ve yine bölgenin gözetlenmesinde uzay teknolojilerinin katkıları. Yani derin operasyonlarla ön cepheye ilerliyorlar. Ve top yekûn ön cepheye ulaşmalarında bu tehlikeli olur, NATO ülkeleri için de çok büyük anlam ifade eder. Ukraynalılar insansız hava araçlarını topçu olarak kullanabileceklerini ümit ediyorlar. İnsansız hava araçlarının savaşta topçu silahların yerini alabileceği, konumsal savaş için Rusları durdurabilecekleri veya zorlayabilecekleri kendi konseptlerini geliştirdiler. Ancak bu Rusları durdurmak için işe yaramadı.

Teşekkür eder, saygılarımı sunarım.

SUNUMUNDAN NOTLAR:

- Ay'ı kim kontrol ediyor, dünya yörüngesini kim kontrol ediyor, Dünya yörüngesini kim kontrol ediyorsa, dünya alanlarını kim kontrol ediyor ve siber dahil, bu alanları kim kontrol ediyorsa dünyayı kontrol ediyor.
- Önümüzdeki on yıllar, yakın yörünge ile ay ve dünya yörüngesi için kontrol, carlık, caydırıcılık rekabeti için olacaktır. Yörüngede ve ayda olmadan büyük güç statüsüne ulaşmak imkânsız olabilir. Peki ya Mars, Mars gerçekten astropolitik bir konu!
- Şeffaflık jeopolitik bir ifadeye sahiptir, çünkü Dünya'nın yörüngesini kontrol eden ve orada kilit bir altyapıya sahip olanlar, Dünya yüzeyine tam sınırsız erişime (izleme, gözetim, proje gücü ve değişiklikleri tespit etme ve etkiyi anlama yeteneği) sahiptir.

SORU: Ben özel harekatta görevli bir memurum. Bir düşmanı sahada görmek istiyorum, fazladan bir iskelet veya demir adamın performansını sahada görmek istiyorum. Örneğin, harekât ve operasyonlarda lojistiğin önemi çok fazla ve çok fazla elektronik sistemin kullanıldığı bir ortamda yüksek bir tepede çok fazla sayıda pil sevkiyatı gerekecek. Örneğin, elektronik bir sistemin pili bittiğinde ben ondan daha güçlü olabilirim. Örneğin Ukrayna Savaşı'nda dron bulunamazsa savaş nasıl olurdu? Günde 3 bin dron harcadılar. Biz de terör örgütlerine karşı insansız hava araçları kullanıyoruz ve bu alanda başarılıyız. Ancak savaşın hala lojistikte devam ettiğini görüyoruz. Yapay zekâ ve yeni teknolojiler konusunda çok sayıda organizasyona katıldım, herkes üst düzey teknoloji silahlardan, optiklerden bahsediyor ama lojistikten veya enerjiden bahseden kimseyi göremiyorum. Bu konuda görüşünüz nedir?

CEVAP: Ben gerçek bir savaş ortamını ve gözlemlerimi, tespitlerimi aktarıyorum sizlere. Savaşta lojistik en önemli konudur, sizinle bu konuda hem fikirim. Ama Iron Man gibi fantastik gelen bir yaklaşımla sadece insan üzerinden hareket etmek de tuzağa düşmek olur. Rakibiniz yeni teknolojiler geliştirirken, siz duramazsınız. Örneğin Selçuk Bayraktar'ın çok geçmişten bir videosunu izlemiştim. 2000'li yıllarda bugünkü vizyonunu birilerine anlatmaya çalışıyordu ve bugün ana akım olmayan fikrini savunuyordu.

O gün, elindeki teknolojinin geleceği yani bugünü etkileyecek bir teknoloji meselesi olduğunu savunuyordu. Size katılıyorum, felsefik bir düşünceye karşı soğukkanlı olmalıyız ama gerçekçi düşüncelerin bir gün geleceği oluşturabileceğini unutmamalı ve bu konuda da soğukkanlı olmalıyız. Gelişmelerle lojistiğin de çözüleceğini unutmamalıyız.



Dr. Jean-Marc RICKLY
GCSP
İSVİÇRE

Nazik davetiniz için teşekkür ederim. Ukrayna'daki savaşta neye tanık olduğumuz hakkında konuşacağım. Yapay zekânın rolünü inceleyeceğiz. Yapay zekânın temel amacı ve yapay zekânın gerçekten iyi olduğu şey, veriyi parçalamak ve verileri analiz etmesi. Dolayısıyla şu anda sahip olduğumuz ve tanık olduğumuz en büyük katkı, analitik bir kolaylaştırıcıdır.

Ancak ayrıca yapay zekânın giderek artan bir şekilde bir kuvvet çarpanı ateşi olarak kullanıldığını görüyoruz. Savaş ortamında yapay zekâ kuvvet çarpanı, analitik etkinleştirici ve yıkıcı güç. Ve size bununla ne kastettiğimi açıklamaya ve bazı somut örnekler sunmaya çalışacağım.

Ukrayna, şu anda Gazze gibi bu teknolojilerin kullanımı ve testi için inanılmaz bir test laboratuvarı. Ve bu yüzden burada birkaç örnek var. Yapay Zekâ şuydu; aslında tüm istihbaratı ve bölge resimlerini geliştirmek için verileri işlemek için kullanıldı. Uber uygulamasını temel olarak taklit eden ancak sürücüyü müşteriyle veya yolcuyla bağlantılandırmak için kullanılan GIS Arta uygulamasını duymuşsunuzdur. Rusların, Shadid 136 kamikaze dron kullanmaya başladığı ve Ukrayna hava savunmasının aniden alt edildiği Eylül 2022'den itibaren benzer şekilde bir uygulama geliştirdiler. Herhangi bir Ukrayna vatandaşı bu uygulamayı indirip topçu saldırılarını veya dron istihbaratının koordine edilmesine destek verebilir.

Herhangi bir Ukrayna vatandaşı bu uygulamayı indirip topçu saldırılarını veya dron istihbaratının koordine edilmesine destek verebilir. Hızlı hedefleme özelliğine sahip ve Ukrayna topçuları tarafından kullanılan bu uygulama ile sadece drona işaret edebilir ve görüntü yerleştirilip analiz edilecek ve istihbarat döngüsüne dahil edilecek, istihbarat döngüsü beslenebilecek. Bilmemiz gereken şey şu ki, artık her birimizin bir sensör haline geldiğinin farkında olmamız, veri üretiyoruz. Bu veri Rusya'da da kullanılabilir ve istihbarat amacıyla da kullanılabilir. Rusya ve Ukrayna'da bazı start-up şirketlerinden destek alır.

Örneğin, primer.ai Google'daki benzer bir soruyu metin üzerinde analiz etmek için temel olarak yeni dil programlamada NLP'yi kullanır.

Yeni bir teknolojiye sahip olduğunuzda, geliştirebileceğiniz ve net görüntü oluşturabileceğiniz ilgi çekici bir sisteminiz olur, temelde iş toplayan bir uygulamadır, oldukça basittir, tüm resimleri topladılar ve bu resimleri başka resimle karşılaştırdılar ve böylece taşınabilir mini bir istihbarat teşkilatı oluşturdular. O savaş sırasında Ukraynalılar, Rus askerlerinin ölü ya da diri olduğunu belirlemek için bu görüntüleri kullandılar. Ve onların kim olduklarını öğrendikten sonra onların ailesi kim olduğunu da bilebilirsiniz. Ve hedefli mesajlarınızı iletebilirsiniz.

Yani yapay zekânın ilk kuvvet çarpanı açıkta bu ve yeni değil ama Ukrayna birçok farklı teknolojilerin kullanıldığı bir savaş alanı ve çok dinamik, buna tanık oluyoruz. Savaşın başlangıcında Ukrayna'nın Rusya'ya karşı avantajı özellikle Bayraktar TB2 ile sağlandı ancak zamanla Ruslar uyum sağladı ve gördüğümüz şey, sürekli bir yenilik hızı. Özel sektör ve yeni girişimler sayesinde savaş alanında sürekli bir yenilik hızı var. Örneğin savunma sektöründe çalışmayan şirketler bile vardı. Temel olarak ağaçlardaki meyveleri tanımlamak için yapay zekâ kullanan bir şirket, savaş başladıktan sonra hedefi ve çevreyi tanımlamak için algoritmada birkaç parametreyi değiştirdi. 2020'de Karabağ'da kamikaze dronların ortaya çıkışına tanık oluyoruz, yani insansız hava araçları ve bölge daha sonra sinyali aldıklarında devreye sokuluyorlar.

Ruslar İran'dan Shahed 146 aldılar ve kullandılar, Ukrayna'nın birçok bölgesinde elektrik dağıtımını hedef alarak Şubat ve Kasım 2022 arasında karanlığa gömülmesine katkı sağladılar. Yani neredeyse hiç ışık yok ve Ruslar Ukrayna'da ışığı kapatmayı başardılar. İster Rusya tarafında ister Ukrayna tarafında olsun savaş alanına giren büyük bir ulustan oluşan bir ailenin tamamını örüyorsunuz. Bu açıkça karşı önlemlere, özellikle, elektronik savaşa yol açıyor ve FPV'lerde başarı oranı jamming (sinyal bozucu) dolayısıyla çarpıcı bir şekilde düştü ve dolayısıyla hem Rusya hem de Ukrayna aktörleri bu gelişmelere uyum sağlamak zorunda kaldı. Her iki tarafta kendi yetenekleriyle baskı kurmaya çalıştı ve bu kez karşı-sinyal bozucu sistemler devreye girdi.

Bu açıkça karşı önlemler, özellikle, elektronik savaşa yol açıyor ve FPV'lerde başarı oranı jamming (sinyal bozucu) dolayısıyla çarpıcı bir şekilde düştü ve dolayısıyla hem Rusya hem de Ukrayna aktörleri bu gelişmelere uyum sağlamak zorunda kaldı. Her iki tarafta kendi yetenekleriyle baskı kurmaya çalıştı ve bu kez karşı-sinyal bozucu sistemler devreye girdi

Ukrayna ile Rusya çatışması, büyük bir robot savaşının ilk örneklerinden biri muhtemelen budur ve büyük bir Rus robotunun, bir insansız hava aracı tarafından yok edildiği ilk robot savaşından biridir. Ve bu yüzden artık burada bilim kurguya girmiyoruz, bu tür bir dinamiğe giriyoruz. Eylül Ayı'nın başında bir Rus siperine karşı Ukraynalıların bir robotla saldırı başlattığı bildirildi.

Açıkça ve gerçekten anlamamız gereken şey, bu teknolojinin çok çok hızlı bir şekilde yaygınlaştığı ve demokratikleştiğidir. Tamam bu nükleerden farklı ve ona benzemiyor ama kod satırları bir kez dışarı çıktıklarında hep dışarı çıkarlar ve legal aktör olmayanlar bunu gerçekten kullanabilirler. Örneğin 2017'de IŞİD'de bu durum böyleydi, kullanılan dronlar küçük portlarla değiştirilerek el bombası içerebiliyordu ve haftada 30'a kadar Irak askerinin hayatını kaybetmesini sağladı. Bu savaş tarihinde ilk kez devlet dışı bir aktörün devlet aktörleri üzerinde taktiksel bir üstünlük sağlamayı başardı tarihi. Artık piyasada bulabileceğiniz türden dronlarla yapılan özellikle uçan AK 47'yi biliyorsunuz. Ve siber uzay, biliyorsunuz Ukrayna'daki savaş süresince çok sayıda siber atak vardı ve hayal kırıklığı oluşturan bir durumdu, savaştan önceden de siber rol oynadı.

Savaş öncesindeki rolümüz ve aynı zamanda yıkımda da önemli rol oynuyor. Ve aslında siber uzay aslında savaştan önce hedefleri susturmak için kullanılıyordu. Savaşın ilk gününü hatırlarsanız, uyduya karşı bir siber saldırıydı ve sistem, Ukrayna, Almanya ve diğer ülkeler üzerindeki uydu etkisini devre dışı bıraktı. Ama ilginç olan şu ki bu uydu sisteminin yerini Starlink aldı ve kim bu Elon Musk, tanıdığınız bir insan ve ilginç olan şu ki siz de varsınız tehdit analizinde stratejik analizinde ve tek bir bireyin gücünü hesaba katıyorsunuz. Çünkü artık Trump'ın başkan olarak seçildiği ve taktığı maskeye göre Trump'ın söylediği şeydu; "Hey Ukraynalı artık barış için Ruslarla konuşmaya ve bir barış planı yapmaya başlamalısın."

Bu adamın eli düşmanın üzerinde ve bu zaten Kırım'da oldu, Starlink bu bölgeyi temelde kör etmişti. Ukrayna yeteneklerini kullanamadı.

Stratejist bir analist olarak son kitabımın adı 'Vekil Savaş'tı ve kitapta gelecekte harbin devletler ve devlet içi aktörlerin, ya insan ya da teknolojik vekiller kullanılarak yapılacağını, kazanç sağlanacağını belirtmiştim. Ukrayna'daki savaşta bunun çok canlı bir iddia ve örnek olduğunu gösterdi.

Ukraynalılar dışarıdan yardım istiyor. Ukrayna Ordusu'na katılmak isteyen herkes katılabilir, ancak bir operasyon şefi veya komutan olarak gerçek bir sorunla karşı karşıyasınız. Vekilleriniz üzerinde kesinlikle bir kontrole sahip değilsiniz ve bir sorumluluk sorunu oluşturuyor.

İlginç bir şekilde silah sistemlerinde özerklik artıyor ve bu özerkliği insanlarla, bu büyüyen özerkliği nasıl entegre edeceğimizi düşünmeliyiz. Şöyle bakalım, hava kuvvetlerinde savaş pilotu olarak eğitildim ve eğitimim yaklaşık 1 milyon İsviçre frangına mal oldu. Ve ABD Ordusu Hava Kuvvetleri bu yıl bir test yapıyor, bir algoritmanın bir jeti özer olarak uçurabildiği testleri yürütüyor ve bu sistem 8 farklı görevi yerine getirebiliyor. O zaman şimdi bu tür yetenekleri gelecekte nasıl entegre edeceğinizi düşünün ve yapay zekânın bizim çalıştığımızdan çok daha hızlı çalışması nedeniyle ne yapılacağını düşünün. Biz yarım veya 1 saniyede çalışıyoruz ama yapay zekâ nano hızda. Gerçekten ortak olmanın yollarını bir araya getirmemiz gerekiyor, insan makine aracılığıyla ortaklık kurmanın yolunu bulmalıyız.

Yapay zekâ savaşları bozabilir, bununla ilgili bir şey giderek daha fazla yapılabilir. Örneğin sürü teknolojileri, en son 10 binden fazla insansız hava aracı Şenzen'de birlikte uçuyordu ve bu bir dünya rekoruydu. İnsansız hava araçları havai fişeklerin yerini almaya başlıyordu. Açıkçası çok güzeldi ama orduda bunun çok güçlü bir etkisi var. Çünkü sürü fikri, düşman sisteminizi doyurmaktır ve örneğin İsrail Hava Savunma Sistemi gerçekten iyi ama o sistemi doyurursanız o zaman bazıları etki alanından çıkacak ve sürü başarıya ulaşacak. Biz buna tanık olmaya başlıyoruz. Savaş buna dönüşüyor, ikinci etki daha az görünür olmasına rağmen daha derin olduğunu gösteriyor.

Örneğin kuş sürüsünde hiçbir kuş oluşan şeklin farkında değil, dev bir bulut gibi. Tek tek birimleri bir araya getirirseniz nitelikleri farklı olan bir şey oluşturursunuz, birçok özelliği bir arada farklı kullanabilirsiniz. Film izleyenler için Transformers ile bu bir sürü fikridir, bir şeyi birbirine bağlarsınız ve aniden kalite ve etki açısından üstün yeni bir şey yaparsınız.

İki yıl önce Google'ın yapa zekâ üzerine çalışan Deepmind ekibiyle bir toplantı yapmıştım ve derin robot bilimi bölümünün başkanıyla bir toplantıdaydım. Yeni ortaya çıkan teknolojiler üzerine bu alanda çalışan diğer şirketler gibi çalışmalar yapıyorlar. Yani ileride giderek artan bir şekilde sürüler göreceğimiz savaşlarda. Ve bunu daha hızlı üretebilirler, sütle artar dolayısıyla düşman sisteminin doyumunu artırabilirsiniz ve artık daha fazla zarar verebilirsiniz. Odessa'da da sığınakları hedeflemek için kullanmışlardı termik bombaları, bu bombaların hedefi bildiğiniz gibi oksijeni emmek ve temelde ciğerlerinizi patlatmak, gözleriniz de patlıyor.

İki yıl önce yapılan bir simülasyonda ABD Ordusu, Tayvan'ın Çin tarafından olası işgali konusunda tamamen otonom bir sürüye dönüşen yeteneklere yatırım yapmamız gerektiğini gösteriyor. Yani büyük oyuncu bunun üzerinde çalışıyor ve bizim de büyük ihtimalle buna hazır olmamız, gelecekte savaş alanında bu sorunla karşılaşmamız çok olası. Gelecekteki savaş alanında sürüyle ilgili sorun şu ki, şu an için hücum savunma dengesi dediğimiz şey üzerinde ciddi bir etkisi var. Bir sürüyü etkileyebilecek, vuruş yapabilecek bir sistemimiz yok. Yani tüm sürüleri karşılayabilecek farklı bir sisteminiz olabilir. Çünkü nükleer caydırıcılık nedeniyle bir savunmaya hâkim bir uluslararası sistemiz. Benim iddiam şu ki, eğer bu saldırgan taktiksel avantaj, stratejik bir seviyeye geçerse, sistem saldırının savunmaya göre avantajlı olduğu anlamına gelir. Böyle bir durumda kendinizi korumanın en iyi yolu nedir? İlk önce saldırmak Birleşmiş Milletler 'in 2.4. maddesinin ihlalidir. BM Sözleşmesi buna önleme deniyor, yani potansiyel olarak bu teknolojinin uluslararası BM şartını tamamen tersine çevirme potansiyeli var.

Yapay zekâyı bir yıkıcı olarak düşünebilmemizin son yolu, bilgi ve yıkımdır ve bilgi operasyonu yıkımı yeni bir şey değil. Roma İmparatorluğu'ndan beri devam ediyor ve sadece araçlar tamamen farklı.

Değişen şey araçlar ve artık ölçeklenebilir, ölçülebilir. Derin sahtekarlıkların evimi (deepfake) 2014'te icat edildi. İki resim veya görüntü arasından biriyle istediğiniz mesajı verdiriyorsunuz. 2018'de başlatılan resimler gerçekten çok gerçekçi. Bunlar 2022 Mart'ta savaşta ilk kez kullanıldı ve Zelensky'i vatandaşlara silahları bırakın çağrısında bulundu. Ukrayna'nın da bu tarz denemelerini video olarak görmüştük. Rusların yine Shahed 136'nın insansız hava araçlarıyla termobarik yükleri (vakum bombası) birlikte kullandıklarını gördük. Geçen yıl Haziran'da Putin'in sıkı yönetim ilan edilmesiyle sonuçlanan kitlesel seferberlik mesajı yayınlandı. Ve Ukrayna'nın bazı şehirlerinde panik sahnelerine yol açtı. Şimdi 2013 yılında bir askeri analist olarak bu bilginin 10 yıl sonra nasıl yönetileceğini nasıl soracaksınız?

Bilimsel olarak olmayan bir teknoloji bulmanız gerekecek, savaş ortamında nasıl çalıştığını anlamak ve nasıl kullanılabileceğini anlamanız gerekecek. Bu katlanarak büyümedir ve savaş alanında da üstel bir büyümedir. Dolayısıyla gerçekten kalıpların dışında düşünmeniz gerekir. Çünkü bu teknolojinin sağladığı düzeyi anlamak çok önemlidir. Örneğin bu yılın başlarında Ruslar, Fransa 24'ün bir TV sunucusunun derin sahtesini yaptı ve temelde sunucu, videoda Fransız Cumhurbaşkanı Emmanuel Macron'un Ukrayna seyahatini ertelediğini, çünkü Fransız gizli servislerinin kendisine yönelik bir suikast girişimini engellediğini duyuruyor. Peki bu ne anlama geliyor? Derin sahtecilik neden bu kadar önemli? Çünkü yapısal olarak hepimizin psikolojik ön yargıları var ve bu önyargılar sırasında bir asimetri oluşuyor. Gerçekler yerine yalanları tercih etme eğilimindeyiz ve yalanlar daha hızlı seyahat eder. Ve insanoğlunun yapısal asimetrisi çok daha geniş bir kitleye ulaşmaktır.

Şimdi Bilişsel Savaş'a geliyoruz. Bilişsel Savaş, savaşın altıncı alanıdır. Beyninizi sizi aslında bir bilgi ortamına kilitleyerek ilk önce savaş alanı haline gelir ve algıladığınız yeri yeniden tamamlayacak bilgiden daha fazlasıdır. Çünkü Bilişsel Savaş neyi ve nasıl düşündüğünüzü kontrol etme yeteneği, nasıl düşündüğünüzü kontrol etmek için yapılandır.

Biliyorsunuz savaş daha fazla bilişsele dönüşüyor. Savaş artık meta evrenlerin ve etkileyici-sürükleyici teknolojilerin de yer aldığı sanal ortamlara kilitleneceksiniz.

Bu yılın başlarında Apple Vision Pro'yu görmüşsünüzdür. Artık beyin aktivitenizi ilemeye başlayan gözlüklere sahipsiniz. Belirli bir nesne veya kişi belirli bir beyin aktivitesi başlatır ve siz nereye bakıyor ve ne hissediyorsunuz gibi duygusal tepkileri de izlemeye, ilişkilendirmeye başlarsınız. Bu da mükemmel bir manipülasyonun kapılarını açar. İnsanları 2018'de bir test için Manyetik Rezonans görüntülemeye (MRI) cihazına koyarak yaptığımız bir testin 2022'de başka bir versiyonunda gördük ki, artık zihin okuma çağına giriyoruz. Yapay Zekânın gördüklerimizi, duyduklarımızı, hislerimizi yorumladığı bir çağa. Tamam makine artıyor ve zihin okuyabilecek? Sonraki adım ne? Sonraki adım, hafızanızı yeniden yazmak olacak. Henüz orada değiliz, oradan çok uzaktayız ama bunu analizinize dahil etmeniz gerekiyor.

Bu bizim için ne anlama geliyor? Burada yeni ortaya çıkan teknolojilerden bahsediyorum ancak Ukrayna Savaş'ında gördüğümüz kayıplar, Fransızların Birinci Dünya Savaş'ındaki kayıp oranına benzer. Açıklanana göre 44 saniye de bir Rus askeri savaş alanında ölüyordu ama aynı zamanda savaşa giren yeni silah türlerine de tanık oluyoruz. Burada size gösterdiklerim aslında şimdilik dengeyi değiştirecek büyük robotlar, teknolojiler değil gibi ama bu şeylerin geleceğinin farkında olmalıyız. Ve bu yeni dinamikler oluşturur, bu önceki silahların, dinamiklerin gittiği anlamına gelmez, hayır yenisi ve eskisini birlikte hesaba katmalısınız. Aynı zamanda gittikçe daha fazla insanı yeniliklere entegre etmemiz ve makine ile insanı bütünleştirmek gerektiği gerçeğini de hesaba katmalısınız. Açıkçası makinelerin akıllanması çok fazla etik kaygı uyandırıyor. Çok fazla can kaybına veya can kurtarmasına dair hesap verilebilirlik açısından da yani etik açıdan da çok fazla etik alanda endişe oluşturuyor.

Teşekkür ederim.

SUNUMUNDAN NOTLAR:

- Yapay zekânın kuvvet çarpanı, analitik etkinleştirici ve yıkıcı etkileri kaçınılmazdır.
- Savaş, giderek artan yeni çift kullanımlı teknolojiler, yeni aktörler ve savaşmanın yeni yolları ile karakterize edilen giderek daha karmaşık hale geliyor. Teknolojilerin istenmeyen şekillerde nasıl kullanılacağını ve kötüye kullanılacağını tahmin etmek zor. Hayal gücünün başarısızlığı her zaman geçerli bir risk.
- Teknolojinin gelişiminde de geleneksel silahlar ve savaşma yolları baskın ve başarının temel belirleyicileri olmaya devam ediyor. Personel ve silahların kalitesi ve miktarı hayati öneme sahip olmaya devam ediyor, endüstriyel savaş geride değil.
- "Hızlanmaları üst üste yığmaya başladığınızda, çok yakında savaş alanında size saldıran yüz tanıma özelliğine sahip otonom dron sürüleriniz olacak. Peki bunun önüne nasıl çıkacaksınız?"

SORU: Tüm teknolojik gelişmelere rağmen geleneksel mühimmata talep ve mühimmat fabrikalarındaki artış konusundaki düşünceniz nedir? Mühimmatların tükenişi kötü bir planlama mı, savaş alanında kullanılan yeni teknolojilerin etkisi mi?

CEVAP: Savaş alanına giren yeni bir teknoloji gördüğümüzde, önceki dinamiklerin oradan kalktığı anlamına gelmiyor. Ukrayna'daki duruma bakarsanız, yani Avrupalılar açısından ve 10 yıl önceki dinamikler açısından kayıplar yönüyle Birinci Dünya Savaşı'na benzer büyük bir savaş olacağını söyleseydiniz kimse inanmazdı. Peki ne oldu, Birinci Dünya Savaşı'na benzer siper savaşları görüyorsunuz. Örneğin, dronların yaptığı piyade askeri için savaş alanının şeffaflığını, görünürlüğünü üst seviyeye çıkarmak. Savaş alanında piyade olmak gerçekten zor iş. Önce uygulama için yeni yollar oluşturuyorsunuz, sonra düşmanı etkisiz hale getirmeye çalışıyorsunuz. Ve bunun için de mühimmata ihtiyacınız var. Geleneksel yöntemleri gelişen teknolojilerle birleştirdiğinizde yeni dinamikler oluşturuyorsunuz. Savaşın sisinden, sürtünmeden bahsediyoruz. Bu gelişen bir oyun, savaş her zaman gelişti. Aslında şu anda beyinle ilgili yolu doğrudan değiştirilebilecek bir şeyden bahsediyoruz.

I. GÜN İKİNCİ OTURUM – YENİ SAVAŞ

TEMA:

Savaşta Modernizm: Teknolojik Aktörler

OTURUM KONUSU:

Karabağ Savaşı: Teknolojinin Savaş
Doktrinlerine Etkileri

OTURUM TEMALARI:

Modern Dünyada Hava Gücü:
Otonom Sistemler ve Savaşlar

Robot Askerler ve Yeni Teknolojilerle Savaşa Bakış
Teknoloji, Güvenlik ve Jeopolitiğin Kesişimi

II. OTURUM ÖZETİ

Karabağ Savaşı'nda TB2 Baykar'ın performansı, Ukrayna Savaşı'nın ilk dönemlerinde Rusya'nın gerilemesini sağlayan ilerleyişi ve daha sonra alınan tedbirler yeni nesil teknolojilerde hızın ve anlık değişimlerin göstergesi olarak kabul edilmektedir. İnsan yoğun muharebe sahasından teknoloji yoğun muharebe sahasına doğru bir dönüşüm gerçekleşmektedir.

Blockchain teknolojileri, kuantum bilgisayarlar ve büyük veri kullanımı ile nesnelerin interneti teknolojileri için büyük önem taşımaktadır. Özellikle güvenli iletişim, karar alma ve güvenli veri paylaşımı için merkeziyetsiz ancak verinin değiştirilemezliği yapısıyla fırsatlar sunmaktadır. Dünya'da DARPA, Lockheed Martin, Boeing gibi firmalar bu alanda çalışmalar yapmaktadır. Geleceğin çoklu farklı ortamlarına hazırlık yapacak planlamalar gerekmektedir. Gelecekte Elon Musk gibi küresel vekil aktörlerin yapay zekâ, neuralink ve uzay gibi noktalarda artabileceği, yeni teknolojilerle tehlikeli aktörler olabilecekleri öngörülmektedir. Nöro savaş, bilişsel savaş gelecekte askeri bir faaliyet olarak görülebilir. Çok farklı alanlarda, çok farklı insan kaynağına ihtiyaç olacak. Siyah Kuğu olarak da bilinen belirsiz ortamlar ve belirsiz olaylara karşı hazırlık yapılması gerekmektedir. Bu da iyi bir insan kaynağı ve dinamik bir yapı kurmak zorunluluk haline gelecek.

Günümüzdeki savaşları, eski ile yeni savaş teknolojilerinin dönüşüm testlerini ve yeniliğin ve mümkün olabirliğin denendiği ortamlar olarak görülmektedir. Sadece insan kararlarının yeterli olmayacağı, hızlı ve doğru karar almak için teknolojinin imkanlarının seferber edildiği bir rekabet durumu söz konusudur. Yapay zekânın insan karar döngüsünden çıkması gibi riskler taşıması geleceğin tartışma konusudur ve 'hayalet savaş' olarak adlandırılan bu dönem geldiğinde hazır olunması gerekmektedir. Siber savaş, küçük bir devletin çok daha büyük bir düşman üzerinde önemli bir yıkıma yol açmasını sağlayabilecek kadar önemli bir potansiyeldir. Uydu ve spektrum teknolojisinde güvenlik açıklarını bulmak ve güvenlik açığı vermemek gibi karşı teknoloji rekabetleri giderek artacaktır. Tüm bunların yanında, son noktayı koyacak yine insan olacaktır.

Tüm bunların yanında, son noktayı koyacak yine insan olacaktır. Tüm teknolojilerin kullanımı ve kentsel operasyonlarda robotik taşıyıcılar, savaş robotların önemi artacak, birbirine entegre olmuş birlikler (insan, robot ve insansız sistemler) geleceğin operasyonel ortamlarının gerçeği olacaktır.

Hava, Kara, Deniz, Siber ve Uzay'daki 5 çatışma ortamı için 'Müşterek Operasyon Merkezi' konseptleri, yedekli teknolojiler, analitik ve otomatik karara hizmet eden yapay zekâ yeni karargah kavramı ve konsepti olacaktır.

Geliştirilen her sistem, gerek bireysel olarak askerin, gerek tank, top, korvet, uçak gibi tüm hareket birliklerinin durumsal farkındalığını ve hareket kabiliyetini artırmaktadır. Ve bundan kaçmak mümkün değildir. Bireysel olarak askerler için de hazırlanacak her teknolojinin savaşçının hareket kabiliyetini artıracak, askeri korumak ve aktif kılmak için olduğunu unutmamalıyız.



**Emekli Korgeneral
Alparslan ERDOĞAN
MODERATÖR**

Hepiniz hoş geldiniz değerli misafirler. Geleceğin askeri ve geleceğin muharebe sahası hep tartışılmalı bir konu. Ben Kara Harp Okulu mezunuyum ve askeri öğrencilik zamanımızda hem öğrencilik hem de kurmaylık eğitiminde geleceğin askeri nasıl olmalı, geleceğin muharebe sonrası nasıl şekillenecek diye konuşuluyordu. Fark ettik ki, askerden ziyade teknolojiye bir dönüşüm var. İnsan yoğun harp

sahasından muharebe sahasına evrilen bir döneme şahitlik ediyoruz.

Yaklaşık 30 yıl önce NATO Kara Silahlanma Grubu'nun organize ettiği 'Future Soldier' konulu konferansına katılmıştım. O konferansta ana tema balistik koruyucu başlık, yelek ve küçük birlik seviyesinde haberleşme nasıl olmalıydı kapsamındaydı. Bugünkü tartıştığımız konulara bakıyoruz yapay zekâ, insan-makine ara yüzü, robotlar, insansız sistemler, otonom sistemlerden ve dijital komutandan bahsediyoruz. Bu da nereden nereye geldiğimizin önemli bir göstergesi. Harp başlığı ve vücut korumasından nerelere geliyoruz. Çoğu orduda otonom sistemler, insansız sistemler için birimler kurulmaya başlandı. Türk Silahlı Kuvvetleri'nde de hava-kara ve deniz birlikleri artık bu sistemleri kullanıyor. EDHOK komutanımız da buradayken, müşterek kuvvetler veya kuvvetler bazında bizde de artık Otonom Sistemler veya İnsansız Hava Araçları Komutanlığı gibi yeniden yapılanmalara gidilmesi gerektiğini de dile getirmek isterim.



**Doç. Dr. Muharrem
Tuncay GENÇOĞLU
FIRAT ÜNİVERSİTESİ**

Çok kıymetli komutanlarım, değerli katılımcılar, hepinizi sevgi, saygı ve hürmetle selamlıyorum. Geçtiğimiz günlerde yaşadığımız menfur saldırıdaki şehitlerimize Allah'tan rahmet, yakınlarına başsağlığı, TUSAŞ ailesine geçmiş olsun diyorum. Ben konuşmamda işin biraz farklı boyutuna değinmeye çalışacağım. Bu yakın coğrafyamızda süre gelen savaşlardan, dron savaşları, hava gücü bakımından icra edilen

faaliyetlerin işin güvenlik boyutuna, çünkü bu savaşlarda üretilen çok ciddi bir iletişim ve veri akışı söz konusu. İşin bu kısmına yöneleceğim. Özellikle blockchain teknolojisinin hava kuvvetlerindeki otonom sistemleri nasıl daha verimli hale getirebileceğini, modern savaş düzenlerinde etkilerini ve bu gelişmelerin jeopolitik sonuçlarını gerçek dünya örnekleriyle ele almaya çalışacağım.

Modern Savaş Alanı, ileri teknolojilerin entegrasyonu ile devrimsel bir dönüşüm geçirmektedir. Bununla birlikte yakın coğrafyamızdaki Suriye, İkinci Karabağ Savaşı, Rusya-Ukrayna savaşı gibi özellikle insansız sistemlerin taktik ve operatif sahada sürekli artan yoğunlukta kullanımına hepimiz şahit olduk. Bu noktada baktığımızda, Karabağ Savaşı özellikle ele alındığında buradaki teknolojinin modern teknolojinin savaşı nasıl bir paradigma değişikliğine doğru götürdüğünü çok rahatlıkla görebilmekteyiz. Otonom sistemleri, İHA'lar ve dijital alt yapıları bu savaşın seyrini belirleyici şekilde etkilemiştir. Azerbaycan'ın etkin SiHA ve İHA kullanımı, düşman savunma hatlarını hedef alarak stratejik üstün sağladığı bu savaş, modern teknolojilerin askeri operasyonlardaki önemini ortaya koydu. Bu açıdan baktığımız zaman otonom sistemlerin daha güvenli ve etkili ve koordineli çalışmasının önemi ortaya çıkıyor. Bunun daha önemli ve hayati bir konu olduğunu söylemek mümkün. Bu noktada geleneksel olarak insana dayanan hava gücü, otonom sistemler, robot teknolojiler ve özellikle de blockchain teknolojisiyle yeniden şekilleniyor. Bu şekillenmede ulusların güvenlik, jeopolitik ve teknolojik üstünlük algısını da tamamıyla değiştiriyor.

Otonom sistemler, özellikle insansız hava araçları ve dron sürüleri gibi teknolojiler, modern hava gücü stratejilerinin vazgeçilmez olmuştur. Karabağ Savaşı'nda kullanılan Türk yapımı Bayraktar TB2'ler, hedef tespiti ve imhasında benzersiz bir rol oynayarak savaşın gidişatını belirlemiştir. Bu sistemler insan riskini azaltırken hızlı ve hassas saldırılar gerçekleştirebilme kapasitesine sahiptir. Ancak, etkili olmaları güvenli iletişim, karar alma ve güvenli veri paylaşımına bağlıdır. Bu noktada otonom sistemler ve hava gücünde yeni bir paradigmanın önümüzde olduğunu görüyoruz. Bunlar otonom hava gücünü yeniden ele almamızı, ele alırken de hep zorluklarından ve fırsatlarından haberdar olmamızı gerektiriyor. Bu noktadan baktığımızda veri güvenliği, koordinasyon, güven ve hesap verilebilirlik noktalarında bu zorlukları inceleyebiliyoruz. İnsansız hava araçlarının iletişim sistemleri düşman tarafından siber saldırılara maruz kalabilir. Rusya örneğinin Suriye'de elektronik harp sistemlerini kullanıyor. İnsansız Hava araçlarına baktığımızda koordinasyon açısından, dron sürüleri gibi dağıtık hava unsurlarını yönetmek, kesintisiz ve merkezi olmayan bir kontrole ihtiyacımız olduğunu gösteriyor bize. Güven ve hesap verilebilirlik noktasında ise otonom sistemlerin karar alma süreçlerindeki sorumluluğun belirlenmesi de önümüzde tartışmalı bir konudur. Blockchain teknolojisi tam bu noktada işimize yarayabilecek ve verebilecek, geleceğin teknolojisi olarak adlandırabileceğimiz önemli bir güvenlik ve teknoloji aracı.

Blockchain teknolojisi, otonom hava gücü sistemlerinin karşılaştığı güvenlik ve koordinasyon sorunlarını çözebilecek önemli bir araçtır. Zira dağıtık, merkezi olmayan, değiştirilemez ve şeffaf yapısı, güvenli iletişim, etkili koordinasyon ve hesap verebilirlik sağlar. Blockchain teknolojisi şöyle kısaca ifade edeyim, aslında hayatımızı işin finans boyutuyla giren bir teknoloji olan, 2008'de bir makale ile hayatımıza giren bir teknoloji. Herkes kripto para, BTC, ETH gibi kripto varlıkların alt yapısıyla biliyor. Herkes bu teknolojiyi finans teknolojisi gibi algıladı ama blockchain 1980'li yıllara dayanan, matematiksel alt yapıyla oluşan bir teknoloji. Temel dayanağı, onun dağıtık yapısı ve oradan kaynaklanan merkeziyetiz yapısı ve şeffaflık. Girilen verinin değiştirilemezliği gibi özelliği, bizi bu anlamda güvenlikte, veri güvenliğinde ve iletişim güvenliğini sağlayabilecek önemli bir teknoloji.

Adı üzerinde her bir bloğun ayrı ayrı bir güvenlik ve hash değerinin olduğu ve bu değerle bir sonraki bloğa bağlandığı bir teknoloji. Bir veri girişi yapıldıktan sonra o verinin değiştirilmesinin artık ağdaki diğer kullanıcılar tarafından da onaylandığı için değiştirilemediği, bu yönüyle değiştirilemezlik ve şeffaflık ile güven ortamını sağlaması. Blockchain böyle bir teknoloji.

Blockchain teknolojisinde ortaya çıkan temel özellikler Dağıtık yapı her bir verinin bir kopyasının ağda bulunan binlerce düğümde kayıt altına alınmış olması. Bir diğer temel özelliği saydamlık özelliği; ağda yapılan bütün işlemlerin takip edilebilmesine imkan sağlaması ve değiştirilemezlik ilkesi, blok zincirde üretilen verilerin üzerinde işlem yapılmasını engellemesi. Bu özellikleriyle blockchain yeni internet yapısının bel kemiği olmaya aday bir oldukça önemli bir teknoloji. Ve biz bu trendi kaçırmamak zorundayız.

Askeri teknolojilerde hangi alanlarda kullanılmakta blockchain? Gizli ve kritik bilgilerin depolanması ve korunması, haberleşmenin bütünlüğü, gizliliği ve doğruluğu, şebeke merkezli muharebe, bütünleşmiş hava savunma sistemleri, küresel tedarik zinciri etkinliğinin artırılması. Bu teknoloji en çok tedarik zinciri alanında kullanılır. Blockchain ile güvenli veri iletimi, merkezi olmayan komuta ve kontrol, tedarik zinciri yönetimi, hesap verilebilirlik ve etik üzerindeki uygulamalarını da görebiliyoruz. Yine blockchain teknolojisinin robotik ve savaşın geleceği açısından da bize kattığı ve katacağı özellikler var. Malumunuz bu otonom silah sistemleri, savaşta insani katılımı en aza indirerek yeniden tamamlıyor. Robotik askerler ve otonom silah sistemleri, savaşta insani katılımı en aza indirerek yeniden tanımlıyor. Blockchain ile robotik teknolojilerin birleşimi, bu sistemlerin güvenilirliğini ve verimliliğini artıracaktır.

Örneğin, Güney Kore sınırında kullanılan otonom robotik savunma sistemleri, blockchain ile desteklendiğinde daha güvenilir hale getirilebilir ve kendi projelerinden bunu takip ediyoruz. Manipülasyona dayanıklı kimlik yönetimi, gelişmiş iş birliği ve haydut davranışların önlenmesinde blockchain teknolojisinin getireceği önemli avantajlar var. Manipülasyona dayalı kimlik yönetiminde özellikle Çin, askeri robotları blockchain tabanlı kimlik yönetme ve donatma ile ilgili bir projeye sahip.

Manipüle edilecek saldırıları blockchain ile önlemeyi hedefliyor. Yine iş birliği noktasında baktığımızda bu otonom sistemler ortak bir ağla güvenli bir şekilde yönetilebilir

Her robot veya dron, yalnızca yetkilendirilmiş parametreler içinde çalışmasını garanti eden benzersiz bir blockchain kimliğine sahip olacağından, sistemlerin yalnızca yetkilendirilmiş kullanıcılar tarafından kontrol edilmesini garanti eder. Çin, askeri robotları blockchain tabanlı kimlik yönetimiyle donatmayı hedefliyor. Otonom sistemler, ortak bir blockchain üzerinde hızlıca istihbarat paylaşabilir ve dinamik savaş ortamlarında stratejilerini birlikte ayarlayabilir. ABD Hava Kuvvetleri, otonom dron sürülerinin blockchain üzerinde gerçek zamanlı olarak bilgi paylaşımını test etmektedir. Bu sistemler, sürü içinde koordinasyonu artırarak hedeflere daha etkili bir şekilde saldırabilir.

Jeopolitik ve Güvenlik etkiler açısından, yalnızca savaş alanı değil küresel ittifak dinamikleri ve ittifakları da etkileyebilir. Blockchain, hava gücünü uzay, siber uzay ve kara operasyonları gibi diğer alanlarla birleştirerek güvenlik doktrinlerini yeniden şekillendirme ve jeopolitik stratejileri yeniden tanımlama gücüne sahip hayati bir teknolojidir. Bu noktada Teknolojik silahlanma yarışı, koalisyon operasyonları ve siber güvenlik önceliği gibi jeopolitik ve güvenlik etkileri gibi başlıkları incelemek mümkün. Blockchain, hava gücünü uzay, siber uzay ve kara operasyonları gibi diğer alanlarla birleştirerek güvenlik doktrinlerini yeniden şekillendirme ve jeopolitik stratejileri yeniden tanımlama gücüne sahip hayati bir teknolojidir. Gelecek uygulamalarda angajman kuralları için akıllı sözleşmeleri getirebileceğini, tahmin analitiği ve yapay zekâ noktasında etkileri gelecek trendler arasında olacak, küresel yönetim alanında da blockchain etkilerini görmek mümkün olacaktır.

Hava kuvvetleri için blockchain uygulamalarında ABD Hava Kuvvetleri projeleri önemlidir. ABD Hava Kuvvetleri, SIMBA Chain ile iş birliği yaparak 3D baskı ile üretilen uçak parçalarının izlenebilirliğini sağlamak ve tedarik zincirindeki güvenliğini artırmak için blockchain kullanıyor. Bu proje; kritik parçaların sahteciliğini önleyip, süreçlerin şeffaflığını artırmayı hedefleyen bir uygulamadır.

ABD Hava Kuvvetleri Stratejik Teknoloji Odak Girişimi (STRATFI) kapsamında, SIMBA Chain'e 30 milyon dolarlık yatırım yapmıştır. Bu fon, blockchain çözümlerinin geliştirilmesine ve tedarik zinciri yönetiminin güçlendirilmesine yönelik projeleri finanse etmektedir. Bu teknoloji, yalnızca Hava Kuvvetleri için değil, aynı zamanda diğer askeri birimler ve lojistik süreçler için de kullanılmaktadır.

ABD Hava Kuvvetleri blockchain teknolojisine yönelik teorik yaklaşımını bir kenara bırakıyor. Bu kapsamda SIMBA Blocks'un kullanımı ile birlikte Digital Blockchain Budgeting Accountability and Tracking (DiBaT – Dijital Blockchain Bütçeleme Muhasebesi ve İzleme) ismi verilen projede fon hareketlerinin takibi, tedarik zincirindeki akışın dolarize edilmesi gibi kritik öneme sahip ihtiyaçların karşılanması hedeflenmektedir. ABD Hava Kuvvetlerinin casusluk çiplerinin askeri teçhizata girmesine izin vermeyecek bir blok zincirinin geliştirilmesi üzerinde çalışmalar başlatması, DARPA'nın, verimlilik, sağlık ve güvenlik konusunda savaş alanı operasyon yönetimi sektöründe yenilikler getirmek için blockchain ile deneyleri, NATO'nun, güvenli askeri tedarik ve izlenebilir lojistik tedarik hizmetlerini sağlamak için blockchain kullanması da takip ettiğimiz örneklerden.

Ayrıca savunmada savaş operasyonlarının yönetimi, lojistik ve tedarik zincirinin yönetimi, otonom sürü dronların yönetimi ve sınır koruması olarak 4 ana başlıkta da fırsatlar sunacaktır. Hava Kuvvetleri'nde aviyonik sistemler ve onların güvenliği açısından da blockchain teknoloji fırsattır. Amerika Birleşik Devletleri biliyorsunuz geçtiğimiz günlerde bir yapay zekâ ile donatılmış bir uçağı (F-16) ile uçurdu. Yapay zekâ tabanlı savunma sistemlerinin blockchain kullanarak güvence altına alınması, DARPA'nın araştırma alanlarından biridir. Yapay zekâ destekli otonom sistemlerde yapay zekâ sistemlerinin blockchain ile entegre edilerek güvenlik ve izlenebilirlik sağlanması hedefleniyor. Yapay zekâyı blockchaini mutlaka entegre etmeliyiz.

İnsansız hava araçları, savaş alanındaki verileri toplar ve analiz eder. Bu verilerin güvenli bir şekilde saklanması ve kaydedilmesi için blockchain teknolojisinin kullanılması gerekir. Blockchain ile bu veriler merkezi olmayan bir yapıda şifrelenebilir ve operasyonların güvenliği artırılabilir.

NATO, siber savunma girişimleri, yapay zekâ destekli siber saldırı tespit sistemlerini geliştirirken, blockchain teknolojisini de bu sistemlerin güvenliğini artırmak için kullanmaktadır. Lockheed Martin ve Boeing gibi Savunma Firmaları, yapay zekâ ve blockchain teknolojilerini savunma sistemlerine entegre etmeye başlamışlardır. Özellikle uçak ve hava sistemlerinin bakım ve operasyonel süreçlerinde blockchain tabanlı çözümler geliştirilmektedir. ABD Hava Kuvvetleri, blockchain teknolojisini uçak bakım yönetiminde ve lojistik süreçlerinde nasıl kullanılabileceğine dair projeler yürütmektedir

Bu projelerde, uçak parça değişim ve bakım süreçlerinin izlenebilirliği artırılarak operasyonel verimlilik sağlanmaya çalışılmaktadır. Gelecek Perspektifinde Güvenlik ve Siber Savunmaya baktığımızda; hava kuvvetleri, gelecekte güvenliğini sağlamada ve siber tehditlere karşı savunmada yapay zekâ ve blockchain teknolojilerinden faydalanmak zorundadır. Özellikle siber güvenlik alanında bu iki teknolojinin entegre edilmesi, Hava Kuvvetleri'nin dijital altyapısının korunmasında kritik bir rol oynayacaktır.

Yapay zekâ, siber saldırıları tespit etme ve engelleme konusunda önemli bir araç iken Blockchain teknolojisi ise bu saldırıların izlenebilirliğini ve kayıt altına alınmasını sağlayarak siber güvenlik açısından ek bir koruma katmanı sunar. Savunma sanayiinde geliştirilen Yapay Zekâ tabanlı projeler, hava savunma sistemlerinin otomatik olarak tehditleri analiz edip savunma önlemleri almasının önünü açacaktır. Yerli yapay zekâ ve blockchain ile bu sistemler daha güvenli hale getirilebilir.

Zaten bu teknolojilerden geri durmuyoruz ve ileriye de götürmeliyiz. Türk Havacılık ve Uzay Sanayii A.Ş. (TUSAŞ) gibi önemli kuruluşlar, yapay zekâ ve blockchain teknolojilerini entegre eden projeler üzerinde çalışmaktadırlar. TUSAŞ tarafından geliştirilen Millî Muharip Uçak projesinde yapay zekâ tabanlı savaş yetenekleri üzerinde çalışmalar yapılmaktadır. Blockchain ile uçuş verileri ve mühimmat yönetimi güvenli bir şekilde kayıt altına alınacaktır. Blockchain teknolojisinin hava gücü, otonom sistemler ve robotik ile birleşimi, yalnızca bir inovasyon değil, modern savaş doktrinlerinin kökten değişimidir. Karabağ Savaşı gibi örnekler, bu teknolojilerin savaşın seyrini nasıl etkilediğini gözler önüne sermektedir.

Güvenli, verimli ve etik operasyonlar sağlayan bu yenilikler, aynı zamanda jeopolitik dinamiklere yön vermektedir. Bu teknolojilere yatırım yapan ülkeler, geleceğin savaşlarında ve küresel istikrarın sağlanmasında belirleyici bir rol oynayacaktır. Blockchain'in otonom sistemlerle entegrasyonu, modern hava gücünü teknolojik olarak geliştirirken güvenlik ve etik sorunlarına da çözüm sunmaktadır. Artık bu teknolojileri benimseyip benimsememekten ziyade, ne kadar hızlı ve etkili bir şekilde uygulayabileceğimiz sorusuyla karşı karşıyayız. Geleceğin hava gücü ve savaş sistemleri bu yenilikçi teknolojiler üzerinde inşa edilecektir. Bu teknolojiler artık kompleksleşen sistemler ve entegrasyonu elzem noktadadır. Bu projelerde, uçak parça değişim ve bakım süreçlerinin izlenebilirliği artırılarak operasyonel verimlilik sağlanmaya çalışılmaktadır.

Gelecek perspektifinde güvenlik ve siber savunmaya baktığımızda; hava kuvvetleri, gelecekte güvenliği sağlamada ve siber tehditlere karşı savunmada yapay zekâ ve blockchain teknolojilerinden faydalanmak zorundadır. Özellikle siber güvenlik alanında bu iki teknolojinin entegre edilmesi, Hava Kuvvetleri'nin dijital altyapısının korunmasında kritik bir rol oynayacaktır.

Blockchain teknolojisinin hava gücü, otonom sistemler ve robotik ile birleşimi, yalnızca bir inovasyon değil, modern savaş doktrinlerinin kökten değişimidir. Karabağ Savaşı gibi örnekler, bu teknolojilerin savaşın seyrini nasıl etkilediğini gözler önüne sermektedir. Güvenli, verimli ve etik operasyonlar sağlayan bu yenilikler, aynı zamanda jeopolitik dinamiklere yön vermektedir. Bu teknolojilere yatırım yapan ülkeler, geleceğin savaşlarında ve küresel istikrarın sağlanmasında belirleyici bir rol oynayacaktır. Blockchain'in otonom sistemlerle entegrasyonu, modern hava gücünü teknolojik olarak geliştirirken güvenlik ve etik sorunlarına da çözüm sunmaktadır. Artık bu teknolojileri benimseyip benimsememekten ziyade, ne kadar hızlı ve etkili bir şekilde uygulayabileceğimiz sorusuyla karşı karşıyayız. Geleceğin hava gücü ve savaş sistemleri bu yenilikçi teknolojiler üzerinde inşa edilecektir. Bu teknolojiler artık kompleksleşen sistemler ve entegrasyonu elzem noktadadır.

İvedilikle devreye almak, entegre çözüm geliştiren ekiplerim komuta, kontrol haberleşme, elektronik harp, keşif, RF, ısı, optik, akustik algılama, sensörler, harp yönetim metodoloji, silah sistemler konularını iyi bilmesi gerekiyor. Ama tüm bunları yapabilmesi için, bizim özellikle temel bilimlere hâkim olmamız gerekiyor. Matematik, fizik, kimya biyoloji alanlarının daha iyi bilinmesi ve eğitilmesi gerekiyor. Millî güvenlik meselesi olarak temel bilimlerin ele alınması gerektiğini belirtmek istiyorum. Teşekkür ederim.

SORU 1: Sunumunuzda insansız hava araçlarıyla stratejik üstünlük kazanıldığını söylediniz, taktik alanda belki bir insansız sistemlerle kuvvet çarpanı olarak düşünebiliriz ama stratejik üstünlük nasıl kazanıldı? Bir de 'otonom sistemler ile hava sistemlerinde yeni bir paradigma' dediniz. Bu paradigmada muharip sistemleri, insanlı sistemleri nerede görüyorsunuz?

CEVAP: İnsansız hava sistemlerinin stratejik üstünlüğünden kastım ve referansım, etkili iletişim halindeki veri paylaşımı ve verinin güvenliği noktasında. Stratejik üstünlükten kasıt, savaşın gidişatının değiştiği bir alana evrilmesi ve blockchain teknolojisinin buna katkısı. Askeri anlamda bir stratejik üstünlük değildi kastım. İnsanlı sistemler konusunda ise, insanlı sistemleri yakın gelecekte zaten devre dışı bırakma şansınız yok. Teknoloji insanla var. Ama bu teknolojiler insanın işini kolaylaştıracak. Aslı bizim baktığımız nokta bu. Özellikle hava gücü noktasında, blockchain teknolojisiyle biz bu iletişimi nasıl güvenli hale getirebiliriz tarafındayız. Malumunuz şu anda en büyük problemlerden biri GPS veya sinyal karıştırma olayları. İnsanlı hava araçları içinde büyük problemlerden biri bu. Ve bu bölüm için de blockchain teknolojisi içeren çalışmalar var. Hava Kuvvetleri en fazla veri üreten yapı. Dolayısıyla anlık verilerle depolanan verilerle birlikte kullanım söz konusu. Daha güvenli bir şekilde nasıl saklanacağı, transferinde nasıl güvenli olacağı ve verinin bütünlüğü noktasına önem veriyor bu teknoloji. Bizim yapay zekâlı sistemlere blockchain tabanlı sistemleri entegre etmemiz, insanlı araçların da anlık farkındalık noktasındaki hassasiyetini bu teknolojiyi kullanması gerekiyor. Bu dağıtık ve merkeziyetsiz yapı bize bu güvenliği sağlayacaktır.

SORU 2: Blockchain'in çok farklı kullanım alanları var ama yönetimi zorlaşacak yapılarda kullanmak mümkün. Fakat verilerin paylaşımı ya da savaş ortamındaki yapının daha iyi hale getirilmesi noktasında pek mümkün gözüküyor. Bu konudaki fikirleriniz nedir?

CEVAP: Bunun üzerinde çok sayıda uygulamalar ve projeler var. Özellikle DARPA'nın, Simbablok ve Simbachain üzerinde projeleri var. Merkeziyetsiz ama Blockchain'in merkeziyetsiz yapısı, kendisinden kaynaklı bir yapı değildir, dağıtık özelliğinden kaynaklıdır. Dolayısıyla hava araçlarının, insansız hava araçlarının da dağıtık yapısı var. Uygulanabilirliği mümkün değildir konusuna katılmıyorum, mümkündür. Üzerinde çalışılması gerekir ve çalışılıyor. Kuantum destekli blockchain ile de ilerleyen projeler var. Kuantum alanı da blockchain ile entegre ediliyor. Bu işe adım atmamak treni kaçırmak olur. Blockchain'in dağıtık yapısından kaynaklı merkeziyetsiz yapı bu işe elverişliliğinin mümkün olduğuna dair projeler de mevcut. Kuantum alanı da ayrı bir şekilde Blockchain ile entegre ediliyor. Bu işe adım atmamak treni kaçırmak olur. Blockchain'in dağıtık yapısından ve merkeziyetsiz yapısından kaynaklı yapısı, bu işe elverişliliğini gösteriyor.



Dr. Marc LACY
LANCASTER ÜNİVERSİTESİ
İNGİLTERE

Merhabalar, genellikle benim ülkemden insanlar, ülkenize sadece hava çok sıcak olduğunda geliyor. Bu yüzden ülkenizin kışın nasıl olduğu görmek büyük ayrıcalık ve buraya gelmek bana ülkenizdeki yemeklerin gerçekten dünyadaki en iyi yemek olduğunu hatırlatıyor. Burada bulunmaktan çok mutluyum. Yaptığım iş açısından Lancaster Üniversitesi'nde ders veriyorum, buradaki öğrencim Waqas Heider

gibi öğrencilerime danışmanlık yapıyorum. Ve kendimi bir savunma antropoloğu olarak görüyorum. Evet ben bu ülkeden değilim ve vaktimi dünyanın her yerindeki ordularda görev yapan ilginç insanlarla konuşarak geçiriyorum, askeri dünya ile akademik dünya arasında ilginç konuşmalar ve diyaloglar kuracak ilginç bir alan oluşturmaya çalışıyorum ve bu konuda neler yapılabileceğini konuşmaya çalışıyorum.

Gelecekteki çatışmaların teorilerini ortaya koyan kitabımda tartıştığım bazı şeylerden biraz bahsediyorum. Kitabımın başlığı 'Gelecekteki Çatışmanın Teorileştirilmesi : 2049'a Kadar Savaş.' Kitabın ismi, Çin'in Amerika'yla rekabet etmek istediği iddia edilen yıla da gönderme yapıyor. Amerika askeri güç açısından eleştirmek için evet ama kitap bu tarihin her iki tarafını da ele alıyor. Bu yüzden önümüzdeki yıllarda bu savaşları ve savaşları, ulusları, uluslararası ilişkileri şekillendirebilecek eğilimlere bakıyorum. Kitabın ilk bölümü, Elon Musk'ın en sevdiği yazar olan bilim kurgu yazarı Douglas Adams'dan bir alıntıdan geliyor; 'aptal oyunu.' Adams, temelde gelecek hakkında düşünmenin bir aptal oyunu olduğunu söylüyor. Evet geleceğin ne olacağını düşünmek aptalca ama bunu yapmak zorundayız. Ben de yapacağım, bu konuşmada yapacağım şey gelecek için düşünmenin ve planlamanın zorluğu hakkında birkaç soru sormaya çalışmak, gelecek hakkında düşünmek de bir aptal oyunu.

Ben, çoğalma çağında yaşadığımız fikriyle çok ilgileniyorum. 1990'larda uluslararası ilişkiler okuyan bir öğrenciyken, Fukuyama, tek tür bir gelecek olduğunu ve bunun temelde liberal demokrasi olduğunu söylüyor.

Ben gelecek hakkında düşündüğümde bu hiç eleştirisel değildim.

Peki, tarihin sonu bu nasıl sonuçlanacak? Çin'in yükselişini düşünmüyorduk. Şimdi bizi vuracak olan bu yeni teknolojik hızlanma çağını düşünmüyorduk, saftık ve gelecek hakkında düşündüğümüzde her zaman öyle kalacağız. Gelecek hakkında düşündüğümüzde naif olabiliriz, 1990'larda Birleşik Krallık ve Amerika'daki bir üniversitede okuduğumuzda da çok saf olduğumuzu düşünüyorum. Bu yüzden benim kilit noktam şu ki; aslında çoklu geleceğin, birden fazla olasılığın olduğu bir zamanda, birden çok geleceği yaşıyoruz. Bu bir çoğalma zamanıdır ve bu çoğalmanın ne anlama geldiğine dair bazı örnekler vermek gerekirse, daha önce gördüğümüz hiçbir şeye benzemeyen aktör ve aktörlerin çoğalacağı bir zamanda yaşıyoruz ve bir gelecek görüyoruz.

Örneğin Elon Musk'ın bir küresel bir aktör olduğunu söyleyebilirim. Bu yüzyılın ortasına geldiğimizde çeşitli alanlarda küresel etkiye sahip olacak 10 Elon Musk figürünü görebiliriz, Yapay Zekâ, neuralink, uzay gibi alanlarda. Ve bu isimler belki Çin'den, belki Hindistan'dan belki de düşünmediğimiz yerlerden birden fazla görecekiz. Açık teknolojik inovasyon çağında, aynı dönemde yaşayan çok sayıda devlet dışı aktör görecekiz. Bu aktörler çok sofistike, akıllı ve muhtemelen tehlikeli şeyleri yapabilecekler. Bu yüzden çok farklı türlerde, farklı yetenek türlerine sahip aktörlerin farklı türlerde şeyler yapabileceğini düşünmelisiniz. Uzayda, deniz altında, metaverse alanında yeni mimari alanlar görecekiz.

Örneğin Suudi Arabistan'da inşa edilen Neom projesi yeni şehir türlerine dair yeni bir proje mi? Hakkında konuşulan bilişsel bir savaş olan nöro savaş, savaşın yeni bir alanı mı olacak?

Ve belki de bu bilişsel savaş alanını da bir askeri faaliyet olarak görmemiz gerekecek. Bunun gibi şu anda bir askeri faaliyet olarak görmek zorunda kalmadığınız yeni alanlarda askeri faaliyet göstermeniz gerekecek. Bu alanlarda faaliyet gösterdikçe ister insansız hava araçları ister robotlar ister siber olsun, kuantum veya nano teknoloji gibi alanlara yönelik araçların çoğalması söz konusu olacak.

Herhangi bir kuruluş için işi çok zorlaştıran çok sayıda yeni araç ve yeni dünya olacak. İngiltere'deki üniversitelerde öğrencilerin yapay zekâyı nasıl kullandıklarına dair büyük sorunlarla karşı karşıyayız ve uyum sağlamak zorundayız. Ve askeri bir organizasyon da benzeri bir şekilde bunun gibi daha fazla teknoloji ve araca ayak uydurmak zorunda olacak, bu aynı zamanda büyük bir organizasyon gerektiriyor, planlama gerektiriyor.

Teknolojik güç, beraberinde insani yetenek ve güç de istiyor. Çatışmanın ayrıntınlığı ya da ayrıntı düzeyi dediğim ve kitapta da bahsettiğim şey; temel şekil olarak her şekil ve boyutta teknolojilere sahip olacağız. Örneğin farklı boyutlardaki insansız hava araçlarının olasılığı ve böyle bir çatışma alanının, çatışma coğrafyasının ne şekilde değişeceğini düşünüyorum. Açıkçası taktiklerin çoğalması, hibrit savaşta gördüğümüz gibi tehditlerin çoğalması ve aynı zamanda ekolojik tehditlerin çoğalmasını da göreceğiz. Ve bununla birlikte çatışmaların etkilerinin ne olacağını bilmiyoruz. Mesela iklim değişikliğinin gezegende nelere yol açacağını bilmiyoruz ama ben bunun yıkıcı ve oyunun kurallarını değiştiren sonuçları olabileceğini düşünüyorum.

İngiltere Ordusu'ndan biri sizlerin bildiğiniz bazı teknolojilerden bahsetti. Örneğin tankların, savaş araçlarının bazı iklim koşulları için tasarlanmadığını anlatmıştı ve bunun oluşturduğu problemlerden. Teknolojiniz olası iklim koşullarına uygun değilse bazen işe yaramayabilir. Farklı siyasi geleceklerin çoğalması hakkında konuşabiliriz, çok kutupluluğun savaş ve barış açısından oluşturacağı çatışma türleri ve son olarak insan vücudunun dönüşümü anlamına gelecek, insan olmanın ne anlama geldiğine dair geleceklerin çoğalması var.

Örneğin neuralink ne anlama gelecek? Cyborg, Robotik olanaklar gibi sibernetik organizma fikri bizleri nasıl değiştirecek? Bunların gelecekteki askerin et ve kan düzeyinde insanı nasıl değiştireceğini biliyor muyuz? Özetle çok sayıda olasılıktan bahsediyoruz ve ufukta ne olduğunu çözmeye çalıştığımız bir aptal oyunu. İşte bağlam bu, zorluk bu ve tabii ki nereye gittiğimizi anlamamanın birçok başka yolu var ve konuşabileceğimiz başka unsurlar da var. Ama hayati önem taşıyan iki tür organizasyonel sorun var, geleceğin askeri konusunda düşünürken.

Yeni Dünya, Yeni Savaş ve Yeni Savaşçı'dan bahsederken, bunu çoğullaştırdım ve Yeni Dünyalar, Yeni Savaşlar ve Yeni Savaşçılardan bahsetmek gerektiğini söylüyorum. Hangi dünyalarda, hangi savaşlar ve hangi savaşçılarla karşılaşacaksınız? İşte bu soruyu cevaplamanın bence iki yolu var. Nassim Nicholas Taleb'in The Black Swan kitabı (Siyah Kuğu – Olasılıksız Görünenin Etkisi) Amerika ve İngiltere'de çok etkili olmuştur. İngiltere'de Savunma Bakanlığı ile birlikte bu tarz bir etkinliğe birlikte gidiyorsanız "Siyah Kuğu" onlar için çok önemlidir.

Temelde siyah olan sizin olayınızdır, yani geldiğini görmemiz gereken bir olay ama geleceğini göremediğiniz, öngörülemeyen bir olay ve bu yüzden Amerika'da büyük bir tartışma var, 'Siyah Kuğu' nedir? 11 Eylül Amerika için bir 'Siyah Kuğu' idi. Ama pandemi bir 'Siyah Kuğu' değildi, çünkü önceden geniş çapta tartışılmıştı. Yani öngörmeniz gereken olaylar var ama siz görmezden geldiniz. Taleb'in bu kitaptaki argümanı, içinde yaşadığımız dünyanın birbirine bağlı yapısı dolayısıyla 21. Yüzyılda daha fazla 'Siyah Kuğu' olayı yaşanacak.' Taleb'in vurguladığı nokta, kuruluşların genelde tünel açma denilen kavram yüzünden 'Siyah Kuğu'yu görmemesidir. Kuruluşlar, bir tür tünel görüşü geliştiriyorlar. Örneğin bir üniversitede bürokratik bir organizasyonda çalışıyorum ve biz sıklıkla önemli insanları bir araya getirmek için çoğu zaman çılgınca bir plan yapıyoruz, işleri yapmanın yeni yollarını oluşturmak için, çünkü üstteki insanlar alttaki gerçeği anlamıyorlar.

Her zaman organizasyonun nasıl çalıştığını anlamak isteyen insanlara, nasıl çalıştığını anlamak istiyorsanız, sekreterleri ve organizasyonun iletişim elemanlarıyla görüşmelerini söylüyorum. Çünkü en tepedeki insanlar güzel fikirlere ve yeni iş felsefelerine sahip olabilirler ama gerçekliğe dair bu kadar ayrıntılı bir anlayışa sahip değiller. Bürokrasiler, organizasyonlar ve kuruluşların sorunları anlamak için daha ayrıntılı bir yaklaşıma izin vermesi gerektiğini düşünüyorum. Örneğin İngiltere Savunma Bakanlığı için sorunun bu çokluluk olduğunu biliyorsunuz ve soru şu buna nasıl ayak uyduracaksınız? Tüm bu yeni teknolojik ivme alanlarının iyi anlaşılması şarttır, bu ister yapay zekâ olsun ister diğer alanlar olsun ya da şirketler, trendler veya bilimler, hepsinin iyi anlaşılması en önemli bölümlerden.

Bence Geleceğin Askeri için plan yaparsanız şunları yapmalısınız; bu tür tartışmalara izin veren süreçlere sahip olduğunuzdan emin olmalısınız. Evet sadece üst yönetimle konuşmak isteyebilirsiniz, evet ama konu siber olunca, ne yapılacağı hakkında düşünceleri için 20 yaşındaki bilgisayar korsanlarını getirmek gerekebilir. Trendleri 25-30 yaş üstü herkesten çok daha iyi anlayacaklar ve uyum sağlayacaklar. Yeniliklere ayak uydurmanın ne kadar zor olduğunu biliyorsunuz. Söylemek istediğim ikinci nokta ise savaşta hız ve savaşta hızlanma hakkında çok şey yazan Fransız yazar ve filozof Paul Virilio'dan geliyor. 21. Yüzyılda savaşın değiştiğini, savaşın barış zamanında gerçekleştiğini, saf savaşın ne savaş ne de barış olduğunu söylüyordu ve bunu saf olmayan saf nitelmesiyle yapıyordu.

Şimdi gri bölge veya hibrit savaş gibi kelimelerle niteleniyor ama onun argümanı, 21. Yüzyılda teknolojik toplumlumuzdaki en büyük zorluklardan birinin teknolojik kaza olacağı yönünde. Onun argümanı herhangi bir yeni teknolojinin yeni bir tür kaza ve muhtemelen küresel kaza ya da kazalara yol açabileceği. İçinde yaşadığımız dünyada çok sayıda teknolojik şirket var ve size işleri nasıl iyileştireceğine dair iyimser vizyonlarla satılan birçok yeni teknoloji var. Ama Virilio, bu yeni teknolojinin oluşturabileceği kazanın ne olduğuna bakmaya yönlendiriyor. Çünkü her zaman 'Siyah Kuğu' olacak ister askeriye ister üniversite olsun tüm kuruluşların satın aldığı yeni teknolojilerden kaynaklanan kazalar olacak, işleri verimli kılsın diye başladığınız süreçlerde oluşabilecek kazalar hakkında düşünmenin yollarını da süreçlerinize dahile etmelisiniz. Çünkü ilerleme vaat eden her yeni teknoloji, yeni ve daha önce karşılaşmadığınız türden bir kaza potansiyeli taşıyor. Bu tarz endişeler gelecekte daha önemli olacaktır.

Yapay zekâ ve insan makine iş birliğinin inanılmaz derecede ikilik oluşturacağını görüyoruz. Yapay zekâ tarafında ilerleme sağlanıyor ancak aynı zamanda inanılmaz tehditler de var. Öğrencilerime sohbet GPT'nin yazmak için kullandığı yapay zekâ ile intihal konusunda büyük bir problemimiz olduğunu söyleyerek geçiriyorum. Evet yazmayı kolaylaştırıyor ama intihal yapan insanları bulmamızın yollarından biri de yapay zekâ. Örneğin geçen yıl bir akademisyenimizin hiç yazmadığı bir kitap için yapay zekâ tarafından üretilen bir referans vardı. Şimdi bu hatanın askeri bir boyutunu düşünmeliyiz.

Buradaki güven meselesini düşünmelisiniz. Eğer insan makine ile ekip oluşturmayı düşünüyorsanız, oluşabilecek bu kazayı ve güven problemini de göz önünde bulundurmalısınız. Terimlerle kastettiklerime aslında en önemli örnek Lübnan'daki çağrı cihazı saldırısı. Dronlar ve yapay zekâ ile ilgili, bu olaylar hakkında düşündüklerimin çoğunu özetleyen bir alıntı var. 1990'ların sonunda Çin'de yazılmış 'Sınırsız Savaş' isimli kitapta temel olarak Çin Ordusu'ndan bazı kişiler tarafından, gelecekteki savaş trendleri ve bilgi savaşının teknolojileri nasıl değiştireceğine dair bir şeyler yazılmıştı. Bu kitapta kendi kitabımda da yer alan bir alıntı var ve Çinli yazarlar; "O zaman söylememiz gereken şey şu olmalı; 'Yeni konsept sıradan insanların ve askerlerin kendine yakın sıradan şeylerin aynı zamanda savaşa girmek için kullanılacak silahlara da dönüşebileceği gerçeği karşısında büyük şaşkınlık yaşamalarına sebep olacaktır. İnanıyoruz ki, bazı sabahlar şaşkınlıkla uyanıp, bu küçük şeylerin oldukça büyük bir silah olduğunu keşfedeceklerdir. Pek çok nazik ve iyi şeyin saldırgan ve ölümcül özelliklere sahip olduğunu şaşkınlıkla keşfetmek..."

Aslında bu satırlar günlük nesnelerin nasıl silah haline geldiğini anlatıyor. Bu yüzden tekrar "Siyah Kuğu" teorisine dönersek, günlük hayatta sizin için silah haline getirilebilecek ve size karşı kullanılacak şeyler nelerdir ve bunun yolları nelerdir, bunun üzerine de düşünmek gerekiyor. Uluslararası politikada Amerika ve Sovyetler Birliği'nin söz sahibi olduğu bir hiyerarşi vardı. Uzmanlık ve bütçelerini askeriye geliştirmek için ne yapacaklarını bildikleri bir hiyerarşi. Teknolojinin bunu zorlayıcı bir şekilde değiştirdiğini düşünüyorum.

Gelecekte askeriye gelecekte düşmanınızın hangi gerçeğiyle başa çıkmak zorunda kalacağını bilerek hazırlanmalısınız. Örneğin mücadele edeceğiniz durum o kadar dinamik olacak ki, uyum sağlamanız ve tepki vermeniz konusunu saatlerce tartışabilirsiniz. Çünkü rakibiniz daha önce açık teknolojik yenilik olarak bahsettiğim şeylerden en iyi şekilde yararlanacak. Açık teknolojik yeniliklerin ortaya çıktığı bir dönemde nasıl kullanıldıklarını dron teknolojileri üzerinden dünya çapında konuşuyoruz. Ucuz, güçlü, hızlı hale geldiklerinde nasıl kullanılıyor görüyoruz.

Beni dinlediğiniz için teşekkür ederim.

SORU: Geleceğin savaş ortamlarında en belirleyici ne olacak?

CEVAP: Çok sayıda aktörün taktikleri var. Teknolojiler ve asimetrik boyut, bunlar Amerika'nın ve dünya güçlerinin büyük baş ağrısı. Yapay zekâ ile düşmanlarınız artık görünmez olabilecek, sizi şaşırtacak şeyler yapacak ve sizin sürekli dikkatli olmanız gerekecek, bu tüm aktörler için temel zorluk. Bundan sonraki savaş süreçleri kimin en çok orijinal olacağıyla ilgili, en farklıyı oluşturabileceğiyle ilgilidir. Çok sayıda farklı araca sahip olduğunuz kadar, bu kaotik ortamda en farklı neyi başarabileceğinizle ilgili olacak başarınız. Bu araçlara erişiminiz olmasıyla çok şey yapabilirsiniz ama bu onları en verimli ve orijinal şekilde nasıl kullanacağınızı bilmeniz anlamına gelmez. Yani yapılanmanız için de her şeyi kontrol ederek en iyi yapabilmeniz ister Pentagon olun ister uyuşturucu karteli olun, en önemlisidir. Ben, üreticiliğin, orijinalliğin ve en iyi yapabilmenin en büyük mücadelesi olduğunu düşünüyorum yeni savaş döneminin.



Muhammed Waqas HAIDER
LANCASTER ÜNİVERSİTESİ
İNGİLTERE

Merhaba değerli bayanlar ve baylar, saygın meslektaşlarım ve sayın yetkililer, Dr. Mark Lacy, 'Gelecekteki Çatışmanın Teorileştirilmesi: 2049'a Kadar Savaş' kitabında, gelecekteki çatışmayı teorileştirerek tartışıyor. Gelecek en çok muhtemelen bir çoğalma zamanı olacak. Taktiklerin, arazilerin, teknolojilerin ve aktörlerin çoğalma zamanı. Savaşların patlak verdiği zaman muhtemelen farklı aşamaların

veya eski ile yeni savaş zamanlarının zorlukları ve ihlalleriyle dolu karmaşık bir ortam olacaktır. Denenmiş ve denenmemiş, deneysel ile tecrübe edilmiş karışık zorlukların birleştiği ortamlar. Taktiklerin ne kadar yenilikçi olduğunun ve mümkün olabilirliğinin, savaş sahasındaki test edilebildiği, etkisinin sürprizlere açık olduğu ortamlar olacak. Yüzyıllarca, savaşın yürütülmesi ve yenilikler tanımlanıyor. Antik Yunanda, Orta çağ Avrupası'nda, süvariler veya tanklarla...

Her teknoloji sıçraması yalnızca savaşların nasıl yapıldığını yeniden şekillendirmekle kalmadı, aynı zamanda doktrinleri, stratejileri yeniden yazdı ve hatta jeopolitiği yeniden şekillendirdi. Günümüzde artık sadece insan kararlarının en hızlı ve doğru yeterli olmadığı, gökyüzünün dron sürüleriyle dolu, yüksek iletişim ağları ve iletişimin bulunduğu, değişken teknolojilerle geliştirilmiş askerlerin bulunduğu bir savaş alanı hayal edin. Teknolojik dış iskeletler, artırılmış gerçeklik ekranları, yalnızca mermilerin değil verilerin de hayatta kalmayı etkilediği ortamları fark edin ve bunun uzak bir gelecek olmadığını fark edin. Rusya ile Ukrayna arasındaki savaşın gerçekliği, teknolojik çatışma ortamının geldiği noktanın en önemli göstergesi haline geldi. Dünyadaki gelişmiş savaş alanı, yeniliğin yıkımla çarpıştığı bir deneme alanıdır. Savaşların nasıl yapıldığını ve kazanıldığını yeniden tanımlar. Bu savaş, askeri öğretileri yeniden şekillendiren ve geleceği etkileyen yıkıcı teknolojileri test etmek için küresel bir laboratuvar niteliğinde.

Bu savaştaki örnekler, askeri doktrinleri yeniden şekillendirir ve gelecek teknolojilerin geliştirilmesindeki global stratejileri de etkiler.

Bu savaştaki stratejiler, yıkıcı teknolojilerin sadece taktikleri değiştirmesine değil, aynı zamanda etkilerinin derin bir şekilde artmasına da sebep olmuştur. Ve savaşın etiği ile ilgili soruları da artırmıştır. Tartışmamız esas olarak savaşın 21. Yüzyılda nasıl değiştiğine dair bir arka plana sahip olma, ardından yıkıcı teknolojilerin boyutu ve bunların gelecek tartışmalarını nasıl yeniden şekillendirdiği üzerine. Geleceğin askeri programlarına genel bir bakış açacağım global ölçekte ve otonom askeri teknolojiler ile bütünleşmiş operasyon konseptinin günümüzde nasıl çalıştığını göreceğiz.

İnsanlık tarihi, savaş ve savaşların toplumun çeşitli düzeylerinde insan etkileşiminin ayrılmaz bir parçası. Kara ve deniz savaşları çok fazla deneyim kazandığımız savaş mücadelesinin birincil alanlarıydı, 20. Yüzyılın başında hava gücünün devreye girdiği ve teknoloji alanında çatışmalardaki oyun değiştirici şeklini gördük. Özellikle son zamanlarda da yeniden şekillendiğini gördük. Karabağ Savaşı'nda da sizlerin de etkinizi gördük. Şimdi uzaya ve sibere adım atıyoruz. Her ne kadar yeni olmasalar da artık çok hızlı tempoda gelişıyorlar. Ve teknoloji olarak gerçekten çok kapsamlı olan bu iki alana, diğerlerine göre daha fazla bağımlı hale geliyoruz.

21. Yüzyılda savaş nasıl değişiyor? 21. Yüzyılda Küresel Güvenlik ortamında devletten, devlet aktörlerinden hem de devlet dışı aktörlerden gelen zorluklarla karşı karşıya olduğumuza dikkat çekiyor. Ve karşı savaşlar için de birbirlerinin araçlarını benimsiyorlar.

Bu noktada David Kilcullen'in Ejderhalar ve Yılanlar kitabında, her iki kesimin de farklı kökenlerden gelmesine rağmen benzer yöntemler kullanarak çeşitli çıkarlar peşinde olduklarını söylüyor. Ejderhaların devlet aktörleri olduğunu ve devlet dışı aktörler olan yılanlardan ders aldıklarını savunuyor. Aynı zamanda yılanlarla savaşmak için ejderhaların savaş yöntemlerinin öğrenildiğini savunuyor. Devlet ve devlet dışı tehditlerin daha önce görmediğimiz kombinasyonlarını yeni alanlarda yaşadığımızı savunuyor. Böylece yeni savaş alanları ve türleri görüyoruz. Hiç görmediğimiz ve düşünmediğimiz yöntemlerle küresel savaş alanı karmaşılaşıyor.

Mark Galeotti de 'Her Şeyin Silahlandırılması. Yeni Savaş Yolu İçin Bir Saha Rehberi: 'Modern Dünyanın Eşi Görülmemiş Birbirine Bağlılığı' isimli kitabında, modern dünyanın benzeri görülmemiş bir şekilde birbirine bağlı olmasını vurgulamakta, yeniliklerin savaşlarda yeni yöntemlere olanak sağladığını belirtmekte, siber, uzay ve elektromanyetik spektrum yoluyla yeni savaş yöntemlerine olanak tanıdığını vurgulamaktadır.

Ben Zweibelson ABD Uzay Komutanlığı çalışmaları kapsamındaki tanımıyla savaşı modern olmayan, modern ve hayalet savaş olarak 3'e ayırıyor. Temel olarak ideolojiler, mitoloji inançlar ve kültürel sistem gibi kökenli çalışmalar üzerinden rasyonalizasyonun gerçekleşmesine dayanan modern öncesi savaşlar ve bu dönemi çatışmada doğaüstü rasyonalizasyon olarak adlandırıyor. Oradan modern savaşlar olarak gördüğümüz, insanların çeşitli araçlarla kararlar aldığı, savaş için insan merkezli rasyonelleştirmeye sahip dönem. Çatışmada insan merkezli rasyonalizasyon, yani devletler, sınıflar, yöneticiler, ekonomiler, teknolojiler, orduların savaş araçlarıyla insan kararlarının olduğu dönem ve bilimsel çağ olarak adlandırıyor. Bazıları halen bugünün modern savaşlar olduğunu savunuyor ama uzay, yapay zekâ, siber gibi özel kuvvetlerin kesiştiği savaş fantastik bir savaş alanı getiriyor. Bu, temelde teknolojik olarak insanları yeniden tasarlayan, gelişmiş savaş araçlarının yeniden tasarlandığı bir savaş olacak. İnsan kontrolünün içinde ama insan kontrolünün karar döngüleri içerisinde devreden çıkabileceği bir durum.

Yapay zekânın tehlikelerinden biri kabul edilen insanın karar döngüsünün dışına çıkıyor olması gibi bir dönem. Çünkü daha önce insanlar karar döngüsünün içindeydi ama şimdi döngünün dışına çıkma ihtimalleri var. Bu dönem, kendi amaçlarını insan kontrolünün ötesinde yeniden tasarlayan gelişmiş savaş araçları ile kavramsallaştırmanın olduğu 'hayalet savaş', teknolojik olarak türleri aşan dönem olarak adlandırılıyor. İnsanlar karar döngülerini kontrol etmiyor, teknolojik olarak güçlendirilmiş çatışmayı kavramsallaştırabiliyor ve buna ayak uydurabiliyor. Hayalet bir savaş, geleneksel ve geleneksel olmayan (düzenli ve düzensiz, simetrik ve asimetrik) her türlü savaştan farklı bir durumu beraberinde getiriyor.

Şimdi Rusya ve Ukrayna Savaşı'nda kullanılan yıkıcı teknolojilerin nasıl kullanıldığını aktarmak istiyorum. Bir uygulayıcı ve akademik bakış açısı olarak, değişen stratejiler üzerinde ne gibi bir etkiye sahip olduklarını göreceğiz. Savaşın değişen stratejileri ve boyutlarını Ukrayna çatışmasında çokça gördük. Ukrayna çatışmasında Türkiye tarafından üretilen insansız hava araçlarının çokça kullanıldığını gördük, TB2 Bayraktar özellikle savaşın ilk günlerinde çok önemli bir rol oynadı ve Rusya Hava Kuvvetleri bu tarz savunma araçlarını tespit etmek için savunmasını ve birliklerini yeniden konuşlandırmak zorunda kaldı. Bu teknoloji savaşların yapılanma şeklinin nasıl değiştiğini gösterdi. Karabağ Savaşı'ndan bu yana çok mesafe katedildi ve bunlar için farklı mühimmatlar geliştirildi. Rusya Kub-BLA adını verdiği yüksek hassasiyetli insansız hava aracı ve gezici mühimmat geliştirdi. Hedefi havada dolaşarak tespit edip saldıran bir teknoloji. Otonom silahlar açısından en son trendlerle uyumlu. Bu sistemler oyunu eşitliyor, daha küçük birliklerin daha büyük düşmanlara karşı rekabet gücünü artırarak, daha etkili bir şekilde karşı koymasını sağlayarak oyun alanını değiştiriyor. Bu teknolojiler ucuz ve yalnızca dost ülkelere sunduğumuz ve kolay erişilen şeyler haline geliyorlar.

Yapay zekâ sisteminin çatışma ortamında analiz ve hızlı karar döngüsüne dahil edilmesinde de Ukrayna Savaşı bir örnek oldu. Hangi alanda olursa olsun uydu ve keşif görüntüleri de dahil olmak üzere, gözlemleme, yönlendirme, karar verme ve düşman harekete geçmeden önce tedbir için, savaş alanı verilerini analiz etmek için yapay zekâdan yararlandı. Rus kuvvetlerinin imkanlarının hedeflenmesi ve karar alma süreçlerinin iyileştirilmesini sağladı. Ukrayna, savaş esirleri ve kayıplar da dahil olmak üzere Rus askerlerini, savaş esirlerini tanımlamak için Clearview AI'nın yüz tanıma teknolojisini kullandı.

Savaş ve kişisel güvenlik arasındaki çizgileri bulanıklaştıran yapay zekâ odaklı tanımlama da savaş alanında test edildi. Özetle, yapay zekâ destekli tanımlama yapan teknolojiler, operasyonel verimliliği artırırken, istihbarat toplama ve teknik dağıtım arasındaki süreyi kısaltırken savaş ve kişisel güvenlik arasındaki çizgileri belirsizleştiriyor. Bu tür yazılımlar, modern yapay zekânın etik ve operasyonel ikiliklerine örnek teşkil ediyor.

Bunlar 21. Yüzyılın yeni teknolojilerle savaş alanlarına dair bize önemli fikirler veriyor. Ayrıca, savaş alanları ve savaş ardından saha raporlamada da yeni teknolojiler kullanılıyor. Örneğin Rusya, keşif ve ateş desteği için robotik bir savaş aracı olan Uran-9'u konuşlandırdı. Operasyonel olarak bazı zorluklarla karşı karşıya kalırken, savaş alanında insan kaybını azaltmak için denendi, robotların vaat ettiği şeylere dair bize bazı ipuçları gösterdi ve yüksek riskli senaryolarda robotiklere artan güvenin göstergesi oldu. Alanda etkinliği korunurken insan kayıplarını azaltma noktasında katedilmesi gereken daha uzun yol var ama bu alanda bir devrim oluşturacaklarını da görebiliyoruz.

Aynı zamanda Blokchain de savaş finansmana noktasında katkı sağladı. Ukrayna'nın uluslararası bağışlar almasını ve Rus saldırılarıyla başa çıkmak için finansman sürdürülebilirliğine dair destekler verildi. Bu tarz finansal sistemler geleneksel bankacılığa bir alternatif sunuyor, özellikle de ülkeler ekonomik olarak yaptırım altındayken. Bu sistem her iki ülkeye de yardımcı oldu çünkü Ukrayna'ya yardımlar yapılırken, Rusya'nın ambargo altındaki bankacılık sistemi için de alternatif ekonomi yolları sundu.

Bu arada her iki ülke de kuantum dirençli teknolojiler kullanıyor. İletişim, hassas verilerin korunması gibi konularda, casusluğun engellenmesi gibi alanlarda da kuantum teknolojileri ülkelere destek oldu. Yüksek Hareket Yetenekli Topçu Roket Sistemi (HIMARS), Ukrayna'nın Rus mühimmat depolarına ve komuta merkezlerine hassas saldırılar düzenlemesine katkı sağlarken, Taşınabilir ve etkili olan MGM 140 ve Storm Shadow havadan havaya ordu taktik füze sistemi ve ile Jawelin Tanksavar Füzelere, güdümlü füzeler, küçük piyade birliklerine ağır zırhlı Rus tanklarına etki imkânı doğurdu.

Zırhlılara karşı anti-teknoloji füzeleri de gerçekten önemli rol oynadılar savaş süresince. Hipersonik füzeler de teknolojinin geldiği noktada önemli göstergeler arasında. Peki akıllı teknolojiler ne yapıyor? Hedefe nokta atışı yapma yeteneği, uzun vuruş menzili, etkili hasarlarla topçulukta bir devrime yol açtı. Son zamanlarda uydu ve uzay tabanlı teknolojiler de büyük etkiler oluşturdu. Ukrayna'da iletişim kesintilerinde starlink uydularının devreye girmesi, Ukrayna'nın bunu kullanması ve bazı raporlara göre Rusya'nın da bu teknolojiyi kullandığı yönünde bilgilere sahibiz.

Bu noktada, bu tür şeyleri yapan devlet dışı aktörler olduğunda, her iki güç tarafından da bu teknolojinin kullanılması durumunda dengenin nasıl kullanıldığını görüyoruz. Dengenin önemini de görüyoruz. Bu, özel sektöre ait, uzay tabanlı teknolojilerin, birden fazla aktörün tartışmalı alanlarda stratejik iletişimi sürdürmedeki rolünün altını çizdi.

Siber savaş ve bilgi operasyonları da önemliydi bu çatışmada. Rus devlet destekli bilgisayar korsanları, elektrik şebekeleri ve finansal sistemler de dahil olmak üzere Ukrayna'nın kritik altyapısını hedef alan siber saldırılar başlattı. Ukrayna'nın elektrik şebekesine yapılan saldırı özellikle önemliydi. Ukrayna BT Ordusu Ukrayna, Rus hükümetinin web sitelerini, iletişim sistemlerini ve propaganda ağlarını bozmaya odaklanarak "Ukrayna'nın BT Ordusunu" oluşturmak için gönüllüleri küresel olarak harekete geçirerek misilleme yaptı. Siber dünyada çok şey oluyor ve siber savaş alanındaki operasyonlar oldukça kritik önem taşıyor. Tüm bunlar bize dijital ve fiziksel dünyanın kusursuz entegrasyonunun ve sonuçlarını göstermektedir. Demek oluyor ki, siber savaşın yaygınlaşması, küçük bir devletin çok daha büyük bir düşman üzerinde önemli bir yıkıma yol açmasına sebep olabiliyor.

Elektronik savaş da Rusya-Ukrayna Savaşı'nın önemli bir parçasıydı. Rusya, Ukrayna navigasyon ve hedefleme sistemlerini bozmak için GPS sinyallerini karıştırdı. Ukrayna'nın Dron Karşıtı Elektronik Harp Sistemleri, Rus insansız hava araçlarını uçuş ortasında devre dışı bırakabilmesini sağladı. Her saldırı için yeni bir savunma teknolojisi döngüsünü de yakından gördük. Spektrum teknolojisinde yeni yeteneklere karşı güvenlik açıklarının bulunmasını, zayıf noktalarının tespit edilmesini ve karşı teknoloji uygulanmasını beraberinde getirdi.

Sosyal Medya ve açık kaynak istihbarat (OSINT) gerçekten stratejik bir rol oynuyor bu çatışmada. Twitter, Telegram ve Tik Tok gibi sosyal medya platformları gerçek zamanlı istihbarat kaynakları haline geldi. Vatandaşlar birlik hareketlerini ve askeri faaliyetleri paylaştı. Memetik Savaş da kullanıldı bu süreçte. Her iki taraf da kamuoyunu etkilemek ve düşman birliklerinin moralini bozmak için memeler ve viral içerik kullanarak yeni bir psikolojik savaş biçimi oluşturdu. Kamuya açık veriler geleneksel casusluğu desteklerken, dijital platformların hızı ve erişimi propaganda kampanyalarının psikolojik etkisini artırdı.

Geleneksel casusluğun yanı sıra gerçek zamanlı bilgi erişimi, dijital casusluğun hızı ve erişimini de artırdı ve destekledi.

Tüm bu gelişmeler ışığında, geleceğin askeri değişen teknolojilerin üzerinde odaklanıldığı bir asker olacak. Akıllı kasklar, artırılmış gerçeklik içeren ve veri erişimi sağlayan ekranlar kullanıyorlar. Bu teknolojilerle donatılmış askerler gerçek zamanlı savaş alanı bilgilerine erişiyorlar. Çok daha az iletişimle harita, tehdit ve görev hedefleri dahil çok daha fazla veriye ulaşıyorlar. Bu onlara savaşın durumsal farkındalığına anında sahip olmalarını ve daha hızlı karar alabilmelerini sağlıyor. Amerika Ordusu, örneğin görsel güçlendirme sistemleri gibi programlara çok önem veriyor. Uluslar yorgunluğu azaltmak ve dayanıklılığı artırmak için dış iskelet teknolojisine yatırım yapıyor. Ukrayna ihtilafında kanıtlandığı gibi kentsel savaş senaryolarında bu teknolojinin hayati öneme sahip olduğu da ortaya çıktı. Kentsel bir ortamda hareketlilik, esnekliğin yanı sıra korumaya da ihtiyacınız var. Bu nedenle bu tarz programlar çok fazla fon alıyor ve çok fazla araştırma yapılıyor bu alanda. Gen ve bilişsel iyileştirmeler çok önem kazanıyor. Genlerle veya takviye teknolojilerle insanların fiziksel ve bilişsel yeteneklerini geliştirmek ve durumsal farkındalığını artırmak yönünde çalışmalar var. Bir taraftan etik tartışılıyor ama operasyonel yetenekleri yükseltmek için biyoteknoloji de popüler konular arasında.

Tüm bu gelişmiş teknolojiler, gelişmiş robotik ve otonom sistemler yetenekleri artırmak için askerlerle birlikte çalışıyor. Lojistik için robotik taşıyıcılar, keşif ve taarruz için savaş robotları ve elbette tüm bunlar için yetenekli ve eğitilmiş, gerekli donanıma sahip insan. Birbirlerini güçlendirebilecekleri bir ortamda birlikte entegre rol oynuyorlar.

Geleceğin askeri sadece yetenek değil, aynı zamanda daha büyük bir alanda tamamen entegre olmuş, yapay zekâ ve ağ çözümleri ile güçlendirilmiş bir operasyonel sistemi anlatıyor bize. Ağ sistemli askerler daha güçlü sensörlerle daha büyük bir veri ağı sistemine entegre edilirler ve bu yazılımlarla teknoloji, çatışma süresince anlık karar almayı ve durumsal farkındalık sağlar. Amerika'da tüm bu komuta kontrol alanının denetimi için 'Ortak Tüm Alan Komuta ve Kontrol (JADC2)' sistemi geliştiriliyor.

Düşmanınız harekete geçmeden önce harekete geçen bir savaş yeteneğiyle hareket etmeyi hedefliyor bu sistem ve tüm bölgelerde birlikte çalışabilirlik ortamı sağlıyorsunuz. Hava, Kara, Deniz, Siber ve Uzay'daki 5 çatışma ortamında eşgüdümle hareket etmeyi amaçlıyor. Ve analitik makine öğrenimini ve yapay zekâyı kullanıyorsunuz ve her imkanınızı eşit, zamanında kullanabileceksiniz. Bu teknolojiler yapay zekâ tarafından etkinleştiriliyor. Ukrayna'da da görüldüğü gibi bu teknolojiler çatışmaların değişimi ve geleceği için temel oluşturuyorlar.

Özerk sistemler ve entegre operasyonlar, Ukrayna ile Rusya Savaşı'nda gösterildiği gibi çatışmalarda geleceğinin temelidir. Başboş mühimmattan insansız hava araçlarıyla savaşmaya kadar özerklik, insan riskini azaltır ve görev esnekliğini artırır. Entegre operasyonlar, uydulardan, insansız hava araçlarından, askerlerden ve sensörlerden gelen verilerin eylemleri yönlendirmek için gerçek zamanlı olarak birleştiği 'savaş bulutundan' yararlanır. Starlink gibi sistemler, merkezi olmayan, yedekli teknolojilerin, altyapıyı bozmaya yönelik rakip çabalara rağmen operasyonel sürekliliği nasıl sağladığını gösteriyor.

Modern savaş, siber ve uzay alanlarını içerecek şekilde kara, deniz ve havanın ötesine uzanır. Bütünleşmiş stratejiler, bu alanların sinerjik çalışmasını sağlar. Yapay zekâ, tahmine dayalı analitik, otomatik karar verme ve stratejik öngörü sunarak entegrasyonun bel kemiği olarak hizmet eder. Ukrayna ihtilafında yapay zekâ güdümlü sistemlerin hızlı adaptasyonu, vazgeçilmez rolünü vurgulamaktadır.

Özerk sistemler daha fazla karar alma rolü üstlendikçe, programcılar, operatörler veya hükümetler gibi istenmeyen veya etik olmayan eylemlerden kim sorumlu tutulur? Programcılar mı, hükümetler mi, operatörler mi? Bu sistemlerde şeffaflığı nasıl sağlayabiliriz? Bu kendimize sormamız gereken soru. Daha sonra entegrasyonun sağlanması gerekiyor. Yapay zekâ, insansız hava araçları ve uydu sistemleri gibi teknolojilerin entegrasyonu savaş alanı verimliliğini artırırken aynı zamanda bağımlılıklara da yol açıyor. Bu sistemler rakipler tarafından tehlikeye atılırsa veya etkisiz hale getirilirse ne olur? Endüstriyel çağ savaşları için tasarlanan geleneksel doktrinler, modern, teknoloji odaklı çatışmaların taleplerine uyarlanabilir mi? Bu tür öğretilerde insan gözetiminin rolü ne olmalıdır?

Teknolojiyi adil ve etik savaş ilkelerine hizmet edecek şekilde mi şekillendiriyoruz, yoksa teknoloji savaşı artık kontrol edemeyeceğimiz bir şeye mi dönüştürüyor? Bu, küresel toplumun bugün durduğu kritik kavşaktır. Sadece bu araçları nasıl kullandığımızı değil, yarının çatışmalarının insani ve jeopolitik anlatılarını nasıl şekillendirdiklerini de düşünmenizi rica ediyorum.

Teşekkür ederim, saygılarımla.

SORU: Askerler öyle kıyafet giyiyordu ki sunumda, artık askerler öyle kıyafet giyiyordu ki, askerler insan değil insanımsı olmuştu. Bana abartılı geldi, yürüyebilirler mi? Örneğin son olimpiyatlarda Millî atıcımız Yusuf Dikeç hiçbir kıyafet giymeden başarılı oldu. Bunu değerlendirebilir misiniz? Asker böyle nasıl hareket edecek operasyon alanında?

CEVAP: Bu alanda farklı ülkeler tarafından takip edilen pek çok program var. Geleceğin askeri ve savaşçıları başlığıyla. Orada yapılmaya çalışılan şey sanki robotik bir taraf var ama insanın yeteneklerini geliştiriyorsun ve robotik özellikleri kazandırıyorsun. Temelde insanı güçlendirmeye çalışıyorsunuz. Örneğin görüntüleme kabiliyeti artırılmış ekranlar ve yapay zekâyı buna eklediğinizde gördüğünüz şey geliyor, daha anlamlı hale geliyor. O ortamdaki durumsal farkındalığınız, tüm sensörlerden gelen gerçek zamanlı görüntülerle artıyor. Dış yani takviye iskelet sistemleri giyiyorlar, bir nevi biyonik motorlu ya da elektrikli kolaylaştırıcılarla. Bu taşımanızı, hareket kabiliyetinizi artırıyor ve yükünüzü azaltıyor. Önceki savaşlarda kalkanları takanlar, ağırlığı artıran şeyleri takanlar da savaşçılar ve hareket kabiliyetlerini azaltıyor. Yeni teknolojiler ise hareket kabiliyetlerini artırıyor. Genetik değişiklikler ve biyoteknolojiler de buna benzer insan vücuduna dair geliştirme programları. Elbette bunun etik açıdan değerlendirmeleri yapılıyor, gelecekte bu programlar nasıl şekillenecek görmemiz gerekecek ama bu tür şeyler şu anda yapılıyor ve önemli olan askeri daha fazla korumak, kollamak, daha aktif kılmak için yapılan programların olduğu ve buna da hazırlanmamız gerektiği. Bu teknolojiler kentsel savaş türü ortamlara askeri daha hazır kılmak için yapılıyor.



I. GÜN ÜÇÜNCÜ OTURUM – YENİ SAVAŞCI

TEMA:
İnsan-Makine Organizması: Tek-Er

OTURUM KONUSU:
İnsanımsı Makine – Makinemsı İnsan

OTURUM TEMALARI:
Beslenme, Fizyoloji, Psikoloji

III. OTURUM ÖZETİ

Askerlerin gelişen teknolojiler karşısında, sahadaki takibini ve kendisini güvende hissetmesini sağlayan sistemler önemlidir. Tek-Er'in gelişen savaş koşullarına yönelik ihtiyaçlarının doğru planlanması ve sahada yönetimi konusunda yeni teknolojilere uyumlarının sağlanması gerekmektedir. Özellikle patlayıcı ya da insansız sistemlere karşı savunmaya yönelik yetenekler geliştirilmelidir.

Sonuç odaklı kararların teknolojinin gelişimine rağmen uzun bir süre daha insanda kalması, insanla insansız sistemlerin entegrasyonu NATO'nun yakın gelecek savaş perspektifini yansıtmaktadır. Teknolojinin hava, deniz, kara, siber ve uzay gibi sistemlerin entegrasyonu ve birbiriyle uyumlu çalışmasına hizmet etmesi yakın ve orta vadeli teknolojiye bakışı yansıtmakta.

Savaş pilotları, aldıkları kararlarla, savaşın gidişatını değiştirmekte önemli rol oynamaktadır, özellikle kara operasyonlarının öncesinde bireysel yetenekleriyle, getirdikleri zekâ, durumsal farkındalık ve çözümlerle fark oluşturabilir. Teknolojilerin kullanımı sırasında da insanlara bilişsel yük yüklenmekte ve bu yükü kaldıracak yetenek ve beceride personellerin seçilmesi, eğitilmesi de giderek önem kazanmaktadır.

Teknolojiden kaynaklı hareket eksikliği, personelin çevikliği ve atikliği önünde büyük engel oluşturmaktadır. Vücuttaki enerji, askerin teknolojik ürünlerle adaptasyon sürecinde de hareketlilik, kuvvet ve dayanıklılık gibi parametreler üzerinde etkilidir. Her vücudun ihtiyacına göre farklı eğitimler ve beslenme uygulanmalıdır. Özellikle de özel birlikler veya masa başında uzaktan sistem kullanacak personel için farklı eğitimler ve taşınacak yüklere yönelik pratik uygulamalar önem kazanmaktadır.

Savaşlar, dayanıklılık savaşından ziyade, hızlı reaksiyon gösterme, reaksiyon süratini artırmaya yönelmektedir. Gelişen teknolojilerin ne getirip götürdüğü, askere etkilerinin ne olduğu iyi analiz edilmeli, eğitim programları da buna göre geliştirilmelidir.



Oğuz Alpay AYDIN
SAVUNMA SANAYİ
BAŞKANLIĞI (SSB)
MODERATÖR

Merhaba, hepiniz hoş geldiniz. Bu bölümde oldukça ilginç bir konu olan ‘İnsan Makine Organizması’ konusunu konuşacağız ve bu konuyla ilgili ilginç bir tespit var, insanımsı makine ve makinemsi insan. Güç, hız, dayanıklılık, psikoloji, karar süreçleri, beslenme, fizyoloji, psikoloji ve teknolojiye uyum gibi konuları ele alacağız.



Ömer DOĞAN
ASELSAN

Merhaba, ben bugün insan-makine çalışmasına komuta ve kontrol perspektifinden bir bakış açısını paylaşmaya çalışacağım. Aselsan uzun yıllardır ‘Geleceğin Askeri’ konseptini çalışmaktadır. Değişken teknolojilerin insan-makine çalışmasında savaş ortamına entegrasyonu için çalışmalar yapıyoruz. Askerin ön safta görev yapması sırasında kara gücünün

harekât ihtiyaçlarını karşılayacak komuta kontrol, haberleşme, durumsal farkındalık, keşif gözetleme ve dost ile düşman takibi ihtiyaçlarına yönelik sistemimizin ismi CENKER.

CENKER, 3 yıldır çatışma ortamlarında sahada kolordu, tugay, tabur gibi bölük seviyesinden tek-er seviyesine kadar askeri birliklerin sayısal ağ yapısı içinde temel komuta, kontrol, istihbarat, lojistik, haberleşme, durumsal farkındalık ve koordinasyon bilgi ihtiyaçlarını karşılayarak askerin bütünsel harp yeteneklerini artırmayı hedefleyen bir sistemdir. Ve tüm bu süreci bilişsel yüke dikkat ederek geliştiriyoruz.. Teknoloji iyi olabilir ama savaş alanının gerçeğine uygun olmalıdır. Bu süreçleri saha tecrübeli emekli askerler ve askeri uzmanlarla geliştiriyoruz. NATO’yla bu alanda iş birliği yapıyoruz ve sahadan gerçek kullanıcılardan da geri dönüşleri alarak projemizi ilerletiyoruz.

Sahada ilk ihtiyaç, personelin gerçek ihtiyaçlarının tespiti ve çözülebilmesi. Muharebe sahasında kişisel su tüketimi en önemli konular arasında. İdeal olarak askerlerin normal şartlarda günlük 3 litre su tüketimi gerekiyor. Komuta kontrol sistemleri ile iklim koşullarına göre personel üzerinde taşınacak su miktarının planlanması, hızlı su tüketimine karşı antrenman aşamasından sahaya su tüketim provaları, suyu idareli kullanmayı alışkanlık haline getirme, yeterli yiyecek ve içecek çeşitliliği, hafif ve taşınması kolay yiyecekler gibi konularda, yetersiz beslenme, su tüketimi gibi konularda, askerin sağlık durumunu izlemek için sesli uyarılar üretilmesi, erzakların kullanımı ve tüketimi için olanakların sağlanması gibi konularda komuta kontrol kademesiyle işbirliği yapılmaktadır. Savaşta savaşçıların ihtiyaçlarının doğru planlanması ve sahada yönetimi konusunda da çözümler üretilmektedir.

Operasyon sırasında da bu sürecin yönetimi için asker ile komuta kontrol arasında iş birliği alt yapısı sunulmaktadır. Askerin günlük yaklaşık 4 bin kalori alması gerekmektedir. Bu da CENKER sistemiyle komuta kontrol merkezi ile asker ve sahada yönetilebilmektedir. Acil ve özel durumlarda sistem üzerinden rapor edilerek çözüm bulunabilmektedir. Askerlerin kendini yalnız hissetmemesini sağlamak, güven ortamına katkı sağlamak, kendi birim ve kıdemli komutanıyla destek sağlamak, aşırı stres, yorgunluk, dikkat eksikliği ve algısal yeteneğin azalmasının etkilerinin azalması gibi durumlar için de alt yapıya sahiptir. Sistem, hedef tanımını basitleştirme, basit, kolay ve anlaşılır bilgi yönetimi ve aşırı bilgi yüklenmesinin önlenmesi, küçük birim liderlerinin komuta ve kontrol yeteneklerinin geliştirilmesi, alt birimler tarafından metin, grafik, şablon ve medya araçlarıyla iletişimi kolaylaştırmakta, uzaktan sağlık desteği ile de ortamın iyileştirilmesine katkı sunmaktadır.

CENKER sistemi, askerlerin sağlık durumu bilgilerinin izlenmesi, erken uyarı, KBRN saldırıları, topçu saldırısı gibi durumlarda uyarı, güvenli rota takibi, olay ve durum hakkında bilgi güncelleme, komuta merkezine bilgi aktarımı, tehlikeli ve önemli noktalar ile alanların işaretlenmesi, uyarı oluşturulması, hedef tespiti ya da uyarısı, lazer ve dokunmatik ekranla hedefe yönelik ikazlar, takım arkadaşlarının durumuyla ilgili bilgi akışı, kişisel ve arkadaş ekibi uyarısı, tehlikeli bölgeler için uyarı ve insansız sistemler kullanımında bilgi akışı yönüyle de kullanılmakta ve geliştirilmektedir.

Bölgedeki insansız sistemlere karşı uyarı için de özelliklere sahiptir.

Sistem, çok alanlı aktörler ve yetenekler dahil olmak üzere gerçek sistem ya da simülasyon sistemleriyle ilgili özelliklere sahip olması için geliştirilmektedir. Mayın tespiti ve temizliğinin yanı sıra yardımcı taşıma sistemleriyle yükün hafifletilmesi, pil gerektiren cihazlar için basit enerji üretimi, eylem inceleme ve yeni planlama için veri kullanımı alanlarında da geliştirilmeye devam edilmektedir.

Yeni jenerasyon olarak yeni nesil çoklu alan entegrasyonu ve derinlemesine komuta ve kontrol sistemleriyle uyumlu sistem inşası için iyileştirmeler ve çalışmalar sürdürülmektedir.

Son olarak malumunuz TUSAŞ saldırı oldu, şehitlerimiz oluyor, kahramanlarımız bizler için sahada çarpışıyorlar. Tüm şehitlerimizin ruhları şâd olsun.

SORU: Dünya literatürü ve modern orduları izlediğimizde komuta kontrol yapısının da değiştiğini görüyoruz. Yani Yapay Zekânın ve diğer teknolojinin girmesi sonucunda otonom ve melez kontrol merkezleri geliştiriliyor. Acaba bu bağlamda yorum alabilir miyim, tutarlı olabilir mi? Nereye kadar otonom?

CEVAP: NATO'nun iki hafta önce bir faaliyetine katılmıştık. NATO'da 'Çok Alanlı – Multi Domain' faaliyetinde bu operasyonları çok ciddi ele alıyor. Edindiğimiz izlenimlere göre, yakın zamanda şu şekilde ilerlenecek; insan biraz daha temel kararlar anlamında geri plana itiliyor, otonom ve makinalar tarafından basit kararlar verilebiliyor olacak. Ama katma değeri daha yüksek, daha sonuç odaklı kararlar yine insan odaklı olacak. Dolayısıyla otonom karar alma, karar sürelerinde yapıları kullanma, insanla insansız sistem entegrasyonu gibi seviyeler de NATO'da da çok ciddi tartışılıyor. İnsan yükünü azaltacak küçük kararlar makinalara bırakılacak. Kara, deniz, hava gibi sistemlerin birlikte çalışması sırasında insanların teknik detaya girmesinin yükünü almak için ise bu ortak entegrasyonlarda cihazlar karar verecek gibi gözüküyor.



Dr. Binbaşı Rifat UĞURLUTAN
Hava Kuvvetleri Komutanlığı
(HUGEM)

Binbaşı Uğurlutan,
komutanım müsaadenizle.

Ben Hava Kuvvetleri'nde
HUGEM Komutanlığı olarak
yapmış olduğumuz insan
yükseltici sistem
araştırmalarımızı sizlere arz
edeceğim.

Konuya hemen yanı
başımızdaki Ukrayna-Rusya
Savaşı'na dair bir podcast ile
başlamak istiyorum. İki tane
NATO'nun en üst düzey

komutanı "Ukrayna-Rusya savaşı hava ve uzay gücünden neler
öğreneceğimizi bize öğretiyor" içerikli yayında, her iki komutan
da, Ukrayna'daki çatışmaların, hava üstünlüğünün savaşın
gidişatını belirlemede kritik bir rol oynadığını vurgulamaktadır.

Hava üstünlüğünün sağlanamaması, kara operasyonlarının
etkinliğini sınırlamaktadır. Bu noktada hava üstünlüğü
sağlanamadığı için kara operasyonlarını, hatta konunun bir
tenis maçına döndüğünü, tarafların birbirlerine çeşitli füzeler ve
roketler attığını ama savaşın hiçbir zaman sona eremediğini
söylüyorlar. İşte bu da bize savaş pilotlarının aslında muharebe
sahasında en etkili güç olduğunu söylüyor. Savaş pilotları
sadece uçağın teknik özelliklerini kullanmakla kalmıyor,
beraberinde kendilerinin getirdikleri zekâ durumsal farkındalık
ve orijinal, ürettikleri çözümler ile savaşın gidişatını baştan sona
değiştirebiliyor. Savaş pilotları az önce de ifade ettiğim gibi
uçaklarıyla bir yok edici müzik çalıyorlar ve bu yok edici müziğin
enstrümanı da her seferinde daha güçlü hale geliyor. Ancak biz
bakıyoruz ki 6. Nesil teknolojilerde bile pilotlar yerini koruyor.
Benim bir nörobilimci olarak söyleyeceğim şey, yapay zekâyı
kullanacağımız yer onunla çatışacağınız alan değil, en iyi
kalibrasyona geçerek onu en iyi kullanacağınız alandır. Bunu
yapay zekâyı sorduğumuzda bile pilotun eline silah veren bir
figür çizdi. Bu ne demek aslında savaşın temel belirleyicisinin
insanlar olduğunu nakşetmeye çalışıyor. Evet biz çok üstün
makinalar üretiyoruz ama günün sonunda siz 50.000 fit
üzerinde uçmak için ürettiğiniz bir sistem, asgari lojistik ihtiyacı
olan insanın havayı veya oksijeni sağlayamadığınız için 25bin
feet irtifa üzerine çıkamıyor. Amerikan Hava Kuvvetleri bu
problemin çözümü için konuyu NASA'ya havale etmiş durumda.

Biz bugün biliyoruz ki, pilotların ya da uçuş fizyolojisinin ilgi alanları sadece fiziksel zorluklar değil, beraberinde gelen bilişsel zorluklar. Neden öyle? Örneğin 1. Dünya Savaşı'nda pilotun yanında kanopi gibi bir şey yok. Sonrasında devam eden teknolojilerde ise inanılmaz bir teknoloji var. Önceki pilotların sadece ata binmesi yeterliyken, bugün biz hem mental hem de psikolojik durumlar için ayrı testler geliştiriyoruz. Biliyoruz ki pilotlar sadece kendi uçaklarıyla değil ortamdaki diğer uçan nesnelerle de iletişim kuracaklar. Ve hangi uçan nesnenin hangi silahı kullanması gerektiğine karar verecek bir noktaya gelecek iş. İşte bu noktada biz önceden şunu sorardık, bu çocuklardan hangisi pilot olacak? Ancak biz bugün biliyoruz ki, üçünün de afacan çocuk, zeki çocuk özelliklerine sahip olması gerekiyor.

NATO, son yayınladığı raporda biyoteknolojiyi 7 ana dalın içine almış durumda ve bu biyoteknoloji nöro teknoloji ve insan performansını artırmaya yönelik araştırmalar olarak gündeme gelmekte. Şimdi nöro teknoloji dediğimiz zaman sinir demeden geçmek istemiyorum. Sinir ve sinir bilimci gerçekten teknolojiye yön verecek alan olarak görüyorum. Ancak, sinir bilimciler nöronu basit bir yapı zannediyorlar. 1981 yılında kajal nöronu farklı yapılarda ve karmaşık yapılarda gördük. Bu komplike yapının birçok bileşeni var. Nöronun aslında merkezi cell body dediğimiz hücre merkezi. Aslında proteinleri burada sentezler ve fonksiyonunu aslında burada başlatır. Burada diğer nöronlarla haberleştiği dendritler bulunur. Bu dendritler, diğer nöronlarla faaliyet içerisinde olup, nöronun faaliyet gösterdiği ya da faaliyet göstereceği duruma hazırlarlar. İşte bu durum uyarılabilir veya yavaşlatan ya da durduran bir durum olabilir. İşte biz nöronu bilgi aktarımını aksiyon potansiyeli dediğimiz elektriksel bir durumla tanımlıyoruz.

Nedir bu aksiyon potansiyeli? Nöron içi normalde dinlenirken, hiçbir şey yapmıyorken dışarıya daha pozitif, dışarıdaki pozitif yükler içeri göç ederek kemotaktik bir elektriksel potansiyel oluşturur. Bu elektriksel potansiyel, işte hani böyle diyoruz ya beynindeki dalgalarını ölçtü, şöyle yaptı böyle yaptı. İşte bu elektriksel potansiyelin kaynağı nörondaki bu basit iyon değişimidir. Bu o kadar basit bir süreç değildir. Bir aksonla dendrit arasında sinaps dediğimiz, kuantum fizikçilerin de bildiği kuark dediğimiz bir alan vardır. İşte bu alanda bilgi aktarımı vardır ve bilgi alışverişi gerçekleşir.

Bu bilgi aktarımının sonunda da nöronlar birbirini geliştirirler, birbirleriyle bağ kurmaya başlarlar. Nöronlar birbirlerine bilgi aktarımı yaparlar. Nöron bir işi yapmak için başka bir nöron ile bağ kurar, ilişkiye girer. Peki biz bu yöntemle, elektriksel potansiyel değişimlerini nasıl ölçeriz? Biz bilimsel yöntemlerle bir canlının beynini açarız, oradaki bir nörona dokunuruz, bu nöronun üzerindeki elektriksel veya kimyasal değişimi ölçebiliriz. Nöronlar konuşa konuşa beyni oluşturur.

Beyin farklı yapıları eş zamanlı farklı noktalarda kontrol etmek üzere özelleşmiş bir organımızdır. Örneğin frontal lobumuz daha çok etkin kararlar verme, yani bizi maymundan ayıran bölge. Temporal lob ise daha çok duyma ve hafıza gibi yetenekleri konuların yoğunlaştığı bir bölgedir. Beyin kökümüz dediğimiz, beynin bir parçası olan kısım tamamen fizyolojik unsurların yönetildiği yerdir. Yani biz burada nefes alma, kalp atımı gibi fiziksel aktiviteleri takip ederiz. Peki biz her defasında insanlardan ölçüm yapmak için böyle kompleks sistemlere mi ihtiyaç duyuyoruz. Hayır, EEG (elektroensefalografi) dediğimiz, çok kanallı bir voltmetre gibi bir sistemle de bu değişimleri analiz edebiliyoruz ve nöronlardaki değişimleri ölçebiliyoruz, aktivitelerinden haberdar olabiliyoruz. Functional Near Infrared spektroskopi (Fonksiyonel yakın-kızılötesi spektroskopisi) ile de beyin bir iş için ne kadar enerji harcadı ne kadar oksijen tüketti gibi beynin enerji sarfiyatını ve fonksiyonunu ölçebiliyoruz.

Beyinden beyine fark var mı, doğuştan doğuşa özellikler var mı var. Erkek beyni 1400 gram ve 100 milyar nörona oluşuyor. Kadın beyni 1300 gram ve 90 milyar nöron. Şimdi ben erkeklerin, 'biz daha zekiyiz, nöron sayımız fazla dediğini duyar gibiyim ama öyle değil. Kadın beyni daha kompakt, sizin hayalde yapamadığınız şeyi onlar yapıyor. Bunu şöyle açıklayabiliriz, 2005 yılında Lucy Brown MRI ile kadın ve erkeğin karşı cins fotoğrafı gördüğünde hangi noktalarının çalıştığını test etmiş. Erkek frontal noktada hiçbir aktivite yok.

Bu ne demek, erkek ne olursa olsun sadece fiziksel görünüşe önem veriyor kadın ise frontal lobu çok ön plana çıkarıyor. Ne yapıyor, bu süreçte benimle nasıl bir paylaşım yaşayacak, ekonomik olarak destek verecek mi, nasıl ilgilenecek, gibi konularda frontal kısım çalışıyor. Peki eğitim, kişide beynsel değişimlere yol açabilir mi? Bunun için de dünyada beyni çalınmış tek adam Einstein'a bakalım.

Onun beynine baktığımız zaman sağ ve sol beyni konuşturan korpus kallosum dediğimiz 3 boyutlu sistemleri ayırt etmeye çalışan kısmın çok daha fazla geliştiğini, matematiksel işlemlerin çok daha yoğun yapıldığı postcentral girus bölümünün daha büyük olduğu görülmüş.

Peki beynin iş yapma potansiyeli? İşte biz beynin iş yapma potansiyeline bilişsel yük diyoruz. Bilişsel yük kişinin kendinden getirdiği birtakım özellikler, dışarıdan kendisine etki eden birtakım değişimler ve işin parçalanarak yapıldığı veya parçalanmadan yapıldığı konusundaki etkilere dayanarak bir yük dinamiği oluşturur. 'Cognitive Load' yani bilişsel yük teorisini ilk olarak 1988 yılında John Sweller isimli bilim adamı ortaya koymuş. Bilişsel yük teorisi (Cognitive Load Theory), öğrenme sırasında beynin bilgi işleme kapasitesinin sınırlı olduğunu ve bu sınırlılıkların öğrenme üzerinde nasıl etkili olduğunu inceleyen bir teoridir. Siz yapısal olarak belli bir şeyi yönetme kapasitesine sahipsiniz, bir öğreticinin bir olayın size yüklediği yük var ve bu olayı parçalayıp sindirip sindiremediğiniz söz konusu. Intrinsic load asıl yükü, extraneous load konu dışındaki yararlı ve faydalı yük ve germagene load ise etkili yani faydalı yük. Biz bunu ölçünce şunu anlıyoruz, bir kişi eğitilirken bu adam buna yatkın mı, değil mi, bu işi yapabiliyor mu veya yaparken ne kadar zorlanıyor. Eğer adamı uyaran olmasa, rahat eğitim alsa, eğitim o zaman da amacına ulaşmıyor. Bir miktar stresin verimlilik üzerinde etkisi olduğunu, optimal bir stresin her eğitim içinde olması gerektiğini Yerkes-Dodson yasası söylüyor bize.

İşte tüm bu veriler ışığında biz 'Genius' projesini ortaya koyduk. Bir uçuş veya F-16 tam görev simülatöründe biz farklı tecrübeye sahip pilotların yetenek ve becerilerini ayırt edebilecek miyiz? Ya da pilota biz nasıl bir eğitim vermeliyiz, kişisel bir eğitim vermeli miyiz bunun ayırımına gittik. Bir sürü sensör koyduk. Elektrokardiyografi, elektroensefalografi, solunum sayısı gibi analizler yaptık. Bu analizler sonucunda kişinin simülatördeki başarısını karşılaştırdığımızda çeşitli metrikler elde ettik. Bu metrikler bu kişinin öğretmen pilot mu, aday pilot mu yoksa bir miktar tecrübe sahibi mi olduğunu ayırt etmemize yüzde 80 oranında sağladı. Peki bu adamı eğittik güzel de uçağın içerisinde bu adam ne yaşayacak? 20 bin – 30 bin 50 bin feet yükseklikte ne yaşayacak? O yüzden siz bu adamı klasik tıbbın yöntemleriyle muayene ve analiz edemezsiniz..

Bunun için de havacılık tıbbı ortaya çıkmış. Havacılık tıbbı 1920'lerin konusu. 1930'larda Gazi Mustafa Kemal Atatürk, ilk uzay hekiminin yetiştirilmesi için Amerika'ya gönderilmesi kararnamesini imzalamıştır. Bu konu ülkemizde bu kadar eski bir konudur.

Uçuş biliminde çok iyi fizik bilmeniz lazım. Çünkü bununla mücadele eden adamın ne yaşadığını biliyor olmanız lazım. İşte biz bu fiziği iki kısımda inceliyoruz Uçuş esnasında biyolojik yanıt oluşturan fiziksel etkilere göre ayırıyoruz. Yüksek İrtifa Kaynaklı Stresörler ve Mekanik Stresörler. Yüksek İrtifa Kaynaklı Stresörler, atmosferik basınç değişimleri, gazların parsiyel basınçlarındaki değişimler ve radyasyon yüksek irtifa kaynaklı stresörler sınıfına giriyor. Mekanik stresörler ise yerçekimi, akselerasyon, yüksek hızlı hareket ve 3D pozisyonel değişim ise mekanik kaynaklı zorluklar olarak tanımlıyoruz.

Peki ne oluyor? İşte bizim havacılık tıbbında üç tane temel problemimiz var. Biri SA kaybı dediğimiz Spatial Awareness (uzamsal farkındalık) kaybı yani kişi uzaysal durumun farkında değil. Aslında bizim uzaysal durumumuzu tanımlayan şey, görme yeteneğimizin, orta kulağımızdaki yarım daire kanallarının ve progresiftik duyuların kombinasyonuyla ortaya çıkmış bir veridir. İşte bunların birisi size ihanet ederse işte o noktada siz SA'nızı kaybedersiniz. Yani 3 boyutlu uzaydaki durumunuzu ve yöneliminizi kaybedersiniz. Peki bu ne sıklıkta yaşanır? İşte bunu en çok raporlama özelliği olan ülkeler İngiltere ve Amerika. Yılda 90 ile 100 arasında SA kaybı raporladıklarını görebilirsiniz. İşte nöronların size ihanet ettiği şey SA kaybı. Konudan bihabersiniz ne dinlediğinizi bilmiyorsunuz ve ne dediğinizi bilmiyorsunuz. Bir çaba içerisindeyiz ama ne yaptığınızı bilmiyorsunuz. Hipoksi dediğimiz süreçte, oksijen açlığı demek. Beynin bir şekilde oksijene olan ihtiyacının karşılanamaması, vücut tarafından yeterince oksijen alınamaması demek. Bu da yaklaşık 100 ila 200 vaka yılda. Hipoksi aslında karar verme sürecini tamamen devre dışı bırakıyor.

Diğer bir problemde A-loc ve G-loc dediğimiz yer çekimi vektörünün şiddetinin ve yönünün sürekli değişmesi. Bizim için en büyük tehdit yukarıdan aşağı ve aşağıdan yukarı olan bu yer çekimi vektöründeki değişim. Çünkü kalbinizin bir gücü ve bir pompalama yeteneği var.

Eğer siz bu pompalama yeteneğinin çok üzerindeki bir yük bindirirseniz, kalp bunu pompalayamıyor. Peki pompalayamayınca ne oluyor? Bizim epileptik krizlere benzettığımız bir bilinç kaybı durumu yaşanıyor. Görme kaybından bilinç kaybına uzanan bir etkiye kadar ciddi etkilerle mücadele eder pilotlar. Bunun için de eğitimler verilir. Biz şunu yapmaya çalıştık, pilotların gerçek zamanlı sağlık verilerini ölçebilir miyiz? Beraberinde maruz kaldıkları fiziksel ölçüleri ölçebilir miyiz?

F-16 Tam Görev Simülatörlerinde eğitim alan pilotların nörofizyolojik ve fizyolojik durumlarında gerçekleşen değişikliklerin ölçülmesiyle eğitim değerlendirmelerinin bilimsel ve nesnel yöntemlerle desteklenmesi ve ilgili simülatör eğitimlerinin kişiselleştirilmesine yönelik altyapı çalışmalarını kapsamaktaydı. Ve bunu çok ucuza yapmayı başardık. 2013 yılında önerdiğimiz proje 2017 yılında kabul aldı ve prototip üretimine başladık. 2020 yılının temmuz ayında ilk testimizi icra ettik ve testleri raporladık ve yılında testler raporlandı. 7 Kasım 2020’de ilk uçuşumuzu başarıyla tamamladık. Peki gelecekte ne yapacağız?

Gelecekte ne yapacağız?

“Uçuşun güzelliği, beyin olmadan hiçbir şeydir.” (VİDEO)

Bizde, Hava Kuvvetleri’nde uçuş tulumu ve buzdağı olmadan sunum hiçbir zaman bitmez.

Arz ederim.

SORU: Bilişsel alandaki muharebe düşünce yapısı, karar verme, elektromanyetik spektrum operasyonları perspektifinde insan beynine ışınlarla veya başka tekniklerle karar verme mekanizmasını engelleme veya destekleme çalışması var mı?

CEVAP: Sorunun içeriği, yüksek enerjili sistemle insan manipülasyonu. Bu konuda önce, yüksek enerjili bir sistem mi uygulamak mı isterim yoksa cep telefonu ile mi yeni nesil harp teknikleriyle manipülasyon mu yapmak isterim? Yüksek enerjiyle beyine bir yükleme sonrasında kişinin ne yapacağını bilemiyorsunuz. Her geçirdiğiniz an kendi üzerinde özelleşmesine sebep olan bir bilgi yükü alıyor. Her an değişkenlik geçirebiliyor.

Bu noktada enerji ile manipölasyon yapılabilir mi, çok zor ama verimli mi hayır. Çalışılmış mı bu konu, evet. Mesela, LSD ajanı ile, bizim ileri seviyede psikiyatrik rahatsızlıkları bulunan insanlar için uyguladığımız elektrokonvülsif dediğimiz bir yöntem var Duygu durum bozukluğundan elektro şarj üretiyoruz. Evet adam bir problemi unutuyor ama yeni bir probleme sebep olabiliyor. Bir enerjiyle bir insanı manipüle etmek çok kolay bir iş değil.



Doç. Dr. Murat ERDOĞAN
BAŞKENT ÜNİVERSİTESİ

Öncelikle Millî Savunma Bakanlığı'na, Savunma Sanayi Başkanlığı'na SASAD'a teşekkür ediyorum.

Multidisipliner bir çalışma olmuş. Mühendislerimiz, hekimlerimiz, askerlerimiz, polislerimiz, tüm geleceğin askerini oluşturacak unsurları toplayamazdık eğer disiplinler arası bir çalışma olmasaydı. Savaşın dönüşümüyle ilgili

birçok şey söylendi. Napolyon'un ateş gücüne bizim bir timimiz sahip. Teknolojideki gelişmelerle beraber, dünya savaşlarındaki yükler incelendiğinde, geline netice teknoloji ilerlemesine rağmen, askerlerimizin taşıdığı yüklerin ağırlaştığı yönünde. 50 kilograma kadar sırt çantasında yük taşıdıkları yönünde bilimsel çalışmalar var. Bu bize şunu gösteriyor, bunu yaparken de teknolojik gelişmelerden bağımsız değiliz. Teknolojinin gelişmesiyle birçok parametreyi biz çok rahatlıkla ölçebiliyoruz. Gözlükler, akıllı saatler, nabızdan tutun oksijen satürasyonuna kadar, akıllı yapılan kemerler, pantolonlar, yere uyguladığınız basınçtan ayak ağırlığınıza kadar ölçen sistemler var. Bunların hepsi teknoloji ile hayatımıza girdi. Ben genelden özele doğru aktaracağım. Bu teknolojiler bizi hep olumlu etkilemedi, olumlu ve olumsuz yönleri de var. Ben burada olumsuzdan olumluya doğru bir harita çizeceğim.

Aslında teknoloji gelişimi bizi daha az hareketli yapıyor. Normal şartlarda fiziksel işler ön plandayken, karargâh kurum daha az hareket edilen alanlar. Bu da bizim günlük enerji tüketimimizi azaltıyor. Obezite, kalp, tansiyon ve şeker gibi 'ölümcül dördü' denen hastalıkları polis, asker gibi silahlı kuvvetlerimizde de görüyoruz. Hiç kimse toplumdan ve gelişmelerden bağımsız değil. Bu defter ve kalem haricinde bugün kimin defter kalemi var desem 10-15 kişi de var, cep telefonu kimde var dediğimizde herkeste var. Teknoloji hayatımıza öyle bir girdi ki bunu uzaklaştıramıyoruz, bunun yan etkileri de bizlere kilo kazanımı olarak geliyor bu. Bunun savaş sahasına da olumsuz etkileri var. Kilolu bir asker mi yoksa çevik atak bir asker mi hasmını alt edebilir?

Yapılan çalışmalardan bir tanesinde yüzde 34 oranında askeri servislerden ayrılma oranı olan bir araştırma var. Tüm ordularda buna benzer araştırmalar ve problemler var. Bu tüm orduların, teknolojiden kaynaklı hareket eksikliği problemi. Buna göre de herkes fiziksel ve eğitim revizyonlarına gidiyor askerlerini aktif tutmak için. Fiziki yeterlilik test değerlendirme testleri yapılıyor, periyodik olarak, bizim ordumuzun da yaptığı gibi. Geçenler ve başarılı olanlar iyi olanlar gidiyor.

İlk insanda nasıldı, antropolistler araştırıyor bunu, insanda ne değişti teknoloji gelişirken? Baktığımız zaman, insanda günlük kalori tüketiminde en büyük açık ve hareket eksikliğine bağlı oluyor. Normalde Avcı toplayıcı ile günümüzün modern insanı arasındaki kalori ihtiyacını karşılaştırdığımızda, günlük bazal metabolizma hızını karşılaştığımız zaman aslında büyük bir fark yok. Fark hareket diyeceğimiz, total enerji tüketiminde oluyor. İşte bunu normal hayatımıza katacağımız hareketlerle telafi etmek mümkün olabiliyor. Savaş alanında, muharebe sahasında performansı neler etkiliyor? Bu taşıdığımız yüklerin artması, ısı, soğukluk, yükseklik, hipoksik ortam, iklimatik şartlar, kas rahatsızlıkları bizi olumsuz etkiliyor. Diğer taraftan biz bir yükseklik eğitimi yaparsak, yüksek irtifa ve yüksekliğe uyum eğitimi (aklimatizasyon) yaparsak askerimiz bugün yüksek bir çevreye gittiği zaman oradaki hipoksik ortamdan daha az etkileniyor veya yine kendi eğitimlerimizi savaş sahasına göre simüle edersek, askerimiz fiziksel olarak bundan daha az etkileniyor. Fitness antrenmanlarını muharebe şartlarına göre güncellersek bizim askerimizin performansı muharebe sahasında artıyor.

Enerjiyi sürekli konuşuyoruz. Bizi ayakta tutan enerjiyi Adenozin Trifosfat (ATP) denen bir bilimsel maddeden sağlıyor vücudumuz ve bu vücudumuzda depo olarak bulunuyor. Bunu çok kısa sürede tüketiyoruz bunu. Muharebe sahasındaki enerjinin kazanımında karbonhidratlar, yağlar ve proteini bu enerji tedariğini kullanıyoruz. Muharebe şartlarında mutlaka bilimsel ve teknolojik yöntemlerle askerin desteklenmesi ve bunun farkındalık açısından bildirilmesi önemlilik arz ediyor. ATP'nin kullanılmasında ilk iki saniyede kasımızda problem olmuyor, çünkü kasımızda var, süre uzadıkça 10 saniyeye geldikçe, 15 saniyeye geldikçe artık kasımızdaki depo izin vermiyor ve biz enerji kazanımını laktik asit dediğimiz sistemden enerji açığını kullanıyoruz.

Bu da iki dakikaya kadar bizi götürüyor, 2 dakikadan sonra laktik asitte azalıp devreden çıkınca oksijenli sistemi kullanıyoruz. Günümüzde ne oldu nasıl etkilendi kalori tüketimi ve askerin nasıl etkilendi? Buna baktığımızda, bizim karargâhta çalışan bir personelin ihtiyacı 2700 kalori iken, savaşçı diyeceğimiz piyade ve özel kuvvetlerin 5000 kaloriye yakın enerji harcadığını gösteriyor bize bilimsel araştırmalar. Sürenin uzaması bir dezavantaj mı? Evet, muharebe alanında sürenin uzaması bir dezavantaj, sadece fizyolojik değil, psikolojik ve motivasyonel problemi de beraberinde getiriyor. Bence bu iki günlük organizasyonun kümülatif işlemlerinden biri sadece askerleri fiziksel, duygusal olarak görmek değil, bütünü bir araya getirirsek muharebe alanındaki etkimiz açısından faydalı olacaktır diye düşünüyorum. Süre uzadıkça yağlardan kazanım artıyor ve karbonhidratlardan kullanım azalıyor. Savaşılan, muharebe yapılan yere göre de enerji tüketimimiz artıyor. Kullandığınız sırt çantası başlangıçta 40 kilo olurken, azalıyor kuvvet ve dayanıklılıkta azalıyor. Eğitimimizi buna göre değiştirmek zorundayız. Harcanan kalori açısından da eğitimler çok önemli. Eğer biz askerimizi sıcak bir ortamda operasyona göndereceksek ve onu soğuk ortamda hazırlarsak, fizyolojik ve psikolojik olarak doğru şeyi yapmayız. Muharebe sahasında kaldırma ve taşıma, cephaneyi nesneyi bırakma, tırmanma, kazma, yürüme, koşma, itme ve çekme görevleri muharebe sahasındaki görevlerden.

Peki savaş sahası bizden neleri talep ediyor? Taktik becerimiz, nişancılık, yön bulma ve ilerlenen noktada göğüs göğse çarpışmaya hazır olmanız gerekiyor. Piyade son noktayı koyabilmeli, birebir temasta gücünüz yerinde olmalı. Bunları nasıl sağlayacağız? Eğitimlerimizde hareketlilik, kuvvet ve dayanıklılık gibi yeteneklerimizin birleşimiyle yapacağız bunları. Fiziksel ihtiyaçlarımıza göre bunları birleştireceğiz. Çok iyi besleyebilirsiniz, çok iyi antrenman yaptırırsınız askere ama uyumazsa getireceği fizyolojik faydaları alamazsanız ya da iyi antrenman yaptırıramazsanız beslenme-dinlenme saç ayağını doğru planlayamazsanız fayda alamıyorsunuz.

TEK-ER'e gidilirken, çalıştırılırken, antrenmanlarımızı mutlaka bireyselleştirmemiz gerekiyor. Herkesin temel ihtiyaçları var, temel aerobik dayanıklılık olmalı ama belli bir seviyenin üzerindeki özel birlikler, özel kuvvetler için ilave bire bir çalıştırılmalarının yeteneklerinin artırılması şart.

Çatışma anında neler oluyor? Spor fizyolojisinde, Guyton isimli yazarın bir fizyoloji kitabı vardı biz üniversitede iken, yazar diyor ki, "Biz neden spor fizyolojisini sona koyduk, 84. bölüme koyduk, en sona koyduk? Egzersiz ve spor sırasında o kadar çok şey oluyor ki insan vücudunda, biz önce normal olanı kalbi, böbreği, ciğeri açıklayalım 83 bölümde, sonra anormal pozisyonları burada açıklayalım dedik." diyorlar. Örneğin 40 kilometre maraton koşan ile bebeğin 40 derece ateşi karşılaştırılıyor. Bir bebeğin 40 derece ateşte metabolik hızı 20 kat artarken, maraton koşusunda bu 20 bin kata çıkıyor. Dolayısıyla savaş alanında yaptığımız işler, kuvvetli bir egzersiz ile yapılan ile benzer işler. Egzersizde biz neyi göz ardı ediyoruz, duygusal ve psikolojik tarafları gözetleyemiyoruz. Teknoloji burada devreye giriyor. Biz egzersiz yaptığımız ortama teknoloji simülasyonunu ekleyebilirsek çok büyük faydalar elde edebiliriz.

Çatışmanın fizyolojisinde kardiyovasküler olarak ciddi değişimler var, venöz dönüşü dediğimiz, kalbin kana dönüşünde değişiklikler oluyor, gerginlik var. Solunumsal değişiklikler var. Göğüs kafesinde sıkışma var. Ölüm ile kalım arasındaki ince çizgideki tüm gelişmeler insan vücuduna büyük stres getiriyor. Kan akımı, yoğunluk, nabız, solunum sisteminde derin ve hızlı nefes gibi çok sayıda birleşenden aynı anda bahsediyoruz muharebe sahasında. Teknoloji ilerlemesiyle, herhangi birimizi MR cihazına soksak birçok olumsuzluklar tespit edebiliriz. İşte biz insan vücudundaki bu değişiklikleri biz muharebe sahasında, nefes nefese ölçtüğümüzde kendimizi biliyoruz. Asker veya polisimizin teknoloji ile fizyolojik kondisyonunu biliyoruz. Eğer sizin verdiğiniz aynı şiddete 200 metrede koşturacaksınız askerinizi, biri 160 diğeri 140 nabızla geldi. Komutan bunu gözlemledi. İkisnin arasındaki fark, aslında o 20, ölüm ile kalım arasındaki mesafe. Belki birisine daha düşük antrenman yapmak zorundasınız. Biz teknolojiden askerin geliştirilmesinde bilimsel olarak bu şekilde yararlanmak zorundayız. Yorgunluğumuzu ölçen cihazlarla askerin yorgunluk ve dinlenme süreçlerini ayarlayabiliriz.

Örneğin duruş bozukluğu (postür) ile ilgili, ağır yük taşımakla ilgili ciddi problemler var askerimizde, polisimizde. Belki statik dinamik egzersizlerden, eksikliklerden veya geri plana itilmeden kaynaklı, sırt çantasının ağırlığından kaynaklı kol uyuşmasıyla başlayıp felce kadar giden rahatsızlıklar görüyoruz.

Bel ağrısı hemen hemen savaşçı personelimizin çoğunda var. Sırt çantasının yüklenişindeki şekil bile bize eşya koyma şekli bile bizim için çok önemli oluyor. Aselsan'ın örneğin geliştirdiğini yük geliştirmeye ilgili aparatı gördük biraz önce. Bunları kullanabilmek, pratik alana döndürebilmek çok önemli.

Baktığın zaman fizyolojik olarak, enerji, beslenme ve biyoteknik metabolizmanın düzenlenmesi gibi işleri mutlaka biz asker muharebe sahasındaki personelin çantasına koyarak verebiliyoruz. Orada asker mutlaka küçük bir takviyeyle, karbonhidratla ilgili eksikliğini, suyla veya sıvıyla ya da ergonomik yardımcılarla alabiliyor.

En önemli nokta, reaksiyon sürati konusu. Bugün askerin verebileceği en önemli fiziksel tepki. Çünkü artık dayanıklılık savaşından ziyade reaksiyon savaşına, reaksiyon vermeye ilgili ve bu süreyi geliştirmeye ilgili, yani fiziksel işleri yapıyoruz. Dünya artık fiziksel reaksiyon süratini nasıl geliştirebileceğini çalışıyor. Bugün antrenmanların büyük çoğunun parametresi artık dayanıklılıktan, sürat ve kuvvete, güce doğru geçiyor. Konvansiyonel harpte daha çok dayanıklılık ön plandayken, askerlerin ulaşması, yürümesi ile ilgili çok sayıda problem vardı. Günümüzde artık ulaşımın daha da ilerlemesi, daha operatif işlerin daha çabuk yapılmasını, kuvvet/sürat ve dayanıklılık dengesi istiyor.

Her görevin görev özelinde ayrı dinamikleri var. Buna göre antrenmanlarımızı, fiziksel çalışmalarımızı devam ettirmek ve yönetmek zorundayız. Silahlı kuvvetlerde çalışma döneminde her askeri sınıfa özel antrenman prosesleri geliştirmiştik. Tek bir görev değil, birkaç görevi birden, birkaç enerji sistemini birden çalıştırmamız bize muharebe sahasında kendimizi tanımamız ve başarılı olmamız açısından önemli veriler verecektir. Önemli olan burada askerimizi, göreve yönelik olarak ne ölçüde tanıdığımız, performansını ne kadar bildiğimiz. Eğer kendimizi bilirsek biz o savaşı kazanırız, kendimizi daha iyi analiz ederiz.

SUNUMUNDAN NOTLAR:

- Eğitimler; tek bir göreve özgü olmayıp, koşma, sıçrama, yürüme, sürünme ve tırmanma gibi birçok hareketi içeren bir hareket kombinasyonu şeklinde çok yönlü olmalıdır. Askerlerimizde bu adaptasyonları oluşturmak için çeşitli muharebe görevlerini içeren iyi planlanmış bir eğitim programı tasarlamalı ve her birini muharebe ortamında olduğu gibi maksimum yoğunlukta uygulamalıyız. Fiziksel Hazırlık komutanın programıdır ve komutan kondisyon hedeflerini birliğin misyonu ve tam spektrumlu operasyonları yürütme kabiliyeti ile doğrudan ilişkili olacak şekilde düzenlenmelidir.

I. GÜN DÖRDÜNCÜ OTURUM – YENİ SAVAŞCI
TEMA: Yenilikçi Dönüşüm: Hibrit Teknolojiler ve
Çok Alanlı Operasyonlar

OTURUM KONUSU:
Dijital Dönüşüm ve Yeni Nesil Teknolojik Aktörler

OTURUM TEMALARI:

Dijital Dönüşüm ve Yeni Nesil Teknolojik Aktörler
Müşterek Personel & Müşterek Kuvvet
Yapay zekâ & Nesnelerin İnterneti & Büyük Veri
Yeni Dünya & Yeni Savaş & Yeni Savaşçı
Yeni Teknolojilere Uyum

IV. OTURUM ÖZETİ

Yapay zekâ alanındaki geliş, neyi istediğiniz veya neyi başarmayı istediğinizle ilgili olacaktır. Ve elbette rakiplerinizin neyi geliştirip, neyi başarmak istediğiyle de alakalı. Diğer ülkeler savunma harcamalarını nasıl yapıyor, hangi alanlara öncelik veriyor, bu stratejiler yapay zekânın savunmada kullanımı noktasında rehber niteliği taşımaktadır. Yapay zekânın ilk dalgasında makineler insanların kodladığı şeyi uygular. İkinci dalgada çok fazla veriyi anlamlandırmanıza yardımcı olur. Üçüncü dalga ise kendi kendine en iyi şekilde nasıl öğrenir ve nasıl uygulamalarla ilgilidir. Türkiye'nin yapay zekâ yol haritası için de en önemli strateji bu olacaktır. Amerika ve Çin binlerce insansız varlığı bir arada kullanmayı hedeflemekte, çoğu ülke yapay zekâ ile insansız sistemleri bir arada kullanma yöneliminde çalışmalar yapmaktadır. Sürü teknolojileri farklı unsurlar arasındaki iş birliğiyle büyük bir katma değere dönüşecektir.

Ülkeler, yapay zekâyı saldırmak ve savunmak arasında eğitmektedir. Saldırı, savunmacı taktiğe yanıt vermezse fayda sağlayacaktır. Örneğin, füzenin hedef tercihinde hangi zararlı nesneyi önceliklendirmesi yeni teknolojilerde avantaj olarak kabul edilmektedir. İnsansız uzaktan kontrol edilebilir sistemlerde, hiyerarşik ve merkezi bir komuta kontrolüne bağlılık, çok alanlı işlemler yapılmasına engel teşkil edebilir. Dolayısıyla yapay zekâ kullanımında rolleri değiştirecek temel noktalardan biri savunma yapay zekâsındaki çarpan etkisi olarak değerlendirilmektedir.

Çok alanlı operasyonlar (kara, hava, deniz, uzay ve siber) içerikli teknolojilerin, aynı anda topyekun savaş alanı ile değil, bölgesel kullanımlarla geliştirilmesine çalışılmaktadır.



Dr. Poyraz Alper ÖNER
SAVUNMA SANAYİ
BAŞKANLIĞI (SSB)
MODERATÖR

Değerli katılımcılar, hepiniz hoş geldiniz. SASAD'ın girişimiyle, Savunma Sanayi başkanlığımız ve Millî Savunma Bakanlığımız desteğiyle düzenlenen bu organizasyonda yer almaktan mutluluk duyuyorum.

Buraya gelirken, anahtar kelimeleri vererek geleceğin askeri nasıldır diye yapay zekâya sordum. En çok dikkatimizi çeken nokta, yüksek hız, çeviklik ve kuvvet. Yani yüksek hız en öndeki parametre.

Hızı ve komuta kontrol karar destek ile giyilebilir sensörleri görüyoruz. Nereye geleceğim? Bir sürü sensör, karar almak için kullanılan yöntemler ama bunları sahaya sürmek için idari olarak bir yöntem düşündük mü? Evet düşündük, Harekât Destek Daire Başkanlığımız kuruldu ve hayata geçirildi. Ana sistem tedariki yaklaşımında operasyona göre Tek-Er'in ihtiyacı olan ve teknolojinin hızı göz önüne alındığında acil kabiliyet kazanımı hedefleyen, harekât destek konseptiyle hızlı çalışmalar yapılıyor. Temel gereksinimlere odaklı çalışıyoruz.

Bu çalışmalar sürdürülürken, çevik proje yöntemini uyguluyoruz. Takvim maliyet ve performansın önünde bu yöntemde. Bugün için sahada mümkün olan çözüm, uzun vadede sunulacak mükemmel çözümden daha değerlidir diyerek hareket ediyoruz. Prototip bazlı ürünlerin geri beslemelerini alarak mükemmelleştirmeye çalışıyoruz. Büyük veri ve yapay zekâ imkanlarını her alanda kullanıyoruz.

Şimdi sözü konuklarımıza bırakmak istiyorum.



Dr. Heiko BORCHERT
DAIO
ALMANYA

Merhaba, sizlerle birlikte olmaktan dolayı çok mutluyum. Almanya'da bir savunma şirketi için insansız deniz sistemlerinin kullanımıyla ilgili çalışmalar yapıyordum, şimdi yapay zekânın kullanımına odaklanıyorum.

Öncelikle savunma yapay zekâsı hakkındaki çalışmalara rağmen, gerçeklik şu ki silahlı kuvvetler tarafından yapay zekânın kullanımı evrimseldir. Devrimci ve evrimsel olduğu için kendinize şu kritik soruyu

sormalısınız. 'Yapay zekâ ne yapmalı? "Yapay zekâdan ne istiyorsun, neyi başarmalı?" Stratejik hırs seviyenizi tanımadan ve belirlemeden bir kıyaslama yapamazsınız. Bir kıyaslamamanız yoksa, bir yol haritanız yoksa neyi takip edeceğinizi ve neyi yapacağınızı bilemezsiniz. Yolda olup olmadığınızı belirleyemezsiniz.

Uzun bir çalışmanın arka planı olarak 'Very Long Game – Çok Uzun Oyun: Küresel Savunma Yapay Zekâsı Durumuna İlişkin 25 Vaka Çalışması" isminde uluslararası karşılaştırmalı analiz içeren kitabımda da yapay zekâyı 25 farklı ulusun nasıl tanımladığını karşılaştırmıştım. Sadece NATO ve AB ülkeleri değil, çok farklı ülkelere baktık, çünkü yapay zekâ konusunda çok fazla grubun düşünceleri ve girişimleri var.

Milletler savunma yapay zekâsı hakkında ne düşünüyorlar, nasıl örgütleniyorlar? Savunma yapay zekânın gelişiminde ne tür araştırma ve öncelikleri var? Nereye harcamalarını yapıyorlar ve yapay zekâ finansmanını nasıl yürütüyorlar? Ülkelerin askeri yapay zekâdaki 6 noktaya yönelimlerini iyi anlamalısınız. Düşünme ve Kavramlar, Organizasyon, Ödenek, Ar-Ge, Uygulama—Dağıtım ve Eğitim alanlarındaki noktaları iyi anlamalısınız.

Batılı ülkelerin stratejik rakiplerine karşı farklı stratejileri var. Bazı batılı ulusların stratejik meydan okuyucuları olarak adlandırdıkları şeye ulaşın, rakipleri karşı nasıl çalışmaları, Çin, İran'a karşı nasıl çalışmaları var ve bu alanlarda ne yapıyorlar?

Yapay zekâ diye bir şey yok. Anlatmak istediğim şu ki, yapay zekâ bir metotlar kutusudur. Yapay zekâ yöntemlerle doludur ve stratejik hedefinize ulaşmak için hangi yöntemi en iyi şekilde kullanılacağını anlamanız gerekir ve buna yardımcı olur. Amerika'nın İleri Savunma Araştırma Projeleri Ajansı (DARPA), ilginç bir ayırım yapıyor. 3 noktadan bahsediyor. Yapay zekânın ilk dalgası, ilk dalga makineler insanların kodladığı şeyleri uygular. İkinci dalga çok fazla veriniz var ve makinelerin bu verileri anlamlandırmasını istiyorsunuz, büyük veri gibi. İlk iki dalganın temel olarak verimlilik ve etkinlikle ilgili olduğunu söyleyebilirim, ancak üçlü dalga ve bu gerçekten potansiyel olarak oyunun kurallarını değiştiriyor. Üçüncü dalga en iyi nasıl öğrenilir, kendi kendine en iyi şekilde nasıl öğrenir ve uygular konusuyla ilgilidir. Bunlar, faaliyet gösterdikleri bağlamı anlayan sistemler olacak, kendi eylemlerinin sonuçlarını anlayan sistemler olacak. Ve askeri açıdan daha da önemlisi, düşmanca eylemlerin sonuçlarını anlayan sistemler olacak.

Sabah dikkatle EDOK konuşmasını dikkatle dinledim. Çünkü o bizim kendimize sorduğumuz bir soruya cevap veriyordu. İkiye iki paradoksu veya 25 ülkeye gruplamaya çalıştığımız ikiye iki matrisi görüyorsunuz. İnsan merkezli ve teknoloji merkezli paradigma ile veri ve bağlam odaklı. Dikeyde ikinci dalga ile üçüncü dalga arasındaki ayırım var. Yatayda ise komutanın yanıtladığı ve insanların her zaman merkezde, kontrolün başında olacağını söylediği durum var, bu da insan merkezli paradigmadır. Daha merkezci, insan merkezli paradigmada, makinelerin ve insanların ekipler halinde hareket ettiği ve çalıştığını düşünebilirsiniz. Ya da üçüncü dalga ve tartışılan nokta olan karar verme yetkisini tamamen makinelere devretmeye hazır olduğunuzu söyleyebilirsiniz.

Şimdi 10 saniyeliğine kendi kendinize düşünün Türkiye şu anda hangi alanda nerede? Rusya nerede? Almanya ya da Fransa? Tüm 25 ülkeyi adlandırma ilginç çözüm ilginç cevap soru: Hepsi aynı paradigmanın içinde. Aynı şeye takılıp kalmış. İşte bu yüzden başlangıçta şunu söyledim; şu anda savunma yapay zekâsı söylemi, ima edildiğinden çok daha az yıkıcıdır. Çünkü eğer herkes veri odaklı, insan odaklı bir paradigmada faaliyet gösterirse hiç sürpriz olmayacaktır, hiçbir sürprizle karşılaşmayacaksınız.

Herkesin aynı paradigmada olması şaşırtıcı değil ama bu paradigmayı soldan kırmaya aday bazı ilginç adaylar var; ilki ABD. ABD, Yapay Zekânın kullanımını bu üçüncü dalga mantığına dahil etmeye yönelik özel bir programa sahip olan birkaç ülkeden biri ve ABD, örneğin replikatör girişimiyle binlerce insansız varlığı bir arada kullanmayı düşünüyor. Örneğin Çin saldırısına karşı Tayvan'ın savunulmasında. İlginçtir ki eğer ABD soldan sağa doğru giderse, yani makine merkezli kararlara yönelirse Çin büyük ihtimalle takibinde ilk sırada yer alacaktır. Çünkü Çin'in stratejik amacı ABD'nin çok fazla ileri gitmesine izin vermemek ve aranın çok fazla açılmasını önlemektir. Türkiye ve Ukrayna'nın bu karşılaştırmada çok ilginç iki ülke olduğunu görüyorsunuz, çünkü az önce de söylediğimiz gibi ikisi de uçta faaliyet gösteriyor ve uçta olmak her zaman konfor bölgesinde olmaktan çok daha ilginçtir. Şu anda Türkiye'nin sol altta mı kalacağını, ya da makine merkezli kararlara mı yöneleceğini siz belirleyeceksiniz. Çünkü 'Dijital Birlikler' konsepti gibi kavramlara bakarsanız, eğer gerçekten yapay zekânın kullanımıyla tek kişilik sistemlerin mevcut portföyünü artırmaya çalışırsanız açıkça bu sol sütunda kalırsınız ama belki de daha fazla makine özerkliğiyle.

Soru şu ki bu teknolojik bir soru değil mi? Bu bir konsept sorusu ve stratejik bir soru. Sol altta mı kalmak istiyorsun yoksa sol üste mi geçmek istiyorsun? Bu yolda kesinlikle ilerleyen diğer ülke Ukrayna'dır. Çünkü Ukrayna'nın Rusya'ya karşı verdiği savaştan elde edilen bulgular açıkça görülüyor. Ukrayna'nın uzaktan kumandalı sistemler kullandığınız sürece çok net bir mesajı var; savaşta ilk kaybedeceğiniz şey, büyük istasyon ile insansız sistemler arasındaki bağlantıdır. Dolayısıyla insansız sistemleri kullanmaya devam etmek istiyorsanız daha az değil, daha fazla özerkliğe ihtiyacınız var. Bunu aynı zamanda, savunma yapay zekâsının araştırma, geliştirme ve kullanımı konusunda mevcut önceliklere baktığınızda söylüyorum. İşte 25 ülkenin çoğunun odaklandığı kullanım örneklerinin resmi, yani gelişme ve uygulama öncelikleri. Çoğu ülkenin yapay zekâ ile insansız sistemleri bir arada kullanma ve birleştirme isteğini açıkça görebiliyoruz. Ve tüm ülkeler yapay zekâyı istihbarat gözetleme ve keşif görevlerinde kullanmak istiyor. Bu, örneğin yapay zekâyı kullanarak şekli ayırt etmenin olağan yoludur, bu bir sivil mi, bu bir savaşçı mı? Savaşçıysa savaşçıya vur ya da sivilse vurma.

Kullanıma yönelik sapmaların ortaya çıkıp çıkmadığını anlamak için yalnızca en uygun kullanım durumlarına değil, aynı zamanda hangi alanlara kullanıldığına da bakmalısınız, şu anda hangi ülkelerin hangi alanlarda yapay zekâ kullandığına bakmalısınız. Afet yardımı, güvenlik, yüzme, hava trafik yönetimi, sınır güvenliği ya da yakın mesafeden silah sistemi gibi. Askeri kullanımlar ile sivil kullanımlar ya da acil durum kullanımları arasında arada ciddi bir fark görüyorsunuz. Çünkü konu taktik. Yüksek puanı alan konular insansız sistemler, sınır gözetleme, keşif, komuta ve kontrol, siber alanlar. Düşük oranlı alanlar ise yine askeri alanlarda kullanılabilecek sınır gözetleme veya acil durumlar gibi alanlar. Bu John Marc Rickly'nin daha önce bahsettiği şey, yani işte savunma meta evreni tam da bu noktada devreye giriyor. Şu anda birkaç ülkenin odaklandığı yer burası, çünkü sürpriz burada olabilir.

Biz de şu anda Alman Savunma Bakanlığı için bir yapay zekâ savunma projesi geliştiriyoruz. Ukrayna'da kullanılan Alman muhafız ve topçu sistemlerinin silah tabanlı bir sistemi temelinde, daha değerli bir hedef için farklı unsurlar arasındaki iş birliği senaryoları çalışılmaktadır. Şu anda 10 santimetreye kadar düşen bir yer çözünürlüğüne sahip bir savaş alanının sanal bir ikizi üzerinde yapay zekâ kullanımına dair. Yapay zekâ insanlı sistemlerdeki belirli varlıkların bütün özelliklerini taklit ediyor, fiziksel özellikleri, hava durumu gibi. Ve bize tamamen kendisinin saldırı yöntemine dair fikir veya alternatif sunuyor. Günümüzde herkes sürü halinde hareket etmekten bahsediyor. Ancak sürü halinde hareket kavramlarının çoğunda, sürünün geri kalanının sürünün liderinin davranışlarını taklit etmesine dayanmaktadır. Hava sistemlerinde her birinin kendi görevi, her birinin kendini sorumluluğu, hedefi ve misyonu vardır. Şimdi ilginç olan şey, yapay zekânın bireyselliği ve bireysel bir görevi bırakmayı iş birliği yararına terk etmeyi öğretmesidir. Sürünün farklı unsurları arasındaki iş birliği, daha büyük değere sahip bir hedefi vurmanız anlamına geliyorsa ve veya daha büyük bir değeri savunmanız, korumanız anlamına geliyorsa. Burada modellenen de bu. Daha büyük bir hedef için farklı elementlerin bir araya gelmesini sağlamak.

John Marc'i dinlediğinizde, yapay zekâ kullanımının büyük olasılıkla saldırıdan faydalanacağını söylemişti. Düşmanın savaşta her zaman söz hakkı vardır. Saldırı, yalnızca savunmacı bu taktiğe yanıt vermezse fayda sağlar.

Kara tabanlı Savunma için geliştirilen başka bir taktiğimiz var, gelen bir nesnenin füze olup olmadığını değerlendiren bir sistem.

Kimse Ukrayna'nın en kritik sorununa bakmıyor mu? Nispeten ucuz insansız sistemleriniz ve savunmak için nispeten pahalı füzeleriniz var. Yani 2000 dolarlık bir platforma karşı 1 milyonluk bir füze kullanmanın maliyet faydası. Bu ekonomik ve sürdürülebilir bir yol değil. Bu yüzden geliştirilmekte olan taktik, bir füzeyle ne tür nesnelerin vurulması gerektiğini ve hangi durumda kara tabanlı bir hava savunması kullanabileceğini öğreten bir taktiktir yapay zekâya.

İşin içinde hiçbir insan yok, hepsi makine ve yapay zekâ savaş alanında nasıl davranılacağını öğreniyor. Yapay zekâ üçüncü nesil ile yapabileceğiniz şey budur. Ve bu sizin bulunacağınız noktayı belirliyor. 25 ülkede gerçekten ilginç olan şeyin, bazı beklentilerin doğrulanmasının bazı sürprizler olduğu sonucuna varıyor. Bu nedenle, örneğin doğrulanmış beklentilerle başlayarak, evet savaşlar öğretmenlerdir, ancak bir savaşta gördüklerinize ve ne öğrendiğinize çok dikkat edin. Örneğin, Batılı gözlemcilerin çoğu şu anda bir savaşta bunu görüyor. Batılı çok sayıda gözlemci, Ukrayna'nın çok kaynaklı bir füzyon resmi olan ortak bir operasyon için yapay zekâyı kullanmasından etkilendiler. Ancak, çoğu AB ve NATO ülkesinde aynı ortak operasyonel tabloyu oluşturamayacağınızı unutuyorlar, çünkü gizlilik sorunları. Verileri farklı hizmetler arasında paylaşamazsınız. Kolluk kuvvetlerinden gelen verileri güçlerle paylaşamayacağınızı söyleyemezsiniz. Ve kesinlikle AB içinde asla yapamayacağınız şey, kendi vatandaşınızın bir iPhone ile dolaşması ve iPhone bilgilerinin ortak operasyonel resminize kaynaşmasıdır. Bunların hepsi Ukrayna'da çalışıyor. Ama bu asla AB içinde olmayacak.

Anlaşılması son derece önemli olan üçüncü konu ise, savunma sanayi inovasyonunun adımlarının çocuk gibi olduğunun unutulmaması gerekliliği. Sanırım sabahları eski sistemlerin performansını yeni teknolojilerle karşılaştırarak eski sistemler için üretim kapasitelerini nasıl artırmamız ya da ayarlamamız gerektiğini soran bir soru vardı. Mesele şu ki, çok az ülke ekosistem yönetiminde yeni başlayanlar, köklü savunma şirketleri, araştırma ve teknoloji organizasyonu ve silahlı kuvvetler getirmekte iyidir.

Bunu yapmakta iyi olduğunu düşündüğünüz tüm ülkelerin hepsinin bir sorunu var ve özellikle kamu sektörünü dijitalleştirmenin ön saflarında olduklarını düşündüğünüz ülkeler, kamu sektöründen silahlı kuvvetlere fayda sağlamada son derece kötüler.

Estonya, e-devlet söz konusu olduğunda liderdir, ancak ordu ve silahlı kuvvetler yeni teknolojiye başlamakta çok tereddütlüdür. Estonya yapay zekâ konusunda planı olan bir ülke değil, İsrail de değil. İsrail'in örgütlü bir karmaşa olduğu noktasında İsrail'e sahibiz. Çünkü yukarıdan aşağıya bir sistemden ziyade aşağıdan yukarıya bir sistemdedir. İsrail'in özel bir savunma amaçlı yapay zekâ bütçesi ve özel bir savunma amaçlı yapay zekâ stratejisi yok. Yani normalde sahip olacağınız tüm unsurlar yerinde değildir, her şey tüm fırsatlarla değil, aynı zamanda risklerle de aşağıdan yukarıya doğru yönlendirilir.

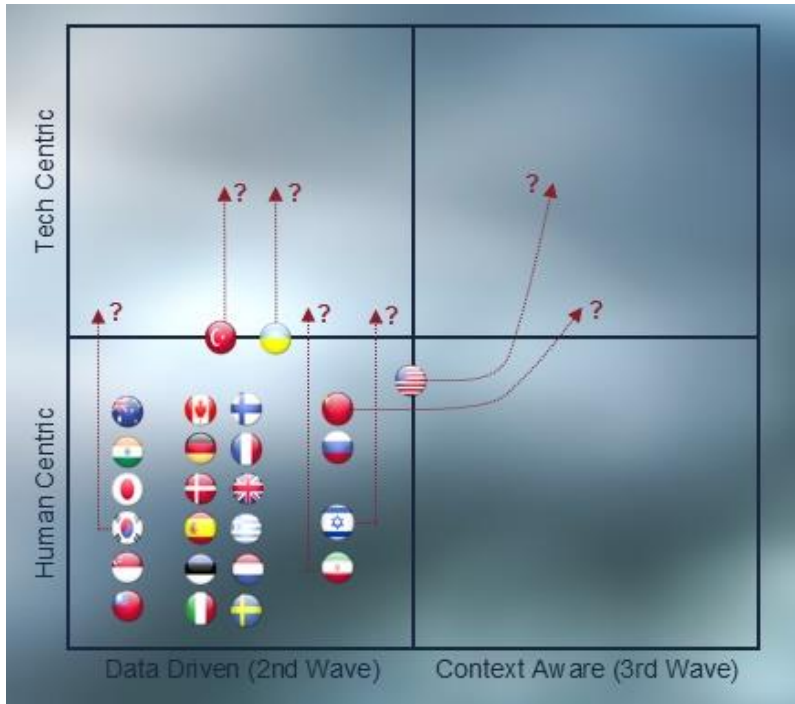
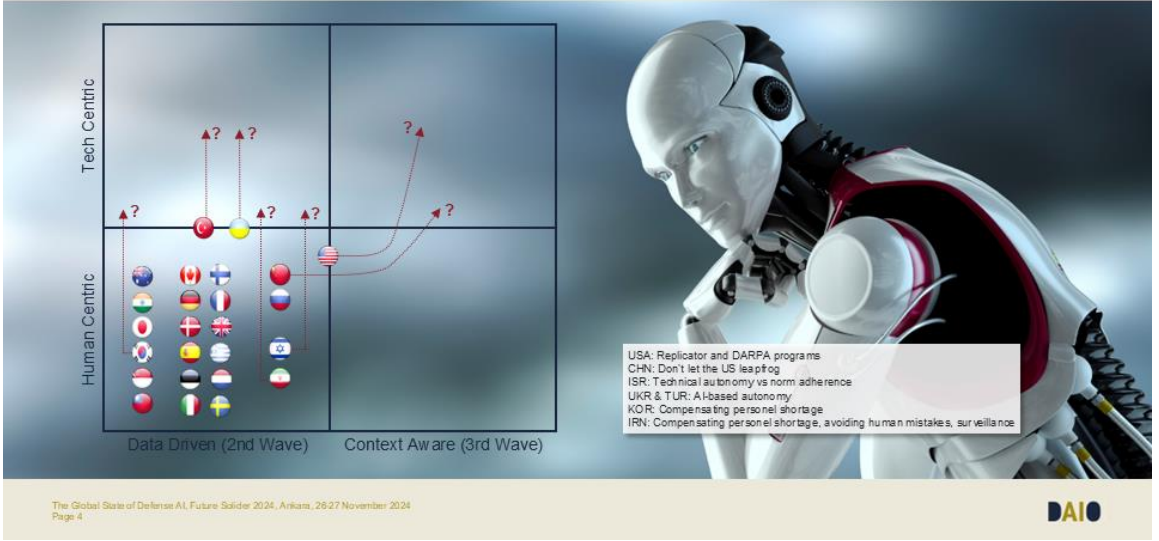
Tayvan'daki TSMC savunma yapay zekâsının en ön parçası çip üretiminin lideri. Üzgünüz, ekosistem tamamen ticari şirketlere dayanmaktadır ama ekosistemin tamamen dayandığı ticari şirketler savunma için çalışmıyor. Bu yüzden bunu, sorduğunuz soruyu sormak olan ekosistem nedeniyle vurguluyorum. Sonunda sahip olduğunuz beklentileri karşılayan çözümler geliştirmek son derece önemlidir.

Ve belki de biraz iç karartıcı bir notla bitirmek istiyorum. Ancak, normatif tercihlerin yeniden düzenlendiğini akılda tutmanın önemli olduğunu düşünüyorum. Bunu Ukrayna'da ve İsrail'de açıkça görüyorsunuz. Bu bir teknoloji sorunu değil. İkincil hasarla başa çıkmak istiyorsan, bu insani bir karardır ve teknolojik bir karar değil. Şu anda savaşlardan ve savaş durumlarından geçen ülkelere baktığımızda, bazı ülkelerin tercihleri, yalnızca yapay zekâyı barış zamanı ortamında ilişkilendirmek için düzenlemeye bakan ülkelere tamamen farklı bir şekilde şekillendireceğini görürüz. Barış zamanında faaliyet göstermekten ve savaş zamanında faaliyet göstermekten doğabilecek bu potansiyel olarak çelişkili tercihleri anlamamız ve dengelememizin bizim için çok önemli olduğunu düşünüyorum.

Teşekkür ederim

Dr. Heiko Borchert'in konuşmasında bahsettiği ve 'Very Long Game – Çok Uzun Oyun: Küresel Savunma Yapay Zekâsı Durumuna İlişkin 25 Vaka Çalışması' isimli kitabında yer alan ülkelerin teknoloji ve insan odaklı yapay zekâ odaklanma eğilimine yönelik çalışması.

Thinking and Concepts: Surprising Harmony



SORU: Ukrayna ve Türkiye'yi insan ve teknoloji merkezli paradigmada ayıracak temel unsurlar nelerdir? Sizce yapay zekâ kullanımında geleceği neler belirleyecek?

CEVAP: Ukrayna Cumhurbaşkanlığı Ofisi tarafından belirlenen stratejik öncelikler açıktır. Öncelik ve gelecek uzaktan kontrol edilebilen değil, otonom sistemlerdedir. Ukrayna'yı net ayıran strateji budur. Bu, tüm farklı gelişim standartlarını hesaba kattığınızda Türkiye'nin alabileceği olası bir geçmiş varsayımıdır. Son 10 ila 15 yılda SSB tarafından başlatıldı Artı Savunma endüstrisinin yaptığı şey bu değil. Türkiye, komuta kontrol insansız sistemlerini öne aldı. İnsansız uzaktan kontrol edilebilir sistemlerde hiyerarşik ve merkezi bir komut kontrolüne bağlı kalmaya devam ederseniz, asla çok alanlı işlemler yapmayacaksınız, bu gerçekten kilit konulardan biridir. Çünkü tüm veri dizileri daha sonra merkeze gelecek ve o merkezden geri dönecek, o zaman elbette düşmanın belli. Ve eğer siz merkezi olmayan komuta kontrol merkezine sahipseniz bunun ilk bertaraf edilmesi gerektiğini bilirsiniz ve ateş edersiniz. O zaman elbette, merkezi olmayan yetenekleriniz merkezi olmayan komuta kontrolüne girmeniz gerekiyorsa ve bu bir zihniyet sorunu ise, rakibin ilk önce neye vuracağı açıktır. Yani insansız sistemler, komuta kontrol mantığı, operasyonel tablo için SSB öncelikleri. Gerçekten ilginç bir unsur var ki, düşük dereceli kullanım durumları şu anda kullanımını gerçekten vurgulayan iki ülke var. Gerçekten ilginç bir unsur var ki, düşük dereceli kullanım durumları şu anda savunma sanayinin yeteneklerini ve yeteneklerini geliştirmek için yapay zekâ kullanımını gerçekten vurgulayan iki ülke var. Biri Türkiye ve diğer Rusya. Bu dört çabayı bir araya getirirseniz, yorumum bu yöne gidiyor. Benim yorumum bu, soru şu: Karar vericiler ne ölçüde ne hissedecekler? Efendi ve hizmetkar arasındaki ilişki. İnsan efendidir, yapay zekâ her zaman hizmetkardır ama sen ne yapmak istiyorsun? Elbette rolleri tamamen değiştirebilirsin. Bu yüzden Ukrayna'nın vurguladığım yolda gittiğinden çok eminim. Türkiye için ise zaman gösterecek ve birkaç yıl sonra tekrar geldiğimizde bunu tartışacağız...



**Hava Mühendis
Üsteğmen Emrah SALAR
Millî Savunma Bakanlığı**

Üsteğmen Emrah Salar, sizlere Hava Kuvvetleri Komutanlığı bünyesinde geliştirilen Hava kuvvetleri Bilgi Sistemi (HvBS) sistemini anlatacağım.

Türk Silahlı Kuvvetleri (TSK) çapında eğitim kurumları ve sosyal tesislerde internet ağı için oluşturulmuş kablosuz ağ alt yapıları mevcut olup, TSK ağına bağlı birlik yerel alan ağlarında hücresel

haberleşme ağları kullanılamamaktadır. Türk Silahlı Kuvvetleri (TSK) çapında eğitim kurumları ve sosyal tesislerde internet ağı için oluşturulmuş kablosuz ağ alt yapıları mevcut olup, TSK ağına bağlı birlik yerel alan ağlarında hücresel haberleşme ağları kullanılamamaktadır. Gelişen teknoloji ile bilgi sistemlerinin mobil olarak kullanım ihtiyacı gün geçtikçe artmakta olup TSK Ağına hâlihazırda hücresel sistemlerin (4.5G-5G) kullanımına yönelik mevcut bir yetenek bulunmamaktadır. Hava Kuvvetleri Komutanlığı'nda uçuş hattı personeli, uçak bakım hangarlarında uçak başında çalışan bakım personeli, eğitim, simülator ortamlarında, artırılmış gerçeklik, sanal gerçeklik uygulamalarında kullanılan gözlük ile teçhizatın ve gelişen teknolojilere bağlı olarak IOT cihazların TSK ağına bağlı kablosuz olarak kullanılmasına ihtiyaç duyulmaktadır. Mevcut durumda wireless (kablosuz) modem vb. sistemler, ihtiyacı kısmen ve lokal olarak karşılayabilmekte, bağlantının olması istenen her yerde wireless modem ve/veya router kurulumu gerektirmekte olup, ilerleyen dönemde kapsama alanları ile hızlarının sınırlı ve düşük kalacağı değerlendirilmektedir.

Bu proje ile Millî yazılımlar ve donanımlar kullanılarak TSK Ağı üzerinde güvenli kablosuz iletişim ağı alt yapısının geliştirilmesi, bu altyapıyı ile Hava Kuvvetleri Bilgi Sistemi'ni (HvBS) mobil cihazlar ile kullanabilir hale getirilmesi ve bu sistemin birliklere yaygınlaştırılması amaçlanmaktadır. Hava Kuvvetleri Komutanlığı'nın ihtiyacının karşılanması yanında TSK çapında kablosuz ortamda 4.5G gibi teknolojiler kullanılarak TSK Ağı ortamında gerekli güvenlik tedbirleri alınarak güvenli ses ve data iletişimin sağlanmasıyla intikal halindeki gemilerde, TSK Ağı ortamında gerekli güvenlik tedbirleri alınarak güvenli

ses ve data iletişiminin sağlanmasıyla intikal halindeki gemilerde, uçak bakım hangarlarında ve ileri harekât noktalarındaki unsurlarında harekâtın etkinliği ve çapının artırılarak TSK'ya mobil yeteneğin kazandırılmasıdır. Günümüz kablosuz erişim cihazları üzerinde bulunan şifreleme protokollerinden faydalanmaya ek olarak donanımsal ve yazılımsal şifreleme yapılacaktır. Erişim ve mobil istemci yönetim fonksiyonu tesis edilecek, bu yetenek ile kullanıcı yetkilendirme ve sistem kontrol mekanizmalarının ayrıştırılması sağlanacaktır. Askeri operasyonlarda hızlı ve güvenilir iletişim sağlanması, özelleştirilmiş uygulamalar ve servisler ile saha operasyonlarının desteklenmesi, acil durum yönetimi ve koordinasyonunun güçlendirilmesi, güvenli veri aktarımı, veri güvenliği ve gizliliği sağlayarak sızma risklerinin minimize edilmesi, hücresel teknolojinin (4.5G-5G); geniş kapsama alanı, yüksek veri hızı, yüksek kalite servisi ve güvenlik gibi birçok avantajı bulunmakta olup, bu sayede sistemlerin lokasyon bağımsız, mobilize edilmiş ve güvenli olarak kullanımı sağlanabilmesi, geniş bant altyapısı; yapay zekâ, otonom sistemler, artırılmış sanal gerçeklik, bulut bilişim, sürü-akıllı sistemler, büyük veri işleme, endüstri 4.0 gibi birçok teknoloji için temel teşkil edebilmesi, hücresel ağ ile gerek sabit baz istasyonu, gerek ileride gerçekleştirilebilecek mobil taşınabilir baz istasyonları vasıtasıyla istenilen bölgeye kablosuz yerel alan ağı taşıma kabiliyeti götürülebilmesi, mevcut iletişim altyapı kullanım sahasının zenginleştirilmesi ve modernize edilmesi, Türkiye'nin stratejisi "5G ve Ötesi" ile hem mevcut ihtiyaçlar karşılanabilecek, hem de ileride gelecek olan 6G teknolojisinin sisteme hızla kazandırılmasına ve altyapı oluşturulması amaçlanmaktadır. Proje ile tesis edilecek altyapı ve yetenekler "Kablosuz emniyetli iletişim sistemlerini bünyesinde barındıran bir kuvvet yapısına ulaşılması" hedefi için temel oluşturacaktır.

SORU: Projenin tamamlanma süresine dair bir şey söyleyebilir misiniz?

CEVAP: : Şu anda Hava Kuvvetleri Ahlatlıbel Hava Radar Mevzi Komutanlığı'nda testlerimiz devam ediyor. TSK 1 numaralı ağda yapmak için de çalışmalarımız devam ediyor. 2025 yılında projenin Millî Savunma Bakanlığımız ve Genelkurmay başkanlığımız izniyle projeyi tamamlamayı ve yaygınlaştırmayı hedefliyoruz.



**Semih DEMİRTOKA
HAVELSAN**

Merhaba, bu güzel organizasyonda sizlerle bir araya gelmekten büyük mutluluk duyuyorum.

Hibrit teknolojilere genel bir bakış ve ayrıca çok alanlı operasyon kavramlarına üst düzey genel bakış ve ardından NATO stratejisi ve ardından Türk stratejisi ve son olarak geleceğin askerine ilişkin bazı ürünler hakkında temel bilgiler vermek

istiyorum. Burada size günümüzdeki modern savaşla ilgili bazı kavramlardan bahsetmek istiyorum. :Bu savaşların bazı temel özellikler şöyledir; 'Yakınsak birlikte çalışabilirlik ve uyarlanabilirlik.'

Dinamik Görev için yapay zekâya bağlı insansız hava araçları (İHA) ve bağımsız İHA planlamak gibi. Şimdi de geleneksel ve gelişmekte olan teknolojileri birleştiren yakınsamalardan örnekler vermek istiyorum. Planlama İHA'lar, muharebe operasyonlarında pilotlu saldırı uçaklarını desteklerken hedefleri bağımsız olarak belirleyebilir ve önceliklendirebilir. Sayın Heiko sunumunda benzer bir senaryodan bahsetti ama burada örneğin sadık kanat konsepti veya İnsanlı-İnsansız Ekip Çalışması (MUM-T) konseptler devreye giriyor veya belki İHA desteğiyle entegre olan bir kara savaş aracı. Havelsan olarak bunu yaptık, insansız hava araçlarımızda bunu yaptık ve insansız kara araçları birbirleriyle iletişim kurabilir. Yakınsama kapsamında sürü dron teknolojilerine bir örnek vermek istiyorum. Yabancıların, ABD donanmasının düşük maliyetli programı var, biz de Türkiye'de savunma tedarik kurumumuz var, benzer programlar var. Burada size verdiğim örnek, ABD donanması gibi, yani düşük maliyetli İHA'lar, sürü teknolojisi programı, yapay zekânın kontrol ettiği sistem olarak dronların toplu olarak görevleri yerine getirmesi şeklinde. İkinci özellik ise birlikte çalışabilirliktir; kara, hava, deniz, uzay ve siber uzaydaki farklı sistemlerin sorunsuz bir şekilde birlikte çalışmasını sağlamak. Daha önce bahsettiğim İHA'ların kara kuvvetleriyle entegre edildiği koordineli hava ve kara saldırıları ya da deniz gözetleme tehdidini etkisiz hale getirme kullanım örneği, kalıcı deniz alanları farkındalığı için deniz gemisini İHA'lar ve uydularla ilişkilendirmek başka bir örnek.

Kara operasyonu için uzay üssü desteği veya hava savunmasında siber elektromanyetik operasyonlar da önemli. Amerika Birleşik Devletleri'nde multi domain komuta ve kontrolleri de en çok çalışılan konulardan. Birçoğunuz JADC2 programını ya da girişimini duymuşsunuzdur; bu girişim temelde tüm askeri platformları tek bir C2 Sistemine bağlamayı amaçlamaktadır.

Sivil tarafta afet yardımı, insani yardım, deniz savaşında da karşı tedbirlerin kullanımıyla ilgili örnekler verebilirim. Üçüncü özellik ise uyarlanabilirliktir. Hibrit çözümler, hem konvansiyonel hem de düzensiz savaş senaryolarında çalışacak şekilde tasarlanmıştır ve görev esnekliğini artırır. Bu, terörle mücadelede hassas saldırılar, otonom konvoy üretimi, kıyı bölgelerinde deniz mayın temizliği, dağlık bölgelerde gerilla savaşları, sınır güvenliği ve kaçakçılıkla mücadele operasyonları, kentsel isyanı bastırma ve psikolojik operasyonlar gibi olabilir. Uyum sağlama özelliği altında size verebileceğim kullanım örnekleri ve uygulama alanları hava sistemleri, deniz sistemleri, siber uzay ve elektronik savaş ve temel olarak uzaydır. Hava sistemleri altında, sürü dronları size verebileceğim ilk örnektir ve aklıma gelen ilk örnektir. Yer sistemleri, bildiğiniz tüm savaş araçları veya muharebe araçları veya ilginç bir şekilde askerler için dış iskeletler. Meslektaşım Çağlar Bey burada çok güzel bir gösteri yaptı ve ben de bu oturumdan sonra bu fırsatı değerlendirmek istiyorum. Eğer bir ara verilirse, herkesi burada panellerde gördüğünüz Cengaver demomuzu sergilediğimiz koridora davet ediyorum, ancak orada gerçek hayatta da görebilir ve soru sorabilirsiniz. Askerler için dış iskeletler, fiziksel güç ve dayanıklılığı arttırırken, gerçek zamanlı durumsal farkındalık için baş üstü ekranları entegre ediyor.

Sayın Heiko etik kaygılardan bahsetti, ben de her şeyden önce şunu belirtmek istiyorum. İlk zorluk birlikte çalışabilirlik ve çeşitli uluslardan veya satıcılardan gelen hibrit sistemin koalisyon operasyonlarında birlikte sorunsuz bir şekilde çalışmasını sağlamaktır, bu bir setten daha kolaydır. Sonra, etik ve yasal kaygılar temelde otonom silah kullanımı, sivil zarar, bulut deneme hasarı, uluslararası hukuka uygunluk ve son olarak siber güvenlik riski gibi konuları ele almamız gerekir.

Birbirine son derece bağlı olan ve onları siber saldırılara karşı savunmasız hale getiren hibrit sistemler, çünkü siber güvenlik alanında, doğal yüzeye saldıramayacakları.

Siber temelde saldırı yüzeyini büyütürsünüz ve temelde daha savunmasız olursunuz. İşte modern savaşta çok alanlı operasyonlar (MOD), çok alanlı operasyonlar, kara, hava, deniz, uzay ve siber uzay gibi tüm operasyonel alanlardaki yetenekleri entegre eden temsili biçimlendirici askeri stratejidir ve hepimiz düşmanlara karşı senkronize ve ezici bir güç oluşturmayı biliyoruz. Amaç bu alanlardaki güvenlik açıklarını patlatmaktır. Çok alanlı operasyon kavramları alan yakınsaması, belirleyici tempo, dağıtılmış operasyonlar ve size birkaç dakika önce bahsettiğim dinamik hedefleme ve uygulama alanlarıdır. MDO'nun teknolojik sağlayıcıları yapay zekâ, veri füzyonu ve bulut bilişim ve birlikte çalışabilir sistemler ve MDO karmaşıklığının zorlukları, birlikte çalışabilirlik, etik ve yasal kaygılar ve çok fazla kaynak yoğunluğuna ihtiyacımız var.

Burada sunumun tamamını okumayacağım ama hepimiz döngünün farkındayız. Ne döngüsü? Ben 1975'te doğdum. Ben 12 yaşında bir ergenken, 1987'de Berlin duvarı yıkıldığında gençler oradaydı ve bunu sadece gazetelerden ya da medyadan, YouTube belgesellerinden biliyorlardı ama o süreçten geçmiştik, ABD ve Batı'nın baskın güç olduğu tek kutuplu bir dünyaydı ve kültürel hakimiyet, hegemonya, teknolojik ekonomik hegemonya ve benim yaşımdaki insanların çoğu Francis Fukuyama'nın "Medeniyetin Sonu" makalesini bilirdi ve verdiği örnek Bill Gates'in Windows 95'i sergilediği zamandı. Ünlü sosyolog Francis Fukuyama, eğer dünya nüfusunun yarısı işletim sistemi vitrinini izliyorsa, o zaman bilirsiniz işte bu benim "Medeniyetin Sonu, Batı Kazandı" makalemin kanıtıdır, bu tartışmasızdır, olacak olan şey şartları kabul edeceksiniz ve neoliberal ekonomi politikaları, serbest ticaret, daha fazla küreselleşme vb. olacak. Artık fiziksel bir savaş olmayacak ama bugün biliyorsunuz sadece birkaç gün önce haber kanalları veya YouTube kanalları Rusya tarafından küçük bir taktik nükleer saldırı olasılığından bahsediyordu. Hayat fizik gibi bir döngüdür, dalgaları bilirsiniz. Işık ve ses dalgalar aracılığıyla iletilir ve bunun gibi hayat da bir döngüdür, bu yüzden bu noktada ne yaparsanız yapın artık tek kutuplu bir dünya değil, bildiğimiz gibi çok kutuplu bir dünya ve tüm rakipler elde edebilecekleri en iyi son teknolojiyi elde etmeye çalışıyorlar.

Türkiye, NATO konusunda da stratejik ortak olarak teknoloji paylaşımı ve ortak avunma projelerinde de önemli roller üstleniyor. İnsansız sistemler, insansız sistemlerin kaynaşması, bulut tabanlı bilgi işlem, askeri uygulamalarda yapay zekâ, savunma uygulamalarında yapay zekâ, istihbarat toplama ve kullanma, elektronik harp yeteneği, yerli teknolojik gelişmeler gibi alanlarda işbirlikleri yapıyoruz ve artırmaya çalışıyoruz. Bu teknolojileri uygulayacak ve geliştirecek olgunluğa sahibiz ve stratejik önemimiz jeopolitik önemimiz konumumuz tartışılmaz. İnsansız sistemler, insanlı-insansız sistemler çalışması (MUM-T systems), yapay zekâ, bulut tabanlı bilgi işlem sistemleri elektronik harp oluşturma ve takımlama gibi konularda birçok gelişme kaydettik. Burada temel olarak Havelsan'ın ne yaptığından bahsedebilirim.

Sadece Havelsan değil, sunumda TAI platformlarını, BAYKAR Platformlarını görüyorsunuz. Havelsan olarak, Türkiye'nin önde gelen teknoloji şirketlerinden, biriyiz. Yeni ve dağıtıcı teknolojilerin geliştirilmesinde rol alıyoruz ve 2020 yılında dijital birlik konseptini sunduk. Vizyonumuz akıllı, otonom, robotik sistem teknolojileri ve CENGAVER'de gördüğünüz dijital ve giyilebilir teknolojiler üzerine inşa edildi. Komuta kontrol (C5ISR) teknolojilerimiz mevcut. Her yıl CWIX NATO 2024 Birlikte Çalışabilirlik tatbikatlarına katılıyoruz. Karar destek ve operasyonel, Analiz, dijital eğitim ve harp hazırlıkları, otonom ve lojistik destek ve bilgi sistemlerimiz var. Ürünlerimizden SANCAR platformu bizim silahlı insansız hizmet aracımız. Bu bir resim değil, gerçek. Aynı şekilde CAKA, Ar-Ge sürecinde. CAKA denizaltında kullanılabilen kamikaze aracı. Henüz Ar-Ge sürecinde ve yüksek süratli bir araç olarak tasarlandı. Bu Barkan, Barkan bizim tasarım ayrıcalığımızdır. Burada belirtmek isterim ki biz bir platform şirketi değiliz. Platform, silah sistemi şirketi değiliz, donanım şirketi değiliz, donanım üretmiyoruz, sistem entegre şirketiyiz. Tüm bu bileşenleri bir araya getiriyoruz ve askeri makamların kullanımı için ürün haline getirip sunuyoruz. Ve sürü kabiliyetine sahip insansız hava araçlarımız bulunuyor. Örneğin BAHA, bulut altı sitem. Ağabeyi BOZBEY, bu daha büyük. Ve BOZBEY'e bazı heyecan verici şaşırtıcı özellikler ekleyeceğiz. Bu quadcopterimiz Poyraz. Ve ayrıca SONGAR, silah döndürme sistemleriyle ünlüdür. Teşekkür ederim, bana ve kurumuma geleceğin askeri konseptine dair vizyonumuzu anlatma fırsatı verdiğiniz için.

SORU: İnsansız sistemler silahlı kuvvetlerde her alanda çoğalmaya başladı. Silahlı Kuvvetlerimiz de kendi bünyesinde buna dair değişimler yaşıyor. ‘Dijital Birlikler’ konseptinde insansız deniz, hava, kara ve insanın içinde bulunduğu bir konsept var mı? Saha çalışmaları yapıyor mu?

CEVAP: Bütün bu çalışmalarda zaten Millî Savunma Bakanlığımız ve ilgili kuvvetlerdeki komutanlarımızla beraber, sahada talepleri toplayarak ve nihai ürünü çıkarmadan önce örnek ve geliştirilmeye yönelik ürünlerden de geri dönüşler alarak ilerliyoruz. Benim düşüncem, teknoloji seviyesi ile askerlerimizi arttırdık ve askerlerimizin kabiliyetini artırdık. Çok özerk platformlar tamamen kendi kendine hareket eden platformlar noktasına henüz yolumuz var. Askere yardım etmek ve destek için geliştiriliyor, şu an ki dönemde bizim hedefimiz bu şekilde.

I. GÜN BEŞİNCİ OTURUM – YENİ DÜNYA
TEMA:
Teknolojinin Paradoksal Sınırları

OTURUM KONUSU:
Enerji, Lojistik, İstihbarat, İstihdam ve
Teknolojik Sınırlar

OTURUM TEMALARI:
Nitelikli Personel
Teknolojik dönüşüm için planlama ve işbirlikleri
Teknolojilerdeki Gelişmelerin Stratejik Önemi
Mobil ve Modüler Operasyonel Yetenekler

V. OTURUM ÖZETİ

Gelişen teknolojilerle birlikte kalıpların dışında, alışılmışlığın ötesinde düşünmek ve konseptler geliştirmek savunma alanında büyük avantajlar sağlayacak bir konu olacaktır. Çevik bir organizasyon, güçlü insanlar, farklı düşünen ve farklı teknolojik yeteneklere hakim ekipler de savaşlardaki başarı veya başarısızlığı etkileyen bir dinamik olacaktır. Ne olacağını bilmediğiniz şeye hazırlanmak ve öngörülmeyle de hazır olmak gibi çoklu alternatifler gerekecektir. Özellikle değişen teknolojiler, yeni ve eski arasındaki koordinasyon için geçiş dönemi ve yeni dönem hazırlıkları gerekecek. Yeni teknolojiler, yeni düşünme ve fikir ortamlarını zorunlu kılıyor. Bu da aşına olunan yollar ve yöntemleri bir kenara bırakarak yeni düşünme yolları ve önlemler için düşünmeyi hızlandırmayı gerektirmektedir. Özellikle insan-makine uyumu sürecinde yeniliklere uyum sağlamak zor olabilir.

Geleceğin askerinin kıyafetlerinin her türlü kimyasal ve biyolojik ortama uygun, iletişim kopukluğu sağlamayacak iletişim sistemlerine sahip ve kullandığı askeri yeni nesil ekipmanlara yönelik enerji üretim sistemlerine sahip olması savaş alanındaki güven duygusunu etkileyecektir. Dış iskeletlerdeki dizaynlar hız, çeviklik ve istikrarı iyileştirerek mobilitayı artırabilir. Özellikle insansız hava ve kara araçlarından gelecek bilgi akışı, sahadaki askerin durumsal farkındalığını değiştiren bir faktör olacaktır. Aynı zamanda yeni nesil mühimmatlara dayanıklı koruma ekipmanlarına da ihtiyaç artacaktır. Patlayıcı şok dalgalarına karşı koruma sağlayacak kask sistemleri önem arz edecektir. Teknolojinin doğurabileceği güvenlik açıkları ve güvensizlik ortamı, kritik başarısızlık noktalarının oluşmasına yol açabilecektir. Bu hem otonom ve robotik sistemler, hem de sahadaki askerin bireysel güvenliği için çok önemlidir. Askerlerin psikolojik durumları da gelişen teknolojilerle birlikte yeni eğitim programlarıyla desteklenmelidir.

Teknolojik ürünlerde, operasyonellik, lojistik ve bakım tasarım aşamasında belirlenmeli, fonksiyonel ihtiyaçlar, operasyonel ihtiyaçlar ve sürdürülebilir teknolojik ile ekonomik sistem tercih edilirliği ve rekabeti belirleyecektir.

Hızlı çatışma ortamlarında her an operasyonel kullanıma hazır ve kesintisiz operasyon sürdürülebilirliği de başarının etkenlerinden kabul edilmektedir. Yapay zekâ ürün ömrü, arıza bakımı, ekipmanların uyumlu çalışması, güncellenme ihtiyacı gibi süreçlerde de sektörün uzun ömürlü ürün üretimi ve sahada kullanımına katkı sağlayacaktır.

Dijital dünyayı anlamak için, dijital dünyanın son gerçeği yapay zekâ çağının iyi anlaşılması gerekmektedir. Aslında yapay zekâ araç, büyük veri de içerik olarak tanımlanmaktadır. Önümüzdeki yılları şekillendireceği öngörülen dönem, düşünebilen makinelerden, düşünebilmeyi taklit eden makineler çağına gelen ve insan algısına yakın çözümler sunduğu bir çağ olarak kabul edilmektedir. Temelini ise büyük veri ve verilerden doğru analizleri almak oluşturmaktadır.

Kara, deniz, hava, istihbarat, operasyon veya lojistik amaçlı veri kullanımı hedefinde, büyük bir karargah olduğu, bunu yönetmek zorunda olduğunuzu, yardımcı olacak araçları da düşünmek, bunu da rakiplerinizin sizden daha iyi geliştireceğini düşünerek hareket etmek zorundasınız. Yapay zekâ siber güvenlikte siber saldırı ve siber savunma alanında da büyük bir fırsatlar ve riskler zinciri oluşturmaktadır.

Yapay zekâ ve büyük verinin hızla geliştiği günümüzde, teknolojik alt yapıların kısa, orta ve uzun vadeli planlamalarla değiştirilmesi, strateji ve politika açısından hızlı güncellemelerin yapılması, bakış açılarının değiştirilmesi hızlı yapılanmaların temeli kabul edilmektedir. Yapay zekâ gelişiminde, dil modellerini eğitip geliştiren, tehdidin ne olacağını ve o olacağında ne yapmamız gerektiğini bilen, yani geliştiren tarafta olmak için hızlı yapılanmalara gidilmesi tavsiye edilmektedir.

İnternet ile veri savaşları döneminin başladığı, elde edilen verilerle de artık dünyaya şekil verilen teknolojilerin ürün olarak çıktılarının alındığı bir dönemin yapay zekâ ile başladığı, yapay zekânın bir komutan gibi isabetli kararlar vermesinin mümkün olduğu dönemlerin de savunma yapay zekâsı sürecinin bir sonucu olacağı ön görülmektedir.

Veri merkezleri ve veri merkezlerinin alt yapısını oluşturan çip sistemleri, kuantum bilgisayarlar gibi malzemelerin giderek önem kazanacağı belirtilmekte, askeri teknolojilerde işlerlik ile güvenlik arasındaki hassas dengenin bu süreçlerde iyi dizayn edilmesi de önemli bir gereklilik olarak dikkat çekmektedir. Kuantum şifreleme sisteminin de bilgi ve veri akışı süreçlerinde kritik önem taşıyacağı, karmaşık teknolojik ekipmanlarının temel bileşenlerine yatırım yapılmasının önemli olacağı vurgusu yapılmıştır. Ayrıca, tüm teknolojik gereksinimlere rağmen, ordunun kuantum veya benzeri güvenli ağ sistemlerini kullanacak alt yapıya sahip olana kadar kapalı ağ ortamında çalışmasının gerekliliğine de dikkat çekilmiştir. Temel olarak teknolojinin kullanımında her ülkenin kendi çıkarlarına yönelik çalışacağı ifade edilirken, yapay zekâ kullanımının bir noktadan sonra milyarlarca ihtimalin içinden en doğru ihtimali seçebilecek noktaya geleceği, karar verme noktasının yapay zekâyı bırakılacağı dönemin 20-30 yıl içinde gerçekleşebileceği öngörüsü paylaşılmıştır.



Dr. Abdulkadir AVCI
Millî Savunma Bakanlığı
MODERATÖR

Hepiniz hoş geldiniz. Bu oturumumuzda nitelikli personel, teknolojik dönüşüm için planlama ve işbirlikleri, teknolojilerdeki gelişmelerin stratejik önemi konularını ele alacağız. Ben bayan Karena Kyne'e sözü bırakmak istiyorum ve kendisi bize gelişen teknolojiler ve silahlı kuvvetler personelinin uyumuna dair tecrübe ve görüşlerini aktaracak.



Karena KYNE
LANCASTER ÜNİVERSİTESİ
İNGİLTERE

Teşekkür ediyorum nazik davetiniz için. 25 yıldır felsefe yapıyorum ve ilk başlarda felsefe yaptım, sadece sistemler ve ekosistemler hakkında düşünüyorum. Felsefi olarak her şey birbirine bağlıydı ama dünyada işe yaramadı. Yani yaklaşık 15 yıl önce felsefemi uygulamaya başladım. Öğrenmek için temel sorum her zaman şu olmuştur; 'Dünyayı nasıl anlarız, mücadelelerdeki, savaşlardaki

yenilikler nelerdir ve bu soruları nasıl ele alabiliriz?' Bu işi Florida Üniversitesi Özel harekât birimi ile yaptım, Lancaster, İngiltere, Kanada yaptım, Lancaster, İngiltere , Kanada Kuvvetleri güvenlik programı kapsamında yaptım ve yapmaya devam ediyorum. Şu anda Archipelago of Design ile askerler için stratejik oyunlar geliştiriyoruz. Kültürel, coğrafi, çevresel, ekosistemleriniz zorlaştığında, hepinizin yapması gereken savunma ve güvenlik durumunda düşünmek, her şeyi en geniş kapsamda düşünmek ama bunu yapmak çok zor. Ve bunu öğretmek çok zordur. Bu öğretilcekti, öğrenilmeli ama önemli olan neydi? Dünyayı nasıl anlarım, bilginin nasıl oluşturulduğunu nasıl anlarım ve sonra bunu paylaşıyorum. Paylaşmak kolaydır, bunu oyunlar aracılığıyla yapmak daha kolaydır.

Bu sabah saat 09: 00'dan beri eleştirel düşünme veya kutunun dışında düşünme veya mavi gökyüzü hakkında konuşuyoruz. Benim işim, atölye çalışmalarımızı savunma ve güvenlik örgütleriyle yürüttüğümde, kutunun dışında düşünmenin ne anlama geldiğidir. Sözde eleştirel düşünmeyi, kutunun dışında düşünmeyi ve mavi gökyüzü düşünmeyi nasıl yaparız? Felsefe tasarımlara yardımcı olur, yeni şeylerle tanıştırır. ABD Özel Birlikler'den operasyonel güçler getirildi bizlere ve onlarla yaklaşık 1 hafta neler yaptıklarını tartıştık. İstedikleri askeri alanda teknoloji ile insan arasındaki değişime nasıl dahil olacaklarını bulmak, yakın arkadaşlıklar kurmak, güçlü bağlar, güçlü dostluklar ve güven hissi. Örneğin, operasyon güçleri askerler, siber askerlerle iletişime girmeyi reddediyordu. Siber alanda görev yapan arkadaşlarının 'Asker' olarak adlandırılmayacaklarını söylediler. Savunmaları ise, 'Çünkü bizim yapabildiklerimizi yapamıyorlar, bilgisayar başında çalışıyorlar. Ve biz daha çevikiz, bizi onlarla nasıl aynı şekilde çalıştırabilirsiniz, aynı şekilde yani 'asker' olarak sınıflandırabilirsiniz?' şeklinde oluyordu.

Çevik bir organizasyona sahip olmak, güçlü insanlarla çalıştırmayı gerektirir. Sizler kadar çevik, güçlü ve formda olmayanlar var. Ama yeni sistemlerde, teknolojik gelişimde siber için ekip üyelerine de ihtiyaç var. Yarın bu başka alanlar veya sistemler için de geçerli olacak. Yani ordu da bir kimlik değişiminde ve bu değişime herkes hazır mı? Biz onlara kimliği ve çevikliği, birlik olmanın ne olduğunu anlamaları ve 'çerçevelemeleri' konusunda yardımcı oluyoruz. Onları içlerindeki tehditlere, iç tehditlere karşı, içsel fikirlere karşı eğitiyoruz. Değişime direnç konusunda Amerika'da ciddi çalışmalar yaptım. Denizaltıcı alımlarıyla ilgili işe alımlarda Amerika Deniz Kuvvetleri ciddi bir sıkıntı yaşıyordu. Aileleriyle uzun süre iletişime geçememeleri, sosyal ağlardan uzak kalmaları gibi konular dolayısıyla gençler bu işi reddediyordu. Bu yüzden işe alım süreçlerini yeniden markalaştırmak zorunda kaldılar. Kimlik, ilişkilerin nasıl çerçevelendiği ve yakınlığın nasıl çerçevelendiği ile ilgili konular gençlerin düşüncelerini etkiliyordu. Onlara, aileleriyle her an iletişim kurabileceklerini söylemek ve bunun için gerekli teknik alt yapıyı sağlamak, işe alımlarını etkiliyordu. İngiltere'de de benzer konularla ilgili çalıştık.

Gelecek nedir ve düşünülmesi gereken şeylerden ve en çok ihmal edilen şeylerden biri şudur; 'Ne olacağını bilmediğiniz

şeye hazırlanmak.’ Bu yüzden ‘geleceğe dair ön görülene ve öngörülme-yene dair düşünmek’ önemli bir önemsiz görünen.

Dünya teknolojik değişimlerle yeniden şekilleniyor. Torumunum bir resmi ve ‘Neden tsunami için insanlar evlerinin çatısında tekne bulundurmuyor?’ sorusunun ardından, örneğin bir tsunamide çatılar üzerinde tekne bulundurmak hakkında konuştuk. Evet çok efektif bir çözüm gibi gelmiyor ama, evlerinin üstünde kurtarılmayı bekleyen insan kalabalığı için parlak bir fikir gibi duruyor. Eğer merkezi olmayan teknolojiler ve yollar konuşuyorsak, bunlara dair de bir şeyler yapılması ve biraz sıradanlığın dışında düşünmek gerekiyor. İnsanlar ve makineler hakkındaki ilişkimizi anlamak hakkında düşünmek, gelecekte çok önemli olacak. Hiyerarşiyle sınırlandırılmış askeri güçler de teknolojiden etkileniyor, dinamikleri değişiyor. Uzmanlık ve uzmanlar etrafında birçok şey değişiyor. Ve şu an bu konularda öngörülebilirlik veya kesinlik vaat etmeyi başarmak imkânsız. Ama konu savunma ve askeriye olunca, çok organize ve çok öngörülebilir, her ihtimale hazır olması gerekiyor. Özellikle değişen teknolojiler, yeni ve eski arasındaki koordinasyon arasında çok yeni şeyler yapmak gerekecek. Askeriye ve savunma organizasyonlarında yeni fikirleri nasıl organize ediyoruz? Gelecek kavramının anlamı ve birbirine bağı derken neyi kastediyoruz? Sorunsuz otonom sistemler, gerçek zamanlı savunma sistemleri. Biz geçmiş tecrübelerimizle bir şeyler bildiğimizi zannediyoruz ama belki de bunların yeniden canlandırılmaya ihtiyacı var ve gelecekte çok anlam ifade edemeyebilirler.

Gelecekte belirli çatışmaların nasıl görünebileceği ve iklim değişikliği gibi belirsiz ortamların neleri getireceği endişeler uyandırabiliyor. Belki de bir selden, tsunamiden nasıl kurtulacağımıza dair bir fikir bulmamız gerekseydi, hepimizin belirli bir şekilde çizgiler çizmesi gerekliliği zorunluydu. Hiçbirimiz tekneleri bu ihtimalle evlerin üzerine koymayı düşünmezdik doğal olarak. Yeni teknolojiler bize kutunun dışındaki düşünce ve fikirler ortaya koymaya zorluyor. Örneğin askeriye-nin, idari teşkilat yapısının, örgütsel yapının, lojistik ve tedarik süreçlerinde işlerin yeniliğe göre güncellenmemesi, işlerin nasıl yenileneceğini değiştirmezseniz, sonucun artık anlamlı olmayacağı bir durum vardır.

Tüm bu yeni kavramlarla, gerçek zamanlı bilgi, insan-makine ilişkilerinde farklı bir şekilde nasıl düşünebiliriz?

Örneğin insansız hava araçlarıyla operasyonlar durumunda operatörlerin tepkileri. Gelecek veya geleceğin askeri hakkında düşünmek belki de aşına olduğumuz şeyleri bırakmak, aşına olduğumuz araç ve yöntemleri bir kenara bırakıp yeni düşünme yolları ve önlemler hakkında düşündürmektir. Burada önceki deneyimlerden kaynaklı sınırları nasıl yıkacağınızı anlamak önemli, bunun için de daha fazla ve daha geniş bir alanı düşünmek gerekiyor.

Örneğin Özel Harekât Kuvvetleri'nde 'başarısızlık' ifadesini kabul etmek hiçbir zaman mümkün değil ve bunun için sadece başarmak zorundalar. Burada başarmak için doğru şeyi yapmak, başarmak zorunda olmak gibi bir durum söz konusu. Yeni, yeniyi geliştiriyor ve biz de psikolojik atölyelerde buna geleceğin askerini ve geleceğin savaş ortamlarına hazırlıkları sürdürüyoruz. Yeni savaşçı, yeni sistemler gibi dönüşümün gerçekleşmesi için psikolojik olarak da ciddi değişimler gerekiyor. Sorunsuz birlikte çalışabilirlik, insan ve makine arasında gerçek zamanlı teknolojilerle uyum yenilikler ve yeni stratejiler gerektiriyor. Bunların derin anlamları ve karmaşık anlamları var ve bunlar yüzeysel ele alınamaz. Biz bir şeyin ne anlama geldiğine göre şekilleniyoruz ama bu mutlaka en iyi yol olduğu anlamına gelmiyor. Yani temelde geleceğin askerini geliştirmek gerekiyor ve bu henüz öğrenilmemiş bir durum. Eleştirisel düşünmeye sahip olmazsak, gerçekleşen değişiklikler etrafında düşünmezsek büyük fikirlerin uygulanması ve yeniliklere uyum sağlamak zor olacak. Beni dinlediğiniz için teşekkür ederim.



Prof. Dr. Svajonė BEKEŠIENĖ
ASKERİ AKADEMİ
LİTVANYA

Nazik davetiniz için teşekkür ederim, aranızda bulunmaktan gurur ve mutluluk duyuyorum. Sunumum geleceğin askeri, teknolojik sınırlılık ve gereklilikleri üzerine olacak. Geleceğin askerinin dönüşümünü anlamak, yarının ihtiyaçları ve gereksinimlerine yönelik ihtiyaçları belirlemekte büyük önem taşımaktadır. Sunumum, dünyadaki tüm çalışmalarda geleceğin askerinin dönüşümüne

dair kısa ve orta vadeli nihai hedefleri içermektedir. Gelecekteki savaşçı kıyafetleri, çok işlevli bir ikinci cilt olarak işlev gören geleneksel üniformaların ötesine geçer. Temel özellikler olarak yaşamsal belirtileri (kalp atış hızı, vücut ısısı, hidrasyon seviyeleri) ve çevresel koşulları izlemek için sensörlerden oluşacaktır. Üniformalar vücut ısını düzenleyerek soğuk iklimlerde ısı yalıtımı, sıcak koşullarda ise soğutma sağlar. Ayrıca, aktif kamuflaj veya kızılötesi ışınları bastırma gibi gerçek zamanlı çevreye uyum sağlayan kamuflaj teknolojisini entegre edecektir. Grafik gibi gelişmiş malzemeler, gerek teknolojinin iletiminde ve taşınabilir hale gelmesinde gerekse giysilerin hafif, nefes alabilen, kesici, delici, alev ve kimyasal materyallere karşı dayanıklı olmasını sağlayacaktır.

Mikro iklim yeleği, aşırı ortamlarda bir askerin optimal fizyolojik durumunu korumak için tasarlanmıştır. Sıcaklık regülasyonuna yönelik tedbirler ısı tüketimi veya hipotermiyi önlemek için termoelektrik sistemlerle çalışan vücudu aktif olarak ısıtır veya soğutur. Ter yönetimi için gelişmiş nem emici ve hava sirkülasyonu sağlayan sistemler yüksek yoğunluklu işlemler sırasında askere rahatlık sağlar. Entegre enerji sistemleri, teknoloji temelli ekipmanların sürekli çalışmasını sürdürürken pil tüketimini en aza indirirken, hareketten enerji kazanımına yönelik önlemler de barındırır.

Dış iskeletler, askerlerin fiziksel yeteneklerini geliştirerek dayanıklılığı, gücü ve hareketliliği artırır. Dış iskeletler, askerlerin ekipman ve silah gibi daha ağır yükleri azaltılmış yorgunlukla taşımalarına izin verir ve kuvvet artırımını sağlar.

Dış iskeletler, özellikle engebeli arazilerde veya kentsel ortamlarda hızı, çevikliği ve istikrarı iyileştirir ve mobilite artar. Aynı zamanda eklem destek sistemleri dizler ve sırtlardaki gerginliği azaltarak tekrarlayan fiziksel efordan kaynaklanan uzun süreli yaralanmaları önler. Bazı dış iskeletler, asker hareket ettikçe güç üretmesini ve genel enerji kaynağına katkıda bulunmasını sağlayacaktır.

Geleceğin savaşçısı, kesintisiz iletişim ve bilgi paylaşımı için gelişmiş, güvenli bir ağa bağlanır: Yüksek bant genişliğine sahip, şifreli iletişim sistemleri, askerlerin komutanlar ve takım arkadaşlarıyla gerçek zamanlı olarak bağlantıda kalmasını sağlar. Haritalar, düşman konumları ve hedefler gibi veriler vizörlere veya kask ekranlarına yerleştirilecektir. Askerler, giyilebilir veya taşınabilir cihazlar aracılığıyla canlı dron yayınlarına, savaş alanı analizlerine ve görev güncellemelerine erişebilecekler. Sesli komutlar ve sezgisel kontroller, savaşa hazır olmayı bozmadan cihazlarla etkileşimi sağlayacak, ellerin serbest bir şekilde kullanımını sağlayacaktır.

Gelecekteki silah sistemleri hassasiyet, güç ve uyarlanabilirliği birleştirecek, akıllı optiklere ve Yapay Zekâ destekli hedeflemeye sahip silahlar, daha fazla doğruluk ve daha az ikincil hasar için gerçek zamanlı rehberlik sağlayacaktır. Askerler, silahları ölümcül ve ölümcül olmayan modlar arasında geçiş yapmak gibi farklı görev türlerine hızla uyarlayabilirler. Lazerler gibi yönlendirilmiş enerjiye dayalı silah teknolojileri, geleneksel mühimmata ihtiyaç duymadan hassas nişan sağlayacaktır. Sadece lazer atışı için mobil enerji üreten araçlar ve askeri birlikler kurulması da planlanmaktadır.

Silahlar, atış doğruluğunu artırmak için çevresel faktörleri (rüzgâr, mesafe, yükseklik) izleyen sensörler içerecektir. Gelecekteki savaşçılar, fiziksel ve siber tehditlere karşı korunacak gelişmiş sistemlere sahip olacaklar. Hafif ancak dayanıklı malzemeler, hareketlilikten ödün vermeden mermilere ve şarapnelere karşı balistik koruma sağlar.

Kimyasal, Biyolojik, Radyolojik ve Nükleer (KBRN) Savunma: Giysi veya kasklardaki entegre filtreler ve sızdırmaz sistemler tehlikeli maddelere karşı koruma sağlayacaktır.

Sistemler, bir askerin iletişimine veya ağa bağlı donanımına yönelik bilgisayar korsanlığı girişimlerini önlemek için siber düzeyde şifreleme ve güvenlik duvarları içerecektir. Patlayıcı şok dalgalarına karşı koruma zırh ve kask sistemlerine şok koruyucu olarak yerleştirilecektir.

Geleceğin savaşçılarının başlıkları koruma, görme geliştirme ve iletişim teknolojisini birleştirecek ve askere durumsal farkındalığı en üst düzeyde sunacaktır. Entegre Artırılmış Gerçeklik (AR) sistemlerine sahip kasklar, haritalar, düşman konumları ve takım durumu gibi gerçek zamanlı bilgileri görüntüler. Gelişmiş optikler, düşük ışııkta veya karanlık koşullarda görünürlüğü artıracak, gece görüşü ve termal görüntüleme yöntemleri geceleri hareket kabiliyetini artıracaktır. Mikrofonlar, hoparlörler ve gürültü önleme sistemleri, yüksek sesli ortamlarda net iletişim sağlarken, mermilere, şarapnelere ve künt kuvvet travmasına karşı üstün koruma sağlayan başlıklar vazgeçilmez olacaktır. Çevresel duyarlılık sensörleri kimyasal veya radyasyon tehditlerini tespit edecek ve askeri anında uyaracaktır. Gelecekteki savaşçılar için güç sistemleri, tüm yüksek teknolojili teçhizatı aşırı ağırlık eklemekten sürdürmek için tasarlanmıştır. Yüksek kapasiteli, hafif piller, giyilebilir teknoloji, dış iskeletler ve silahlar için genişletilmiş çalışma sağlayacaktır. Cihazlar, askerin hareketinden (örneğin kinetik enerji) veya çevresel kaynaklardan (örneğin güneş panelleri) enerji toplayacak ve depolayacaktır. Taşınabilir şarj sistemleri veya baz istasyonları, askerlerin sahadaki teçhizatı yeniden şarj etmelerini sağlayacaktır. Verimli güç yönetimi sunacak kılı sistemler, kritik cihazlara güç dağıtımına öncelik vererek kesintisiz çalışmayı sağlayacaktır.

Geleceğin askeri konseptinde askerin fiziksel, zihinsel ve bilişsel yeteneklerinin optimize edilmesini sağlamaya odaklanan çalışmalar oldukça yaygındır. Bilişsel gelişimde, beyin-bilgisayar arayüzleri (BCI) ve sinirsel uyarım karar vermeyi, odaklanmayı ve durumsal farkındalığı artıracaktır.

Sensörler stres seviyelerini izleyecek ve yüksek basınçlı senaryolarda soğukkanlılığı korumak için rehberli nefes egzersizleri gibi gerçek zamanlı müdahaleler sağlayacaktır. Akıllı sistemler bir askerin enerji ihtiyaçlarını izleyecek ve beslenme ve hidrasyon için özel öneriler sunacaktır.

Tükenmişlik, travma sonrası stres bozukluğu (TSSB) ve diğer zihinsel sağlık sorunlarını önlemek için psikolojik destek sistemleri zihinsel dayanıklılık desteği verecek, bu programlara ihtiyaç artacaktır. Tüm bu teknolojik durumsal farkındalık ve yoğun teknolojik ortamlar için de sanal gerçeklik (VR) ve yapay zekâ güdümlü simülatörler, askerlerin gerçekçi eğitim ortamlarına alışmalarını, karmaşık görevlere hazır olmalarını sağlayacaktır.

Teknoloji, hassasiyet, iletişim ve istihbarattaki ilerlemeler savaşlarda devrim niteliği taşımaktadır. Zorluklar, teknolojinin yanı sıra insan uyarlanabilirliğinin önemini vurgulayan teknik, operasyonel, etik ve stratejik faktörlerden kaynaklanmaktadır.

Operasyonel güvenlik açıkları da teknoloji yoğun ortamda riskler içermektedir. Siber saldırılara, sıkışmalara ve aksamalara karşı hassas bir ortam oluşmaktadır. Aşırı güven, kritik başarısızlık noktaları oluşturmaktadır. Maliyet ve sürdürülebilirlik yüksek geliştirme ve bakım giderleri artmaktadır. Küçük ülkeler için bütçe kısıtlamaları da güç dengesi için risk faktörüdür. Geleceğin askeri konseptinde yapay zekânın bağlamsal anlayıştan ve etik akıl yürütmeden yoksunluğu boşluk doğurmaktadır. Karmaşık senaryolar hala insan yargısını gerektirmektedir. Etik olarak hesap verilebilirlik ve özerk silahlarla ilgili zorluklar, küresel kabul ve düzenleme konusundaki endişeler de etik ikilemler olarak dikkat çekmektedir. Düşük maliyetli taktikler gelişmiş sistemlere meydan okumakta, gerilla savaşı gibi asimetrik tehditler gelişen teknolojilerle daha da güç kazanmaktadır. Bu da düşmanın da yeni teknolojilere adaptasyon seviyesinin yüksekliği için önemli bir göstergedir.

Öte yandan, sert hava koşulları, araziler ve elektromanyetik ile siber girişimler insansız sistemlerin en büyük çevresel kısıtlama etkisi olarak dikkat çekmektedir. Artan güven, bilgi aşırı yüklenmesi ve karar yorgunluğu 'geleceğin askeri' konseptinin en büyük teknolojik paradokstur. Teknolojik boşluklar, askeri güçteki eşitsizliklerin genişlemesi ile doğan küresel eşitsizlik bölgelerdeki istikrarsızlığı artırmaktadır.

Geleceğin askeri konseptinde ordu hazırlığının temelinde de değişiklikler gerekmektedir. Yeni teknoloji konseptlerinde 'ne hazır?' sorusunda esneklik, bireysel ve kolektif ekip eğitimi,

liderlik yoluyla verilen görevleri yerine getirme yeteneği cevap bulmalıdır.

‘Dayanıklılık Nedir?’ sorusu teknolojik gelişmeler ışığında zorluklarla yüzleşmek ve başa çıkmak, değişime uyum sağlamak, iyileşmek, hatalardan ve aksiliklerden ders çıkararak öğrenmek ve zihinsel, fiziksel, duygusal ve davranışsal yetenek gelişim programları gözden geçirilmelidir.

Onlarca yıllık operasyonel deneyimlerden ve öğrenilen derslerden yola çıkarak, "hazır ve dirençli" girişim, birkaç temel bileşen aracılığıyla asker dayanıklılığını teşvik etmeyi amaçlayan kapsamlı bir stratejiyi resmileştiriyor:

Bütün Kişi Kavramı: Fiziksel, zihinsel, duygusal ve sosyal sağlığın karşılıklı bağımlılığını kabul eden bütün kişi yaklaşımı, bireyin yaşamının tüm boyutlarında esnekliğin gelişimini vurgular. Bu kapsamlı bakış açısı, askerlerin çeşitli ve zorlu durumlarda hazır olmalarını sağlamak için gereken kaynaklarla donatılmasını sağlar.

Eğitim ve Öğretim: Esneklik geliştirme, askerlerin eğitim programlarında yerleşik olarak bulunur ve esneklik becerileri konusunda sistematik eğitim sağlar. Kanıta dayalı uygulamalar yoluyla askerler bilişsel, duygusal ve fiziksel yetenekleri güçlendirmeyi, stres altında uyum sağlama ve gelişme kapasitelerini artırmayı öğrenirler.

Bütünsel Yaklaşım: Bu girişim, dayanıklılığı askeri yaşamın her yönüne entegre ederek, uyumlu, misyon odaklı bir topluluğu desteklemek için bireysel eğitimi birim düzeyindeki programlarla birleştirir. Dayanıklılık ilkelerini tüm örgütsel düzeylere yerleştirerek, askerlerin hem üniforma içinde hem de üniforma dışında refahını destekleyen bir özen ve hazır olma sürekliliğini sağlar.

Ukrayna ve Litvanya’da yapılan askeri analizlerde, askeri örgütler için entegre eğitim programlarının duygusal, bilişsel ve fiziksel gücü güçlendirmek için esneklik geliştirmeyi rutin askeri eğitime dahil etmenin çok önemli olduğunu gördük.

Ayrıca, liderleri esnekliği modellemeye ve teşvik etmeye teşvik etmenin, uyarlanabilirlik ve destek kültürünü teşvik etmede de büyük değer taşıdığı belirlendi. Bütünsel destek sistemleri kapsamında, askerlerin refahını teknik rollerinin ötesinde sürdürmek için ruh sağlığı, aile desteği ve toplum katılımı için kaynaklar sağlamanın da teşvik edici olduğunu belirledik. Bu tarz motivasyonlar insan-teknoloji uyumunda büyük önem taşıyacaktır. Aynı şekilde, askerlerin bireysel düzeydeki temel birleşenlerinde zorlu durumlarda moral ve motivasyonu artırmaya yardımcı olan iyimser ve umutlu bir bakış açısını sürdürmenin önemi, problem çözme ve duygusal düzenleme gibi sağlıklı stratejiler kullanarak stres ve sıkıntıları yapıcı bir şekilde yönetme yeteneği, başkalarına yardım etmek ve sosyal bağları ve kişisel refahı güçlendiren bir amaç ve bağlantı duygusunu geliştirmenin askerin kendisini takım çalışmasında rahat hissettirdiğini belirledik. Ve onlar için önem seviyeleri de bu sırayla.

Bir asker, kendini asla yalnız hissetmiyor ve bir takımın içinde kendisini takıma ait hissediyor. Aynı şekilde aile olarak gördüğü ortamda açık, dürüst ve etkili iletişimin anlayış, çatışma çözümü ve duygusal desteği teşvik ettiğini, bireylerin zor zamanlarında odaklanma ve dayanıklılıklarını korumalarına yardımcı olduğunu ve duygusal güvence sağladığını tespit ettik. Esnek ve uyarlanabilir aile dinamiklerinin konuşlandırma, yer değiştirme ve stres faktörleri gibi değişikliklere uyum sağlamalarına katkı sağladığını tespit ettik.

Özetle bu konuda da söylemek istediğim, jeopolitik durum bizi en iyi trene yani taşıma ve lojistiğe, ekipman ve kaynaklara sahip bir orduya sahip olmaya zorladı ve zorluyor. Dünyadaki zorluklar, askerlerimizin ileriye doğru en doğru, en dayanıklı güç olmasını zorunlu kılıyor. Bu nedenle askerlerimize, sivillerimize, birliklere ve ailelere değişen ve gelişen teknolojiler kapsamında yatırım yapmaya kararlı olmalıyız.

Saygılar sunuyorum.



Özgür ÖZDEMİR
SAVUNMA SANAYİ
BAŞKANLIĞI (SSB)

Merhaba, sunumum Toplam Ömür Devri Maliyeti ve Lojistik Destek (TSSÖDYP) faaliyetleri ve yapay zekâ ile kestirici bakım alanında olacak. Dünyada da Türkiye'de de son 20 yıldır da odaklanılan nokta, ordumuzu, silahlı Kuvvetleri bir askerden başlayarak, timi, tugayı tümeni, her türlü düzeyde yeni silah ve sistemlerle donatmak. Burada bir buzdağı modelimiz var. Bu konuyu kısa yoldan iyi bir yöntem. İster

satın alma olsun geliştirerek ve hızlıdan tedarik her türlü buzdağının üstünü oluşturmakta, ancak sadece siz bir cihaz sistemi bir eri askeri donatmak radar tankı almakla iş bitmiyor. Bunların hayatta kalması için Eğitim ve eğitim ihtiyaçları maliyeti, özel test ekipmanı maliyeti, tamir-yedek parça maliyeti, işgücü ve personel maliyeti, ikmal desteği maliyeti, envanterden çıkarma maliyeti, teknik veri maliyeti, tesis maliyeti, paketleme, elleçleme, depolama ve ulaştırma maliyeti gibi tedarik ve sahip olma maliyetlerini, entegre destek elemanları maliyetlerini de düşünmek gerekiyor, tümünü tedarik etmek gerekiyor. Dünya Savaşları özellikle bu sonuçları ortaya çıkardı. Savaş kazandıran öğelerden birisi teknolojik üstünlük, birisi üretim kapasitesi birisi taktiksel üstünlükle biri de lojistik destek, bugünkü adıyla ömür devri yönetimi. Yani donattığı cihaz, sistem, , silahların sürekli ayakta hazır ve kullanılabilir olması. Dolayısıyla üst taraf tedarik maliyeti ise alt taraf mülkiyet maliyeti ve toplamı, toplam sahip olma maliyeti toplamı.

Siz eğer sadece sahip olma ve elinizde bulunmasını önemsenirseniz, bunlar sadece parayla çözülemeyecek sorunlar doğrulanabilir. Bir kısmını parayla giderebiliriz dersiniz ama hepsini parayla çözemezsiniz. Ordularınız, cihazlarınız, ekipmanlarınız, donanımlarınız, karakollarınız doğru görevi yapamazsa sonunda bir beka sorunu, harekattan sakıt kalma sorununa yol açabilir. Bunlar bir bütünün ayakta kalmasının bileşenleri. Şimdi bunların önemini, burada hep donatım ve teknoloji öne çıksa da görüyoruz ki ABD bu verileri daha sağlıklı tutuyor bu verileri, NATO çapında ve NATO ülkelerinde var. Tedarik işin fikir aşamasından, tasarım geliştirme de dahil, başlangıç üretim süreci sonuna kadar yani mal, cihaz, sistem,

ürün, elinize geçene kadar platform bakılsa yüzde 20 ya da 30'unu bütün maliyetinizin oluşturuyor. Ancak, o cihaz o platform o tank envanterinizden çıkana ve hurdaya gidene, bir yere bağışlanıp hibe edilene kadar ortada devam eden işletme idame maliyeti işin ana kısmı. Ve bir de envanterden çıkarma maliyeti var işin bu kısmını planlı yaptığınızda ABD'de yüzde 70-72 ediyor. Bunu eğer doğru planlamazsanız, bire aldığınız bir malzemeyi ona idame etmeye çalışabilirsiniz. Ki bu ülkemizde ve diğer ülkelerde de başa gelen.

Bir diğer konu da sizin tüm bu sistemi ayakta tutmak için bir şekilde maliyetinizi, maliyetin büyük bir kısmını oluşturan o idame işletme kullanım destek aşamasının maliyetlerini en aza indirebilmeniz için tasarım sırasında kararlar vermeniz gerekiyor. Ve bu maliyetleri etkileyen kararların yüzde 85'i kritik tasarım aşamasının sonuna gelindiğinde verilmiş oluyor. Yani üretime geçildiğinde, artık üretime geçildiğinde artık envantere alma söz konusu olduğunda da kararların yüzde 95'ini vermiş oluyorsunuz. Yani aslında tankınızı, uçağınızı, helikopterinizi, geminizi artık nasıl bakım idame edecekse öyle tasarlamış oldunuz. Bakım, idame, lojistik yönetime hükmedecek olan diğer hususlara bundan sonra müdahil olamazsınız. Çünkü tasarımınız tamamlanmış ve ürün de ortaya çıkmış oldu. Bu sürece lojistik destek, bakım idame konularında etkili olmak maliyeti düşürmek, bunları kolay yapmak istiyorsanız, kararlarınızı sürece müdahil olup, silahlı güçlerimizde de, lojistik desteğiyle ilgili bakım idaresi ile ilgili birimlerimizin veya bugün firmalarımızın içindeki ürün kaybı, entegre lojistik kaybı, lojistik birimlerinin işleyişe erken müdahil olması lazım ki tasarım yapılırken sadece fonksiyonel gerekler değil fonksiyonel ihtiyaçlar, operasyonel ihtiyaçlar, yani aracın cihazın çalışması bir yandan da bu bir silahlı kuvvetler aracı ise attığını vurması gibi göreve ilişkin fonksiyonlarının yanında bakım idame destekle ilgili ayrıntılara da karar verilmeli. Çünkü bunlar, siz bu cihazı kullanırken ilerideki konulara, esas olarak sizin bu cihaz, bu ekipman üzerinde harcadığınız paranın çoğuna hükmedecek. Dolayısıyla üretime kadar olan süreçte bu kararlar verilirken, lojistik destekten bakım idameden sorumlu olan, tedarik makamlarında SSB gibi, bizlerde, silahlı kuvvetlerinde, kolluk kuvvetlerinde ve firmalarda bunların da masada olması gerekiyor.

Diğer açıdan bugün özellikle de bizler, NATO'daki AC 327 ömür döngü yönetimi programlarına da katılıyoruz.

Yani NATO ülkeleri çapında, özellikle batı ülkelerindeki bu konudaki görüşler ve değerlendirmeler müttefikler tarafından ele alınıyor. Sizin bir cihazı bir sistemi bir ekipmanı, yani bir uçağın bir tankı bir helikopteri bir gemiyi her ne alıyorsanız, onu tedarik etmek demek, sadece onun kendisini almak anlamına gelmiyor. İhtiyaçların karşılanması nedir? İhtiyaç savunma ve güvenlik sistemin 30-40 yıl boyunca, yani envanterinizde kaldığı süre boyunca istenilen performans seviyesinde en az maliyetle kullanılabilmesi ve görevini başarıyla yürütebilmesidir. Yani bunu karşıladığınız zaman ihtiyacı karşılamış oluyorsunuz. Sadece bir tankı yerine koyduğunuzda, bir gemiyi denize indirdiğinizde değil. Dolayısıyla bunu da ayakta tutabilmeniz için sizin kullanıma hazır olma, kullanılabilirlik, güvenilirlik, göreve hazır olma gibi konuları dikkate almanız gerekiyor.

Herhangi bir platform veya sistemi alırken desteklenebilir ve sürdürülebilir olmasına dikkat etmeniz ve bütçelenebilir maliyetle almanız gerekiyor. Onun yanında tüm bu tedarik faaliyetlerini sadece teknik özellikleri, performansı karşılamaya dikkat ederken, entegre destek elemanları dediğimiz ve sahada yer alan tüm unsurların planlanması, hazırlanması ve bunların hepsine dikkat edilmesi gerekmektedir. Bunların hepsi bir araya geldiği zaman sizin ihtiyaçlarınız karşılanmış oluyor, silahlı kuvvetler ve güvenlik kuvvetleri olarak. NATO'da da genel kapsamda da söz konusu tank, uçak için 'odak sistem' deniyor. Ancak tamamıyla, etrafındaki tüm bu süreçle bir bütün oluyor. AC 327 sürecinin ülkemizin ihtiyaçlarına göre uyarlanmış hali olarak düşünebilirsiniz.

Biz bunları Türkiye'de SSB olarak öne çıkarmak, destek vermek, tüm sektörümüzü, silahlı kuvvetler, emniyet, jandarma, sahil güvenlik gibi tüm kullanıcı makam unsurlarımız ve bizimle çalışan entegratörler, yüklenici ve alt yüklenicileri desteklemek için 2017 yılında Türk Savunma Sanayii Ömür Devri Yönetimi Platformu (TSSÖDYP)'nu kurduk. Bunu ülkemize özgü, Millî bünyemize uygun çözümler üretmek için 2017'de proje olarak gerçekleştirdik. Bir nevi, NATO'daki de 2017 yılında tamamen bu amaçla kuruldu ve planlandı. Ömür Devri Yönetimi (ÖDY) yaklaşımının projelerde uygulanması, yerli yükleniciler, kullanıcılar/ihtiyaç makamları ve ilgili tüm paydaşların katılımı ile Ömür Devri Yönetimi Platformunun kurulması hedefleniyor. Amacımız, tedarik dönemi ile kullanım ve lojistik destek dönemini bir bütün halinde ele alan Ömür Devri Yönetimi (ÖDY) ilke ve uygulamalarını yaygınlaştırmak, savunma ve güvenlik

alanında gerçekleştirilecek programlarda/projelerde ömür devri yönetimi, ürün destek ve ilgili konularda millî bünyemize uygun, ülkemize özgü çözümler üretmek.

Organizasyon Sistem Ömür Devri Yönetimi (ÖDY), ÖDY ve Lojistik Analizler, Ömür Devri ve Lojistik Maliyetler ve Özel Mühendislik olmak üzere 4 çalışma gurubundan oluşuyor. Sistem Ömür Devri Yönetimi ve Ömür Devri Yönetimi (ÖDY) ve Lojistik Analizler süreçlerini yürüten çalışma grupları gerekli araştırmalarını tamamladı ve raporlarını yayınladı. Çalışma Grubu 3 Ömür Devri ve Maliyetleri konusunda kuruluyor ve henüz faaliyete girmedi. Şu an Çalışma Grubu 4 kapsamında da Güvenilirlik, Kullanıma Hazır Olma, İdame Edilebilirlik, Bakım, Emniyet, Yazılım, Test Edilebilirlik konularında çalışmalar devam ediyor. Çalışma Grubu 1 ve 2 altında yayınlanan 16 doküman bulunuyor. Tüm bu süreçlere Savunma Sanayi Başkanlığımızın web sitesinden ulaşılabilir.

Teknolojinin geliştiği yerde bakım, idare lojistik noktasında yapay zekâda ele alınmaktadır. Planlı ve plansız bakımları bizler de konuşuyoruz. Diğer taraftan tedarik edilen ürünlerin bakım süreçlerinde günümüzde Kestirimci Bakım söz konusu. Bunu bize yapay zekâ ve teknolojinin getirdiği nokta mümkün kıldı. Kestirimci bakım nedir? Makine veya ekipmanların arızalanmadan önce elde edilen verilerle arıza riskini tahmin etmek veya önlemek amacıyla yapılan bakım türü. Yani siz insan gücüyle pratik ettiğimiz planlı bakım için entegre lojistik destek planları, bakım planları yapıp bunları zaten işletiyoruz. Diğer taraftan da planlamadığımız, başımıza gelen arıza, operasyon sonrası durum için de nasıl müdahale edeceğimiz için plan da bulunduruyoruz. Bunlar başımıza geldiğinde veya planladığımız anda gerçekleştiriyoruz. Bir arıza çıkmadan müdahale edebilir miyiz, konu bu. Amacımız arızaların önceden tespit edilmesi, planlı veya plansız bakım öncesinde bulunması. Bakım maliyetlerinin azaltılması, ekipman ömrünün uzatılması, sanayide üretkenliğin, verimliliğin artırılması. Askeri platform sistemlerin operasyonel kullanıma olma oranının ve kesintisiz operasyon süresinin artırılması. İsteddiğiniz anda istediğiniz ekipmanı kullanabilmeniz.

Bunu nasıl ifade edebiliriz. Bugün bir şekilde kestirimci bakım, arıza ortaya çıkmadan önce koşulları değerlendirerek toplanan veriler aracılığıyla ekipman ve cihazda ne olduğunu tespit edip bakım ihtiyaçlarının tahmin edilmesi.

Bu bir motorda, hidrolik sistemde, mekanik sistemde, elektronik bileşende sıcaklık takip edilebilir, titreşim takip edilebilir, akustik ses sensörü bir problemi belirtebilir. Bunları sensörler aracılığıyla kontrol edip o verileri analiz ederek karar vereceksiniz. Bunu mümkün kılan teknolojiler yapay zekâ. Yapay zekâ ve büyük veri analizinden yararlanarak ekipman durumunu tahmin etmek ve olası arızaları belirlemeye çalışıyoruz. Yapay zekâ bunu makine öğreniminde verilerden öğrenme ve cihazların birbirine bağlanarak veri toplaması ve paylaşılması süreçleriyle yapıyor. Veri analizi gerçek durumu canlı olarak takip ve geçmiş verilerle kıyaslanarak mevcut durumun karşılaştırılması ve anormalliğin tespit edilmesini sağlıyor. İnternet of Things (IoT), yani nesnelerin interneti bunu mümkün kılıyor.

Elimizde olan yapay zekânın şu gün elimizde var olan, jandarma, emniyetin yüz tanıma, araç tanıma için belli bir amaca kısıtlı hizmet eden 'narrow, kısıtlı AI, dar, zayıf' denilen yapay zekâ var. Bunlar öğretim yoluyla çalışıyor. Diğer taraftan Artificial General AI, güçlü yapay zekâ var. Bunlar insanlarla benzer düzeyde öğrenmek, düşünmek ve performans göstermek için tasarlanan yapay zekâlar. Bugün elimizde en çok yoğun olarak kullanılan dar ve zayıf kategoride. Artificial General AI şu an gelişme aşamasında ve 2025 yılında Artificial Super Intelligence yani Süper Yapay Zekâ, bir üçüncü kademe, insanların bilgi ve yeteneklerini aşan yapay zekâ çıkacağı belirtiliyor. Bu kalifikasyon IBM'e göre. Bir diğeri Reactive Machine AI, yani Reaktif Makine Yapay Zekâ olarak geçiyor. Yapay zekâ burada dış uyaranlara gerçek zamanlı olarak yanıt verebilme yeteneğine sahip. Geleceğe yönelik hafıza oluşturmuyor, bilgi saklayamıyor. Bunun bir öteki adımı, Limited Memory, yani sınırlı belleği var. Bilgiyi depolayabilen ve bunu öğrenmek ve gelecekteki görevler için eğitmek için kullanabiliyor. Bunun bir adım ötesi Theory of Mind AI, Zihin Teorisi. İnsan ve insan ötesine geçiyor artık seviye. İnsan duygularını algılayabilen ve bunlara yanıt verebilen, ayrıca sınırlı bellekli makinelerin görevlerini yerine getirebilen. Sizinle etkileşime girebilen yapay zekâ. Ve sonu Self-Aware AI, kendini bilen, başkalarının duygularını tanıyabilen, ayrıca benlik algısına ve insan düzeyinde zekaya sahip yapay zekâ ve yapay zekânın son aşaması. Aslında sanal insana ulaşmaya çalışıyorsunuz. Bunlar geleceğin hedefleri ve kategorizasyonu. Bunlar geliştikçe, yapabildiklerinizin sınırları genişleyecek.

Makine öğrenmesi yoluyla denetimli öğrenme, arıza geçmiş olan verilerle modelin eğitilmesi mümkün, denetimsiz öğrenme yoluyla da verilerin analiz edilmesi ve anormalliklerin keşfedilmesi. Karmaşık veri setlerini daha derinlemesine analiz etmek için Derin Öğrenme kullanılabilir. Bununla görüntü verisi, sesli uyarılar gibi farklı veri türleri üzerinden arıza tespiti yapılabilir. Eğer bir sistemi sensörlerle takip ediyorsak elimizde sürekli güncel veriler olacak. Canlı bir takiple büyük veri kümelerindeki desenlerin keşfiyle anormallikleri tespit ederek veri madenciliği de mümkün olacak. Kestirimci Bakım da bu sistemlerin bir bütünü ve entegrasyonunu oluşturuyor. Veri toplamalıyız bunun için. Askeri araçlar, uçaklar ve diğer ekipmanlar üzerindeki sensörler, sıcaklık, titreşim ve basınç gibi verileri IOT, yani nesnelerin interneti ve sensörler ile toplayacağız.

Diğer taraftan bunları veri işleme ve analiz, yapay zekâ ve makine öğrenmesi yoluyla analiz edeceğiz. Sonuçta arıza tahmin ve uyarı yapacağız. Yapay zekâ, geçmiş veriler ve öğrenilen modelleri kullanarak arızaların tahmin edilmesini sağlamak ve bakım ekiplerine erken uyarı da ana hedefimiz. Arıza ve sıkıntı gelmeden çözüm. Sensörler, veri, sistem, cihaz ile en geniş kapsamda takip edildiğinde nereye gelirsiniz? O sistemin, uçaklarda havacılıkta geçtiğimiz dönemlerden bu yana yapılıyor, dijital ikizini oluşturursunuz. Bu şekilde de o sistemin canlı takibini yapıyor ve uç bir noktaya ulaşmış olursunuz.

Yapay zekâ makine öğrenmesi bunları gerçekleştirirken karar ağaçlarından, veriyi sınıflandırmak ve arıza durumlarını tahmin etmek için kullanılacak. Destek Vektör Makineleri (SVM) kullanılacak. Verileri mantıklı sınıflandıracak, potansiyel arızalar için net tahminler sağlayacak. Yapay Sinir Ağları (ANN) daha karmaşık ve büyük veri setlerini işleyerek, arıza tespiti ve öngörülerini oluşturacak. Zaman Serisi Analizi de, zamanla değişen veriler üzerinde yapılan tahminler, gelecekteki olası arızaları tespit edecek. Makine öğrenmesi ve yapay zekâ bunları kullanıyor.

Bunları savunma sanayinde nasıl kullanabiliriz? Havacılık sektörü özellikle yıllardır bunu kullanıyor, F-35 bunun en güzel örneği. Her türlü faaliyet, yapısal durumu ve durumsal farkındalığına sahip olmak için sensörlerle, bilgilerle donatıyor Amerika ve bu veri akışını sağlıyor. Biz de bunu zırhlı araçlar, helikopterler, savaş uçakları, İHA'lar ve gemiler gibi kritik

araçların bakımını önceden tahmin etmek için bunu kullanabiliriz. Aynı zamanda radar sistemleri, iletişim ekipmanları gibi elektronik sistemlerin sürekli çalışabilirliğini sağlamak için de kullanabiliriz. 7/24 çalışması gereken gözümüz kulağımız gibi sistemlerin sürekli çalışabilirliğini sağlamak, kör kalmamak, kesintiye uğramamak için kullanabiliriz. Aynı şekilde silah sistemlerinin doğru ve güvenilir çalıştığından emin olmak için kullanabiliriz.

Bu faaliyetleri gerçekleştirirken, kestirimci bakım yaparken neye dikkat etmeliyiz? Bu hemen yapılabilecek bir şey değil. Platform, sistem, araç, cihaz neyse neresini takip edeceksek, yıpranma olabilir, harabiyet, bozulma olabilir. Mekanik, elektronik, kimyasal nasıl gerçekleşiyorsa bozulma yıpranma, mekanizmasını bilmelisiniz ki bunu modelleyebilesiniz, aldığınız verilerden yorumlayabilin. Bunu bilmeden yola çıkamazsınız. Mekanizmayı çözdükten sonra nelerle takip edebileceksem, neyi nasılölçeceğimi bilmem gerekiyor. Neyi nasılölçeceğimi bilirim bu takibi yapabileceğim. Diğer taraftan bu takibi yapabilmem, sensör ve ölçümle olacak bu, bu verileri saklamalıyım ve eski ile yeniyi sürekli kıyaslamalıyım. Durumun nasıl gittiğinden, durumsal farkındalığından her zaman haberdar olmalıyım. Eğer bu kestirimci bakım faaliyetine giriyorsak, parçaların kendisinde işlevsel bir arıza gerçekleşene kadar kalan ömrü tahmin etmelisiniz. Eğer tahmininiz bugüne kadar insanlar yoluyla yaptığınız, bugüne kadar olduğu gibi, bir tahmin yoksa, planlanan tarihte yapacaksanız bunun bir anlamı yok. Ya da arıza oldu ve siz bunu tahmin edemediniz, bunun da bir anlamı yok. Bu sistem kendini başarısız kılar. Gerçekleşmesi için bunların arızalanmadan önce yapılması lazım ki, bu sistem bir işe yarasın. Bunu yakalamalıyız. Bunu yaparken de şunu unutmamalıyız. Bir mühendis hayaliyle bunu bir fabrikada yapmayacağız. Evet fabrikada başlayacak ama araçlarımız, silahlarımız, tanklarımız, uçaklarımız olduğu yerde durmayacak depoda, üste, hangarda. Saha görecektir bunlar. Bunlar nerede kullanıyorsa, kullanıldığı yerde, helikopter ve uçağın uçtuğu, geminin bulunduğu kendi bulunduğu ortamdaki etkileri unutmayacağız, normal etkileri bileceğiz.

Diğer taraftan da askeri ve savunma sanayide her zaman önemli olan çevre koşulları etkisini bilmeniz gerekiyor. Bir cihaz - 25 dereceye gittiğinde bir sonucun normal olduğunu +20'deki normal tepkilerini etkilerini bilmelisiniz. Koşullardan etkilenecek anormallik olduğunu düşünmemelisiniz.

Bunun avantajı ne? Erken arıza tespiti, olası arızalar erken aşamada tespit edilecek. Bunu yapabilirsiniz diğer taraftan, erken müdahale edebiliyorsanız, beklenmedik arızalara yol açmıyorsa maliyetler azalacak. Kaza kırma gitmeden, arızalanmadan, büyük zarar başımıza gelmeden engellemiş olacağız. Bu da bize göre bugün planlı, 50 bin saat çalışmasını öngördüğümüz bir şey 10 bin saatte arıza verebilir. Ya da 10 bin saatlik öngörü 50 bin saat gerçekleşebilir. Erken ve gereksiz müdahale, ekipmanı 5 kere değiştirmek veya verimli çalıştığında 50 bin saat çalıştırmak. Gereksiz tüm masrafı engelleyecek.

En önemlisi, kesintisiz operasyon, operasyona uygunluk anlamındaki artış silahlı kuvvetlerimiz için en önemli konu. Erken tespitlerle sürekli bakım yapabildiğiniz için her an operasyona hazır olma oranında artış sağlayacak. Ekipmanların arıza yapmamasını sağladığınız için hareketlerin kesintisiz olmasını sağlayacak. Aynı zamanda güvenlik artışı sağlayacak. Askeri ekipmanların daha güvenli bir şekilde çalışmasını sağlayacak, askerimizin ve personelimizin daha güvenli ortamda çalışmasına zemin hazırlayacak. Ayrıca bu süreç verimlilik artışını getirecek. Gereksiz bakım faaliyetleri ortadan kalkacak, faal olma süresini artıracak, operasyonel verimliliği ve sürekli çalışmayı artıracak. Bunlar bu sistemin getireceği avantajları.

Şimdi biraz da tersinden bakalım. Yapay Zekâ Tabanlı Kestirimci bakımın zorlukları ne? Evet öncelikle yüksek maliyet. Teknoloji güzel, kullanması iyi bir şey. Yapay zekâ, makine öğrenmesi, son teknoloji sensörlerle bir cihaz veya ekipmanı donatmak isterseniz, bir gemiyi bunlarla donatıp takip etmek istiyorsanız yüksek maliyetlerle karşılaşabilirsiniz. Bunların bir maliyeti vardır. Yapmanız mı daha ekonomik, yapmamanız mı?

Diğer taraftan veri güvenliği. Burası savunma sanayi, konuştuğumuz güvenlik. Veri toplamaya başlayacaksınız, her alanda veri güvenliği önemli ama savunma sanayinde her türlü ekipmanın veri güvenliği daha kritik önemdedir. Dolayısıyla siber saldırılara karşı korunmalıdır. Veri kalitesi, konuşulan platformlar askeri olduğu için, zorlu askeri koşullarda, operasyonel kullanımı sırasında, sensör verilerinin doğruluğu da bazen sorunlara yol açabilir.

Algoritma zorlukları da var. Bugün elinizde olan bir yapay zekâ ile başlayacaksınız. O yapay zekâ verileri birbiriyle eşleyecek, öğrenecek, karşılaştıracak ama bu da eskiyecek

zaman ilerledikçe. Eğer siz geleceğin koşullarına göre, gelişen teknolojilere göre yenileyemezseniz eski verilerle doğru tahminler güçleşecek veya sağlıklılaşacak. Veriler birikecek, yeni sensörler oluşacak, daha kaliteli eklentisi olan veriler gelecek. Ama yapay zekâ eski tarihli olacak. Dolayısıyla algoritmalarda, veri tahminleme ve sağlıklı sonuçlar vermek için güncel olması gerekecek.

Entegrasyon sorunları da olacak. Bugün hepimizin yaşayabileceği konulardan biri bu. Elimizdeki duruma göre, mevcut veriler var. Kağıtta, birliklerde, firmalarda tutuldu. Bunlar sisteme nasıl konulacak? Mevcut bir envantere aldığımız ve böyle tasarlanmamış bir uçağı, radarı, tankı bu sensörlerle donatmak istersek bunu nasıl yapacağı ve nasıl sisteme ekleyeceğiz? Çünkü tasarımında bunlara yer verilmedi, mevcut operasyonu zedelemekten bunu nasıl yapacağız?

Sistemin değerlendireceği veri için elimizde olan dijital olan veya olmayan yöntemlerle sunulmuş eski veri ile dijital sensörlerin, yeni teknolojilerin sağlayacağı verilerin nasıl karşılaştırılacağı da problem olacak.

Ana konuda yine insan var. Bu sistemlerle yaşadığımız zaman insanların eğitim ve adaptasyon süreci de bir zorluk olacak. Çünkü insanların da bu teknolojilerin kullanımında bu alt yapıya göre çalıştırılması, insanların da buna uyum sağlaması gerekecek, personel de bilinçlenmeli.

Elimizde neler var ve gelecekte olabilecek? Bunu kurgularken, biz görüp göremeyeceğiz ama artık otonom, tam robotik sistemler ortaya çıkacak. Şu an bile yapay zekâ ve makine öğrenmesiyle bunları yapabileceğimizi biliyoruz. Gelecekte belki de makineler bunu kendi kendine yapabilecek, kendi kendini tamir edebilecek. Filmleri izleyen, senaryoları görenler vardır. Örneğin I robot filminde küçük küçük naniteler vardı. Küçük küçük robotların, basit basit robotların nasıl insan vücuduna, damarına verilip insanı genetik tamir etmesi düşünülüyorsa, çevredeki ekipmanın kendi kendine tamir edebileceği ortamlar düşünülüyor. Dolayısıyla belki bu gelecekte gerçekleşecek.

5G ve 6G yolda, IoT entegrasyonu artacak, veri iletim hızı artacak ve veriyi takip kolaylaşacak. Dolayısıyla daha hızlı veri iletimi ve IoT cihazlarının daha fazla entegrasyonu, Kestirimci Bakım yapmak daha etkili hale gelecek. Daha kolay hale gelecek. Neticede bütün sistemler dünyaya gittiği gibi

askeri sistemlerde de gelişecek, güvenlik ön planda olduğu için zor olsa da bütün askeri ekipmanlar birbirleriyle iletişimde olacak. ABD ve Türkiye gibi kürenin belirli yerlerine birliklerinizi dağıtmışsanız bunların hepsini izlemek, takip etmek isteyeceksiniz. Global bir veri sistemi, eko sistemi oluşacak. Uydularla bütün cihazlarla veri akışı ile birbiriyle konuşturacaksınız. ABD bunu Starlink veya askeri uydularıyla yapabiliyor. Dünyanın her yerine her türlü bilgi getirilip götürülebiliyor ve bu daha da ilerleyecek. Bütün bunlar, teknoloji bir yere giderken insan bu durumun tersini de düşünüyor.

Endüstri 5.0 kapıda. 4.0 ile karanlık fabrikalar gördük, 5.0 ile insanlar ile teknolojinin birlikte olduğu bir üretim modeline geçilmesi hedefleniyor. Çünkü, teknoloji insanı öteliyor, kenarda bırakıyor, işsiz bırakıyor, olumsuz tarafları da var. İnşallah insanların becerilerini kullanarak teknoloji ile insanın birlikte çalıştığı bir ortam modellenmek isteniyor. Bakalım yapay zekâ veya teknolojiler insanı işsiz mi bırakacak yoksa uyumlu bir birliktelik sağlanabilecek mi?

Bu konu çok uzun. Bunlarla da bitmiyor. Bu konular Türkiye’de yaparsanız, ülke çapında ulusal olarak konuşulacaksa kendi konuşacağımız konular var. NATO çerçevesinde de çoklu müttefikler, ülkeler bir araya geldiğinde konu daha da derinleşiyor. Farklı ülkeler, farklı platformlar, farklı sistemler bir araya gelecek ve müttefik sistemler kullanılacak. Birlikte operasyonlar, hareketler yapılacaktır, sistemler ve askerler farklı ülkelerden gelecek ve bunlar çalışılmalı. Örneğin neler bunlar? Yapay zekâ ve kestirimci bakımın güvenlik riskleri neler? Veriye girmeye başladığınızda sahadaki bir ekipmanın zafiyeti, hassasiyeti, açık veya karşı unsura, düşman unsura karşı eksikliğiniz canlı olarak tespit edilebiliyor. Bu hassas verinin ve bilginin kıymetli bir şekilde iletilmesi, karşıya iletilmemesi gerekecek, dışarıya gitmemesi gerekecek. Her zaman askeri faaliyetlerde hassas bir konu olacak bu. Kullanımda olan sistemlerimiz var, bu konularda müttefiklerimizle ya da içeride ilerleme olduğunda, nasıl bir entegrasyon yapılacaktır, ne kadar kolay ya da zor olacak? Mevcut sistemleri yönetmek istediğinizde nasıl olması gerektiği çalışılacaktır. Kestirimci Bakım örneklerinde ticari uygulamalar Siemens, BMW gibi kurumlarda uygulamaları var, savunma sanayine özel değil. Biz bunu uygularsak verimlilik artışı, maliyet azalışı, operasyon sürekliliği, cihazların operasyona hazır olma oranı yükselme ve uzun süre

kullanımı sağlanacak. Peki bunları uygulamanın fayda maliyet analizi yapılmalı? Bir gemiyi sensörlerle donat, planlı bakımlarıyla, plansız arıza, zaman maliyet etkinliğiyle maliyet hesapla. Hangisi daha faydalı? Maliyete ve zamana etkinliği nedir? Yapmaya değer mi özetle. Bunu da anlamak gerek. Teknoloji güzel ama sonuçlar çok fark oluşturmuyorsa anlamsız olabilir.

Diğeri askeri platform ve sistemlere ilişkin veriler var, silahlı kuvvetlerimiz, emniyet, jandarma, sahil güvenlik gibi ihtiyaç makamlarında, kullanıcılarda, idame makamı dediğimiz tersanelerde, askeri fabrikalarda. Bu bilgilerin veya o tankın, uçağın, platformun, radarın, zırhlı aracın, füze sistemi üreticisinin verileri var. Bir gemi donatılmışsa, geminin ve üzerine konan donanımın ayrı ayrı verileri var. Bu bilgiler nasıl ele alınacak? Ticari özel, gizli gibi hassasiyetler var.

Diğer taraftan veri söz konusu olduğunda verinin güvenilirliği ve erişilebilirliği konusu hassas ve nasıl ele alınmalı? Bu konuşulmalı. Veri yapısı nasıl olacak? Veri toplayıp bunları yöneteceksiniz. Sağlıklı veri nedir, hatalı nedir? Sensörlerle alıyorsunuz ama verinin kendisi de hatalı olursa, size de hatalı ulaştıracak. Her zaman doğruluk payı ve değeri önemli olacak. Tüm bu veri konuları gündeme geldiğinde, NATO gibi uluslararası organizasyonlarda bunlar konuşulduğunda verilere ilişkin düzenlemeler. Ulusal olarak Millî verimiz, ABD, NATO, ihracat kontrol mekanizmaları da, yurt dışından alınan ve satılan için nasıl ele alınacak? Karşılıklı nasıl düzenlenecek, bunlar çok önemli. En önemli kalem bunu yapmaya değer mi, maliyet ve fayda analizi. Zarar ve tehditler de olabilir, ve bunların hepsi açık konular.

Örnek olması açısından Amerika'dan bir çalışmayı ele alalım. Amerika'nın kendi askeri aircraft yani hava araçlarının bakım idamesi konusunda çalışan C3 firması var. Chris Byrne'ın bu konuda bir analizi var. Amerika'nın 5 bin 400 hava platformu var ve 200'e yakın üsse yayılmış. Global bir operasyon yapılıyor. Bahsettiğine göre 24 haftalık bir sonuç sonrası görev kapasitesinde yüzde 6, planlanmamış bakım zamanlamasında ise yüzde 40 verimlilik sağladıklarını söylüyorlar. ABD şu anda tüm dünya çapındaki hava platformları için bu yapay zekâ yazılımını kullanıyor. Burada savunma sanayimiz için de güzel bir örnek var.

Teşekkür ederim.

SORU: Merhabalar, sizin de belirttiğiniz gibi lojistik destek bakış açısı kavramsal tasarımdan başlayarak ürünün ömrünü tamamlamasına kadar bir süreci kapsayan, aslında kavramsal tasarım bölümünde tasarım gruplarıyla arasında hiçbir faz farkı olmaması gereken bir disiplin. Çünkü ürün müşteriye teslim edildiğinde, onun düzeltilmesi, tasarım grupları bir şekilde dağılacak, ürünün idamesi lojistik kısma geçecek ve üründe oluşabilecek kullanım sırasındaki arızaların düzeltilmesi pahalı veya imkânsız olabiliyor. Bu bakış açısıyla lojistik destek analizi konusundaki görüşlerinizi paylaşır mısınız? Vaktinizi almadan A400M uçağıyla ilgili bir tecrübemi paylaşmak istiyorum. A400M uçağının aileron fittinglerinde bir çatlama meydana gelmiş. Bunda retrofit yapabilmek için 350 tane bilendrivot, 350 tane boldnut kombinasyonu sökmek zorundasınız. Peki 380’de durum nasıl, 380’de 4 tane civatayla çözülebiliyor. İşte lojistik desteğin önemi tam burada başlıyor. Eğer siz bunu kaçıırırsanız ücretsiz değişim yapmak zorundasınız ve iş gücünüz boşa harcanıyor. O yüzden lojistik analizi, sözleşmelerde özellikle olmazsa olmaz noktasında dayatılmalı, özellikle Savunma Sanayi Başkanlığı’nda.

CEVAP: Teşekkür ederiz. Sunumda gösterdiğimiz Türk Savunma Sanayi Ömür Devri Yönetim Platformu ile, 2017’de kurulan bu sistemi tüm sektör paydaşlarıyla firmalarımız, büyük entegratörlerimiz, silahlı kuvvetlerimiz, hava, kara, deniz, sahil güvenlik gibi arkadaşlarımızla yaptık ve söylediğiniz bakış açısını dikkate aldık. Sektörde, Savunma Sanayi Başkanlığı ve Millî Savunma Bakanlığı yürüttüğü faaliyetlerde lojistik destek yani genel adıyla ömür devri yönetimi bütününe dikkate alıyoruz. Bununla ilgili herkes proje ön aşamadayken, başlangıç aşamasında olmalı, dizaynı etkileyecek kararlar alınırken onlar da istediklerini söylemeli. Görev açısından da, nitelik açısından da sahada bakım idare lojistik desteği çok külfetli, zor, cepheden geriye almayı gerektiren, sizi anlamsız bedeller ödettiren sonuçlar oluşabiliyor. Biz de her platformda sizlerin katılımınızı bekleriz, bunun öne çıkmasını, unutulmamasını istiyoruz. Bu unutulduğunda telafisi yok, çok küçük görünen, kendi kültürümüzden bir örnekle ‘tulumbacılar gibi’ yangın olduğunda koşan bir ekibe dönüşmemeli sonuçlar. En başta müdahale etmeliyiz ki, o ekipman doğru tasarlansın, kolay müdahale edilebilir olsun, arıza durumunda cephede kolay müdahale edilebilmesi veya fabrikada giderilebilir olması

önemli. Bu maliyetleri düşürecek. Bu da onun kullanıma hazır olma oranını her zaman yükseltecek. Biz de dile getiriyoruz bunu her ortamda. Birimimizin görevi bu ve bunun için çalışıyoruz.

Bizim buradan söylediğimiz kadar, Türkiye'deki gelişim gereği de, talep halktan doğmalı veya halk sahip çıkmalı denir ya, sizler gibi sektörün içinden insanların, savunma sanayi firmalarımızda sanayi, üretim, tasarım tarafındaki insanlar da bunu dile getirmeli ki, ihtiyaç makamı, kara, hava, deniz, emniyet, güvenlik, sahil güvenlik fark etmeksizin, ayrıca tedarik makamı da Savunma Sanayi Başkanlığı ve Millî Savunma Bakanlığı da, bununla görevli sistemin bütünü, proje geliştirme ve tedarik etme sürecindekiler de bu sesi duymalı. Böylece en başından tedbir alınabilsin. Saniyeden de silahlı kuvvetlerin kendisinden de gelmeli ki, herkes sözleşme, sözleşmedeki performans gereklilikleri, sistem gereklilikleri, doğru takvim, cezaya girmemek ve ödemeleri zamanında alma noktasında bu hassasiyetin ezilmemesi lazım.



II. GÜN BİRİNCİ OTURUM – YENİ SAVAŞÇI

TEMA:

Stratejik Komuta ve Dijital Komutan

OTURUM KONUSU:
Enerji, Lojistik, İstihbarat, İstihdam ve
Teknolojik Sınırlar

OTURUM TEMALARI:
Operasyonel Yetenek Dijital Karargah
Operasyon Merkezi
Veri Analizi ve Kullanımı
Bilgi paylaşımı
Süreç Yönetimi

VI. OTURUM ÖZETİ

Dijital dünyayı anlamak için, dijital dünyanın son gerçeği yapay zekâ çağının iyi anlaşılması gerekmektedir. Aslında yapay zekâ araç, büyük veri de içerik olarak tanımlanmaktadır. Önümüzdeki yılları şekillendireceği öngörülen dönem, düşünebilen makinelerden, düşünebilmeyi taklit eden makineler çağına gelen ve insan algısına yakın çözümler sunduğu bir çağ olarak kabul edilmektedir. Temelini ise büyük veri ve verilerden doğru analizleri almak oluşturmaktadır.

Kara, deniz, hava, istihbarat, operasyon veya lojistik amaçlı veri kullanımı hedefinde, büyük bir karargah olduğu, bunu yönetmek zorunda olduğunuzu, yardımcı olacak araçları da düşünmek, bunu da rakiplerinizin sizden daha iyi geliştireceğini düşünerek hareket etmek zorundasınız. Yapay zekâ siber güvenlikte siber saldırı ve siber savunma alanında da büyük bir fırsatlar ve riskler zinciri oluşturmaktadır.

Yapay zekâ ve büyük verinin hızla geliştiği günümüzde, teknolojik alt yapıların kısa, orta ve uzun vadeli planlamalarla değiştirilmesi, strateji ve politika açısından hızlı güncellemelerin yapılması, bakış açılarının değiştirilmesi hızlı yapılanmaların temeli kabul edilmektedir.

Savunma yapay zekâ gelişiminde, dil modellerini eğitip geliştiren, tehdidin ne olacağını ve o olacağında ne yapmamız gerektiğini bilen, yani geliştiren tarafta olmak için hızlı yapılanmalara gidilmesi tavsiye edilmektedir.

İnternet ile veri savaşları döneminin başladığı, elde edilen verilerle de artık dünyaya şekil verilen teknolojilerin ürün olarak çıktılarının alındığı bir dönemin yapay zekâ ile başladığı, yapay zekânın bir komutan gibi isabetli kararlar vermesinin mümkün olduğu dönemlerin de savunma yapay zekâsı sürecinin bir sonucu olacağı ön görülmektedir.

Veri merkezleri ve veri merkezlerinin alt yapısını oluşturan çip sistemleri, kuantum bilgisayarlar gibi malzemelerin giderek önem kazanacağı belirtilmekte, askeri teknolojilerde işlerlik ile güvenlik arasındaki hassas dengenin bu süreçlerde iyi dizayn edilmesi de önemli bir gereklilik olarak dikkat çekmektedir.

Kuantum şifreleme sisteminin de bilgi ve veri akışı süreçlerinde kritik önem taşıyacağı, karmaşık teknolojik ekipmanlarının temel bileşenlerine yatırım yapılmasının önemli olacağı vurgusu yapılmıştır.

Ayrıca, tüm teknolojik gereksinimlere rağmen, ordunun kuantum veya benzeri güvenli ağ sistemlerini kullanacak alt yapıya sahip olana kadar kapalı ağ ortamında çalışmasının gerekliliğine de dikkat çekilmiştir. Temel olarak teknolojinin kullanımında her ülkenin kendi çıkarlarına yönelik çalışacağı ifade edilirken, yapay zekâ kullanımının bir noktadan sonra milyarlarca ihtimalin içinden en doğru ihtimali seçebilecek noktaya geleceği, karar verme noktasının yapay zekâyâ bırakılacağı dönemin 20-30 yıl içinde gerçekleşebileceği öngörüsü paylaşılmıştır.

Her türlü teknolojiyi üretirken, askeri sembolojinin ortak bir dilde olması, uluslararası standartların da ihracat boyutuyla düşünülmesi önerilmektedir. Teknoloji geliştirilme safhalarında uluslararası ve ulusal camiaların içinde olmanın, geliştiren tarafta olmak için geliştirenlerin yanında olmanın faydalı olacağı ve işbirliklerinin geliştirilmesi önerisinde bulunulmuştur. Değiştirme, geliştirme ve farklılaştırmanın temeli olarak modellerin fayda ve risk analizlerinin iyi yapılması ve yol haritalarının buna göre izlenilmesi gerektiği kaydedilirken, dünyada geliştirilen projeksiyonların da dikkate alınmasının önemine vurgu yapılmıştır.

CENGAVER ve CENKER sunumlarında geliştirilen teknolojilerin efektif, etkin haberleşme ile ekip ve karargahla sürekli iletişim sağlayan, durumsal farklılığı artıran kamera ve insansız ekipmanlarla uyumlu, hareket kuvveti ve yeteneği ile hareketliliği sağlayan teknolojileri birleştiren, operasyonel kabiliyeti artıran teknolojilere öncelik verildiği vurgulanmıştır. Tüm bu teknolojilerde X, Y ve Z nesli gibi üç kuşağa hitap eden, doktrinlerin gelişmesine imkan sunan ve amaçlarına uygun sistemlerin tasarlanmasına öncelik verildiği belirtilmiştir.



**Emekli Tümamiral
Hasan ÖZYURT
MODERATÖR**

Ben emekli Tümamiral Hasan Özyurt. En son görevim Deniz Kuvvetleri Harekât Başkanlığı idi. Daha sonra Meteksan'da yönetim danışmanı olarak görev yapmaya başladım. Harekât merkezi işletmiş biri olarak, harekât merkezini iki yıl çoğun yoğun kullanmış biri olarak dijital karargâh konusuyla çok yakından ilgilendim. Harekât ortamında yüksek veri geliyor ve bu veriyi değerlendirmek zorundayız. Gerçek bir harekatta

bizim baş edeceğimizden çok daha fazla veri yükleniyor. Harekatin yükselişiyle, sahaya unsurlar çıkmaya başladıktan sonra veri çok artış gösteriyor. Logaritmik bir artışı oluyor. Bu veriyi tüketmeye ve kontrol etmeye ihtiyacımız var. Karar vericilerin de kararlarında bu verileri kullanmaya ihtiyacı var.

Bilgisayar teknolojisinin ve yapay zekâ kullanımının bu işe yarayacağını sezgisel olarak biliyoruz, ancak katılımcılarımızın buna büyük katkı sağlayacağını düşünüyorum. Dijital karargâh keriminden çok anlaşılan bir şey, robotlar karargâhı kontrol edecek, yapay zekâ kararları verecek, insana ihtiyaç kalmayacak gibi yorumlar var. Karargâhın bilgi işleme kapasitesini nasıl artırabiliriz? Bir karargâhın görevi bilgiyi işlemek ve işleyerek karar üretmek. Daha sonra da verilen bu kararın icrasını takip ve analiz etmek. Bu temel fonksiyonlar nasıl daha iyi hale getirilebilir. Bir de bizim karargahlarımızda bilgi PowerPoint veya Word'de kaldı. Bir daha bir sene önceki yansıya bakıyoruz ve tarıyoruz. Bu zaman alıcı bir durum oluyor. Bilgiyi işlemek ve kullanılır halde tutmak da önemli. Dijital karargâhın PowerPoint'in ötesine geçmeli diye düşünüyorum. Şimdi sözümü sayın hocama bırakıyorum.



Prof. Dr. Şeref SAĞIROĞLU
GAZİ ÜNİVERSİTESİ

Davet için teşekkür ederim. Gazi Üniversitesi :Bilgisayar Bölümü'nde öğretim üyesiyim, 30 yıl önce yapay zekâ ve robotlar konusunda yapmış bir kişiyim. Ülkemize de bu alanda katkı veren hocalardan biriyim. Bugün sizlere belki karargahlarda yapay zekâyı anlatmasam da aslında anlattığım her şey, buradaki pek çok şeyin, dijital karargahların altyapısını oluşturacak bakış açısını sizlerin

burada yakalayabileceğini düşünüyorum. Dijital dünyadan bahsedildi biraz önce. Bu dijital dünyayı anlamak için yapay zekâ çağını anlamamız gerekiyor. Yapay zekâ çağındayız diye konuşuyoruz ama biz yapay zekâ değil, aslında büyük veri çağındayız. Bugün üretmiş olduğumuz verileri değerlendirecek bir araç bizim için yapay zekâ. Ama geline nokta yapay zekânın bunun çok ötesine geçtiğini ifade edelim. Bu büyük veri çağını doğru anlamamız lazım. Burada gördüğümüz şekil aslında internetin büyük resmi. Farklı renkler farklı domainleri gösteriyor, konuştuğumuz büyük veri altlığını oluşturuyor.

Bu dünyayı nasıl algılıyorsak, öyle yönetiyoruz. Eğer bunu gerçekten dünyamıza şekil veren bir veri altlığı gibi görüyorsanız dünyaya şekil vermeye çalışıyorsunuz. Bu algımız burada çok önemli. Bu önemli olan tabii ki çok büyük fırsatlar var, zorluklar var tabii ki tehditler de var. Bu da bizim gelecek bakış açımızı oluşturuyor. Savaş meydanlarında bunu ilişkilendirdiğimizde savaş meydanlarını yönetmek için, başarılı bir şekilde bunları hayata geçirmek için önemli bir kavram olduğunu söylemeliyiz. Büyük veri dünyasını anlamak ne demek. Verinin aslında tanımının bile değiştiğini anlamamız gerekiyor? Verinin aslında bilimin temeli olan verinin nasıl evrimleştiğini, tanımını değiştiğini de burada görüyoruz tanımların da nasıl değiştiğini ve hayatımıza yaptığımız işlere nasıl yansıdığını burada çok net olarak görüyoruz. Bakıyoruz 2012 yılından sonra büyük verinin hayatımıza kavram olarak gelmesiyle beraber de artık kavramlar, smart big data ve şimdi de generative big data çağındayız. Yani makineler da artık ne yapıyor veri üretiyor ve bu verileri değerlendiren bir ortam olarak bunları görüyoruz.

Şimdi yapay zekâ çağında dedik yapay zekânın tanımı da değişiyor. Artık işte düşünebilen makineler hedefti, düşünebilmeyi artık taklit edebilen makinelere geldik bu makineler çağında. Verinin her türlü işlenip insanın anlayabileceği formata dönüştürülen bir yapı içerisinde bunların hayatımıza geçtiğini biliyoruz. Peki bu yeni çağda ne var? Yapay zekâ veya büyük veri çağında dediğimizde, hakikaten önümüzde müthiş verilerle gelen fırsatlar var. Ve bu fırsatların da getirdiği tehditler de önümüzde, şimdi baktığımızda burada tabii ki geliştirilen algoritmalar insanın algısına daha yakın nasıl çözüm geliştirilebilir bizlere sunuyor.

İşte başlangıçta sadece doğal dil işleme ile başlayan, yani yazdığımızda text to dediğimiz kısmın artık resimdi, görüntüydü, bunun kodu sesti bunların birleşiminin artık analiz edilen ve metin, ses, görüntü, kod gibi pek çok ortama dönüştüğü bir yapı içerisindeyiz. Tabii ki bu yapı bize öyle farklı ortamlar sunuyor ki her alanda istediğimiz her şeyi çözebilecek yapılar gündemde. Büyük başarı hikayeleriyle karşımızda da tabii ki, buna baktığımızda içerisinde pek çok bilim dalının olduğunu işte doğal dil işleme ile başlayan sürecin aslında doğal dil işlemenin çok ötesine geçtiğini ve işte ses teknoloji görüntü teknolojileri, bilgisayar programlama teknikleri gibi pek çok hususun hayatımıza geçtiğini ve büyük modellerle bunun hayatımıza yansıdığını biliyoruz. Şimdi biliyoruz, bu gelişmeler aslında 2022 Kasım ayında 1 milyona ulaştığında, aslında dünyada büyük bir değişimin başladığını da gördük. Yani bunu 30 yıldır bekleyen bir hocayım, buna çalışıyoruz ama bu değişim ve dönüşüm, verinin büyümesi, büyük verilerin işlenmesi, büyük verilerini ortak bir platformda vektörel forma dönüştürülerek bunların analiz edilmesi veya sunulmasıyla, yani bir sonraki kelimenin tahmin edilmesi prensibine dayanan basit olarak bir yapıyla hayatımıza girdi.

Bakın bu kadarcık bir basit yaklaşım bile insan hayatında ne kadar büyük değişimlere sebebiyet veriyor, bugün sizlere onu anlatmaya çalışacağım. Şimdi baktığımızda buradaki temel prensip büyük veri demiştik, işte başlangıçta iki büyük veri tabanı öğretilerek başlayan süreç, o da 410 milyar token olarak başladı.

Ciddi verilerden bahsediyoruz, bu milyar token dediğimizde kelimelerin her bir kelimenin token olarak ifade edildiğini veya deyimlerin token olarak ifade edildiğini düşünürsek, bu dünyadaki veri büyüklüklerinin modellere nasıl aktarıldığının da daha iyi yorumlanması, işte biraz önce dijital karargâh dediğimizde bunun altlığını oluşturan verilere sahip olmanın önemini daha iyi anlayacağız. Şimdi baktığımızda 410 milyar token işte 2022’lerde başladı ama günümüzde bunun çok farklı boyutlara gittiğini biliyor olmamız gerekiyor Özellikle de chat gpt 5.0’la da Amerikan Savunma Bakanlığı’nın bir ürünü haline gelen 5.0 stratejik bir ürün olarak karşımıza çıkıyor ve izni olmadan da satılamaz noktasına gelen bir konuda.

Dijital karargâhın çok ötesinde, stratejik bir ürün olduğunu biraz sonra sizlere bu gelişmelerde hızlıca aktarmaya çalışacağım. Peki gelinen nokta nedir, şimdi biz 500 milyar token’den bahsettik. Biraz önce 400, işte 10 milyar tokenlardan ama baktığımızda artık büyük dil modelleri evrim geçirdi. 410 milyarla başlayan süreç bakın aynen giyim kuşamda ayırttığımız gibi, Nano, XS, Small, Medium, Large, XLarge gibi modellere dönüştü. Bu büyüklükler veya bu sıralama veya bu ayırttırma, sizin modelinizin ne kadar çok token sahip olduğuyla orantılı bir noktaya geldi. Şimdi 410 milyar dedik bakıyoruz, trilyon toklar çıktı, şimdi bu trilyon tokenlar işte, Cloud 3 ile başlayan süreç, şu anda 3,5’ünü çıkardılar. Bakın bu Ekim’deki modelin büyüklüğü, şimdi 3,5 çıktı ve 20 trilyon token. Yıl sonunda 40 trilyon token. Bu şu demek, Cloud 3.5 tüm dilleri konuşuyor. Dünyadaki tüm dilleri konuşan, karşısında size destek veren bir alt yapıdan bahsediyoruz. Sorduğunuz tüm sorulara cevap verebilecek her dilde cevap veren bir ortamdan, yapıdan, bir kütüphaneden adına ne diyorsanız bir yapı geliyor karşımıza. Arkasında GPT, GPT 4.0 gibi büyük ürünler de var. Bunları takip ediyorsunuz, bunların sıralamaları değişebiliyor ama buradaki temel ilke sizin ne kadar çok veriyle bunları eğittiğiniz. 2024 yılı sonundan sonra 2025 başı dünyada yapay zekâda yeni bir dönemin başlangıcı olacak.

Dolayısıyla bu yeni çağın, yeni yapının, yeni bakış açısının, bize çok farklı düşünceleri getireceğini, çok farklı soruların cevabını verebilecek yapılar olduğunu ifade edelim.

Büyüklikleri ve sıralamaları değişebiliyor, çünkü bunlar sürekli eğitiliyor. Bakın 40 milyar tokenla eğitim 6 ay sürüyor. Yani bu 6 ay süre, eğitim yaptığınız makinalar, işlemciler gerçekten yüksek enerji harcayan ve yüksek hızda çalışan ortamlar, veri merkezlerinde çalışan yapılar, eğitilen modeller. Bunların büyüklikleri, yerleri değişebiliyor ama burada değişmeyen bir konu var. Bunların gittikçe büyüdüğü, büyüyeceği, veri sunduğunuz takdirde pek çok yapıyı burada görebileceğimiz gelişmelerden.

Çip takılan maymunlar bilgisayar oyunu oynuyor, Tesla 40 bin aracı kontrol edebilecek bir sistem, ek noktadan bütün flaşörleri tüm ışık sistemlerine girip bunları aynı anda senkron edebilen, gösteren gösteri yaptı. büyük büyük gösteriler yapıldı. Live The World Behind (Dünyayı ardında bırak) filmindeki o gerçeğin nasıl gerçeğin nasıl yapılabileceğinin belki değişik bir demosu oldu.

Sinirsel veriler artık Amerika'da kişisel veri olarak kabul ediliyor, detayını yorumlamıyorum ve sizin düşünüp değerlendireceğinize inanıyorum. Mimiksiz ifadelerden kişinin siyasi eğilimi bulunabiliyor, yani siz kendi fotoğrafınızı verin hangi partiye eğiliminiz olduğu MIT'de bir proje olarak hayata geçti. Zihin kopyalama dönemi var, kişinin dijital ikizleri hemen oluşturuluyor, girip sitelerden yapabilirsiniz.

Şimdi Da Vinci robotu, robotik cerrahi sistemi var. Gazi Üniversitesi'nde de var, orada değerli bir hocamız var, hep ona takılıyorum, dünyada 7 bin tane Da Vinci robotundan gelen tüm veriler birleştirilip öğretiliyor ve bizim doktorumuzu taklit edebiliyor. Yani girip operasyon yapabilecek nitelikte artık, ünümüz teknolojisi 7 bin Da Vinci robotundan veri topladığınızda. Bunların eğitilebilen büyük sistemler olduğunu bilmemiz gerekiyor. Yani büyük veri çağı dememizin arkasındaki temel husus işte bunlar. 20 metreden artık mayınları bulabiliyorsunuz, resim kalitesini 8 kat arttıran sistemler, yapay zekâlar yapılıyor. Yani bunun arkasında büyük veri analitiği, tabii ki burada büyük dil modelleri olduğunu söylemek gerekiyor.

Şimdi enerji yetmiyor, enerjiye ihtiyacı 100 kat artıracak deniyor bu verileri sağlamak için. Bunu sağlamak için nükleer santrallere ihtiyaç var, siparişlerini veriyorlar. Süper bilgisayarlar artık bakanlıkların emrinde, dünyanın en hızlı gelişen süper bilgisayarları. Geçen hafta açıklandı 'El Kaptan', kullanıldığı alan dünyadaki nükleer saldırıların veya nükleer gelişmelerin simülasyonunu yapabilecek. Süper bilgisayarlar internet hızını şu andakinden 3.3 milyon kat hızlandıracak teknolojiler çalışılıyor. Bakıyorsunuz Mars'a internet götürme, Mars'taki bilgilerin transferiyle artık dünyayı anlama değil evreni anlamaya doğru adımlar atıldığını, proje yapıldığını görüyoruz. İşte uzaydan veri transferini bırakın, enerji transferi için projeler başlatıldığını bilmemiz gerekiyor, hedefler konulmuş. 30 MW gücünde bir enerji aktarımı için projeler yapılıyor, irtifa 35 bin kilometreden enerji transferi gibi konular.

Şimdi dronların, 10 bin tane dronun hakikaten ışık gösterisini izleyip büyülenmeyen yoktur ama bunu savunmaya aktardığınızda gerçekten düşünmek gerekiyor. 10 bin dronu bir amaç için kullanabiliyorsunuz, adına sürü teknolojisi deniyor. Artık dron ontolojisi diye yeni isimler ve kavramlar verildiğini ifade edelim. Dolayısıyla bunu kara, deniz, hava, istihbarat, operasyon veya lojistik amaçlı kullanmayı düşündüğünüzde ne kadar büyük bir karargâhta bunu yönetmek zorunda olduğunuzu, yardımcı olacak araçların hangi teknolojiler olduğunu söyleyecek pek çok adımları görebiliyorsunuz. Yani işin bir şov tarafı var ama işin bir de gerçek tarafı var. O gerçek tarafında da pek çok şeyi burada görebilme imkânı var. İşte bazılarını burada söyleyebiliriz, hibrit savaş taktikleri, asimetrik tehdidin yapabileceğini, bilgi paylaşımında kopukluklar olabileceği, yanlış anlaşılmanın ölümcül sonuçlara gidebileceği gibi. Tabii ki gelişmiş teknolojilerle tehditler oluşturabileceğinizi de burada bulunan herkes düşünüyor ama en büyük tehdit de otonom olarak kapılabilecek saldırıların olduğunu, silah sistemlerinin olduğunu burada ifade etmek herhalde yanlış olmaz diye düşünüyorum.

Gelişmelere baktığımızda artık dijital ikiz dönemi. Siz kişiyi klonlayan dijital çıkarıyorsunuz demektir. Red Hoffman'ı izleyenler mutlaka vardır, izlemeyen varsa izlesin. LinkedIn patronu, Microsoft'un yönetim kurulu üyesi. Onu bir izleyin, dijital ikizi ile sohbet ediyor, dijital ikizi kendisine akıl veriyor.

Bu hakikaten değişik bir süreç ama artık pek çok şeyin dijital ikizi çıkıyor. Yani ölümsüzlüğü insan yakaladı, dijital çağda. İkinizi oluşturun, bu ikizler ne yapıyor, alt yapınızı sağlayabiliyor.

Aslında bu ilk yapılan, İngiltere'de 2022'de sunulan bir strateji raporunda, o zaman General AI diye ifade ediliyordu, şimdi Generatif AI diyoruz, süper yapay zekâya geçişin, genel yapay zekâya geçişin altlıkların nasıl oluşturulduğunu görebiliyoruz. Şimdi öyle bir çağdayız ki artık veri alabildiğiniz her ortamdan yapay zekâ ajanlarıyla veri toplayıp, siz istediğiniz tüm kararları bu ortamlarda hızlıca verebiliyorsunuz. Yapay zekâ ajanlarıyla her ortamdan veri toplayarak, tabii ki komutana yardımcı olacak karargâhtan da bunları yapabilecek ortamları burada oluşturabileceğinizi ifade edelim. Tabii ki burada üretken yapay zekâyı stratejik kararlarda, karargâh bazlı düşündüğümüzde stratejik ve operasyonel kararların hepsinde kullanılabileceğini burada küçük örneklerden anladığınızı düşünüyorum.

Risk analizinden kaynak yönetimine, uzun vadeli planlamadan anında gerçek zamanlı karar verecek sistemlere dönüştürebileceksiniz. Operasyonel olarak, hedef takibi, harekât planlamasını gözden geçirme veya sahada karar verme gibi tabii ki Hedef takibi pek çok hususu da burada gündeme getirebileceğimizi ifade edelim. istihbarat en önemli kısım, tüm verileri sahadan, kişilerden, ortamdan, cihazlardan, silahlardan, ekipmanlardan veya platformlardan aldığınız tüm verileri füzyon yapıp bunun istihbaratını çok farklı ortamlardan yapabilirsiniz, elde edebilirsiniz. Artık dünyanın tüm dilinden otomatik veri alıp kendi dilinize çevirebileceğiniz ortamlar olduğunu da ekleyelim.

Tabii ki bunlar bir tehdit oluşturursa da siber güvenlik açısından da önlem olarak da otomatikleştirerek çözebilirsiniz. Siber güvenlik açısından siber saldırı ve siber savunma da yapabilirsiniz. Saldırıların anlaşılması için onu farklı bir resim formatına dönüştürüp resimden saldırılar oldu mu, değişiklik oldu mu onu da gözlemleyebiliriz. Otomasyon ve otonom en önemli kısım tabii ki. Çok sayıda cihazla sürü halindeki dron gösterilerinde de bunu görüyoruz. Elon Musk, bu zamanda F-35 yapmanın, yani insanlı sistem yapmanın vakit kaybı olduğunu söylüyor.

Dolayısıyla, strateji ve politika açısından yaptığımız her şeyi güncellememiz gerekiyor. Teknolojik alt yapılarımızı iyileştirmemiz, bakış açılarımızı değiştirmemiz gerekiyor. Nitelikli insan gücünü artırmamız gerekiyor. Bu çağda veriyi, veri toplumunu, veri yapılarını, askeri olarak da veri yönetimini, veri bilimini, büyük veri bakış açısını, veriden elde edilebilecek değeri de iyi anlamamız gerekiyor. Buna göre yapılar oluşturmamız, yani verinin stratejik bir altlık olduğunu anlamamız gerekiyor.

Bakın büyük veride verinin bile tanımlaması değişiyor verileri v'lerle tanımlıyorlar, başlangıçta 3v olarak tanımlanıyordu, şimdi 32v olarak ifade ediliyor, veriyi bile tanımlama şeklimiz değişiyor. Ayırıştırıyor, anlıyoruz, anlamaya çalışıyoruz, verinin bile akıllı olanı var şu anda. Dolayısıyla bunları bu çağda kullanarak yeni yetenek, kapasite artırımı konusunu gündeme getirmemiz gerekiyor. Tabii ki bunu yaparken, her şeyi yaparken etik davranmak, kurallara uymak, güvenliği sağlamak, mahremiyete saygı duymak, kişisel, kurumsal, ulusal ve uluslararası yönetmeliklere de kurallara da uyarak bunları hayata geçirmek gerekiyor.

Şimdi isterseniz bir daha düşünün nasıl algıladığımızı, ne yapmamız gerektiğini, bundan sonraki süreçte karşımıza çıkabilecek riskleri, zorlukları veya fırsatları daha iyi değerlendireceğinizi düşünüyorum.

Teşekkür ediyorum.

SORU 1: Elon Musk müthiş bir kaynağa sahip ve bu çağda bunu yapmak aptallıktır gibi bir şey söylemişti. Space X, Tesla gibi gücü var Elon Musk'ın. Ne yapılacağını söylüyor mu bunun yerine veya sizin öngörünüz var mı?

CEVAP: Tabii ki öngörüler var, dron teknolojisi, drontoloji kavramına daha fazla önem vermemiz gerekiyor. Ukrayna'da binlerce tankı, 5 milyon dolarlık tankların nasıl yok edildiğinin sayısı da ortada. Binlerce tankın küçük, 3 bin dolarlık dronlarla nasıl yok edildiğinin hikayesini de anlatıyor arka tarafta. Boş konuşmadığını değerlendiriyorum, bu değişim ve dönüşümde biz geleceği konuşuyoruz, mevcut bulguları değerlendiriyoruz. Sizler mevcudu daha iyi değerlendiriyorsunuz. Olay sadece dronlardan ibaret değil ama stratejik taktik operasyonel olarak neler yapılması gerektiği ile ilgili bize farklı fikirler veriyor.

Dijital ortam dronlar veya savaş uçaklarından da ibaret değil. Ama şu bir gerçek siz belli bir limitlere kadar savaş uçaklarını kullanabiliyorsunuz ama 20 kat fazla G'de uçabilen bir uçak yaparsanız farklı bir kazanım elde edebilirsiniz, söylemek istediği şeyi ben böyle anlıyorum. Arka tarafında söylerken de şimdi dünyaya Starlink ile internet veren, tüm kaynaklardan tüm sensörlerden veri toplayan ve bunu yeterli görmeyip Mars'a bile bir link kurarak veri toplayacak, o evreni de anlayacak yapılara kafa yoran bir kişiden bahsediyoruz. IQ seviyesi 154, en ileri IQ olan Einstein 160 seviyesinde. IQ seviyesi yüksek birinden bahsediyoruz, Genitive AI'nın IQ seviyesi de hesaplanıyor ve 120 civarında olduğunu ifade edeyim. Bazı tartışmalar var ama 12 bin olarak ifade eden kaynaklar da var. Bakın koddaki başarısı yüzde 92.

Başarılı oyun geliştirelim diyorsunuz, GPT'nin yeni bir ürünü oyun istiyoruz diyorsunuz istiyorum diyorsunuz yazıyorsunuz oyun ekranını çıkartıyor oyun oynuyorsunuz hiçbir şey yapmanıza gerek yok artık, kod yazmanıza gerek yok. Sadece promptları (bir modeli yönlendirmek veya belirli bir cevap üretmesini sağlamak amacıyla kullanılan kısa metin parçaları) daha iyi ifade edebilmekle sonuca ulaştığımız bir çağa geçiş yaptığımızı anlamamız gerekiyor. Bunu ne kadar güzel ifade ederseniz ne istediğinizi belirlerseniz arkada o kadar bilgi, veri. İşte o tokenlarınızın o alanla ilgili sayısı ne kadar çok olursa, size o kadar büyük destek verecek bir sistem yanınızda veya arkanızda.

Ne diyorsanız, dolayısıyla böyle bir ortam bizim geleceğe farklı şekilde bakmamızın da alt yapısını oluşturuyor. Bu tür etkinlikler de eminim buna katkı sağlayacaktır diye düşünüyorum.

SORU 2: Türkiye’de insanlı ve insansız sistemler deniyoruz. Değerli Feride Bahar hocamız var ‘gelecek geldi’ diyor, ‘geleceğin neresindeyiz?’

CEVAP: Gelecek geldi artık, size 3,5’un yeteneklerini söyledim. 2025’ten sonra yapay zekâ çağına geçiyoruz. Şimdi yapay zekânın evreleri var, siz makineye bilinç kazandırdınız mı pek çok şeyi kendisinin yapabileceğini biliyoruz. O bilinç kazandırma dönemine girdik, 2025’te de makine bilinç kazanacak. Yani kendi kendine pek çok şeyi otomatik yapabileceğini söyleyelim. Dolayısıyla bu ileride falan değil, önümüzdeki süreç. Ama tabii ki buna şu ana kadar yapay zekânın gelişimine trilyon dolarlar harcanıyor, daha çok harcanıyor. Çünkü bu ışıltı, ışık falan değil. Güneşi gördük, bunun büyük bir değişim olduğunu biliyoruz Herkes bundan etkilenecek, az veya çok olumlu veya olumsuz. İşte biz burada olumlu etkilenip bundan faydalanabiliriz. Tabii ki zararlarından da korunmak gerekiyor, tehdit gördüğümüz en büyük tehdit olarak bunu ifade etmek mümkün. Ne açıdan? Şimdi siz bunu farklı amaçlar için kullanırsanız, çok başarılı sesi taklit ediyor, görüntüyü taklit ediyor. Bakın hafta sonu deneme yaptık, Karadeniz şivesiyle ‘Uşağım diyorum, nasıl yapacağız bunu?’ Anlatıyor yine Karadeniz şivesiyle, bunu yapan bir sisteme dönüşüyor. Dolayısıyla tehdit dediğimiz dolandırıcılık artacak, başka şeyler olacak, kendimizi bunlara da hazırlamamız gerekiyor. Risk sadece askeri alanda değil, her alanda büyük risk var, bunlara da hazırlık yapmamız gerekiyor. Yani bu gelecek falan değil, artık geldi, dünyanın tüm dilini konuşan hiçbir kişi yok benim bildiğim, varsa siz söyleyin. Ama bakın yapay zekâ artık tüm dilleri konuşuyor, neden, şu anda 20 trilyon tokenla eğitilmiş, bu yılın sonunda 40 trilyon tokenlarda. Yani 40 trilyon kelime biliyor, deyiimi biliyor, birçok şeyi bilen bir sistem var. IQ’su çok yüksek, 120 gibi söyleniyor ama sorduğunuz tüm soruya cevap verebilen ve doğruluk oranı da yüksek. Yalancılığı öğretmişler, süper yalan söylüyor, ikna edemediği kimse yok. Akademik olarak test edilmiş. Dolayısıyla her şeyin mümkün olduğunu ifade edebiliriz.

SORU 3: Hocam, özel sektör boyutuyla, teknolojiler tarafında biz yapay zekâ gelişiminde hangi alanda yoğunlaşmalıyız savunma alanında? Hava, kara, uzay, siber gibi alanlardan da bahsediyoruz.

CEVAP: Burada taraf tutmamak lazım, her alanda ama esas geliştiren tarafta olmak lazım. Siz eğer o modelleri eğitip geliştirebiliyorsanız zaten güç sizde. Bizim zamanımız da He-Man çizgi filmi vardı, çok popülerdi, Heman'ı oluşturmak modeli oluşturmak. Yani eğer biz önde olmak istiyorsak, bu büyük dil modellerinin ana korlarını biz geliştirmeliyiz ki, tehdidin ne olacağını veya o olacağı orada kendimiz görebilmeliyiz. Yani en azından kendi modelimizi geliştirmeliyiz.

SORU 4: Yapay zekâ konusunda işin veri boyutu ve Millî veri boyutunu nasıl ele almalıyız?

CEVAP: Verimize daha çok sahip çıkmamız gerektiğini anladığımızı düşünüyorum. Yani siz verinizi kaptırdınız mı, yapılacak bir şey yok. Her şeyi biliyorlar, bakın zihin okunuyor. Siz bilgisayara şifrenizi girin, şifrenizi biliyor. Buraya gelen topluluğun genel davranışının verisini alın, buradaki genel ortak aklın ne olduğunu çıkartabilecek bir sistemden bahsediyoruz. Sistem bir komutan gibi de çalışıyor, bir asker gibi de çalışabiliyor. Yeter ki doğru promptları verin. Dolayısıyla bir ülkeni ortak aklı nasıl, onu da çıkartabiliyor. Bir kişinin düşünce sistemi nasıl bunu da biliyor. Bakın benim adıma, benim fikirlerimi ve düşüncelerimi savunan, benim stilimde makale yazabiliyor. Yapamaz denilen konular vardı, şiir yazamaz deniliyordu, en duygulu şiirleri yazan yapay zekâ sistemleri şu anda test edilmiş durumda, müthiş duygulu yazıyor. Yani bizim kalelerimizi birer birer aldığının, kalelerimizin gittiğinin farkında olalım. Yapay zekâ böyle bir çağ, böyle bir değişim, böyle bir dönüşüm.

SORU 5: Günün sonunda esasında bizim için kararlar operatif ve stratejik seviyede çıkacak. Ama Millî çıkarlarımız ve bizim kültürel ihtiyaçlarımız, yaşadığımız ortam, bizim Millî hedeflerimiz çok öncelikli. Bir konu bu noktada da oluşturulan yapay zekâ modelinin bizim gerçekliğimizi bilerek, bize has ve hâkim, uluslararası bir hukuk var ama herkes bunu da kendine göre yorumluyor, bize göre yorumlaması gerekiyor, buna göre bir çalışma var mı?

CEVAP: Aslında biraz önce sektör ne yapmalı konusundaki soruya verdiğim cevap gibi kendi Millî algoritmaları ve büyük dil modelimizi oluşturmaliyiz. Çünkü siz doğru veriyle besliyorsunuz, yanlış veri girerseniz yanlış cevap veriyor Buna da halüsinasyon diyoruz biliyorsunuz. Dolayısıyla doğru veriyle beslemek gerekiyor, çünkü öğrenme ortamında siz neyi veriyorsanız onu öğreniyor. Eğer Millî manevi değerler, ulusal çıkarlar, diğer konuları ifade ederseniz ona göre sonuçlara varıyor. Bakın uluslararası, yanlış olarak verilen veriler olsun, Ermeni problemini oradan siz eğer kendi verilerinizle yapmazsanız, konuyu izah edemezsiniz, sistem çünkü öyle cevap veriyor. Yeni nesilde bu şekilde öğrenecek, ya ulusal çıkarınız veya doğrular konusunda kütüphaneler, veriler o ortamları hemen oluşturmak gerekiyor. Algoritmasında bilmiyorum yok, en yakın cevabı veriyor. Bilmiyorum dediğine hiç rast gelmedim.

SORU 6: Askeri harekatta yapay zekâ çıktılarına nasıl güveneceğiz, hata yapma riskine rağmen? Yapay zekâ dilleri birbirleriyle alışveriş yapıyor mu, konuşuyor mu?

CEVAP: Bir komutan kullanabilir mi, cevap evet. Çünkü komutan önüne gelen veriyle karar veriyor. Komutan ne kadar sağlıklı veri alırsa, o kadar doğru karar veriyor. Şimdi siz tüm networkten gelen verilerinizi anında işleyip size bilgi sunan bir sistem varsa bunu işte büyük veri, analitik diyoruz, yani bunu Yapay zekâ sistemleri de buna entegre oluyor. Dolayısıyla komutan inanın diğer verdiği karardan daha üst seviyede daha doğru karar verebilir. İkinci bir konu, agentlar birbiriyle konuşuyor, yani tek sistem çalışmıyor, diğer yapay zekâ sistemleriyle de görüşüyor. Oradan da veri alıyor.

SORU 7: Hocam 7 bin Da Vinci robotundan bahsettiniz. Teknolojiden kaçmamız mümkün değil, teknolojiyi hemen hemen her alanda yaşıyoruz bankacılıktan, askeri kuvvetlerde veya iç güvenlik, sınır güvenliğinde, hemen hemen her yerde. Kolumuzdaki saat, diz üstü bilgisayar. Ben sıkıntı olarak şunu görüyorum ve açıkçası korkuyorum. 7 bin tane fiziki robottan bahsediyoruz, bu robotların normal şartlarda bizim kontrolümüzde olduğunu düşünüyoruz, biz kontrol ediyoruz. Peki tehlike yok mu, yani bunlar ileride kendi aralarında konuşup kendi dillerini ürettiklerinde ne olur acaba, bunu öngörebiliyor muyuz?

CEVAP: Öngördüğümüz zaten yapıldı. Kendi aralarında düşünebiliyorlar, böyle bir şey yaşandı ve konu kapatıldı. Düşünebiliriz tabii ki, tehdit olabileceğini. Onun için buradayız. Onları konuşmak için. Bu yıkıcı tehditlerin arkasında nerede zafiyet var, nerede problem olabilir, onlara odaklanmak gerekiyor diye düşünüyoruz.



Binbaşı Emre AYVAZ
Millî Savunma Bakanlığı

Binbaşı Emre Ayvaz, komutanım müsaadenizle. Hava Uzay Gücü Geliştirme Komutanlığı ara kısım amiriyim. Sunumumuz savaş oyunu planlama aracı (SOPA) içeriğinde. Hava Uzay Gücü Geliştirme Komutanlığı (HUGEM) olarak bölge de saygın, etkin ve caydırıcı bir güç olmanın sürdürülebilmesi için Hava Kuvvetleri Komutanlığı'nın ihtiyaç duyduğu dönüşümlerin geliştirilmesi, tarihte görülmemiş

bir hızla gelişen teknolojinin takip edilmesi, bu kapsamda yapay zekânın etkisiyle her alanda yaşanan paradigma değişiminin askeri havacılık üzerindeki etkilerinin de araştırılması üzerine çalışıyoruz.

Peki bu kapsamda savaş oyunu planlama aracı ne yapıyor diye baktığımızda, Türk Hava sahasını savunmak üzere tüm değişkenlerin az önce de bahsettiğimiz tokenize edilen tüm değişkenlerin dahil edildiği ve güncel olarak dinamik olarak sisteme aktarıldığı yaşayan bir sistem. SOPA aslında bunun ilk adımı olacak. Devamında neler olabileceği ile ilgili görüşlerimizi paylaşacağız. Tabii bu yapı tatbikatlar, harekât planları, harp oyunları gibi sistemleri kullanabileceğimiz bir uygulama olacak. Mikro ajan tabanlı dediğimiz bulut sistemlerinin temelini oluşturan bir yapı aslında. Her geçen gün daha maliyet etkin, daha gerçekçi sonuçlar üreterek, genel yapay zekâyı destek verebilecek bir yapıdan bahsediyoruz. Tabii bunun sanal evren boyutuna giden bir boyutu var aslında. Hani bu ilk adımı dediğimiz, bunlar basit simülasyon uygulamaları. Ama bunun bir adım ötesi sanal evren, yani şu an trilyonlarca dolar harcanan, Meta ve benzerleri olan Mark Zuckerberg'in 3 yılda 40 milyar dolardan fazla para yatırdığı ve artırarak devam ettiği sistem. Sanal evren bize çift amaçlı kullanım sunuyor. Hep askeri boyutundan bahsettik ama sivil olay, yangın, deprem, felaket, insani yardım gibi konularda, ilk şok aşamasından planlama aşamasına, karar desteğine kadar uzanan, meteoroloji, finans, iç güvenlik hatta politikayla ilgili karar vericilere inanılmaz bir vizyon veren, arkada devasa bulut sistemlerinin çalıştığı, ZettaByte olarak adlandırılan devasa verileri işleyen bir yapıdan bahsediyoruz. Tabi veri çiftlikleri, veri

merkezi çiftlikleri kurmaya ihtiyaç var. NVidia firması, 2026 yılına kadar bütün üretilebilecek ürünlerini sattı, yani seri üretimden çıkmadan şimdiden hepsi ayırılmış durumda. Çünkü bunlar artık biyolojik zekâ değil, biyolojik zekâdan arındırılmış dijital zekâ. Bu sistemlerin önüne geçmek gerçekten imkansıza yakın bir şey. Yani bunun önüne geçtiğimizde maalesef bunun ileride sıkıntılarını çekeceğimiz öngörülüyor. Bununla ilgili, 25 yıl önce hava kuvvetlerinin bunu ön gördüğü ve bununla ilgili karar verici durumunda olan değerli komutanlarımızın da şu an burada olduğu bir süreçten de bahsedeceğim.

Peki askeri havacılıkta teknolojik gelişmeler nelerdir? Biz, bizim takip ettiğimiz kadarıyla, gördüğümüz kadarıyla 5. Nesil yani uzun süredir sahada olan uçakların bile bir sortide havadan terabaytlarca veri işlediğini biliyoruz. Yani havada aslında sadece uçak yok. Aynı zamanda veri füzyonu yapan, bunu değerlendiren ve pilota bilmesi, gerektiği kadar, farkındalığına zarar vermeyecek veri sunabilecek makinalardan bahsediyoruz. Kuantum haberleşme artık teorik olarak uygulanıyor, hatta bunun pratikte uygulandığını da biliyoruz. Türkiye’de de küçük küçük uygulamalarla yapabildiğimizi biliyoruz. Nedir kuantum haberleşme? Yüzde yüz güvenlik sağlar, askeriyede en önemli şey güvenlidir. Sivilde bunun tam tersidir, önce işlerlik daha sonra güvenlidir. Ama askerde güvenlik yoksa işlerlik olamaz, güvenli değilse her şey bizim için çöptür.

Diğer gelişmelere bakıyoruz, İHA’ların inanılmaz gelişmeleri, mikro ve nano boyutta, enerji yönlendirme silahları dediğimiz lazer sistemleri ya da hipersonik füzeler, uzay, uydu sistemleri, bilişsel elektronik görünmezlik teknolojileri, gözetleme, radar sistemleri gibi birçok konuda inanılmaz hızlı gelişen sistemler. Kendi alanındaki uzmanların bile takip edemediği kadar hızla gelişen bir yapıdan bahsediyoruz. Bunun temel katalizörü yapay zekâ. Yani şu an bizim ChatGPT’nin son versiyonu bile, savunma amaçlı kullanılan yazılımından emin olun çok daha ilkel versiyonu inanılmaz kalitede ve hızla kod yazıyor. 20 yıldır kod yazıyorum, mümkün olmadığını düşünüyorum.

Çip teknolojileri 2 nanometre diyerek ifade ediyoruz. Terim olarak kolay ama söylemek kolay, terimleri söylemek kolay detayına baktığımızda inanılmaz bir teknoloji. 2 nanometre dediğimiz şey aslında bir DNA molekülü boyutu, bir saç kılı bunun 20 bin katı ve 30 bin katı. Yani bu boyutta çip üretiyorlar.

Bir çip DNA molekülünün 20-30 bin katı. Bunu 1 nanometreye de düşürmeye yönelik çalışmalar var.

2017-2018-2019-2020 yılları arasında gök yüzündeki uydu değişimine baktığımızda her geçen yıl hızlı bir artış görüyoruz. Bunların 40 bine yakını yakın yörünge, 10 bine yakını orta bölgede, en azı da en dış katmanda. Karınca sürüsü, yani yukarıdan bir şey atsanız aşağıya düşmeyecek kadar uydu var. Bunların hiçbirisi birbirine değmiyor, eş zamanlı devamlı çalışıyor. Teknolojinin boyutlarının 2017'den bu yana gelişimini bu rakamlarla görebiliyoruz. Aslında yapay zekânın bu alana kattığı yeteneklerden birisi diyebiliriz ve 2029'a kadar 57 olması düşünüyor bu sayının.

Sayısal verinin ve verinin anlamlandırılmasının önemine bakalım. Petabayt, bir üstü Exabyte, bunun bir üstü Zettabyte. Yani özetle veri o kadar hızlı büyüyor ve o kadar değerli ki. Bunları sabah akşam hiç yorulmadan 7/24 işleyecek makinamız var. Bunlara bilinç kazandırabilecek, bizim gibi bağlam kurabilen, bizden daha iyi bağlam kurabilen algoritmamız var. Dolayısıyla bu hakikaten önümüzde duran, Hava Kuvvetleri açısından çok önemli bir alan.

Yakın gelecekteki teknolojik gereksinimler nedir diye baktığımızda Hava Kuvvetleri olarak, aslında ihtiyacın tanımı genel olarak küçük, hızlı, etkin, online çevrim içi, yani devamlı haberleşen ama kendi ağında haberleşen yapılara ihtiyacı olacak diye değerlendiriyoruz. Harekât merkezlerinde ne gibi ihtiyaçlarımız olacak? Mikro saniye mertebesinde tahminleme yapabilen ve karar desteği sağlayabilen sistemlere ihtiyacımız olacak. Yine kuantum şifreleme çok önemli olacak. Eğer bizim şu an kullandığımız şifrelemeler çöp olacaksa, ki kuantum hesaplama bunu sağlayan bir mekanizma, bizim şu an kullandığımız iletişim aracı değildir diyebiliriz. Çünkü bizim asimetric şifreleme yöntemlerimiz var ve kuantum bunu çok kısa zamanda çözebiliyor. Dolayısıyla bizim kuantum anahtar dağıtımı ve şifreleme ihtiyacımız olacak. Az önce de bahsettiğim gibi iç içe gelişmiş ağlar ve bunların farklı geçirgenlikteki güvenlik seviyelerini yapılandırmaya ihtiyacımız var. Bunlar iki boyutta iyi çalışıyor ama hava ve uzay boyutunda ciddi bir karışıklık var. Manyetik alan, güneş patlaması gibi birçok parametreyi hesaplamalıyız ve bunlar iletişimde kritik hassasiyeti olan konular.

Ve yine saniyede terabaytlarca veri akışını, yani 10 mili saniyenin altında, 10 milisaniye insanların anlayamayacağı bir algı düzeyi, biz insanlar 200 mili saniyeye kadar tepkiler verebiliyoruz. Yani artık gerçek zamanlı bir zaman diliminde birlikte çalışabilirlik ortamında simülasyon sistemleri tasarımı ile eğitim tatbikat ve strateji geliştirmesi sonucunda adım adım sanal evreni oluşturacak bir yapı ile geleceğin tahminlenmesi. Biz az önce de bahsettiğim, 20 yıl önce verilen çok değerli bir kararın Hava Kuvvetleri Bilgi Sistemi'nin nimetlerini yaşıyoruz. Hava Kuvvetleri'nin birçok yönetsel aracı hava kuvvetleri bilgi sistemi üzerinde çalışmakta ve bütün kurumsal veriler tam olması gereken yerde. Çok güzel bir şekilde iş zekâsı olarak adlandırdığımız bir yöntemle gayet güzel işlerlik kazandırıyor ve bizim kurumsal hafızamızı mükemmel bir şekilde yerine getiriyor. Yani savaş oyunu planlama aracı için deterministik ve gerçekten verdiği bilgilerin ne kadar doğru olduğu çok değişken, dünya gibi kaotik bir anlatacak kadar bir altyapısı olmayan sistemler.

Az önce de bahsettiğim gibi her geçen gün daha gerçekçi olacak iyileştirmeler bahsediyoruz. Bizim bir ASELSAN'ın geliştireceği bir sistemin dijital ikizini de bu arayüze göre bugünden yapması, 15 yıl sonra keşke hepsini yapsaydık diye geri döndüğümüz kaosu inanılmaz artıracak. Dolayısıyla bugün başlatılan bir proje, her şeyin bu projeye göre yapılmasını sağlayacak ve bundan 10-15 yıl sonra bize büyük avantajlar kazandıracak diye değerlendiriyoruz. Sistemin her geçen gün daha gerçekçi olacağı iyileştirmeler ile yaşayan bir sistem olacağı, gerçek dünya ile sanal evren arasında insan ve makine arayüzü kapsamında sanal gerçeklik, artırılmış gerçeklik ve karma gerçeklik teknolojilerindeki gelişmelerin entegre edilebileceği bir alt yapı sunacağını düşünüyoruz. Eğitim tatbikat ve istihbarat konularında hem maliyet etkin hem çok daha gerçekçi çözümler sunacak demistik bu sistem. Sadece taktik sahada değil, stratejik ve operatif, sahada kara deniz, hava, uzay, siber, sosyal harekât ve elektronik harp konularında da çok büyük faydalar sağlayacağı bir çalışma olacak. Konvansiyonel harekât dışında; hibrit ortamlar (fiziksel ve sanal ortam), gri bölge çatışmaları (resmi savaş yerine belirsiz ve düzensiz savaşlar), bilgi manipülasyonu, siber saldırılar, ekonomik baskı, sosyal mühendislik vb.), kinetik olmayan etkiler, KBRN senaryoları ve çeşitli doğal afet senaryolarının kurgulanabilmesine katkı sağlayacak.

Kinetik olmayan etkilere, yani Kimyasal, Biyolojik, Radyolojik ve Nükleer (KBRN) senaryoları bile uygulayabileceğimiz bir yapıya kavuşacağız.

Peki neye ihtiyacımız olacak? Sanal küresi ve fizik motoru olan, yatay ve dikey genişleyebilen, mikro servis tabanlı, büyük veriden bilgiyi çekebilen ve çekilen bilginin geçerliliğini tamamladıktan sonra blok zinciri (blockchain) temelli veri tabanında birleştiren, aslında 3. Parti uygulamalar olarak erişilebilen şeylerle üretilecek. Ama bunlar askeri amaçla kullanıldığında Millîleştirilmeye ihtiyacı olacak. Günün sonunda bugünden bir perspektif ve regülasyon planlarsak, ona göre savunma sanayimizi yönlendirirsek, bugünden alt yapısı yavaş yavaş kurulan bir yapının zaman içerisinde sanal küresi ve fizik motoru da Millîleştirilebilir diyoruz. Kolay değil, entegrasyonu gibi bunlar zaman alıcı süreçler ama yapay zekâyla da hızlanacak diye değerlendiriyoruz. Açık kaynaktan veri işleyebilmesi lazım ve böyle bir modülün olması lazım. Gerçek zamanlı istihbarat, çok katmanlı ağların benzetimi ve siber güvenlik ihtiyaçlarına da cevap vermesi gerekiyor. Öngörülen geliştirme takvimine başlığında, bugün Metaverse neyse, ülke veya firma olarak yapacağımız da yaşayan, bizim gibi gelişen ve devamlı öğrenen, kaotik süreçleri öğrenip karar vermeye destek olacak bir yapıdan bahsediyoruz. Ama 5 yıl içerisinde karmaşık askeri ve sivil senaryoların koşabileceği bir sanal ortam olabileceğini değerlendiriyoruz.

Sonuç olarak teknolojiadaki gelişmelerin ülke güvenliği için en etkin formlara dönüştürülmesi önem arz etmektedir. Sanayi devrimlerine baktığımızda 100 yıllarda olan, 1800 yıllarda başlayıp bugünlerde artık 5 yılda bir olan sanayi devrimlerinden bahsediyoruz. 2030'da gelecek kuantum teknolojilerinin bugünden artık sahaya inmeye başladığını görüyoruz. Bu insanoğlunun çok alışık olmadığı bir yapı, hiç bu kadar hızlı bir gelişim olmamıştı ve bu yapı hiç yorulmayan makinalardan dolayı daha da hızlanarak devam edecek diye değerlendiriyoruz.

Bu kapsamda küresel ölçekte özellikle yapay zekâ kapsamında Türkçe büyük dil modelinde çok temel bir ihtiyaç olduğunu, bugün hazır modelleri kullanarak bir yere kadar gideceğimize ama zamanında kullandığımız F-16'ların zor durumda e yapacağını bilmeyeceğimiz gibi Türkçe dil modeli de olmazsa benzer sıkıntılar yaşanacağını öngörüyoruz.

Sanal evrene, kuantum teknolojilerine yatırım yarışının bir parçası olunmasını da kıymetli olduğunu değerlendiriyoruz. Nitekim, teknolojiye yön veren, Amerika'nın Magnificent Seven denilen büyük firmalarının (Apple, Microsoft, Alphabet, Amazon, Nvidia, Meta ve Tesla) 10 trilyondan fazla değerlemesi olan firmaların tamamıyla yönünü buna döndüğünden de aslında birtakım ipuçları alabiliriz.

Teknolojiyi yakından takip eden en yüksek teknolojilerin kullanımını zorunlu kılan hava kuvvetlerinde bahse konu teknolojilerin adaptasyonu ve etkin şekilde kullanımı yaşamsaldır.

Özellikle yapay zekâ ve sanal Evren teknolojilerindeki gelişmelerin karar destek fonksiyonlarını desteklemesinin vazgeç olduğu bir harekât ortamında bu tarz yeteneklerin etkin kullanımının komutana kesin zafer yolunda bilgi üstünlüğü sağlayacağı değerlendirilmektedir. Boston Dynamics'in Atlas robotunun otonom, Cyborg diyebileceğimiz, insandan bile daha üstün hareketler yapabilen, kafasını 360 derece ya da 180 derece çevirebilen yeteneklerden bahsediyoruz. Bu da teknolojinin nereye gidebileceğine dair göstergelerden diye düşünüyorum.

Teşekkür ederim.

SORU 1: Büyük veri tabanlarının yönetiminde biz çok güvenlikçiyiz. Siz de yapay zekâ ile ilgili bir çalışma başlatmışsınız. Şimdiki öngörünüz, veri tabanlarımızı sadece kendi verilerimizle mi besleyeceğiz yoksa büyük veri tabanlarından destek mi alacağız. Kendi veri tabanlarımızla beslemeye devam edersek bu bize yetecek mi, kurguda şu an ki yeriniz ve düşünceniz nedir?

CEVAP: Veri tabanı bilgi sahibi olduğum bir konu. Verileri alıp, aynı insan gibi, insanın işlediği gibi özet veriler çıkarıp koyuyoruz. Yani bizim hazır kullandığımız modeller aslında tam olarak bu devasa veri kümelerinden, işlemcilerin çalışması sonucuyla özet görüntülerle besleniyor. Yani biz yazdığımızda mili saniyeler içinde cevap gelmesinin sebebi, aslında daha

daha önce o soruların sorulmuş olması, vektörünün çıkarılması. Dolayısıyla ne kadar veri işlerseniz o kadar avantajlı. Dolayısıyla ne kadar veri işlerseniz o kadar avantajlı. Bizim şu an bütün verilerimiz gidiyor, cep telefonundan taktığınız kol saatine kadar. Bütün verileri alıyorlar ve bunun önünde duramıyoruz. Yani durmak da işte demokrasi ve benzeri usullerden dolayı önlenemeyen bir durum. Sizin sabah ne zaman kalkacağınızı, bütün rutinleri takip ediyorlar. İhtiyaç olması halinde o veri orada duruyor. Sizi sizden daha iyi tanıyacak sistemlerden bahsediyoruz. Biz açmamalıyız veri tabanlarımızı. Ordunun en büyük gücü kapalı ağda çalışmasıdır, kapalı ağ gerçekten bir şey yapılması çok zor. Ama o kablolar üzerinden her şey yapılabilir, ama kapalı ağ orduyu en iyi koruyan konuların başındadır. Bu her zaman devam etmeli ne zamana kadar kuantuma geçene kadar belki, çünkü kuantum inkâr edilemezliği fizik olarak birebir sağlıyor. Yani nasıl biz bir elmayı attığımızda yere düşeceğinden eminsek haberleşmeye de kuantum anahtar değiştirmeye aynı güvenliği sağlayabiliyoruz.

SORU2: İnsan, yapay zekâ kritik kararların içinde mi kalmalı dışında mı?

CEVAP: Yapay zekâ bebek adımlarını atıyor. 1990'larda internet veya Google neyse 2000'li yıllarda ilk çıktığında, bugün de yapay zekânın ilk adımları bunlar. Dolayısıyla olgunluk seviyesinde yapay zekâyı ulaştırmaktan bahsediliyor. 'Yeni bir ışık gördüm, cahilliğim aydınlandı' gibi bir durum, dünyadaki bütün her konudaki uzmanlardan daha iyi bir yapı kurduk demek aslında. Bilgi verebilen ve bunu çok hızla yapabilen bir sistem. Alaaddin'in cini gibi, yani sihirli lambadan çıkan bir cin gibi de düşünebilir. Hakikaten birçok söylediğimizi yapabilecek bir makine grubundan bahsediyoruz. Yani insan tabii ki de karar vermenin içinde olacak. Çünkü bir noktada bir onu kendi çıkarlarımız için kullanacağız. Ama ne kadar az olursa, bir noktadan sonra, zaman içerisinde hiç görülmeyen milyarlarca ihtimallerin içinden en doğru ihtimali seçebiliyor. Dolayısıyla, biz de belki kararı ona bırakmayı isteyebileceğimiz zaman içinde.



Fatih Bilge İZGİ
HAVELSAN

Hepiniz hoş geldiniz, ben Fatih Bilge İzgi. Harbiye ürün ailesini anlatmadan önce kendimin de bir Harbiyeli olduğumu vurgulamak istiyorum. 1991 yılında Harp Okulu'ndan mezun oldum, 2015 yılında Türk Silahlı Kuvvetleri'nden emekli oldum, 2016'da Havelsan Komuta Kontrol Bilgi Sistemleri alanında çalışmaya başladım. İşin mutfağında mühendislik tarafıyla ihtiyaç makamı olan makam ile

tedarikçi makam arasında köprü görevi görüyoruz. Bu vesileyle bu alanda yetiştirmemizi sağlayan Türk Silahlı Kuvvetleri ve buradaki kazanımlarımızı bir nebze de olsa yansıtmaya çalıştığımız Komuta Kontrol sistemimiz hakkında bilgi vermemiz için fırsat veren SASAD organizasyonuna da teşekkür ederim.

Dijital karargâh dediğimiz zaman, tabii her şey dijital, havada sıfırlar birler uçuşuyor, ileriye dönük yaklaşımlar muhakkak olacak. Dün EDOK komutanımız Korgeneral Zorlu Topaloğlu'nun da söylediği gibi, proaktif davranmak durumundayız. Proaktif davranırken, bugünün çözümlerinde neler yapmışız bu anlamda bizim Havelsan tarafından geliştirilen Harekât Bilgi Yönetim ve Entegrasyon ürün ailemizi tanıtmış olacağım. Bu arada yine bütün bu anlatılanlar içerisinde bizim açımızdan gerçekleştirmeye çalıştığımız önemli bir konu da birlikte çalışabilirlik çözümü. Diğer standartlarda geliştirilmiş ya da dünyanın farklı bölgelerinde üretilen modeller, sistemler, yeteneklerle irtibatı da sağlama noktasında. Bir de veri analizinde de Havelsan'ın geliştirdiği yaklaşımları da aktarmaya çalışacağım.

Bizim ürün ailemiz aslında stratejik seviyede Harbiye, Karargâh, taktik seviyede Harbiye Taktik, TEK-ER mobil seviyesinde Harbiye TEK-ER uygulamamız var. Bunlar arasında entegrasyonda yine bu çözümümüzün bir parçası.

Biz Harekât Merkezi'nde cari hareketin takibi noktasındaki çözümler üzerine odaklanmış durumdayız. O yüzden cari hareketin takibi ve yönetiminde klasik işte durum haritaları üzerinden hareketin takibini yapma noktasına odaklanmış durumdayız, buradan aynı zamanda sevk ve idare yeteneğimizi sağlamış oluyoruz. Gerek dost durumunu gerek düşman durumunu bu şekilde takip ediyoruz. Tabii bu arada karargâhın en önemli görevlerinden bir tanesi de aslında karar vermek. Bu karar vermenin sonunda oluşan ürün de ne aslında ya plandır ya emirdir. Plandır sonra emre dönüş ya da direk emir olabilir. Ama burada bütün karargâhın ortak, yani paralel bir şekilde aynı planın ya da emrin ekleri, layihaları, cetvelleri üzerinde tasarruflarda bulunabilme yeteneği de yine önemli bir yetenek. Sadece plan, emir değil, burada karargâh durum muhakemeleri, işte direktifler hazırlanması da yine yeteneğimizin bir parçası. Muharebe için teşkilatlanmayı da burada merkeze almamız gerekiyor, çünkü bir muharebeyi ya da uzun soluklu bir muharebeyi icra ederken, hem normal bilgi akışının olması gerekiyor. Hani biz hangi birliğin altında, hangi birlik var, biz neredeyiz, yine özel bir durum için kısa süreliğine geçmiş olduğumuz organizasyon diye de tarif edebileceğimiz muharebe için teşkilatlanmayı da sistem için de oluşturulmalı, alt üst birliklere de yayınlanmalı ki, nasıl bir oluşum içerisinde olacağız hareketin ortasında veya sonunda, her safhasında.

Tabi bunların hepsi yapılırken askeri sembololoji çok önemli, buradaki askeri sembololoji de bir standart gerekiyor. Özellikle durum haritaları üzerinde baktığınızda, aynı bir nota gibi, nasıl bütün dünyada evrensel, bütün farklı ilgi alanlarındaki operatörler de aynı şeyi anlayabilmeli. Birlikte çalışma araçlarımız da işte briefing hazırlama araçları, beyaz tahta üzerinde çok farklı karargahlarda zamansal ve mekânsal olarak farklı ortamlarda olan unsurların sanki aynı odadaymış gibi bir beyaz tahta üzerinde çalışabileceği uygulamalarda yine ortak çalışma yapmamızı sağlıyor bize. PowerPoint'lerle boğuşma noktasından komuta kontrol bilgi sistemlerine geçiş aşaması. En azından 1999 yılında Kara Kuvvetleri Komutanlığı'nda başlamıştı, birinci ve ikinci yönetim aşamalarından sonra 3. Aşaması devam ediyor. Komuta Kontrol alanında Kara kuvvetleri bazında da yine çok güzel gelişmeler var.

Çatışmaların önlenmesinde yapay zekâ elbette çok önemli ve ilerliyor ama bizim yine insanın merkezde olduğu bir çakışma önleyen yeteneğimiz de olması gerekiyor. Yani bir bölgeye baktığınız zaman farklı teyit kanallarından gelen bilgileri de desteklememiz, çalışmamız gerekiyor ki, komutan baktığı zaman bu mudur bu mudur noktasında kendisine kolaylık sağlıyor.

Ayrı çalışma modları da gerekiyor bu karargâh ortamlarında, bu gibi karargâh yönelik komuta kontrol sistemlerinde. Çünkü siz bir yandan harekâtı yönetiyorsunuz, bir yandan tatbikatlar devam ediyor, bir yandan eğitim veriyorsunuz, bir yandan da kozmik odalarda dış dünyadan tamamen bağımsız olarak çok gizli planlar, genel savunma ya da taarruz planları geliştiriyorsunuz. Bunların hepsine cevap veren uygulamanın modları da olmalı. Ayrıca çoklu dil desteği de sağlayabiliyoruz.

Çatışmaların önlenmesi sürecinde, bir bölgede birden fazla teyit kanalından gelmiş olan, birden fazla haber kanalından gelmiş olan bir düşman birliği bilgisini, hakikaten bahsedilen düşman birliği mi yoksa farklı bir düşman birliği mi olduğunu tanımlayabilmek de çok önemli. Yani bizim askeri jargonda teyit edilmemiş veriden teyit edilmiş veriye ve teyit edilmiş durum haritasına ulaşmamızı sağlayacak olan yeteneğimiz de mevcut. Görevin yeniden oynatılması çok önemli bir kabiliyet. Çünkü özellikle faaliyet sonu incelemelerde, vardiya brifinglerde, geriye dönük verilere de hâkim olmak gerekiyor. Teknolojik anlamda hâkim olmak mühendisliğin alanı ama operasyonel anlamda hâkim olmak da yine bu özellikler vasıtasıyla hem vardiya brifinglerinde, hem de faaliyet sonu incelemelerinde, büyük bir operasyondan sonra geriye dönüp biz ne yaptık ne yapamadık sürecini değerlendirme noktasında önemli bir girdi olacaktır. Görevler veriyorsunuz birliklere, bunlar hep görevlerle oluyor, hani emir, emir, emir diyoruz ya. Ama alt tarafında aslında mühendislikle de aşağıya doğru testler atmaya başlıyorsunuz, operasyonel dünyada da görevler atmaya başlıyorsunuz. Ve bu görevlerin de yine çok iyi bir şekilde görsel takip edilmesi, birbirlerinde hangi görev, ne kadar görev var önemli. Hangi görevler çakışabilir, farkında olun diyebilecek özelliği de büyük önem arz ediyor.

Standart raporlarla birlikte vardiya raporları gibi raporlarla birlikte ihtiyaç duyulan raporlarla birlikte günlük raporlarla kişinin kendi çalışma şekline özel, ihtiyaç duyduğu ya da kendine özel geliştirdiği raporlar da yine sistem tarafından sunulabiliyor.

NATO'nun standart mesajlarını da yine bir yetenek olarak kullanıyoruz. CBS (Coğrafi Bilgi Sistemleri) yeteneklerimizde, yani harita analizi yetenekleri de teker veya taktik saha da değil, operatif ve stratejik, yani tugay ve üstü merkezler için de ulaştırılıyor. Bu da bize büyük bir kolaylık sağlıyor. Saha durum ve görünürlük analizinin yanında acaba ne taraftan ilerlemeli ne kadar güç gibi seçme alternatifleri sunan çözümlerimiz de var. Havelsan'ın KBRN yeteneğiyle de entegre olduğu zaman bu durumlarla ilgili de öngörüler sunabiliyoruz.

Proaktif davranmak noktasında yapmamız gereken şeylerden biri de aslında camiaya dahil olmak. Yani her şeyin bir camiası var. Ben, perküsyon diyorlar ama aslında darbuka kursuna gittim. Mesela onun farklı bir camiası var, adam bize anlattı. Mesela bir darbuka 22 cm'den başlıyor 26 cm'e kadar gidiyor. Hatta benim almış olduğum darbukayı da sen kazıklanmışsın, dedi. Çünkü ben o camiaya tam dahil olamamıştım, çünkü onun da kendine göre bir standart var, darbuka camiasının. Gelişmiş Komuta Kontrol sistemlerinin de takip etmesi gereken bir camia var. Bir önceki oturumda çok güzel bir soru soruldu ve hocam da ona güzel bir cevap verdi, 'Birçok alanda gelişme var, biz özel sektör olarak hangi alanda gelişmeliyiz, ne tarafa yönelmeliyiz?' şeklindeki soruya hocamız da 'Geliştiren tarafta olmalıyız' demişti. İşte bizim o 'geliştiren tarafta olmamızın şartı öncelikle bir camiaya dahil olmak.' İkinci şart ne, bir şeyler yapmak için oraya gideceksiniz. Bir şeyler yapmak için de konuya hâkim olmanız lazım. İlk toplantılarda gidersiniz böyle arkalarda oturursunuz, el kaldırsam mı, başıma iş açar mı dersiniz. Ama bir süre sonra tecrübe kazandığınızda, siz orada edilgen değil etken olmaya başlarsınız.

Değişiklik teklifleri vermeye başlarsınız ve evet, biz bunu düşünmedik demeye başlarlar. Biz bunu verirken de neyi düşünüyoruz? Millî tarafta bize lazım olanı. Çünkü bir model var, bizim takip ettiğimiz modeller var. Kara domainin de bizim takip ettiğimiz bir model var.

MIP ürünleri (Karşılıklı Çalışabilirlik Programı). Ne var, modeller var, veri modeli ve veri değişim modeli. Bunun içerisinde bizim dahil olmamız, etkin olmamız sonucunda bu modellerde de gerekli değişiklikleri yaptırıyoruz. Neyi takip ediyoruz, NATO'nu standartlarını. NATO'nun bir sürü standardı var ama özellikle Federasyonlu Görev Ağı (FM) tarafında bütün bu standartları paket haline getirdiği standartları takip ediyoruz. Şu anda 2030 yılında devreye girecek olan standartlar üzerinde çalışıyoruz ve bunlara katkı sağlıyoruz. Bazen bunu bir parçası olabilir miyiz diye abartıyoruz konuları ama onun çözüm noktasında cesaretle davranan 3-4 partnerden biri olabiliyorsunuz Havelsan gibi. Şu anda tam o pozisyonda gelecek olan bir standartta ne yapıyoruz proaktif davranma noktasında? O standardın bir parçası olarak ona kendi uygulamalarımızla çözüm sunuyoruz, standartların olgunlaşması noktasında da değişiklik tekliflerimizi sunuyoruz. Nereye gidiyoruz? İşte uluslararası NATO tatbikatlarına gidiyoruz, CWIX tatbikatlarına gidiyoruz.

Her yılın sonunda NATO'nun aslında işin hasılasının alındığı nokta ve buralarda odak noktaları görüyorsunuz. İşte burada hava, kara, deniz, siber, ayrıca bu yıl modelleme ve simülasyon gibi konular da dahil oldu. İşte konuşuyoruz, çoklu alan operasyonları, güzel projeksiyonlar, ileriye görecektir projeksiyonlar. 2030 yılında NATO ne yapacak? İşin geliştirme tarafında ya da emekçi tarafında olduğunuz zaman şunu görüyorsunuz, bu seneki CWIX tatbikatında odaklanan alan Multi Domain Command Control (Çoklu Alan Yönetimi Komuta Merkezi). Yani orada başlıyor bu konular, birtakım projeksiyonlar yapılıyor, tasarlanıyor, şöyle, böyle olmalı deniyor. İşte oradaysanız bu süreçlere dahil oluyorsunuz. Biz bunlara hep dahil olduk, 2018, 2019, 2021, 2022, 2023 dönemlerinde çeşitli versiyonlarına da dahil olup bütün testlerden başarıyla geçtik. Niye geçiyorsun, bunu da arıyorlar sizden ve sadece NATO ülkeleri aramıyor. Standardı karşılayan yetenek istiyor.

Harbiye Taktik dediğimiz ise tabur ve altı seviyede daha çok dar bant genişliklerde, haberleşme imkanlarının daha kısıtlı olduğu noktalarda ve daha hareketli olduğunuz noktalarda, yani taktik seviyedeki bir çözümümüz.

Karargâh çözümünün yeteneklerinin daha azaltıldığı ama bazı yeteneklerin yani taktik daha da artırılmış olduğu bir çözüm. Çünkü özellikle birlik takibi, hedef takip, yakın takip gibi daha hassas davranmamız gereken durumlarda yeteneklerin dahil olduğu ve yine dar alanda size haberleşme imkânı sağlayan bir sistem. Yine mesaj tanımlıyoruz, cari hareket yönetiyoruz. Mesela, navigasyon ve görevlendirmeler var. Yani stratejik seviyede ihtiyacımız olmayan bir yetenek burada artık bir yetenek olarak taktiğin içerisinde yer alıyor. Çünkü arazide navigasyon analizi ihtiyacı olabiliyor. Yine hareketli haritanız olması gerekiyor ki sürekli haritayı güncellemeyin.

Burada dost ve düşman durum bilgisi çok daha ön plana çıkıyor. Çünkü burada hakikaten sizin verdiğiniz girdilerle verilerle bütün o sistem besleniyor. Hani o karargâh dediğimiz karargâhın kararını alma noktasında, yürütmüş olduğu adımların çoğunun verisi buradan sağlanıyor. Madem mobiliz, aracın kendi üzerindeki sistemlerle de entegre olalım, kuledeki mühimmat sayısı, çevredeki tehdit tespit edilen unsurlara kadar entegrasyon da sağlanıyor.

Mobile geldiğimizde mobil bir cep telefonu uygulaması. Bunun üzerinde de ilave yetenekler var. Cengaver oluşumundaki roller ve ihtiyaç duyulan yetenekler de bütün sisteme dahil olmuş oluyor. Mesajlaşma, sensör verileri de bulunuyor mobil uygulamamızda.

Birlikte çalışabilirlik çözümünde farklı standartlarla oluşturulmuş sistemler ya da farklı zamanlarda oluşturmuş olan sistemler ya da aynı standardın farklı versiyonunu kullanmakta olan sistemler için çözüm sunuyor. Mali boyut, tasarruf, bir arada çözüm ve iş birliği gibi çok farklı kazanımlar sağlıyoruz bu şekilde. Burada size güçlü bir entegrasyon yeteneği sunuyoruz Octopus ile. Yani farklı sistemlerin farklı olarak geliştirilmiş olduğu alanlara da dahil olmadan, onların serbestliğine bir etkide bulunmadan ben farklı sistemlerden farklı veri alırım ve kullanırım diyebilirsiniz. Bunu yaptığınız zaman aslında bütün entegrasyon işiyle ayrı bir yetenek uğraşmış oluyor zaten. Komuta kontrol sistemlerinin hepsi ayrıca bir de entegrasyonla uğraşırsa üzerlerine ekstra bir yük binmiş olur. Bu alanın ayrı bir yetenek havuzu şeklinde yönetilmesi zamandan, finanstan tasarruf sağlamış oluyorsunuz. Veri analizinde de böyle bir yaklaşımımız var.

Yani bizim neye ihtiyacımız var aslında haber toplama planı içerisinde dengelenmiş olan haberlere ve verilere ihtiyacımız var. Bu bir ihtiyaç ve bu nasıl sağlanmalı? Doğru ve zamanında sağlanmalı, yani siz bir veriyi yanlış sağlarsanız, yanlış zamanda sağlarsanız olmaz. Doğru veriyi geç sağlarsanız o da güncelliğini yitirmiş olur. Dolayısıyla zamanında sağlamanız gerekiyor. Bunun için de bu haber toplama süreçlerinde operasyonel kullanıcıya yardımcı olacak özellikle de geliştirilmiş durumda.

Bütün kaynaklar taranmakta mimari yapıda. Metin, web, sosyal medya, görüntü ve videoların hepsini işleyerek gerek yazılı, gerek görsel bilgi çıkarımını yapıp son kullanıcıya yine web üzerinden masaüstü uygulama ya da mobil üzerinden sunabilirsiniz. Metinden bilgi çıkarımlarında siz bir set hazırlıyorsunuz, şu bölge, şu veriler lazım dediğinizde o size, o zamanda, geçmiş zamanda, hareketin ilerleyen zamanlarında verileri ulaştırıyor. Eğer ihtiyaç varsa dil çevrimi de yapıyor, aynı zamanda tasnif ediyor. Yani sizin önünüze internet sayfasına girip onun görüntüsünü alıp vermiyor. O işi sizin adınıza çok daha detaylı bir şekilde yapıyor. Görselden bilgi çıkarımı da yine aynı şekilde, örneğin Deniz Kuvvetleri uygulamasında, siz konuya dahil olmadan bir geminin belli başlı özelliklerini ortaya çıkarıp size sunuyor. Sadece görsel değil, metinsel bilgisini de sunuyor. Metni de olmayıp görselde olan verileri de ayrıca sunabiliyor. Veri hazırlama çalışması bütün bu sistemler için veriyi çok iyi hazırlamalısınız ki size iyi sonuç versinler.

Veri konusunun odak noktası, doğru veri, gerekli veri ve zamanlı veriyi operatöre, komutana veya karar vericiye sunmak.

Teşekkür ederim.

II. GÜN İKİNCİ OTURUM – YENİ DÜNYA
TEMA:
Müttefik Teknoloji ve Ulusal Uyum

OTURUM KONUSU:
İstihbarat ve Analizden Operasyonlara

OTURUM TEMALARI:

Dijital Merkez Yönetimi
Veri Yaşam Döngüsü
Müttefiklerle Teknoloji ve İstihbarat Paylaşımı
Yenilenen Savaş Teknolojileri
İstihbarat ve Operasyonda Otonom Teknoloji Kullanımı
Kapasite ve Kapasite Gelişimi

VII. OTURUM ÖZETİ

Verinin toplanması, depolanması, güvenliğinin sağlanması, iletilmesi ve yorumlanmasında yapay zekânın getirebileceği riskler için hangi verilerin nasıl kullanılacağı belirlenmesinin önemine dikkat çekilmiştir. Yapay zekânın şu anki döneminde verilen veriyi taklit ettiği, henüz orijinal bir fikir vermekte aşamasına gelmediği dile getirilirken, özellikle bu dönemde ordunun göze alamayacağı riskleri barındırmasından kaynaklı farklı alternatifler üzerinde çalışmalara yoğunlaşılması yönünde tavsiye paylaşılmıştır.

Farklı istatistiksel yöntemler ve yazılımlara öncelik verilebileceği önerisi getirilirken, veri filtrelemesinin ya da sensör füzyonu gibi yöntemlerin alanlarına göre tercih edilmesi tavsiyesinde bulunulmuştur. F-35, yani 5. Nesil uçak örneğinden yola çıkılarak, görüntü işleme noktasında yapay zekânın kullanılabileceği, ama hedef tespiti, takibi, durum vektörü, nerede olduğu gibi veriler için kinematik vektör, sensör füzyonu gibi çözümlerin hem güvenlik hem de veri yükü açısından daha kullanışlı olabileceği belirtilmiştir. İnsan geri beslemesiyle bütünleştirilecek bu yöntemlerin karar alacak yapay zekâ model eğitimlerinde daha isabetli kararlar sağlayacağı vurgulandı. Ayrıca, TUSAŞ saldırısı örneğinde, binanın planlarının internette bulunmasının ve bunu önleyecek yazılım veya filtrelemenin yapılmamasının askeri güvenlik boyutuyla oluşturabileceği risklere dikkat çekilirken, yapay zekânın kritik durumda 'ben bunu anlamadım' diyebileceği ortamların da kısa ve orta vadeli dönemler için riskli durumlar oluşturabileceği kaygısı dile getirilmiştir. Bu tarz farklı çözüm önerilerinin test edilebilmesi için veri paylaşımı konusunda işbirliklerinin artırılması talep edilirken, akademik çalışmalardaki geliştirme çalışmalarında bu problemin kaldırılması halinde ürün, proje ve çözüm geliştirmeye süreçlerin hızlanabileceği belirtilmiştir.

Son bölümde, uzay, uydu, ağ merkezleri, yapay zekâ gibi konularla modernizasyon ve dönüşümler dünya genelindeki çalışmalarla örneklendirilmiştir.

Teknolojilerle harp ortamlarında yaşanan değişiklikler, komuta-kontrol kademesindeki değişimler, geleceğin harp ortamlarında teknolojilerin kullanımına dair öngörüler paylaşılırken, otonom helikopter, otonom tank, yapay zekâ bilgi sistemleri, insansız sistemler ve sürü teknolojilerinin stratejik seviyede, operasyonel seviyede, taktik seviyede ve angajman seviyelerinde doktrinleri yenileyeceği düşüncesi paylaşılmıştır. Bilgiyi yapısallandırarak en hızlı gözlemleyen, yönlendiren, karar veren ve hızlı karar verenin en büyük rekabetçi üstünlüğe sahip olacağı vurgusu yapıldı. Savaşlarda değişmeyen en büyük gerçeğin 'muharebesiz muharebe olmayacağı' doktrini olduğu vurgusuyla, elektromanyetik spektrumu ele geçirmenin önemine dikkat çekilirken, sürü zekâsının da öncelikle bu tarz hedeflere yöneleceği tahmini paylaşıldı. Rakip teknolojilerin yakından takip edilmesiyle asimetrik mukabele teknolojilerinin geliştirilmesinin önemine dikkat çekildi.



**Emekli Korgeneral
Nihat KÖKMEN
MODERATÖR**

Merhabalar, ben Hava Kuvvetleri Kurmay Başkanlığı ve NATO'da NATO Türk Askeri Temsil Heyet (TMR) başkanlığı yaptım. İlgili alanımla ilgili düşünce kuruluşlarında makalelerim yayınlanıyor. Teknolojiyle ilgim noktasında geçmişte, Hava Kuvvetleri Komutanlığı'nda Plan Prensipler Başkanlığı yaptığım dönemde yoğun olarak Hava Kuvvetlerimizin projeleri ve geleceğe yönelik öngörülerıyla

ilgili çalışmalar yaptık. Bunlardan birçoğunu da gerçekleştirdik. Her ne kadar insansız sistemler, otonom sistemler, dronlar konuşuyoruz ama ben hala insanlı sistemlerin kuvvetlerimizin asıl vurucu unsuru olduğuna inanların tarafındayım. Diğer taraftan 2010-2012 yılları arasında MSB Müsteşar Yardımcılığı görevi yaptım. Göktürk-2 uydu fırlatma sistemi üzerine çalışmıştık. Sonda roketi üzerinde çalıştık, nüfuz edici bomba ve cirit gibi birçok projeye katkı sağladık değerli arkadaşlarımızla.

Elbette yapay zekânın hayatımıza girdiğini görüyoruz ve artık bundan kaçış olmadığını biliyoruz. Hayatımıza günlük teknolojilerle girdi. Ama tabii ki, bizim askerler olarak güvenlik ve beka olduğunun altını da çizmek istiyorum. Sohbet ortamındaki oturumumuza başlıyoruz. 'Müttefik Teknoloji ve Millî Uyum' temasında istihbarat, analizler de belirgin olarak ifade edilmiş. Tabii ki, harekât ortamında en fazla ihtiyacımız olan konulardan biri istihbarat. Bu istihbaratın elde edilmesi, depolanması, iletilmesi, saklanması ve saha kullanıcılara, karar vericilere ulaştırmanın ne denli olduğunu hepimiz tahayyül edebiliyoruz.



Doç. Dr. Ahmet GÜNEŞ
GEBZE ÜNİVERSİTESİ

Merhaba herkese verinin karargâhta kullanılması ya da herhangi bir yerde kullanılması ile ilgili ilk aşama veri yaşam döngüsüne bir bakmakla başlıyor. Tabii bunu artık hangi kanallardan ileteceksek, verinin depolanması ve veri güvenliğinin sağlanması, veri erişimi kısıtlarının belirlenmesi ve en sonunda da ne yapacağız; yorumlama ve analiz. Veriyi topladıktan sonra verinin ilk olarak

bakılması gereken kısmı, verinin kalitesi. Veride ne yapmak istiyoruz da bu veriyi topladık, bu veri kendi içinde tutarlı mı diye bakmamız gerekiyor. Farklı bir operasyonel bölgede biz bu aynı verilerle başka bir yerde de çalışabiliyor muyuz? Yani ortam değişikliğinde ne gibi sıkıntılar olabilir, bu parametrelerin değerlendirilmesi lazım.

Veri kalitesini değerlendirirken, orada insan kalitesinin de olması gerekiyor ki, veriye baktığı zaman bu bizim yönlendirilebilmemiz gerekiyor. İstihbarat kaynaklarımız, veri kaynaklarımız ne diye bakarsak iletişim tabanlı (SIGINT), elektromanyetik harp ve müdahale, görüntü analizi, coğrafi zekâ (uydular, GPS verileri gibi), siber istihbarat (çevrimiçi etkinlik, sosyal medya, izinsiz girişler), akustik istihbarat (deniz ve su altı tehditleri) ve biyometrik istihbarat (şehir güvenliği, Mobese) gibi alanları görebiliriz. Elektronik harp Türkiye’de oldukça çok konuşulan bir konu. Ben de bir kısa baktığım zaman, neredeyse her şeyin sonuna INT konularak istihbarat haline getirildiğini gördüm. Özellikle bu veri toplama kısmında Türkiye fena değil. Farklı sensörlerden farklı kanallardan veri almak mümkün. MOBESE’den, Infrared’den, insansız hava araçlarına kadar. Sadece akustik intelligent pek duyulmamış olabilir. Orada da gemilerin akustik imzalarının toplanmasından bahsediliyor. Verinin toplanmasından sonra ise işler karışıyor bence. Verinin şifrelenmesi, siber güvenlik gibi konulara dikkat edilmesi gerekiyor. Ancak, bir önceki oturumda binbaşım demişti ki, ‘Biz askerler olarak verimizi koruma taraftarıyız’. Tamam çok güzel de biz mühendisler olarak bu verilere ihtiyaç duyuyoruz. Burada sıkıntı şu oluyor güvenlik mi, çalışma kolaylığı mı?

Gidip çok gizli ülkenin güvenliği için kritik bilgileri vermekten bahsetmiyoruz burada ama, katmanlı bir erişim tanımlanabilir, şifreleme, güvenlik sistemleri artırılarak bu tarz verilere daha rahat ulaşım tanımlanabilir, araştırmacılar ve şirketler için.

Çünkü mesela hiper spektral görüntü işleme, konu çok zor değil ama sensörler çok pahalı. Bununla ilgili Türkiye’de bir iki şirket çalışabiliyor. Ama belki özel sektörle bazı oyuncak problemler tanımlanıp veri dağıtabilsek, çok daha fazla şirketten daha fazla veri alınabilir hale gelecek. Su altı akustikte benzer sorunlar var, sensörler ve araçlar, cihazlar çok pahalı. Hava görüntülerinde de benzer sorunlar olduğunu zannediyorum. Böyle bir ikilem var. Güvenlik tarafına fazlaca kaymış durumdayız.

Bu arada veri yaşam döngüsünde verinin analizi ve yorumlanması kısmında veriyi aldık, verimiz doğru mu, hata var mı? Örneğin bir yerden sızma bekliyorsunuz, siz kamerayla 10 kişi yakaladınız ama sınırın iç tarafında 10 katına çıktı telsiz haberleşmesi. Demek ki bir şeyleri kaçırmışız. Tutarlı mı elimizdeki veri, hata yapıyor muyuz diye bakılması çok önemli. Örnekte tanıma ise, bilgisayar ve elektronik mühendisliğinde derslerin ismi. Verinin kendi içindeki korelasyon ya da anomali analizlerinin yapılması gerekiyor. Maalesef verileri alıyoruz ve sadece görselleştirmede kullanıyoruz. Veri analizinin başlığı görselleştirme ama biz genel olarak burada kalıyoruz. Sadece savunma sanayi tarafında değil, endüstri 4.0 alanında da böyleyiz. Dijital veri sadece yöneticilere rapor vermek için kullanılır gibi bir durumdayız, bundan dolayı da dijitalleşme endekslerindeki sıralamamız belli. Peki veriyi aldık, önden analizi yaptık? Benim özellikle değineceğim konu şu. Yapay zekâyla yatıp yapay zekâyla kalkıyoruz, ben de çalışıyorum konuyu.

Ancak, şimdi anomali tespiti yapacağız mesela. Ne oldu bir yerdeki verilerde sapma var. Mesela bir aktivite var bir yerde. Görüntülerde beklemediğimiz bir şey çıktı. Biz burada yapay zekâ tabanlı bir çözüm üretmek yerine, lise öğrencisi matematiği seviyesinde çözümlerle işin çoğu kısmının çözümü mümkün. Dahası, yapay zekânın saçmalama, olmayan şeylerle size verebileceği ihtimali de var. İstatistiksel, matematiksel yöntemlerle yaptıklarınızda size ‘hata var’ diyor, size önereceğim, anomali var diyecek, kararı yine karargâh versin, sorumlu karar versin.

Yapay zekâda şöyle bir sıkıntı var, yapay zekâ taklit eder, sizin verdiğiniz veriyi taklit etmektir onun asıl vazifesi. Çok orijinal bir şey bulacağım diye uğraşmaz. Kullanmayalım demiyorum, verimliliği artırır mı, evet. Ama sahaya çıktığında ne yapağını bilemezsin. Örneğin, Tesla'nın kazaları da kurban olan insanlar da bu eğitimlere dahil edilebilir. Hala otonom bir araç yok piyasada. Yani veri geldi deyip ona göre yeniden uyum sağlamaya çalışacağız. Şimdi bu evet ordunun göze alabileceği bir risk olmadığı için, yapay zekânın nerede nasıl kullanılacağı konusunda bir dikkatli düşünülmesi lazım.

Bir kez daha söylüyorum, şu andaki problemlerin birçoğunun standart, daha geleneksel, daha matematiğe dayalı yöntemlerle çözülmesi mümkün. Mesela, Boston Dynamics robot yapıyor. Ben de pekiştirmeli öğrenme çalışıyorum. Bunlar robotlarda, otonom araçlarda kullanılan algoritmalar genel olarak. Boston Dynamics kendi robotlarında pekiştirmeli öğrenme kullanmıyor. Niye, çünkü kontrol ve optimizasyon adamlara yetiyor. Şimdi burayı biraz kaçırıyoruz gibi geliyor. Verinin filtrelenmesinde LLM ile ihtiyacınız olan şeyleri filtreleme şansınız var. Veriyi veriyorsunuz, önemli kısımları veriyor. Diğer taraftan yine istatistiksel yöntemlerle de bunu yapabilirsiniz. Alternatif yöntemlerde ise F-35'in, yani 5. Nesil uçakların kullandığı kritik teknolojilerden bir tanesi sensör füzyonu. Neden? Çok fazla sensörden çok fazla veri geliyor. Uçakların birbirleriyle de haberleşmesi gerekiyor. Burada da yapay zekâ kullanılmıyor. Görüntü işlemek, sinyalleri işlemek için kullanabilirsiniz ama hedefi takip, tespit, nerede olduğunu, durum vektörünü, kinematik vektörü için sensör füzyonu algoritmaları var, bunları kullanmak durumundasınız.

Harekât için hazır deterministik toollar var denmişti. Birbiriyle rakip olan çoklu unsurların eğitildiği, birbirleriyle yarıştığı senaryolar geliştirilebilir. Benim bildiğin kadarıyla, SSB'nin de böyle projeleri de var. Ancak, deterministik olması, o projelerin ucu nereye gittiğinin ucu bende yok? Ancak ortamda senaryoları kurup, Türkiye'ye özel ve özgü problemleri çözme şansımız var. Demek istediğim, asıl mesele 6. Jenerasyon jet uçağı diyoruz. Amerika bunu Güney Çin Denizi'nde Tayvan'a Çinliler saldıracak korkusuyla geliştirmeye çalışırken, biz burada başka sorunlarımız varken, biz bunu mu yapmalıyız yoksa kendimize özel teknolojiler mi geliştirmemiz gerekiyor. Buna yönelik teknolojiler mi geliştirmemiz gerekiyor.

Bundan dolayı bu tür yaklaşımlarla analizler yapabiliriz. Son olarak bu LLM'lerde, bu modellerde, simülasyonlar içinde yapay zekâ öğrendi. Yeni bir taktik silah aldık ve bize taktik önerdi. Ama bakıyorsunuz ki, burada şöyle çalışmaz yorumunu yapıyorsunuz. Buna insan geri beslemesi vererek, karar alacak modelleri eğitmek de mümkün. LLM ve Chat GPT son versiyonlarında da yapılan buydu. Yani geri beslemeyle bunları eğitebiliyoruz.

Otonom sistemlerin istihbarat için kullanılması biraz daha zorunluluk dolayısıyla aslında. Şöyle ki, savunma sanayi ile ilgili bir panel olup da Ukrayna Savaşı'ndan bahsetmemek mümkün değil. Savaşın ilk başında TB2 kullanılıyordu, şu anda ise göremiyoruz. Neden? Elektronik Harp 'ten kaynaklı bazı sıkıntılar var. Şimdi buradaki kritik noktalardan bir tanesi de siz operatörle yönetmek zorundaysanız insansız aracı, karşı taraf o aradaki bağlantıyı koparabiliyor. Siz haberleşmeye geçtiğiniz anda zaten buradayım demiş oluyorsunuz, tespit konusunda da sıkıntı oluyor. Bundan dolayı otonom araçları kullanmak istihbarat açısından tabii ki daha mantıklı. Ayrıca, otonom araçların, başında bir personel beklemesi gerekmediği için çok daha uzun süre çalışabiliyor.

Yaklaşık 2 ya da 3 ay önceki bir haberdi galiba, daha uzun süre de olmuş olabilir. Bunun deniz su araçlarında uygulamaları var, zaten suyun altında haberleşme sıkıntımız olduğu için, elektromanyetik dalga kullanamadığımız için. Amerikalılar Guam'dan Tayvan veya Filipinler'e kadar güneş enerjisiyle çalışan sabit kanatlı bir sistem uçurmuştu. Yani insansız ve otonom gidebilen sistemler. Payload, yani sahada madem böyle bir çalışmaya girdiniz artık bunların sürü halinde kullanılması ve dağıtık sistemler halinde otonom araçların kullanılması da yaygınlaştı. Bir de self learning sistemlerle ilgili yazılımda ben bunun çok kullanıldığını maalesef görmedim. Ne demek istiyorum, bizim özel sektörde, mobil oyunlarda ne zaman satın alma tavsiyesi versin model, ya da oyun veya yazılım diye çalışmamız var. Kendi kendine öğreniyor ve kim ne zaman almış üzerinden karar verebiliyor. Oysa askeri sistemlerde yazılımı koydum, interneti taradı, mesela TUSAŞ'ın 3-4 aydaki patlama olmuştu. Sonra dendi ki, binanın planları internette varmış, buranın mimarı bunu internete koymuş. Peki neden bir tane yazılım gidip bunu bulmadı, burada bir anormallik var demedi.

Şimdi normalde bunların yapılabiliyor olması gerekmez mi? Şimdi bunun gibi yazılımdaki kendi kendine öğrenebilen sistemlerden kastım da bu. En azından bir modelin, ya burada bir tuhafılık var demesi lazım.

Yapay zekânın ya da diğer teknolojilerin de tabii ki kullanılacağı yer var. İnternet derya deniz, sosyal medya derya deniz tabii buraya botları atıp sizin analizi oradan otomatik yapmanız gerekiyor. NLP özellikle veri analizinde ihtiyacımız olacak bir şey, çıkarım yapabilecek, bazı yetenekleri de var. Ama mesela, gürültülü ortamlarda helikopterlerde komut tanımayla ilgili LLM kullanılabilir mi diye soruluyor? Buna gerek var mı, ben şüpheliyim. Daha farklı yöntemler daha iyi sonuç verebilir. Biz üniversite olarak buna çalışıyoruz ama biz soran olursa cevap vermek için çalışıyoruz. Ancak, ürünleşecek bir şeye bunu koymak tartışılır, ne kadar makuldür? Çünkü sizin LLM ben bunu anlamadım demeyecek, bu komuta daha yakın derse ve karar verirse ne yapacaksınız? Ön analizde, senaryoların kestirimini yapıp, örneğin belirli bir bölgeye sensörleri, multi static radarı koyduk. Buraya nereden taarruz yapılabilir, bunun analiziyle ilgili de evet yapay zekâyı kullanmak çok mantıklı. Bu çerçeveyi veriyor ama yapay zekâ bir yerde hata yapıyor mu diye bir insanın kesinlikle orada bulunması gerekiyor, onay için.

Son olarak da sensör füzyonu kısmında, sensör füzyonu teknolojilerinin yani diğer algoritmik yaklaşımların yapılması gerekiyor. Örneğin, Mobese sisteminde biyometrik veri alınıyor. Yüz, plaka tanınıyor. Ankara'daki patlamayı hatırlarsanız, yani neredeyse 10 sene oldu Kızılay'daki. Orada Şanlıurfa plakalı bir araç Kızılay'dan 7 kere geçmiş, biz bunu haberlerden öğreniyoruz. O dönem bir emniyet müdürüyle bunun bir algoritmasının yapılabilceği yönünde konuşmuştum. Anomali tespiti yapılabilir, şu veya bu plakalarda size sıkıntı olabilir diye sizin önünüze sunulur. Bana gelen cevap şu; 'Ben zaten aradığım plakayı zaten bulabiliyorum. 1 milyon tane plakadan hangisini arayacağını söylemem lazım benim. Bu sistemlerde algoritmadır, yapay zekâ nedense henüz yok. Bu da bize gerçek zamanlı veri ve anomali sağlanmasıyla ilgili beceri kazandırılması gerektiğini gösteriyor. Ben neden yapılmadığını bilmiyorum, neredeyse bu noktada tez verme noktasına geldim.

Mevcut beceriler, biyometrik veriler, gerçek zamanlı görüntüleme gibi Kent Güvenlik Yönetimi Sistemleri (KGYS) var biliyorsunuz. Ama olası tehditleri filtreleme, daha kolay karar verme, zayıf noktaların analizi ve sistematik iyileştirmeler, güvenlik yönetim sistemi gibi yetenekler eklenebilir.

Bir başka örnek uygulama, Türkiye’de yapılıyorsa ben de öğrenmiş olmak isterim. Türk boğazları var değil mi İstanbul, Çanakkale gibi. Biz torpido yapıyoruz, sonar yapıyoruz yani su altında hedef tespiti alakalı sensörlerimiz var. Peki Türk boğazlarının benim çok yetkin sonar sistemim olmalı ki, ben buradan imza, pervane, makine gürültüsü imzası toplayayım. Örneğin, böyle bir imza toplayan sistemimiz yok. Böyle bir sistem olsa bile, otonom olarak suyun altında kullanılan sistemler var, ancak Ege gibi çok da kullanışlı olabilecek yerlerde uygulanmıyor. Üstüne sensör koymanız durumunda 7/24 çalışabiliyorlar. Çin Denizi’nde Amerikalıların 6 ay çalışan sistemleri var. Buradan ne çıktımız var peki? Veriyi topluyoruz, veriyi saklama konusunda da hassasiyet var. Peki bir kuru yük gemisinin pervane gürültüsünü saklamaya ihtiyaç var mı? Algoritma konusunda eğer kimse görmezse veriyi, çalışabilecek 2-3 tane şirketimiz var. Bu algoritmaların geliştirilmesi için, biz bu veriyi sadece belirli hedefler için açsak ne olur? Adamın elinde parası olsa, su altı ekipman alabilse kendisi yapacak. Ayrıca üniversitenin ihtiyaçlardan haberi yok. Özel sektör de bir bariyer var ama alt yapısı olmadığı için giremiyor. Bu yüzden, algoritma gelişimi için verinin oyuncak verilerle paylaşılarak özel sektör ve üniversite tarafından kullanımını sağlamak noktasında bir farkındalık oluşturulması gerektiğini düşünüyorum.

Ben verinin gizlilik dereceleri konusunda kuşkucuyum. Veri paylaşım kültürü ile alakalı bir problemimiz olduğunu düşünüyorum, geliştirilmesi gerektiğini ve bunun da gelişmelere katkı sağlayacağını düşünüyorum.

Taktiksel veya stratejik geliştirme için sahada uygulanabilecek neler olabilir? OpenAI’nın çok unsurlu pekiştirme unsurlu pekiştirmeli öğrenme modelleriyle yapmış olduğu bir oyun çözümü var, yakalamacılık işte ya da saklambaç. Burada iki tane takım var, iki takım çok unsurlu pekiştirmeli öğrenmeden, çoklu ajan takviyeli öğrenme (MARL) birbirine karşı oyun oynuyor.

Senaryoda tanımlanan ancak kullanıcıların düşünmediği bir çözümle geliyor agent unsurlar, modeller. Bunu niye söylüyorum, yani senaryo bizim insan olarak göremeyeceğimiz, çünkü adam milyonlarca defa deniyor, deneme yanıyla öğreniyor ortamda zaten. Çok zeki mi değil, ama 1 milyon defa deniyor. Biz de denesek 1 milyon defa biz de buluruz. Ama ne zamanımız ne durumumuz var. Bundan dolayı modele veriyoruz, o senaryodan bunu öğreniyoruz. Peki insan geri beslemesi nerede olacak burada? Burada da şöyle, diyelim ki senaryoda hata var, ya da beğenmediğiniz bir performans gösterdi ya da işte beğenmediğiniz bir performans gösterdi. Bir şey koymak istiyorsunuz. Orada insan geri beslemesini verme veya senaryoyu yeniden düzeltebiliriz.

Veri süreci demiştik ya, en son analiz ettik, kararlar alınacak. Belki bu bir stratejiye, doktrine dönüştürülecek. Burada da bir takım Rusya örneği üzerinden gidelim. Şimdi Ukrayna Savaşı'nda Rusya'nın takıldığı yerler belli, 3 katı kadar askeri olmasına rağmen ilerlemiyor. Ama mesela Halep'e saldırdıkları zamanı hatırlarsanız. Açık kaynakta hassas bombaları yok, Halep'ten çıkmaları mümkün değil diye ilk başta haber geliyordu. Sonra onu şöyle çözdüler, hassas bomba kullanmayıp şehrin hepsini yıktılar. Sonra ne oldu? Ruslar orada zafer kazanmış oldu. Grozni mevzusunda da kayıp verdiler ama başarılı oldular mı evet, orayı ele geçirdiler. Ama neden başarılı olduklarını analiz etmedikleri için, sonradan neden başarısız olduklarını analiz edecek durumda değiller. Burada da böyle bir kültür var. 1500'lü yıllarda ilk gizli polis teşkilatını kuruyorlar. Tuhaf bir devlet gelenekleri var. Sahadan ya da bürokrasiden almak istediği haberin, doğru değil iyi olmasını tercih etmesine neden oluyor yöneticilerin. O zaman da zaten aslında veri gelmiyor, size bunun üzerinden de sizin öğrenebilen bir yapı, sensörlerden veri gelmiş, istihbarat gelmiş önemli değil, siz bunu kullanmıyorsunuz ki. Bir de bu bizim tatbikatlarda da maalesef gördüğüm bir sıkıntı. Tatbikatlarda sürekli yüzde yüz başarı olduğu ibaresini görüyordum. Yüzde 100 başarı olduğu zaman zaten çözülecek bir şey yok o zaman zaten başarılıyız.

Örneğin, Amerika'da sığ su destroyeri geliştirilecekti, 30'dan fazla yapılacaktı, sayısı 3'e düşürüldü. Neden, proje başarısız oldu. Yine okuduğum kadarıyla 6. Nesil Savaş Uçağı geliştirme projesi yine durdurulmuş, çünkü bütçenin dışına çıkmış.

Şimdi burada şöyle bir durum var, Amerika Ar-Ge projelerinde başarısız olabiliyor. Ben, bizde başarısız olan Ar-Ge projesi bilmiyorum. Ama Ar-Ge zaten riskli bir şey, başarısız olması lazım bir oranda. Bu ikilemi bilemiyorum, burada bir sıkıntı var gibi geliyor bana.

Üniversite, sanayi, devlet sektörün iş birliği konusunda bazı kopukluklar var. Personel yetiştirilmesiyle alakalı devlet tarafından yapılıyor ama hala bazı kopukluklar var. Ama oradaki bağlantı hala kurulamıyor. Çünkü bazı alışkanlıklar, kültürel bazı sıkıntılar var gibi görünüyor. Bunların çözülmesi gerekiyor ki, sizin sahadan topladığınız istihbaratın en son sağlıklı karar verecek ve sonra strateji geliştirecek hale getirebilirsiniz.

SORU: Güvenlik mi, kolay çalışma mı dediniz. Bunun iki neden bir arada olmuyor?

CEVAP: Açık söylemeliyim, 2009'da Ergenekon meselesi ülkenin üstüne çökmeden önce, biz rahat rahat bir yerde çalışabiliyorduk. Sonra istihbarat ve veri kaçağı ile alakalı aşırı bir hassasiyet başladı ve gerçekten aşırı bir noktaya geldi. Yani ben internetten bir makale araştıracağım, örneği oyun teorisi ile ilgili bir makale araştıracağım. Şimdi bilgisayarlar ayrıldı, kapalı devre, şimdi internetle ilgili önlemler alındı, kapalı devre sistemler kuruldu ama. Ama internet bilgisayarında bir araştırmada oyun teorisi ile ilgili bir şey arandığında sistem erişimi engelliyordu. Bunlar belki aşılmıştır ama alt tarafın daha rahat çalışmasıyla ilgili belirli kararlar alınabilir, bunlar aşılmalı, bu değerlendirilmiyor gibi.



Dr. Hüseyin BEYAZIT
KOLOMBİYA ÜNİVERSİTESİ

karşısında, tıpkı Çinlilerin keşfetmiyoruz, asimetrik zorundayız.

Sayın oturma başkanım ve değerli komutanım, Türk Silahlı Kuvvetleri'nin değerli mensupları ve değerli katılımcılar hepinizi saygıyla selamlarım. Bilginin zekâtı yüzde 100 olduğu için, bana bu fırsatı verenlere teşekkür ederim. Angajman, taktik, operasyonel ve stratejik seviyeler artık aralarındaki hatlar birbirleriyle geçişmeye başladı. Bizim gibi ülkeler, yapay zekâ ve benzeriler gibi konular yaptığı gibi, Amerika'yı yeniden mukabele paketleri geliştirmek

Thomas Barnet, Pentagon'un yol haritasını yapan, bir YouTube kanalında seyretmişim canlı konferansta, diyor ki 'Şu gördüğümüz sistemlerin sonunda Çin, Rusya, Amerika, Hindistan da dahil olmak üzere çıkacak bir savaşın 5 saniye, ben 15 saniye yaptım, herkes birbirini kör, felç edecek. Bunun için Çinlilerin önce askeri alanda devrim konsepti, ki ağ destekli, yanlış söylüyoruz, şebekenin muktedir kıldığı yetenekler, daha sonra şebeke merkezi, ağ statistik şebeke, ağ merkezli operasyonlar, şebeke merkezli muharebeler. Buna ben mukabele edeceğim diyor, ben uzaya bütün keşif gözetleme, istihbarat ve casus uygulamalar koyacağım, bunun yerine ben uydu savar füzeler geliştiririm ve hava araçları geliştiririm. Kocaman nükleer denizaltılar yerine küçük deniz altılarla mevcut şartlarla mukabele ederim. Altını çizmek istiyorum, herkesin asimetrik mukabele paketlerini düşünmesi lazım.

Gazi Mustafa Kemal Atatürk, 1933 de, 'Bizce olayları değerlendirirken, zamanın sürat ve hareket konseptine, mefhumuna göre hareket etmeliyiz' diyor. O zaman biz olaylar bizi değil, biz olayları yönetiriz.

Türkiye'de ağ merkezli muharebeler hakkında konuşuyoruz, Savunma, bilgi felsefedir ve bilim felsefesidir. Pozitif bilim, matematiktir. Çok önemli bu konu, matematik gittiği zaman olmaz, yapay zekânın bütün algoritmalarının temeli matematiktir. Nörolog Profesör İsmail Hakkı Aydın diyor ki, 'Matematik, Kur'an dilidir, yani kâinatı okuyabilmek.'

Bunları nasıl yabancıların ve bizi çok seven komşu ülkelerimizin kullandıklarını da arz edeceğim. Tabi fiziktir, kimyadır, biyoloji ve sosyal bilimler gibi diğer bilimlerdir. Gödel'in bir teorisi var; 'Sorunsuz bir sistem yok, kâinatta hiçbir şey yüzde 100 değildir.' Bizde buna İslam geleneği üzerine Sünnetullah deniliyor

Bir olaya baktığımızda çok farklı perspektiflerden bakmak zorundayız, dünya da böyle yapıyor. Yoksa o ne diyor, bu ne diyor gibi değil. Amerikalı ne diyor ve ne yapıyor? Matematik, fizik, kimya diyor. Bu teknolojileri fizik, kimya, biyoloji gibi bilimleri bilmeden yapamazsınız, makineleri yapamazsınız, pilotları uçuramazsınız. Heidi Shyu, ABD Savunma Bakanlığı'nın araştırma ve mühendislikten sorumlu başkan yardımcısı hanımefendi, 5 Nisan 2023'te şunu söylemiş:

«Rekabetçi üstünlüğün sürdürülmesi, hayati derecede önemli olan yetenekli öğrencileri ve bireyleri eğitmektir. Bu da bilim, matematik, teknoloji, mühendislik programları ile mümkündür.» Buluşçuluk, inovasyon dedikleri çok önemli konu. ABD Eski Genelkurmay Başkanı Joseph Francis Dunford da 'Bilgiyi kontrol eden ordu, dünyanın en güçlü ordusu' demiş.

Yapay zekâ ne? Her şeyden önce bir muktedir kılıcı. Bir Millî güç unsurudur, kuvvet çarpanıdır ama harekât nevi ve tarzına bağlıdır. Muharebede oyun değişir. Oyun kurucu, oyun değiştirici ve oyun bozucudur. Savunma, güvenlik, istihbarat için yeni yetenek geliştirici, imkân kabiliyet geliştiricidir. Tıpkı yeni harekât ve muharebe konseptleri gibi. Stratejik, operasyonel ve taktik seviyelerdeki yetenektir. Savunma, güvenlik ve istihbarat kurumlarının yeteneklerine ve gücüne farklı boyutlar kazandırmaktadır. Yani, yeni bir alan ve yeni bir devrimle yüz yüze yüzeyiz. Dönüşüm ne demek? Modernizasyon, otomasyon demektir, dönüşüm demektir. Bir iş dünyasından farklı iş modelleri, gelir modelleri ve operasyonel yani idame ettirebilmek için şirketlerin gelişimi demektir. Askeriyede nedir? Yeni harekât ve muharebe konseptleri, her harekât nevi ve tarzına çok farklı konsept geliştirmek zorundasınız demektir. Aynı zamanda kapasitedir ve yeni operasyon, harekât, hareketten gelir, nevi tarzlarının muktedir kılıcıdır.

Rusya Federasyonu Başkanı Vladimir Putin, 'Yapay zekâ alanında lider olan dünyayı yönetecektir' demiş.

ABD Kara Kuvvetleri yetkililerinden Albay Jon Ercisson, ‘Yapay zekâyı ordusu ile başarılı kullanan ülke, kesin bir avantaj elde etmekle beraber, gelecek nesiller için muharebenin karakterini de değiştirecektir’ demiş. Kimisine göre de muharebenin tabiatının da değiştiğini, yani her muharebe çeşidi ve harekât nevi tarzına baktığınızda, muharebenin tabiatı, icrası, taktik ve teknik prosedürleri değişmiştir. Karakteri değişmiştir. Bazı harekât nevi ve tarzlarında ne tabiatı ne de karakteri değişmiştir. Bu çok önemli bir konsepttir ki, rakiplerimizin, modern orduların nasıl hareket ettiğini anlayabilmek için. Bir de işte muharebenin tabiatı ve karakteri, bunu iyi anlayabilmek, muharebenin tabiatı ve karakterini çok iyi anladığımız zaman, modernizasyon dönüşüm ve bir de evrimleşmeyi anladığımız zaman o zaman çok rahat, esnek, kıvrak, çabuk ve mukabil olan kurumlar oluştururuz.

ABD Genelkurmay Başkanı Mark. A Milley, ise şunları söylüyor Eylül 2023’te; “Sürekli geliştirilmekte ve yeni yeteneklerle donatılan otonom sistemler, istihbaratın ve muharebenin tüm sahalarında, komuta kontrol kademesinde ve icrasında, günümüzdeki örneklerinden çok daha etkili olacaktır. Gelecek 10-15 sene içinde modern orduların kuvvet yapısının üçte 1’ini robotlar oluşturacak. Savunma, güvenlik, istihbarat alanlarında en büyük değişiklikleri kuantum bilgisayarlar sağlayacaktır.” Bakın insansız ayrı, otonom ayrı. Onlara göre böyle. Bak gitti, yapay zekâ bitti.

Yapay zekâ teknolojilerinin modern savunma, güvenlik ve istihbarata etkileri, istihbaratın güvenliğinin ve muharebenin tabiatı karakteri ve icrasının değiştiği değerlendirilmektedir, bazıları karakteri diyor.

Modern, savunma güvenlik ve istihbarat kurumları devrimsel nitelikte yeni bir dönüşüm, transformasyon, yani yeni harekât ve muharebe konseptleri, kurumsal yapı, doktrin, talim, terbiye, liderlik, eğitim, personel, tesisler gibi yedi kritik faktörleri yeniden belirlemektedir. Bu da dönüşümün ana kuvveti, muktedir kılıcıdır. Dönüşüm stratejinin anahtar muktedir kılıcıdır. Batılı modern ordular, tabii Çin Halk Cumhuriyeti ve Hindistan da dahil olmak üzere, Rusya Federasyonu dahil olmak üzere mesela otonom helikopterler, otonom tanklar oluşturmuşlardır.

Yapay zekâ istihbarat ve muharebede, yeni davranış biçimlerini ve yeni modellerin üretilmesini mümkün kılarken, uzun yıllardır kullanılmış, oluşmuş geleneksel mekanizmaları da değiştirmektedir. Yapay zekâ tabanlı, akıllı komuta kontrol sistemleri hızlı karar vermeye yardımcı olmakla beraber, akıllı kıymetlendirme, analiz, istihbarat çarkında kullanılan kapasitesini de genişletip daha ileri seviyelere taşımaktadır. Yapay zekâ veri paylaşım mimarisini ve otonom sistemlerin işlemlerini ve kullanımını kolaylaştırarak daha ileri seviyelere doğru geliştirmektedir.

Yapay zekâ şebeke bilgi sistemleri, insansız ekipmanlar ve hassas vuruş mühimmatlarının, birleşik ve yamasız kullanımını sağlayarak istihbarat muharebe bulutu, bakın teknolojik kavramlar kurumların olaya bakışını değiştiriyor, sürü taktikleri, sürü zekâsı konseptlerinin yanında, yeni akıllı istihbarat ve muharebe teorilerinin ve doktrinlerinin ortaya çıkmasını sağlamıştır. Stratejik seviyede, operasyonel seviyede, taktik ve angajman seviyelerinin de doktrinleri farklıdır.

Postgraduate School'dan Dr. John Arquilla tüm modern savunma, güvenlik, istihbarat kurumlarının yeni dönüşüm stratejilerindeki ana hedefini 'Büyük Veri'deki temizlenmiş ve yapılandırılmış bilgileri kullanarak, yapay zekâ teknolojilerinin bulunduğu en uygun harekât tarzı için hızlı karar verme üstünlüğü' olarak özetliyor. Bunun altını iddiayla çiziyorum ki, bilgiyi yapılandırmadınız mı olmaz, temizlemek ve yapısalılık çok önemli. O zaman size söylüyor; 'şu hareket tarzı daha iyi' diye. Havacılar John Boyd'un 'Gözlemle, Yönlendir, Karar Ver ve Harekete Geç – OODA döngüsü'nü iyi bilir. Bu çemberi hızlı döndüren kazanır, en hızlı karar veren, en büyük rekabetçi üstünlüğe sahip oldu. Yapay zekâda bu noktada önemli.

Yapay zekâ çağı çatışmalarına hazırlıklı olmanın ilk şartı; bilgi konseptinin yeniden düşünülmesi, ilk önce bilgiye bilgiyi işleme değil, bilginin yapılandırılması olarak yaklaşım tarzı olacaktır. Bunu yapamazsanız kaybedersiniz. Bilginin tüm hareket nevi ve tarzlarında kullanılması yani faaliyete dönüştürülen bilgi, kullanılabilir bilgi olması önemli. Üstün bilgi, öz bilgi kuvvet çarpanıdır. Faaliyete dönüştürülen bilgi olarak yapılandırılması bir kuvvet çarpanıdır. İstihbarat, siber, elektromanyetik, spektrum, uzay, dron ve diğer muharebelerin olmazsa olmaz şartıdır.

Bakın Çin Halk Ordusu, harekât sahaları, fiziki alandan bilgi alanına, bilgi alanından bilişsel alana doğru genişleyecektir. İnsan beyni yeni bir muharebe sahası olacaktır. 1985'te Amerika'da uzaktan zihin kontrolü anlatılıyordu. Zbigniew Brzezinski Hoca şunu söylüyordu; 'Bir insana uydudan 6 dW verirsiniz depresif, 8 dW verdiğiniz zaman mutlu oluyorsunuz.' Hatta 2000'li yılların başında Silahlı Kuvvetler Akademisi'nde Amerika'nın komando denilen bir elektronik harp uçağı vardı ve bu uçak Kanada'da gidiyor, bu bir senaryo değil uygulanmış. Farz edin TRT'yi izliyoruz, o frekansa giriyor ve size bir dizi izletiyor. Ama sizi var ya amiyane maymun ediyor, depresif oluyorsunuz, sokağa çıkamıyorsunuz. Kurşun atmadan hedefi gerçekleştirmek kavramı, yıllar önce, 2000'li yıllarda bu şekilde tartışıldı. Devamında, gelecekteki başarı kriterlerinden biri biyolojik hakimiyetten geçecek. Bana göre 'Korona' kesinlikle bir biyolojik silahtır. Gidin doktorlarla profesörlerle konuşun. Çinliler uyandı, ne diyorlar, biyolojik hakimiyet.

Onun yanında bilişsel alanda hakimiyet, hem de insan-makine etkileşimi ile elde edilen istihbarat üstünlüğünü talep etmektedir. İstihbaratın alanları da genişledi, eski istihbarat paradigması bitti. İstihbaratla ilgilenenler yeni doktrinleri geliştirmek zorunda olduğunu bilecek. Ne yazık ki, bu imkân kabiliyet yok. Doktrin nasıl düşünüleceğini size anlatan bir algoritmadır. Ne yapmanız gerektiğini değil, nasıl düşünülecek onu anlatır. Bakın NATO, 2000'li yıllarda, kaç sene önce, ağ merkezli muharebeye, etki odaklı hareketin bir güç kaynağı olarak bakıyordu. Fiziksel alan, muharebenin olduğu alan. Enformasyon ki, burada bilgi savaşları, bunun yanında elektronik harbin değişik boyutları, psikolojik harp gibi bunların hepsi psikolojik bilgi harbinin içerisinde. Bilişsel alan ve ondan sonra da sosyal alan.

Bakın hepsini geçelim, burada human process dedikleri, insanın bilişsel alanda nasıl düşündüğünü, nasıl karar vereceğinizi etkileme olarak da literatürde yer alıyor. İnsanın bilişsel alanda nasıl düşündüğünü etkilemek. Nedir yeni bilişsel alana yaklaşım. O zaman durumsal farkındalığınızı oluşturmıyorsunuz.

Elektromanyetik spektrum bir muharebe sahasıdır. Niye, bakın denizaltı unsurlar, deniz sathında ve karada, havada, yani mavi vatan, gök vatan, uzay vatan, siber vatan ve kara vatan. Bunların hepsini siber vatandır.

Bakın, 2020’de, American Join Vizyon (Müşterek Vizyon) çalışmasında ‘iletişim’ altın anahtar gibi görülüyor. Yamasız bir entegrasyon, ağ merkezli muharebe çalışması yapılıyor. Buna hep böyle bakıyorlardı ve uyguluyorlardı.

Ve en kritik yerlerden biri, ‘Cognitive War’ diyor, ne diyor, «Elektromanyetik Spektrum Operasyonları (EMSO), operasyonların kalbidir» diyor. Komuta, kontrol, iletişim, bilgisayar yani C4 savaşın kalbidir. Bakın bilişsel dünya, burada komutanların, pilotların, hepsinin bir sistemi var. Uzay platformu olabilir, başka bir platform da olabilir. Oradan beynimizi, zihnimizi dumura uğrattıyorlar. Bunlar IBM ve diğer kurumlarla beraber araştırılıyor, kuvvetler ve ülkeler tarafından yapılıyor. Orduların ilk prensibi, elektromanyetik spektrumu ele geçirmektir. Çünkü muhaberesiz muharebe olmaz.

Ontolojik muharebe, bunu çok araştırdılar. Epistemolojik muharebe, algoritmik muharebe, bilişsel muharebe, beyin kabuğu (neocortical) muharebe, bağlamlandırılmış bilgi, sosyolojik muharebe, sosyal medya harbi, artık sosyal medya tugayları tümen seviyesine geldi. Kamuoyu fikrini oluşturma muharebesi ve bu da Çinlilerin, Göbel’in dediğine göre; «Bir sistemin içindeki sorun, kendi içinden çözülmez, muhakkak dışarıdan müdahale gerekir.»

Bazen bana ‘Ne diyor bu?’ gibisinden bakıyorlar, diyorum ki ‘Ne yazık ki bizim gibileri de dinlemelisiniz, çünkü biz başka açıdan bakıyoruz. Düşüncenin kutudan çıkması dedikleri çok farklı yaklaşımlarla.’ Bunları yapmak zorundasınız yoksa çok hızlı akıp gidiyor her şey. Bakın Algoritmik Muharebe, ne diyor bununla ilgili? Artırılmış gerçeklik, ölçülebilir muharebe. sürü zekâsı ve ontolojik düşünme. Bunları öğrenmeli ve uygulamalıyız, bunlar yıllardır dünyada yapılan işler. Bunları bilmediğimiz zaman dost, kardeş, müttefik anlayamayız. NATO bu işlerle çok ilgileniyor. Yenilikçi istihbarat kurumları, istihbaratın amacı, istihbarat çarkını çok hızlı tarzda döndürerek karmaşıklığı, kompleksiteyi azaltarak ve ilgili konuda en kapsamlı bilgiyi çoğaltarak çok hızlı karar vermeyi güçlendirmektir. Karar vericilere verir, istihbaratın amacı budur. Asker, sivil ve birbirine çok yakınlaşmaya başladı. Hatta şöyle derlerdi; ‘Biri mehter takımı müziği, öteki ise filarmoni orkestrası, her ikisi beraber çalışıyorlar.»

Muhasıma karşı karar verme üstünlüğü elde etmek hedef. Karar verme üstünlüğünü yakaladığınız zaman olay bitiyor. Yapay zekâ istihbarat çarkının tüm safhalarını, istihbarat faaliyetlerinin tümünü, kestirimci analiz, siber güvenlik ve diğer konuları da devrimselleştirmektedir. İstihbarat analiz süreçlerinde ve operasyonların hazırlanması ve icrasında, karar vermeyi güçlendiren muazzam fırsatlar sunmaktadır. Yapay zekâ, küresel, bölgesel ve ülkesel istihbarat operasyonlarının alanlarını da dönüştürmektedir. Muharebe dışında da diyorum, çünkü muharebede sis ve sürtünme artmakta. Sürtünme artmadan sis oluşmaz, burada dron muharebesi çok önemli. Küresel ve bölgesel yayılmış büyük ve karmaşık yapıdaki istihbarat kurumlarının iş süreçlerini, cari işlemlerini ve diğer hizmet fonksiyonlarını, daha etkili ve maliyet etkin tarzda yönetilmelerini sağlamaktadır.

Yapay zekânın istihbarat görevlerine entegre edilmesi sonucu, sensör, keşif, gözetleme, dinleme ve takip teknolojilerinin ürettiği ve sinyal istihbaratı, geometrik uzam istihbaratı, sosyal istihbarat, geleneksel medya istihbaratı ve diğerleri, insan istihbaratından gelen çok büyük miktardaki verilerin eritilmesi çok önemli. Füzyon merkezleri oluşturmadık mı, işimiz bitti. 2017 yılında İçişleri Bakanlığı için bunu konuşmuştuk, karar destek merkezleri için, bu çok önemli. İstihbarat vizyonu yönetimi ve bu verilerden ilgilenilen konu hakkında tespitler yapılmasını, çözümler elde edilmesini ve çok hızlı karar verilmesini mümkün kılmaktadır yapay zekâ. Yapay zekâ sistemleri ile istihbarat paylaşımını gerçek zamanlı çok hızlı bir tarzda yapmaktadır. Bu İran'da da var, Suudi Arabistan'da da var.

Örneğin, bilinen modern istihbarat kurumları, analistlerine gelen çok büyük miktardaki bilgileri çok hızlı bir şekilde işlemesi için yapay zekâyı içerik sıralaması, öncelikli işlenmesi, içeriğin özelliklerinin tasnifi, tercüme ve kaydetme işlemlerinde de kullanmaktadır. CIA'nin Açık Kaynak Kuruluşu'nun (Open Source Enterprise) geliştirdiği ve diğer ABD. istihbarat kurumları ile paylaştığı OSIRIS platformu, yukarıda bahsedilen işleri icra etmektedir. CIA'nın OSIRIS platformu, önceki yıllarda insan tecrübesine ve iş gücüne dayanan açık kaynak istihbaratı işlevlerinde yapay zekâyı kullanmaktadır. İnsanın 10 saatte yaptığı işi 1 dakika yapıyorlar.

OSIRIS makine öğrenmesi, derin öğrenme, büyük dil modelleri, çok modlu dil modelleri, doğal dil işleme modelleri, semantik yapay zekâ, yapay zekâ ajanları ve diğerleri vasıtasıyla çok büyük hacimli açık kaynak istihbaratı verilerini sentezleyerek, istihbarat çarkını çok hızlı bir şekilde o fazları geçerek kullanılmaya sunmaktadır. Yapay zekâ tabanlı sistemlerin ürettiği chat botlar vasıtasıyla, kullanıcı katılımlarını analiz ederek değerlendirerek sonuç özetlerini sunar. Hindistan'da örneğin, Facebook, X ve benzerleri Hindistan Sağlık Bakanlığı'ndan önce ülkede salgın olduğunu buluyor.

Muharebenin çok yakın geleceğinde, yapay zekâ robotlar, akıllı dronlarla askeri hareketleri ve muharebe sahalarını biçimlendirmeye devam edecek. Sürü zekâsı, dronlar küçülmekte ve meskûn mahallerde kullanımı genişlemekte. Yeni nesil hava hakimiyeti konsepti ve otonom işbirlikçi muharebe uçağı, bu önemli. F35 konseptinde farklı görevler için uçak gibi dronlar yardımcı olarak kullanılmakta. Kimisi bombalama görevini üstleniyor, kimisi sinyal kesme için kullanılıyor. Bu teknolojilerin kullanımı, yönetimi ve amaca uygun kullanımı için hibrit-melez komuta ve kontrol merkezi, otonom komuta ve kontrol merkezi çok önemli. Sürü zekâsı, yapay zekânın ve bilgisayara dayalı bilgi hesaplama metodunun dalıdır.

Sürü zekâsı, yapay zekânın ve Bilgisayara Dayalı Bilgi Hesaplama (computation) metodunun dalıdır. Sürü zekâsı, yapay zekânın yanında bilgisayara dayalı bilgi hesaplama metodu aracılığı ile, problemleri çözmek maksadıyla, otonom platformların, natüralistik, yani doğadaki canlıların hareketlerini taklit eden algoritmaları kullanmasını sağlar. Bu teknoloji, merkeziyetsiz kolektif davranışlar sergileyen ve kendiliğinden organize olan otonom sistemleri kendi bünyesinde kullanır. Sürü zekâsı, hareket etme, uçma, arama, doğurma, nüfusun artması, barınma ve çekirge, böcek, arı, kuş, balık ve diğerlerinin sürü halinde hareket etmeleri gibi hayvanlar aleminde, kendiliğinden organize olan grupların ortaya koyduğu davranışlarından ve kolektif zekâlarından ilham alan ve okuyan, biyoloji biliminin prensiplerini kullanan bilgisayarlara dayalı bilgi işlemedir. Dron sürüsünün üyeleri adapte olma, birbirleriyle etkileşme yetenekleri sonucu gayrette birlik sağlayarak grup seviyesinde akıllı ve bilinçli davranışlar sergilemektedirler.

Sürü üyesi tüm dronlar otonom ve merkezsizdir, yani merkezi bir kontrol veya üyelerin nasıl davranacaklarını emreden Komuta ve kontrol ve direkt bir koordinasyon mekanizması yoktur. Sürü sisteminin davranışları, sürü üyelerinin birbirleri arasındaki etkileşim sonucu ortaya çıkar. Bu durum, sürü hatta sürü üyelerinin bazıları sürüden ayrılrsa veya imha olsa bile, sürü zekâ sistemlerini çok yüksek derecede sağlam ve dayanaklı kılmaktadır. Sürü zekânın arkasındaki ana konsept, sürünün birlikte davranışı sonucu ortaya çıkardığı kolektif zekâ sürüdeki herhangi bir bireyin zekâsından çok daha büyüktür. Bunun sebebi de sürünün birlikte daha çok seçeneği değerlendirmesi ve bir sürü üyesinin tek başına bulduğu çözümlerden çok daha fazlasını sürünün kolektif olarak üretmesidir. Sürü zekâsında hem avantajları hem de dezavantajları olan çok farklı algoritmalar vardır. Algoritma seçimlerinde ise çözülmeye çalışılan mevcut problemler belirleyicidir. Bu algoritmalarda merkeziyetsizlik, kendi kendine organize olma, otonomluk ve uyum sağlamak ise dört ana ortak noktadır.

Günümüzde modern savunma, güvenlik ve istihbarat kurumlarının ana hedefi genel yapay zekâda bilinci olan sistem, semantik yapay zekâ ve yakın gelecekteki otonomi alanında uzmanlaşmış yapay zekâ ajanları alanında hızla uzmanlaşmak ve etkin gücü artırmaktır. Sürü zekâsının yeteneklerindeki hedeflere ulaşmak için de buluşçuluk ekosistemini güçlendirmek, devlet kurumları, endüstri, iş dünyası, şirketler, bilim insanları, uzmanlar, üniversiteler, müttefik dost ve kardeş ülkeler ile işbirliği oluşturmuşlardır.

Yapay zekânın muktedir kılıcısı ontoloji bilimidir. Ontoloji nedir; yapılandırılmış bilgi modelleridir. On nesne demektir, ton -eliği, nesnenin ne olduğuna dairliğidir. Bunu kuramazsanız, hiçbir şey yapamazsınız. Bilgileri yapılandırır, bir alandaki bilgilerin yapılandırarak temsil edilmesini mümkün kılar. Bilgileri tanımlamayı, kategorize etmeyi ve temsil etmeyi mümkün kılan 'Yapılandırılmış Standart Yöntemler' sağladığı için yapay zekâ teknolojilerinin ayarlanmasında, kullanılması düşünülen sistemlere ayarlanmasında en önemli belirleyicidir. Yapay zekâ sistemlerinin kullanıcı niyetleri ve değerleri ile tutarlı olarak, yapay zekânın anlaması ve icra evrelerinde hayati derecede önemli olan konseptlerin arasındaki ilişkiyi netleştiren standartlaşmış sözcükleri oluşturur.

Ontolojileri kullanarak, veriler hakkındaki ‘anlamı anlamaya’ ve verileri ‘muhakeme etmeye odaklanmış semantik yapay zekâ’ zeminini oluşturur. Robotlardan, yazılımdan ve basit otomasyondan daha fazlası olan yapay zekâ ajanları, öğrenen, muhakeme yapan, durumdan vazife çıkararak harekât icra eden ve karar veren otonom icracılardır, bilinçleri vardır. Yakılım yıkıcıları olan yapay zekâ ajanları çok yakın geleceğin otonom uzmanlarıdır.

Günümüzde bu teknolojinin en büyük sorunu, büyük veriyi yapısallaştırmaktır. Dünyanın en iyi kuantum bilgisayarınız olsa da ilk işiniz bilgiyi işlemek değil, yapısallaştırmaktır. Veri ve bilgi yapısallaştırılamadığı sürece, en gelişmiş yapay zekâ, kuantum bilgisayarlar gibi teknolojiler de kullanılsa, konseptler, doktrin yazılımı, harekât planlaması, durumsal farkındalık, durumsal anlama, ortak harekât resmi ve kapsayıcı istihbarat resmi ile ilgili sahaların gerçekliği net bir şekilde temsil edilemez. Bilgisini elde etmek istediğimiz saha, ‘Nasıl bir gerçekliktir ve olgudur?’ sorusuyla başlar. Ontoloji bu soruya cevap veren hem bir metot hem de bu metodun ürünüdür. Bilgisini elde etmek istediğimiz alanda, elde edilen bilgileri yapısallaştırarak, temsil etmek istediğimiz sahayı oluşturan tüm boyutlarında, katmanlarında ve sahalarındaki, aktörlerin, nesnelerin, unsurların, olayların, karakteristik özelliklerin, süreçlerin ve ilişkilerin ne olduklarını, yapılarını ve tiplerini ya da sınıflarını temsil etme, tanımlama, ilişkilendirme ve bütünleşik bir tarzda tüm boyutları, alanları ve aktörleri entegre etme disiplini. Askeriyede pilotların durumsal farkındalık, karacıların kum sandığı dedikleri ‘ontoloji’, yani anında ilişkileri kurmak.

Nasıl kullanılıyor? Ağ merkezli muharebede Amerikan ordusu en az 20 yıldır kullanıyor. İstihbarat ontolojisi, istihbarat bilgi ontolojisi, tehdit değerlendirme ontolojisi, durumsal değerlendirme ontolojisi, terörist takip ve gözetleme ontolojisi, meskûn mahal ontolojisi, uzay ontolojisi. Bütün varlıkların ne yaptığını kuramazsanız uyduları ve kimin ne yaptığını takip edemezsiniz. Uzay sahasında kullanılan tüm ontolojiler, sürü saldırısı ontolojiler, askeri planlama ontolojisi, kuş sürüsü halinde saldırı ontolojisi gibi bir sürü durumda kullanılıyor.

Peki ontoloji ne getiriyor? Yeni bir müştereklik yaklaşımı ve bakışı getiriyor, ortak akıl, ortak dil getiriyor. Yani stratejik, operatif ve taktik seviyelerdeki doktrin yazıcıları, planlamacıları, komuta kademesi için ortak sözlük vazifesi görüyor.

Bu da ortak harekât resmi ve kapsayıcı istihbarat resminin stratejik, operatif ve taktik seviyelerde oluşturulmasının temeli ve bunu sağlıyor. Ortak anlam birliği sunuyor, yine stratejik operatif ve taktik seviyede ortak ve kontrol edilen terimlerle hareket edilmesini sunuyor. Ortak durumsal farkındalık ve durumsal anlama, ortak operasyon resmi ve semantik birlikte çalışabilirlik sağlıyor.

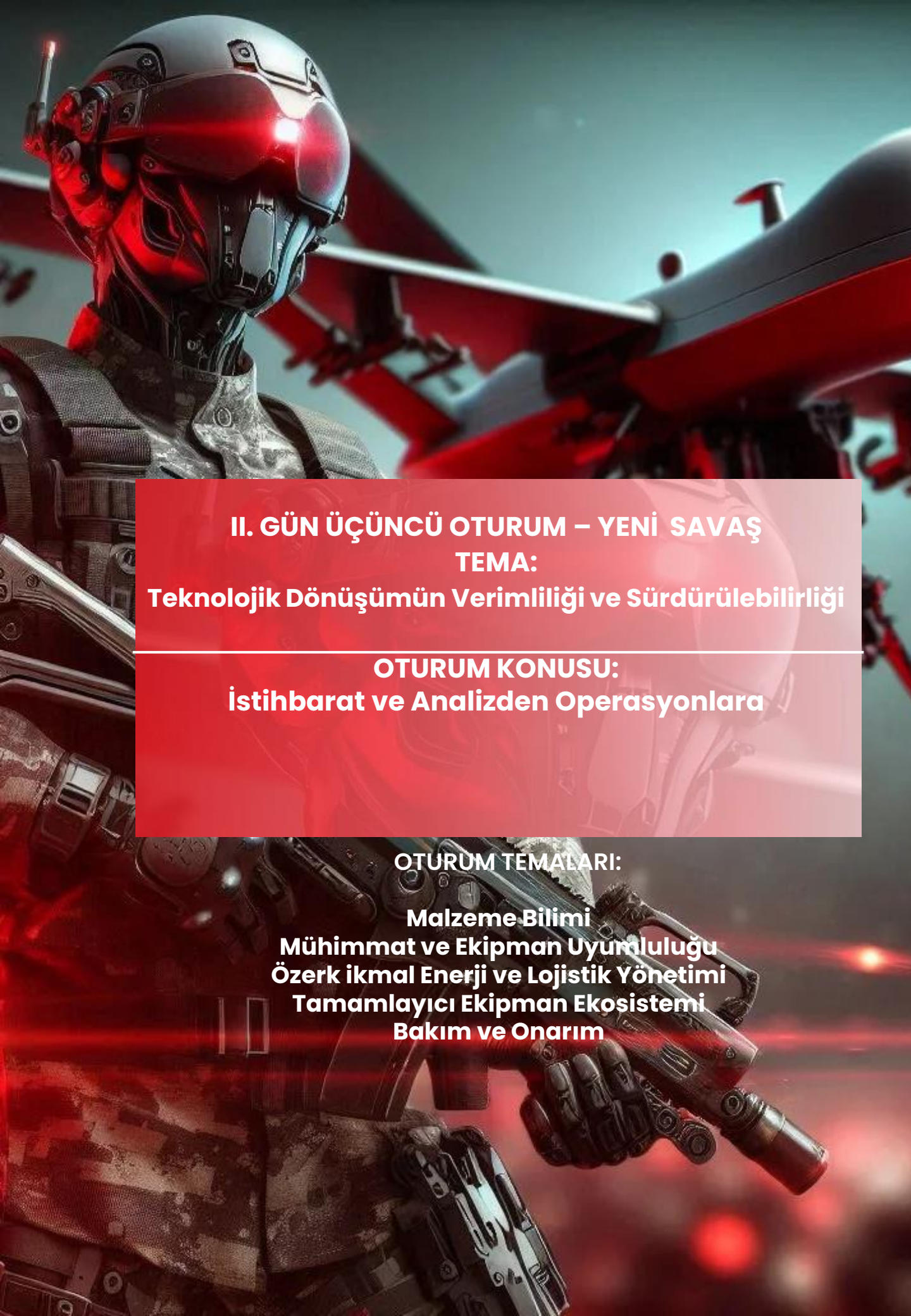
Komşularımız ne yapıyor? Selanik'teki Aristo Üniversitesi yapay zekâ üniversitesi kurmuş ontolojisini. Midilli'deki Ege Üniversitesi'ndeki bir bilim insanı, sürü şeklindeki saldırı için ontoloji kurmuş. Ne yapmış yapay zekânın bilgi grafiğini kullanmış. Tüm bu bilgi akışı yani ontoloji kurulduktan sonra SARISA SRS-1A, RL275-1S roket atar isimli bir dron ürünü geliştirdi. Dünyada ilk quadro kopter üzerine 70 milimetrelik, Thales'in, yani helikopterden atılan roketini kullanan dron modelini yerleştirdi. Şimdiye kadar geliştirilmemiş ve güdümsüz roket kullanıyor. Bir veya iki Hydra 70, 2.75 inch 700 mm çaplı roketi atış sistemiyle sunuyor. Bir metreden az bir mesafede veya kilometrelerce uzaklıktan hedefini çok hassas şekilde vurma yeteneğine sahip. Uydu da dahil herhangi bir iletişim sistemi ile uzaktan sevk ve idare ediliyor.

Bitti mi, uzun menzilli kamikaze dron AIHMI AHM-1X'i geliştirmiş yine. Otonom mühimmat, büyük dron, İHA veya helikopterden bırakılıyor ve 15 kilometre süzülebiliyor. Uzaktan kumanda merkezinden motoru çalıştırıldıktan sonra 140 kilometre süratle 50 kilometre daha uçuyor, yani menzili artıyor. Bu da Thales'in 70mm ve Hydra 700 mm roketleri kullanabiliyor.

İran'da Amerika'nın insansız hava aracının GPS koordinatlarını yeniden yapılandırarak düşüren bir teknolojiye sahip olduğunu duyurdu. İran ordusu, düşürülen drondaki tüm verilerin alındığını, tersine mühendislik tekniği ile dronun kopyalandığını, drona karşı anti teknoloji geliştirdiğini ve yeni bir model insansız hava aracı üretildiğini duyurdu.

Evet yapay zekâ teknolojilerinin sebep olduğu dönüşüm için en büyük zorluk teknolojik alan değil, entelektüel ve düşünsel engellerdir. İnsan, sonra fikirler yani bilgi, içerik, konsept, doktrinler ve sonra da teknoloji. Ama önce insan, temeli insan. İnovatif düşünen, yenilikçi, mucit ve keşif eri insan.

Sürü zekâsını çok iyi incelemek lazım. Çinli general diyor ki, 'Her bir teknolojiye bağımlılık sonucunda, o konseptlerde, doktrinlerde, taktiklerde, muharebe teorisinde bazı karanlık alanlar oluşturur. Bu karanlık alanları bulup istismar etmek gerekli. Yapay zekânın boyutlarını, algoritmaları, makine öğrenmesi ve diğer yapay zekâ teknolojilerini anlayıp asimetric muharebe paketleri geliştirilmeli. Bunu anlayamazsak işler zorlaşıyor ve bize muazzam zararları oluyor, olabilir. Bize entelektüel bir şekilde çalışmak, teknolojinin zafiyetlerini anlamak ve bunlara karşı asimetric mukabele paketlerini geliştirmeliyiz.



II. GÜN ÜÇÜNCÜ OTURUM – YENİ SAVAŞ TEMA:

Teknolojik Dönüşümün Verimliliği ve Sürdürülebilirliği

OTURUM KONUSU:
İstihbarat ve Analizden Operasyonlara

OTURUM TEMALARI:

Malzeme Bilimi
Mühimmat ve Ekipman Uyumluluğu
Özerk İkmal Enerji ve Lojistik Yönetimi
Tamamlayıcı Ekipman Ekosistemi
Bakım ve Onarım

VIII. OTURUM ÖZETİ

Future Soldier kavramının bireyden robotik askerlere dönüşümü, müşterek teknolojik sistemlerinin kullanımıyla askeri doktrinlerin ciddi değişiklikler göstereceği, teknoloji yoğun muharebe sahasına yönelik 5-10-20 yıllık planlamaların yapılması gerekliliği dile getirildi. İnsan makine uyumu sürecinde insanın mı makineye, makinenin mi insana uyum sağlayacağı, sürat ve dayanıklılık noktasındaki uyumun da geliştirilen teknolojilerde ve karşı teknolojilerde dikkate alınması gerekliliğine vurgu yapılırken askeri yeteneklerin ve teknolojilerin gelişimindeki her aşamanın dikkatle takip edilmesinin önemi vurgulandı.

Günümüzde geliştirilen her teknolojinin mühimmatlarla sonuca gittiği, teknolojinin geçirdiği dönüşüm sürecinde eski ve yeni ekipman uyumu ile karma çalışma prensiplerinin önemi ifade edilirken, birlikte çalışabilirlik ve modülerliğin kabiliyetler açısından getirdiği avantaja dikkat çekildi. Akıllı mühimmat teknolojilerinin öneminin giderek arttığı, bu alandaki gelişmeler açısından da sensörlerin üretiminin zaruri ihtiyaç olduğu kaydedilirken, istihbarat ve operasyonel verinin elde edilmesi, kullanımı ve paylaşılması için her türlü teknik ve teknolojik donanım alt yapısına yatırım yapılması gerektiği belirtildi.

Geleceğin askeri teknolojilerinde kullanılan malzeme bilimi kapsamında kurşun geçirmez, dayanıklı, yaralanmaları en asgari seviyeye indirgeyen malzemelerle ilgili çalışmaların önemine dikkat çekilirken, bireysel ve sistemlerin balistik korunmasında ürün çeşitliliğine duyulan ihtiyaç vurgulandı. Giyilebilir iletişim teknolojileri ve antenlerin kullanımı ve tespitini engelleyen karşı sistem üretiminin yakın ve uzun vadede büyük önem arz ettiği, yüksek manyetik alan oluşturan silah ve lazer teknolojilerinin geliştirilmesine yönelik çalışmaların gerekliliği ve yine bu tarz teknolojilere karşı önlemler için de projelere ihtiyaç duyulduğu ifade edilmiştir.

Füze teknolojilerinde orta ve uzun menzil projeler için çalışmaların sürdürüldüğü, bu kategorilerde yerli üretimin gerek muharebe ortamında gerekse diğer ülkelerin satmak istememesi dolayısıyla ihracat potansiyeli yönünden büyük önem taşıdığı vurgulanmıştır.



**Emekli Hava Tümgeneral
Reha UFUK ER
MODERATÖR**

Değerli konuklar, misafirler hoş geldiniz. Konular önemli, Türkiye'nin geleceği açısından konuşulması, bugünden tartışılması gereken hususları içeriyor. Üç değerli konuğum ve ortak noktaları ODTÜ. Konumuza geçmeden önce, ben görev icabı hem Hava Kuvvetleri Plan Prensipler Başkanlığı, hem de hem de Genelkurmay da Genel Plan Prensipler Başkanlığı yaptım emekli olmadan önce. Taktik ve operatif seviyede bu çalışmalar

sürüyor. Ancak bizim genel olarak ülkemizde çok az yapılan bir şey var. O noktadan hareketle konuklarımın takdimlerinden önce çok kısa bazı konuları hatırlatmak istiyorum.

Asker var ortada, biz Future Soldier diyoruz. Acaba Future Soldier bir asker mi yoksa sinir sisteminde bir nokta mı? Acaba bir askerden mi bahsetmeliyiz, ben bir tanımlama yapmıyorum, tespit yapmıyorum, soru işareti bırakmak istiyorum. Ulaşmak istediğimiz husus bu askere özellikler kazandırmak mı, Future Soldier'ı bir bütün bir kavram olarak mı ele almalıyız? Yoksa bu canlı mı, robot mu? Bunu düşünmek zorundayız, canlı robot bir arada mı yoksa ayrı ayrı mı?

Diğer taraftan canlılar geride operatör mü, ön safta robotlar mı olacak? Bugün bunları konuşurken, 5-10-20 yıl sonrasının teknoloji ve konseptlerini ve bunlardan oluşacak doktrinleri de düşünmek zorunda mıyız? Bunları biraz irdeleyelim ve sorgulamalarımızı sürdürelim. Bugünden yapılan savunma sanayi eko sisteminde bir sürü başarılı faaliyet var. Öngörü yapabildiğimiz çok alan var, acaba geriye dönük çıkarım yaptığımız çok sayıda alan var. Acaba 20 yıl sonrasının teknoloji yoğun muharebe sahasını düşünüp, oradan geriye dönük çıkarım yapıp kabiliyetleri düşünebiliyor muyuz? Bunlara da ayrı ayrı yoğunlaşmak lazım, bir safha da bence geleceğe yönelik belirsizliklerin giderilmesinde karmaşık sorunlar içerisinde mevcut eğilimlerin de problemlerin bir parçası olduğu durumlara dair çıkarımlar da yapmalıyız.

Geleceğin teknolojilerinin geleceğe adımlarında bu önemli bir nokta. Bir dışişleri bakanı bir açıklama yapmıştı, bunun değerlendirmesini, bunu sizin takdirlerinize bırakıyorum; NATO'nun en ucuz askeri Türk askeridir, 23 cent'e mal oluyor. Sizin takdirinize bırakıyorum. Acaba ön saflarda canlılar mı robotlar mı olmalı? Biz bunu hak ediyor muyuz? Bunları bir düşünelim. 1793, 1944, 2023, bakın seneler değişiyor ama düzen değişmiyor. Bir sonraki düzen acaba değişecek mi? Askerlerin içinde robotlar olacak mı bu askeri törendeki birliklerin içinde? Sürat dayanıklılık düşündüğümüzde ikisi birlikte çalışabilecek mi? Future Fighting Tech, geleceğin harp teknolojileri ne olacak. Muharebe yoğun teknoloji sahasını bütün literatüre katmamız lazım. Yabancı bir organizasyondan alınan bir örnek, hangi ülkeler teknoloji yoğun harp çalışan ülkelerden örnek. Ne kadar bütçe ayırıyorlar bilmiyoruz ama ayrılan bütçeleri var. Bu konunun çalışılması ve ileri götürülmesi için organizasyon kuran ülkeler, organizasyon kurmuşlar, araştırma, geliştirme yapıyorlar, en önemlisi fon ve bütçe tahsis ediyorlar. Bayraklarda Avrupa'dan Güney Amerika'ya, Uzakdoğu'dan Balkanlara ülkelerin olması, farklı bütçeli nüfuslu ülkelerin olması da sizler de değişik duygu düşünce uyandırabilir.

Katmanlar, Future Soldier dediğimiz zaman acaba havacı mı, karacı mı, denizci mi yoksa hepsi bir bütünün içinde mi? Bu katman içindeki herkes nasıl uyum ve ahenk içinde hareket etmeli, bu bütünlüğü nasıl sağlamalıyız? Bu konseptleri tanımlamaları nasıl yapmalıyız ve bu organizasyonu nasıl kurmalıyız? Bu anlamda da SASAD'a çok teşekkür ediyorum, böyle bir gündemi burada gündeme getirdikleri için. Ahenk içinde nasıl bir arada tutmalıyız ve organizasyonu kurmalıyız? Bu amaçla biz Savunma Sanayii Başkanlığı akademi içinde bir çalışma grubu kurduk. Savunma Sanayi Başkanımızın direktiflerini de aldık. Teknoloji yoğun muharebe sahasının 2040'lerde nereye evrildiğini, hangi askeri yeteneklerin, proje-teknoloji demiyorum, askeri teknolojilerin nereye evrileceğini, artık muharebe sahasında nelerin ön plana çıkacağını kendimize dert edindik. Bu dokümanı da STM Think Thank ile bu dokümanı da 1 yıl içerisinde sisteme kazandırma gayreti içindeyiz. Bunların ötesinde söylemem gereken, organizasyon, gayret sarfiyatını önlemek için organizasyon, bütçe, yapı ve kavram tanımlamaları ile konseptlerin bir an önce hayata geçirilmesi önem arz ediyor.



Bülent SEMERCİ
ROKETSAN

Çok teşekkür ederim, iki bölüm halinde icra edeceğim sunumumu. Bugünkü oturumumuzun ana temalarından bir tanesi mühimmat ve ekipman uyumluluğu. Bununla ilgili ürün çeşitliliği ve birlikte çalışabilirlik konulu bir sunum hazırladım. İlk sunumda birlikte çalışabilirlik ve ürün aile yaklaşımımız hakkında bir miktar bilgi paylaşımından sonra taktik füze sistemleri hakkında

bilgiler paylaşacağım. Biraz daha bu konu üzerinde anlattıklarımı detaylandıracağım. Günümüzün değişen savaş ortamı, operasyonel çeşitliliğin artması, envanterimizdeki silah çeşitliliğinin de artmasını beraberinde getiriyor. Yeni bir operasyona gireceğimiz zaman envanterimizdeki nispeten eski silah ve mühimmatlarla, nispeten son teknoloji silah ve mühimmatların birlikte çalışması, birbirleri yerine kullanılması ya da karma kullanılmasının son derece olduğunu değerlendiriyoruz. Birlikte çalışabilirlik nedir? Büyük kompleks sistemlerin bir arada uyum içerisinde çalışması olarak geçiyor genel tanımı. Bunu başardığınız zaman operasyonel etkinliğinizin son derece etkili olacağını, yukarı çıkacağını, gereksiz kaynak kullanımının ise o seviyede düşeceğini ve veriminizin artacağını değerlendiriyoruz. Birlikte çalışabilirlik için ürün ve ekipmanlarımız ortak ara yüzlerinden faydalaniyoruz. Geliştirdiğimiz taktik füze operasyonel çeşitliliğe imkân veren, birlikte çalışabilirliği temel alan ürün ailesi temelli bir yaklaşımımız sök konusu. Bunun en kritik iki adımı standardizasyon ve modülerlikten geçiyor. Yani sahadan yeni bir ihtiyaç önümüze geldiğinde, ürün ailesi içerisinde hızlıca türev ürün yaklaşımıyla bu ihtiyacı karşılayıp envantere sokuyoruz. Paralelinde lojistik olarak da müşterilerimizin taleplerine çok hızlı cevap verebiliyoruz.

Geliştirdiğimiz füzelerde ürün ailesi bütünlüklerini dikkate alıyoruz. Ortak mimari, ortak veri yolları ve ortak donanım çözümlerini öncelikliyoruz. Bunu yaparken, sadece ordumuzun değil uluslararası standartları da gözetiyoruz. Birlikte çalışabilirlik, modülerlik, standardizasyonu sadece silah ve mühimmat veya fırlatma sistemlerinde uygulamıyoruz.

Lojistik destek kapsamında da birbirleri yerine kullanılabilirlik, ortaklaşabilirlik ve uyumluluğu gözetiyoruz. Hangi lojistik destek unsurları? Silah test ekipmanları, taşıma yükleme sistemleri, eğitim sistemleri, simülatörler gibi.

Ürün çeşitliliği ve birlikte çalışabilirliği, ürün ailelerimizle ilgili bilgilerle devam edeceğim. Mini akıllı mühimmat ürün ailemiz, bunun hikayesi MAM-L ve MAM-C mühimmatları ile başladı. Bugün itibariyle toplamda 7 üyesi vardır bu ailenin. Taktik İHA'lardan atmak üzere geliştirdiğimiz sistem, bugün itibariyle insanlı insansız hafif taarruz ve jet uçaklarından dahi kullanılabilir haldedir. Önümüzdeki dönem bunların hibrit arayıcı başlıklı, yapay zekâlı versiyonlarını da yine ordumuzun envanterine sunuyor olacağız. Bir sonraki ürün çeşidi ailemiz bu MAM ailesinin de doğmasına sebep olan tanksavar sistemleri ürün ailemiz. Omtas, Umtas ve Cirit ile başlamıştır doğumları. Devamında lazer UMTAS ve Karaok ile devam eden bir tarihçemiz var. Önümüzdeki yıl da yine ordumuzun talepleri çerçevesinde Lazer Omtas füzesiyle LumtasGM dediğimiz hali ordumuzun envanterine girecek. Bilindiği üzere tanksavar ürün ailemizi biz taarruz helikopterden atmak üzere geliştirdik. Ama bugün bu itibariyle 7 ürün çok çeşitli insanlı ve insansız hava araçları, deniz araçları ve Hürkuş gibi hava platformlarından atılabilir durumdadır. Ürün çeşitliliği ve birlikte kullanılabilirlik kapsamında KMC, kaideye monteli cirit sistemimiz buna çok güzel bir örnek. Lazer güdümlü cirit füzesini atmak üzere geliştirdiğimiz bir silah sistemi, bugün itibariyle iki değişik güdümlü, dört değişik füze sistemini atabilir haldedir. Gerçekten çok yüksek teknoloji kabiliyetleri mevcut. Hareket halindeyken hareketli bir hedefe atış yapabilmek gibi.

Hava sistemleri ürün ailemiz ise Hisar'la başlayan Siper'le devam eden bir hikayesi mevcut. Şu anda 4 ürün görünüyor ama önümüzdeki dönemde Sapan projesiyle beraber buraya 4 tane daha yeni ürün ekliyor olacağız. Bilindiği üzere hava savunma sistemlerimizi kara mobil platformlarından atmak üzere geliştirdik. Ordumuzun talebiyle başlatılan Millas projesiyle hava savunma sistemlerimizi deniz platformlarından da atabilir hale geldik. TGC İstanbul gemisinden yaptığımız atışla entegrasyon yapıp farklı platformlardan atış yapabilmenin heyecanını ve gururunu yaşadık. Ürün çeşitliliği kapsamında Kara-Hava-Deniz sistemlerinden bahsettim ama biz tek-er kullanımı için de ürünler geliştirdik.

SUNGUR, KARAOK ve METE bu ürünlerimiz. TEK-ER kullanım konseptinde istihbarat ve operasyonel verinin alınmasının çok kritik olduğunu değerlendiriyoruz.

Geleceğin TEK-ER konseptinde, teker askerinin kritik olduğunu söylediğim istihbarat ve operasyonel veriyi almak, kullanmak ve paylaşmaya yönelik mutlaka teknik, teknolojik donanım alt yapısına sahip olması gerektiğini değerlendiriyoruz. Bir nevi sensör askere dönüşmesi gerekliliğinin zaruri bir ihtiyaç olduğunu değerlendiriyoruz. Her ne kadar TEK-ER kullanımı için bu sistemleri kullansak da bunları çok çeşitli insanlı ve insansız platformlardan atıyor olabileceğiz, bunların çalışmalarında da sona gelmek üzereyiz. KARAOK en son bu yıl içerisinde seri üretime soktuğumuz ve envantere verdiğimiz en teknolojik ürünlerimizden bir tanesi. Ve gerçekten sahada oyun değiştirici bir ürün. 2 kilometreyi geçiyor ama daha iyisini hedefliyoruz.

Dinlediğiniz için teşekkür ederim.

SORU: Uzun menzilli füzelerde haberleşme konusunda bir alt yapımız var mı?

CEVAP: Evet var ve yoğun olarak çalışıyoruz. Hibrit arayışı başlıklar, görüş ötesi ve otonom sistemlerin ortaya çıkacağını yakında düşünüyoruz.



Dr. N. Kaan ÇALIŞKAN
TÜBİTAK

Herkesi saygıyla selamlarım. Geleceğin askeri konu başlığı altında malzeme bilimi ve mühendisliği uygulamaları konusunda sizleri bilgilendirmek istiyorum. Öncelikle Tübitak Sage'nin tanıtımı, sonra da 3 ana başlık ile bilgi vereceğim. Yaklaşık 21 yıldır Tübitak Sage'de çalışıyorum. Roket füze teknolojilerinde öğrendiğimiz malzeme teknolojilerini çift kullanım hem sivil hem de askeri

kullanım alanları olarak çalıştığımız için bu konularda da yolları çakışan, ayrı olan veya farklı değerlendirme içeren konu başlıklarını da içeren bir sunum hazırlamaya çalıştık. 3 milyon 100 bin metre karelik açık alan, 75 bin metrekarelik kapalı alanda çalışmalarımızı sürdürüyoruz. 1300 çalışanımız var.

Misyon ve vizyonumuza gelirsek Türk Silahlı Kuvvetleri ve Savunma Sanayi'ne küresel ölçekte rekabet gücü ve katma değeri yüksek Millî teknoloji ürün ve hizmetleri Ar-Ge yoluyla sağlamak misyonumuz. Vizyonumuz ise, savunma sanayinde yenilikçi teknolojiler ile Türkiye'yi tam bağımsız kılmak ve küresel ölçekte etkin olmak. Bu misyon ve vizyon altında çalışmalarımızı bazı uzmanlık alanlarından da yararlanarak, sistem mühendisliği çatısı altında kullanmaktayız. Bunlar pil teknolojileri, güdüm kontrol sistem tasarımı, yazılım, malzeme tasarımı, farklı konvansiyonel dışı üretim teknolojileri gibi sistem mühendisliği altında çalışmalarımızı sürdürmekteyiz. Güdüm kitleri, Sığınak delici mühimmatlar, İHA mühimmatları, seyir füzeleri, hava hava, hava savunma füzeleri diye sayabiliriz. Aslında 2000 yılında topçu roketi ile başlayan, şu anki mevcut konumumuzda ramjet motorlu hava savunma füzelerinden Çelik Kubbe'nin ana roket füzesinden biri olan Cirit'i yapabilen bir kurum haline dönüşme sürecimiz bu şekilde. Çok farklı ürünlerimiz mevcut. Hem geliştirme aşamasında, envanterde veya üretimde veya savaş ortamında kendini kanıtlamış ürünlerimiz bulunmaktadır. Sistem çalışmaları yaptığımız gibi aynı zamanda alt sistemlerimiz de mevcut, ürünlerimiz de mevcut. Çünkü kendi kullandığımız ürünlerde, projelerde tedarik sıkıntısı olan, tedarik edilemeyen bir alt sistem varsa bunu mutlaka Tübitak Sage'de gerekli uzmanlıkları da birleştirerek kendimiz geliştiriyoruz.

Bunların başında ısıtıcı piller, neredeyse savunma sanayindeki bütün ısıtıcı pilleri Tübitak Sage sağlamakta. Piroteknik aygıtlar, navigasyon birimleri, antenler, arayıcı başlıklar, termobarik patlayıcılar ve tıpa gibi alt bileşenleri de biz Tübitak Sage bünyesinde geliştiriyoruz. Elektronik donanımdan RF donanımdan, alıcılardan patlayıcıya kadar geniş bir ürün ailemiz mevcut.

Türkiye’de de ilk yerli Millî karıştırmaya dayanıklı antenleri yaptığımız gibi ilk pasif aktif GPS antenini de Tübitak Sage alt yapılarında gerçekleştirmiş bulunuyoruz. Bunları yaparken hem sistem seviyesi hem alt sistem seviyesi bazı alt yapılardan yararlanıyoruz. Kendi alanlarında örnek teşkil edecek alt yapılar. Ankara Rüzgâr Tüneli, Çevresel Test Merkezimiz Avrupa’nın en büyüğü, Denizaltı Testleri Alt Yapısı, Hedef Balistiği Raylı Sistem Dinamik Test Altyapısı (HABRAS), Arayıcı Başlık test merkezi, Harici Yük Sertifikasyon, Tahribatsız Kalite Kontrol, Hedef Balistiği ve Yer Testleri, Ataletsel Ölçüm Laboratuvarı olmak üzere birbirinden farklı alt yapılarımız mevcut. Tabii ki bunu kendi projelerimizde kullandığımız gibi proje paydaşlarımıza da alt yapılarımızı kullanıdırıyoruz. Aynı zamanda dost ve müttefik üyelerin ordularına da veya ilgili kurumlarına da bu konularda hizmet veriyoruz. Tübitak Sage ne yaptı, işe yaradı mı, ne işe yaradı gibi sorular varsa yurt içinden ve yurt dışından elde edilen ürünlere bakabilirsiniz. Farklı batı menşeli olan ve Türk Silahlı Kuvvetleri tarafından kullanılan çok sayıda ürün, bunlara muadil veya çok daha iyi ürünler yerli ve Millî olarak yurt içinde geliştirilmiş ve kullanılmaktadır. Biz de bununla çalışanları olarak gurur duymaktayız.

Malzeme bilimi ve uygulamalarında giyilebilir zırh teknoloji başlığıyla devam edebiliriz. Aslında malzeme bilimi ve uygulamaları, bir roket ve füze de kullanılan bir malzeme bilimi bir geleceğin askeri konseptinde nasıl kullanılabilir bunları anlatmaya çalışacağım. Çünkü neredeyse ortak bir konsept üzerinden çalışılıyor ve geliştirilen ürünlerde kullanılıyor. İlk başta kurşun geçirmez ve darbeye dayanıklı kumaşlarla başlamak isterim. Aslında ilk çağlardan beri insanlığın kullandığı bir teknoloji.

Tahta, deri, metal ve benzeri malzemelerle yapılanlar, ondan sonra savaş ortamında kullanılan primitif tasarımlar. Tabii bunlar ağır, rahatsız, tam koruma sağlayamayan ürünler. Fakat teknolojinin gelişimiyle, yani üretim ve malzeme teknolojisinin gelişmesiyle birlikte yeni nesil yeleklerde üretilmiş ve kullanılmış durumda. Hafif, hava geçiren, terletmeyen, yanmaya dayanıklı kumaşlar veya son 10-15 yıla damgasını vuran üç boyutlu üretim yöntemlerinin de kullanıldığı bazı türevler, varyantlarda bu teknolojilerde kullanılmaktadır. Daha çok bildiğimiz zırh ticari ismi kevlar olan ama teknik olarak aramid diye geçen, belli bir reçine içerisinde emdirilmesiyle, üretilmesiyle yapılan zırhlar en çok kullanılan zırhlar. Dünyada da çok kullanılıyor, Türkiye’de de çok rahat üretilabiliyor. Yurt dışından bazı parçalarla çok rahat üretebilen yerli kurum ve kuruluşlarımız da mevcut. Ancak aramid dışında farklı fiberlerde kullanılıyor. Bunlar polietilen, polipropilen olabilir. Bu tip malzemeler de kullanılarak farklı balistik korumalarda kullanılabilen kurşun geçirmez ve darbeye dayanıklı kumaşlar olarak kullanılmakta. Yakın zamanda da çalışılan, batıdaki araştırma merkezlerince yürütülen, yerli ve Millî olarak da yurt içinde çalışabilen bazı çalışmalar da seramik kaplamalı kumaşlar var. Bununla ilgili de çalışmalar yürütülmektedir.

Özellikle sertlik ve aşırma dayanımı artırılarak balistik korumasının artırıldığı örnekleri de bu teknoloji sayesinde yapılmaktadır. Aynı zamanda bu aramidin farklı oksit kaplamalarıyla, plazma sprey kaplamalarıyla farklı dayanıklı kumaşlarda üretilmektedir. Kumaşın bir bağ oluşturarak kaplama yüzeyi oluşturarak farklı özellikle bir balistik koruma sağlaması da bu çalışmalar kapsamındadır. Onun dışında bu aramid epoksi içerisinde üretilmesi sonrası bor, karbür gibi bir seramikle kaplanması, düz dokuma veya farklı dokumalar dokunarak dayanıklı kumaşların üretilmesi veya aramidin bildiğimiz aramidin farklı reçinelerle üretilip üzerine silikon karbür gibi farklı seramiklerle üretilerek farklı malzeme parametreleri çalışılarak balistik koruma çalışmaları dünyada yürütülmektedir. Biz de yürütüyoruz. Sadece askeri personelin kıyafeti değil, kullandığımız sistemlerde de balistik koruma ihtiyaçları oluyor. Burada da kendi bilgimizi kumaş teknolojisine aktarmak üzere de çalışıyoruz ki tekstil sanayide Türkiye’de çok gelişmiş durumda. Bu iki teknolojiyi birbirine yakınlaştırdığında iyi ürünler ortaya çıkacağı da bariz.

PDMS malzeme denilen, çok silikon bazlı bir polimerin yeni nesil zırhlarda nasıl kullanıldığı, giyilebilir zırh teknolojisinde nasıl kullanıldığı da yeni bir konu. Bu malzemeler aslında vücut şeklini rahat alabilen, esnek malzemeler ve tampon malzeme olarak kullanılabilir.

Ancak, şöyle bir özellikleri var. Darbeye maruz kaldığı anda form değiştirerek sertlik seviyesi miktarın çok yüksek seviyesinde sertleşerek, bir zırh gibi davranarak, bir personeli veya korumakla yükümlü olduğu arka panele az darbeyi ileterek bir zırh gibi davranıyor. Şu an mevcut kevlar kumaşlarla yapılan bir yöntemi var fakat kevlar kumaşlarla arasındaki fark, darbe oluştuktan sonra, darbeyi önlerken zararını daha geniş bir alana yayarak personelin korumasını enerjiyi dağıtarak, vücudunu korumasını sağlamakta.

Asıl amaç darbeyi önlemek olduğu kadar büyük bir alanda da darbeyi emerek personelin darbe karşısında uğrayacağı etkileri en aza indirmek. Bu yeni malzeme teknolojisinde kullanılıyor, bununla çalışılabilir. Bizim de ilgilendiğimiz bir konu, Türkiye’de bazı üniversiteler de ve yurt dışında da üzerine çalışmalar var.

Dış iskelet örnekleri yerli firmalarımız tarafından, bazı firmalar tarafından fuarlarda, seminerlerde de gösteriliyor. İlk örnekleri, dünya da öyle başarılı olmamakla birlikte sonradan malzemelerin değişimiyle hafifletilmiş ve saha koşullarında çalışan askeri personelin daha fazla yükü daha hızlı bir şekilde taşıyacak şekilde evrimleştirildi. Özellikle metal parçalara hafifi ve sağlam materyaller sağlanarak, dış iskelet konsepti aslında başarıya doğru ilerlemektedir. Bununla ilgili de asıl ana yapısal parçaların yoğunluk ve mukavemet oranı düşük olan malzemelere yeni nesil malzemeler eklenerek dış iskelet konsepti de başarılı hale gelmektedir.

Nano mikro sistemlerdeki malzeme teknolojilerini de anlatacağım ikinci başlık olarak. Özellikle bizim de son yıllarda takipçisi olduğumuz RF ve elektronik donanımlarda kullandığımız, dielektrik malzeme teknolojilerindeki gelişmeler, özellikle üretim teknolojilerindeki gelişmeler bize çok küçük alanlarda farklı özellikler sağlayabilen elektronik donanımlar yapma şansı sağlamıştır.

Özellikle elektromanyetik özellikle Electromagnetic Directed Energy Weapon konsepti altında da çok kullanılan elektromanyetik darbe verici namlu adaptörü gibi konsept tasarımlarda aslında bu tip gelişmeler sayesinde yapılabilir hale gelmiştir. Özellikle EMP darbesi dediğimiz Elektromagnetic Past darbesiyle İHA'ların elektronik devrelerinin bozularak kontrolsüz hale getirilebilmesi askerler için de çok önemli. Gerek ticari gerek askeri İHA'lar gerçekten büyük tehdit oluşturmakta. Bunlarla ilgili taşınabilir ve entegrasyonu kolay bu tip tasarımlar aslında şu anda dünyada da çalışabilir tasarımlardır. Buradaki adaptör çıkarıldığında silah sistemi de eski fonksiyona tekrar devam ederek bir kolaylık da sağlamaktadır.

Onun dışında Nano İHA konusunda çok yoğun bir faaliyet sürdürülmekte. Çünkü istihbarat çalışmaları için çok küçük İHA'lar kullanan askeri personelin bu konuda çok büyük ihtiyacı ve gereksinimi bulunmakta burada. Burada pil ömrü ve yük kapasitesi gerçekten kısıtlayıcı bir faktör olsa da malzeme teknolojilerindeki gelişmelerle birlikte 250 gramdan daha hafif İHA'lar, nano İHA'lar yapılarak istihbarat çalışmalarında da rahatlıkla kullanılabilir hale gelmiştir. Anten aslında bizim özellikle çok yoğun bir şekilde ilgilendiğimiz bir konu. Özellikle roket ve füze sistemlerinde karıştırmaya dayanıklı antenden GPS antenine, uçuş sonlandırma, veri antenlerinden telemetri antenlerine kadar tüm antenleri biz kendi alt yapılarımızla, yerli ve Millî olarak, dielektrik malzemesi de dahil olmak üzere üretebiliyoruz. Onun için anten konusunda çok yoğun çalışıyoruz. Bu yeni teknolojilerdeki gelişmeler, özellikle anten ve malzeme teknolojilerindeki gelişmeler, antenin, mevcut askeri personelin koşullarındaki çalışan askeri personele entegrasyonu da kolaylaştırmıştır. Burada çip antenler, farklı çip antenler, GPS antenleri sayesinde iz sürülebilirlik, sağlık verilerinin takibi, hücresel iletişim gibi gözüken ama kolaylaştıran sistemler de şu an yapılabilir durumdadır. Özellikle entegrasyonunda ele, vücuda veya giyilen kıyafete entegrasyonu da bu yeni teknolojilerle kolay ve basit, sürdürülebilir teknoloji haline gelmiştir. Ama bizim de özellikle yoğun olarak kendi çalışmalarımızda kullandığımız, bunun da bir başka sonucu olan, giyilebilir antenler. Giyilebilir antenler gerçekten ilgi çekici bir konu ve hem ülkemizde hem de yurt dışında çok fazla ekibinde, çok fazla akademik grubunda çalıştığı bir konu.

Kumaşa entegre edilmiş şekildeki anten, yalıtkan yüzeyi ve petle bir kumaşın üzerine, belli bir dokuda belli bir desende işledikten sonra, insan vücudunu dielektrik bir malzeme gibi kullanarak tüm vücudu bir anten haline döndürmek. Aslında bu konseptin temel konusudur. Böylece sağlık verilerinin takibi, uydudan yerin takibi gibi konseptler veya tasarım kriterleri, gereksinimler bu teknoloji sayesinde rahatlıkla yapılabilir halde olabilir. Biz de kendi yaptığımız antenlerde özellikle farklı dokularda anten yaptığımız için, kumaşa entegrasyonu bu tip teknolojilerin yapılabileceğini de öngörebiliyoruz. Bir de üretimde küçük üretimleri yüksek hassasiyetli yapabilme, dielektrik malzemelerdeki gelişmeler aslında konforlu ve güvenli kask üretimlerini ve tasarımını da rahatlıkla yapılabilir hale getirmiştir. Bu özellikle baş monteli güneş panelinden tutun termal kameraya, hareket sensörleri ve iletişim modelleri gibi bileşenlerin artık çok rahatlıkla kasklara entegre edilmesini sağlamıştır. Ve sürdürülebilir, istenen çevre koşullarında çalışabilir halde yapılabilir hale gelmesi, bu malzeme bilimi ve üretim teknolojilerindeki gelişmeler sayesinde özellikle rahatlıkla yapılabilir hale gelmiştir. Bunun dışında kızıl ötesi yansıtıcı kumaşlar, kızıl ötesi görünmezlik zaten vazgeçilmez bir konsept. Bu görünmezliğe yarayacak, aynı zamanda termal konfora yarar sağlayabilecek kızıl ötesi yansıtıcı kumaş teknolojileri de şu an sahalarda kullanılmaktadır.

Özellikle toz, pasta ve köpük formunda kumaş kaplama teknolojisiyle üretilen tekstilin dokunmasıyla tente, çadır bezi veya askeri giysilerde farklı özelliklere sahip. Kızıl ötesi görünmezliğe gerek yok, görünürlüğü artırıcı da olabilir, onun da bazen gereksinimleri olmaktadır. Bu tip teknolojilerde yapılabilir haldedir şu anda. Onun dışında çok basit egzotermik reaksiyon dediğimiz, yani ısı verici reaksiyonların kullanıldığı ve dış dış herhangi bir harici kaynak dış kaynak ihtiyacı olmadan ısı sağlayabilen, kendi kendine ısınan konserve teknolojisi de aslında çok basit bir kimyasal reaksiyona dayanmaktadır. Bununla ilgili de çalışmalar yapılabilmekte ve kullanılabilir. Basit bir reaksiyonu yiyecekten ayırarak kullanılması durumunda 30 derece 40 derece, yeri geldiğinde daha yüksek sıcaklıkları artırarak askeri personelin rahatlıkla kullanılabilir, yiyebilir bir konserve içeriğine ulaşılabilir. Şu an çok sıcak bir konu olan çalışmalardan biri giyilebilir ısıtıcılar.

Bu nano kalınlıkta, bu arada nano dediğimizde biz her zaman bir mikronun altı kalınlıklardan bahsediyoruz. Nano kalınlıklarda entegre edilmesiyle her türlü çevresel koşullarda askeri personelin vücut sıcaklığının sabit tutulması çok önemli bir konsept. Bununla ilgili de çalışmalar mevcut hem ülkemizdeki hem de yurt dışındaki bazı çalışmalarda. Bunun şu an ki dezavantajı dışarıdan bir pil gibi harici bir kaynak istemesi. Fakat bununla ilgili de yeni gelişmeler var.

Enerji ihtiyacını gidermeye yönelik çalışmalar da önemli. Buradaki malzeme teknolojilerindeki gelişmeler bizim çok küçük birimlerde yüksek manyetik alanı oluşturabilme şansı da doğurduğu için aslında saha operasyonlarında yeni nesil silahların gelişmesine de yol açmakta. Özellikle raylı top dediğimiz bu yüksek manyetik alanda çalışan ve bir mermiden çok daha yüksek hızda dışarıya delici parçacık çıkartabilen sistemler, yeni teknolojilerle ulaşılabilir hale gelmiştir. Yakın dönemde bununla ilgili ürünlerin çıkma olasılığı da vardır. Taşınabilir güneş panelinde de uygulamalar da mevcut. Fakat verimliliğin artırılması ile ilgili gereksinimler bulunmaktadır. Kullanılan silisyum gibi yarı iletken malzemeler kullanarak saha koşullarında çalışan personelin enerji ihtiyacının rahatlıkla sağlanabildiği güneş panellerine doğru da bir yol haritası mevcuttur. Onun dışında termoelektrik malzeme bizim de yoğun bir şekilde kullandığımız tasarımı ve üretimini yapabildiğimiz, peltier effect dediğimiz, yani sıcak soğuk durumundan faydalanarak elektrik üretme veya elektrik verilmesi durumunda, sıcak soğuk iki farklı alan üretebilen termoelektrik malzemelerinin kullanımı da aslında yaygın ve yeni, inovatif çözümleri bize sunmaktadır. Bununla ilgili yerli ve yurt dışında da çalışan çok fazla sayıda gruplar var. Özellikle bunu kumaş haline getirerek insan vücudunun sıcaklığının elektrik ihtiyacını sağlayabilecek yönünde bir teknolojiye evrilmesi, şu an yol haritasında da mevcuttur. Enerji ihtiyacının giderilmesi için termoelektrik kumaşın kullanılmasıyla ilgili de çalışmalar yapılacaktır.

Benim anlatacaklarım bu kadar, teşekkür ederim beni dinlediğiniz için.



Taylan ERCAN
KALE JET MOTOR
(KALE ARGE)

Merhabalar herkese meslekteki 27. Yılım ve 27 yıldır da gaz tribünlü motorlar üzerine çalışıyorum. Bugün sizlere seyir füzelerinin motorları ile ilgili bir sunum hazırladım. Malum günümüz savaşlarında seyir füzeleri çok gündemde. Dolayısıyla biz ülke olarak bunun motorlarıyla ilgili ne durumdayız onlarla ilgili konuşacağız. Meslektaşlarım hem Roketsan hem de Tübitak Sage'den, kısaca seyir füzelerinden bahsettiler. Ben ise tabi bu füzelerin olmazsa

olmazı gaz tribünlü motorlarda ne noktadayız, onunla ilgili bir sunum yapacağım. Özellikle mevcut teknolojilerde neredeyiz, hangi füzelerimiz, motorlarımız var. Kale Ar-Ge olarak yaklaşık 12 yıldır bu konuda çalışıyoruz. Bugünün de konsepti, yani Future Soldier konsepti Future Cruise Missile Engine, yani geleceğin seyir füzelerinde neler yapmayı planlıyoruz.

Bugün itibariyle 3 tane yerli ve özgün füze motorumuz var, seyir füze motorumuz. KTC 3200 motorumuz 3200 newtonluk bir motorumuz. Som ve atmaca seyir füzelerine güç veriyor. KTC 1750, 1750 newtonluk, daha küçük yaklaşık yarı itki seviyesinde bir motorumuz, çakır platformu için geliştirilmiş bir motorumuz. KTC 3700 ise geliştirilmiş bir motor, 3200'ün bir üst modeli ve kara atmaca versiyonu için geliştirdiğimiz 3 farklı motorumuz. Kısaca 3200'den bahsederseniz, 3200 newtonluk bir motor. Yakıt tüketimi Newton başına .18/kg/saat özgül yakıt tüketimi var ve 50 kilogramlık bir motor. Som için geliştirilmiş bir motor ve Türkiye'nin ilk özgün turbojet motoru. Bizim de motor ailesinin, seyir füzesi ailesinin ilk üyesi. Füzemiz 0.6 km irtifada füzemiz Som, 0-0.95 mach hızlarla giden bir füzenin tahriğini sağlayacak bir motorumuz ve şu an seri üretim faaliyetleri devam ediyor.

Diğeri ise KTC 1750 ve çakır füzesi için geliştirdiğimiz motorumuz. Ağırlığı 22,5 kilogram ve 3200'ün yarısı. Bu da sınıfının en iyisi, tabii ki sonradan bu işlere başlamış olmak daha yeni teknolojileri aslında birlikte tasarlayıp koymak anlamına geliyor motorlarımıza.

Dolayısıyla rakip platformlara baktığımız zaman en yeni motorların olması, bize yanı zamanda daha yeni teknolojileri de bu motorlarda geliştirme şansı sağlıyor. Kompakt bir tasarım, yüksek performans ve de uçuş testleri de başarıyla devam ediyor 3 motorumuzun da. Bir sonraki motorumuz da 3700 ve atmaca füzesinin kara atmaca versiyonu için geliştirdiğimiz bir motor. Bir miktar Newton itki işlevinin daha fazla olduğu, benzer yakıt tüketimi, benzer hacimde ve ağırlıktaki bir füze motorumuz.

Peki gelecekte, bundan sonrasında ne yapacağız? Bu füzeler ve kullanıldığı platformlar aslında orta menzil, belki 1000 kilometrenin altındaki menzillerde aslında ülke olarak bir noktaya gelmiş durumdayız. Yaklaşık 45 dakika ve daha az uçuşlar yapan seyir füzelerimiz ve bunların Millî ve özgün motorları şu anda mevcut. 3200 ile aslında envantere giriyor, seri üretimde. Diğer 1750 ve 3700 için de kalifikasyonlarını tamamlayıp kuvvetlerin kullanımına verilecek. Bundan sonraki 10 yıllık süreç için, ilk 15 yılda motor teknolojilerinde bunları geliştirdik. Bundan sonrası için uzun menzil, dünyadaki gibi teknolojilere sahip olmamız için daha uzun menzile geçmemiz gerekiyor. Dolayısıyla bunun da en önemli bileşenlerinden biri gaz tribünlü motorlar. Burada teknolojik bir ülke olarak hamle yapmamız gerekiyor. 2013'ten beri ODTÜ havacılıkta yarı zamanlı öğretim üyesi olarak da çalışıyorum.

Bugünkü mevcut teknolojiler, mevcut füze motorlarımız aslında basit anlatımıyla bir turbo jet mimarisiyle yapılıyor. Bir kompresör yanma odası ve tribünden oluşan, yakıt verdiğimiz yanma odasına ve kinetik enerji elde ettiğimiz, bu kinetik enerjiyi de egzoz lülesinden hızlandırarak, atarak itki sağladığımız bir mimari. Tabii çok kullanışlı, yıllardır turbojet motorlar ve günümüzde seyir füzelerinde de kullanılmaya devam ediliyor. Çünkü basit bir mimari. Fakat problemi ne? Bunların bir tarafta termal verimi var diğer tarafta tahrik verimi var. Toplam verimiz de aslında bu iki verimin bir birleşimi.

Turbojet mimarisindeki ana problem, üst tarafta termal verimi arttırabilmek için, verimler en sonunda yakıt tüketimini etkiliyor. Menzili arttırmamız için de bu gaz tribünlü motorlar, mümkün olan en az yakıt tüketimini sağlasın ki, füzeler daha yüksek menziller gidebilsin.

Turbo jet mimarisinde termal verimi artırmak istediğimiz zaman, çıkış hızımızı, yani motordan çıkış veya füzenin çıkış hızını çok yükseltmemiz gerekiyor. Fakat bu bize tahrik veriminde düşüş olarak geri dönüyor. Çünkü tahrik verimi de seyir hızıyla benzer bir seviyede olmasını istiyor en verimlilik noktasında. Dolayısıyla termal verimde belirli bir noktaya kadar motorun kendi ısını artırmak, hem de motorun içindeki basınç oranını arttırarak aslında termal verimi arttırabiliyor. Fakat bu termal verim artışı bize çıkış hızının artışı olarak geri dönüyor. Dolayısıyla tahrik verimlerimiz düşme eğilimine giriyor. Toplam verim olarak düşündüğümüz zaman da bizi gerçekten yakıt tüketimi anlamında kısıtlayan bir durum söz konusu. Dolayısıyla uzun menzile geçmek istediğimiz zaman, bir sonraki nesil geleceğin seyir füzeleri için, ülke olarak yapmamız gereken turbo fan mimarileri, bugün uçaklarda da kullandığımız mimariler.

Tribün motorlarında da kompresör, yanma odası, türbin gibi aynı turbo jet mimarimiz var fakat ekstra bir türbin ekleyerek bu motorun arkasına ve onunla beraber ürettiğimiz gücü ön tarafta bir fanı çevirerek, aslında düşük hızlar elde ediyoruz. Dolayısıyla tahrik verimlerimiz çok iyi hale geliyor hem de termal verimler hala yüksek kalmış olabiliyor. Dolayısıyla termal verim turbo jetle çok benzer fakat esas farkı oluşturan toplam verim çok yükseliyor. Bu bize bu motorların çok daha düşük bir yakıt tüketimi olmasını sağlıyor ve bu sayede de saatlik yakıt miktarı tükettiği newton başına düşüyor ve dolayısıyla füzelerde uzun menzili sağlıyor. Amerika'da AGM serisi füzeler 1000-2500 kilometrelik menzilleri var. Dolayısıyla ülkede 1000 kilometrenin altındaki füze teknolojileri, Roketsan, Sage ve bizle beraber motorlarıyla beraber özgün halde envantere girerken, bundan sonraki 10 yılda hedeflediğimiz, elbette beraber 1000 ve 2500 kilometrelik yani orta menzil veya uzun menzilde seyir füzelerimizin geliştirilmesi olacak.

Son konu ise yurt dışına satışlar konusu. İki önemli kriter var tabi teknoloji olarak yurt dışındaki rakiplerle benzer seviyede motorlarımız olması. Bu daha geç ülke olarak daha geç başlamamız, daha yeni teknolojileri koyup mevcut piyasadaki 10 yıllık. 15 yıllık. 20 yıllık motorlarla çok iyi rekabet edebileceğimiz anlamına geliyor. Dolayısıyla burada bir sıkıntımız yok. Tabii başka ne avantajımız var? Bir seyir füzesi hükümetler arası satışları da çok sıkıntılı konular.

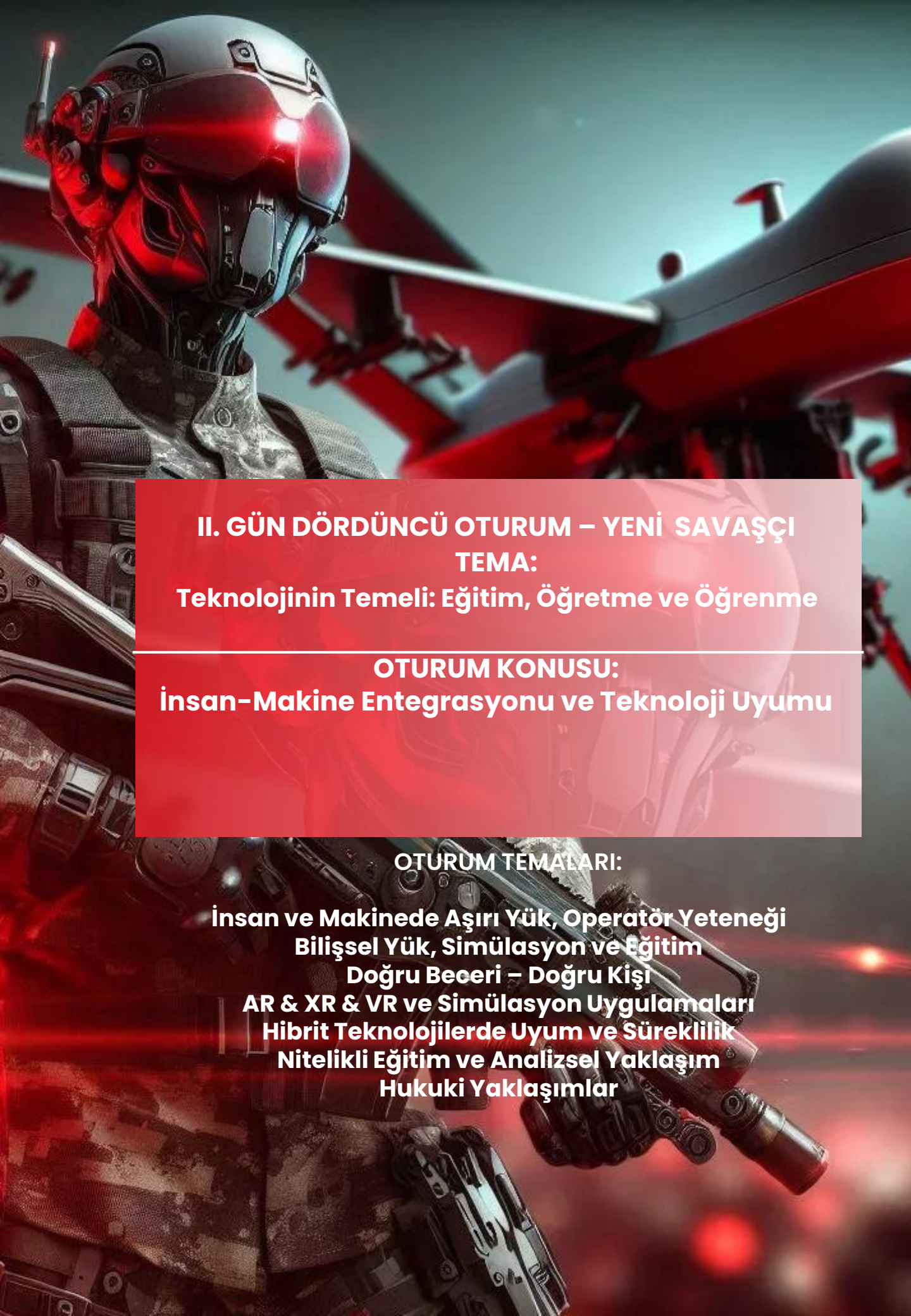
Bugün Fransa, Amerika bu füzeleri hiçbir yere satmıyorlar, bu teknolojileri vermek istemiyorlar. Biz ülke olarak bu teknolojileri geliştirdikten sonra hem Roketsan tarafı yurt dışına füzeleri satıyor, hem de biz müttefik ülkelere daha kısıt olarak satıyoruz. Dolayısıyla bunlarla ilgili de son dönemde, özellikle seyir füzelerinin çok popüler olması ve Amerika ve Fransa gibi ülkelerin satmak istememesi dolayısıyla bizler önümüzdeki 10 yıl boyunca bu füzeleri yurt dışına satıyor olacağız.

SORU 1: Taylan hocam Türkiye'ye hoş geldiniz yeniden. Eskiden Stealth Motor Teknolojileri alanında çalışmalarınız vardı? Bu çalışmalara devam edecek misiniz? Seyir füzelerinde de stealth motor katma değer sağlanabilir mi?

CEVAP: Kısa vadede düşünmüyoruz neden düşünmüyoruz. Çünkü şu anda biliyorsunuz Millî Muharip Uçağımız KAAN'ın da gaz tribünü motorunu geliştiriyoruz. KAAN 5. Nesil bir uçak ve dolayısıyla onun motorunun da o özellikte olması gerekiyor. Öncelikli hedefimiz uzun menzilli turbo fan mimarisi ama hemen arkasından, KAAN'daki gelişmelerle birlikte, stealth motor teknolojisini de seyir füzeleri üzerine uyguluyor olacağız.

SORU 2: Motorları üretiyoruz, Millî üretmemiz gerekiyor. Özellikle alt bileşenlerde ne kadar yerlileşebildik?

CEVAP: Seyir füzelerinde daha şanslıyız, sofistike malzeme noktasında. Daha az teknolojik ürünler. Esas zorluk ve sıkıntılar GÖKBAY ve KAAN motorlarında. Yüksek sofistike alışimlarla ilgili problemler var. Bunlar için çalışmalar devam ediyor. TEI özelinde belirli boyutlarda üretilemeyecek alışım yok, süper alışimlardan yüksek sıcaklıklarda çalışan alışimlara kadar gerekli teknolojiye erişildi.



II. GÜN DÖRDÜNCÜ OTURUM – YENİ SAVAŞÇI TEMA:

Teknolojinin Temeli: Eğitim, Öğretme ve Öğrenme

OTURUM KONUSU:
İnsan-Makine Entegrasyonu ve Teknoloji Uyumu

OTURUM TEMALARI:

**İnsan ve Makinede Aşırı Yük, Operatör Yeteneği
Bilişsel Yük, Simülasyon ve Eğitim
Doğru Beceri – Doğru Kişi
AR & XR & VR ve Simülasyon Uygulamaları
Hibrit Teknolojilerde Uyum ve Süreklilik
Nitelikli Eğitim ve Analizsel Yaklaşım
Hukuki Yaklaşımlar**

IX. OTURUM ÖZETİ

Yeni teknolojilerin yeni eğitim metodları gerektirdiği vurgulanılan bu bölümde, simülatör teknolojileri, artırılmış gerçeklik (AR), karma gerçeklik (XR) ve sanal gerçeklik (VR) teknolojilerinin eğitimdeki önemine dikkat çekilmiştir. Gerçeğe en yakın ortamlarda verilecek eğitimin farkındalığı artırıcı ve hızlı karar almadaki etkisi vurgulanırken, yapay zekâ entegrasyonu ve dijital ikiz kavramıyla senaryoların ve eğitim kalitesinin de artacağı öngörülmüştür. Biyometrik verilerin de elde edilmesiyle personel eğitiminin doğru zamanda, doğru müdahaleyi yapabilmesi yönünde kabiliyeti artırdığı ve baskı altındaki tepkilerinin ölçülebilmesinin sağlandığı vurgulandı. Bu alanda hava, kara, deniz, siber ve uzay gibi müşterek operasyonel ortamlarının artırılmasının tüm askeri personeli daha etkin bir şekilde harbe hazır hale getireceği, bireysel eğitimlerin de bu teknolojilerle daha mümkün olduğu görüşü paylaşılmıştır.

Mühimmatların, silahların, geliştirilen sistemlerin simüle edilerek test edildiği uygulamaların da fayda-maliyet analizinden daha önemli olan doğru ve verimli ürün geliştirilmesini sağladığı kaydedilmiştir. Gerçek savaş ortamlarının veya hedeflerin gerçekçi bir şekilde simüle edilerek, geliştirilen silah ve mühimmat sistemlerinin test edilebildiği ve yapılan analizlerle doğru ürün gelişiminin sağlandığı modellemelerin yapıldığı, etkilerinin ve eksiklerinin incelenemediği ortamların oluşturulmasının faydaları aktarıldı. Geliştirilen askeri sistemlerin kabiliyetlerinin gerçeğe en yakın ortamda karşılaştırılabildiği ve en ideal askeri sistemin kullanımının da bu sistemlerle mümkün olduğu ifade edilen örneklerle paylaşıldı. Simülasyon sistemlerinin sanal ortamlarda aşırı derecede uygulanması halinde oluşturabileceği 'sahte güven' kaygısı ve sanal gerçekliğin kaybettirebileceği 'gerçeklik algısı' endişeleri de dile getirilirken, eğitim programlarında bu boyuta da dikkat çekildi.

Otonom sistemlerin uluslararası hukuki boyutlarının da konuşulduğu bu bölümde, otonomi seviyesi, operatör bulunup bulunmaması, kontroldeki insanın etkisi, uzaklığı gibi çok farklı tartışmaların bulunduğu belirtildi.



Dr. Oğuz HAMŞİOĞLU
SASAD
MODERATÖR

Değerli konuklarımız hoş geldiniz. Akşamın bu vaktinde oksijenimizin azaldığı, ağırlığın üzerimize çöktüğü bir saatte sizlerle birlikte olduğunuz için ve sabrınızdan dolayı teşekkür ediyorum. Bu anı bizlerle paylaştığınız için sağ olun. Bu an bizim için çok değerli. Çünkü bu tip etkinliklerde son oturumlar her zaman çok risklidir katılım bakımından, biz de bu riski göze aldık. Bu oturumdaki konu başlığımız, teknolojinin en önemli

temeli eğitim ve öğretim ve bu konudaki süreçler.

Biz bu oturumda makine-insan entegrasyonunu, bu konuda teknoloji ve insan alanındaki eğitim hususunu konuşacağız. Aşırı teknoloji yükleme ve kapasite sorunsalına, kullanıcı yeteneklerine, bilişsel yük kavramına değineceğiz.

Askeri simülasyon konusu da gündemimizde olacak ve bunlarla ilgili eğitimler, hibrit savaşlar, dijital savaşlar ile bilgi donanımı, personel ile ilgili hususlar da gündemimizde olacak. Öldürücü teknolojiler bölümünde de AR, XR ve VR uygulamalarından bahsedeceğiz. Sanal tatbikatlardan, karma teknolojilerdeki uygulanabilirlikler ve gelişmeler, teknoloji nitelikli eğitim konularına değineceğiz. Yine yapay zekânın ölümcül otonom sistemlerle ilgili insan-makine etkileşmesine ilgili olarak da hukuki konuları özellikle, ahlaki boyutu da var malumunuz, hukuki rolüne de ilişkin değerlendirmeler yapacağız.

Birbirinden değerli insanlar bizimle paylaşımlar yapılacaktır. Tüm oturumlarda son derece değerli isimleri burada ağırladık. Ve onlardan geleceğe perspektif sağlayacak çok güzel düşünce ve görüşler elde ettik. Bunlar, bizim hem sektör hem de kullanıcı için kaynak niteliğinde bir doküman olarak sizlerin istifadesine sunulacaktır.



**Mehmet Onur ÖZÇELİK
HAVELSAN**

Teşekkür ediyorum. Sunuma öncelikle Havelsan'dan bahsederek başlayacağım. Sonra Askeri Eğitim Sistemleri'nde, Yeni Teknolojiler ve Harp üzerine etkileri kapsamında Havelsan neler yapıyor, teorik olarak ne yapıyor, çalışma, ürün olarak ne yapıyor. Projeleri nelerdir bunlardan bahsedeceğim. Bunların da eğitim sistemleri üzerine, yani askeri eğitimlerde ve özellikle harp alanındaki etkilerine de değinmeye çalışacağım. Havelsan, yaklaşık 40 yıldır simülatör işinde faaliyet gösteriyor. Bundan yaklaşık 35-40 yıl önce silahlı kuvvetlerimizin envanterindeki yabancı menşeli eğitim sistemlerinin bakım idamesi kapsamında destek vermek için 56 kişilik bir ekip kurmuş. Yaptığı çalışmalarla büyümüş ve şu anda Türkiye'de simülatör alanında, simülasyon alanında ciddi bir kabiliyet haline gelmiş. Neler yapıyoruz, anahtar teslim simülatör eğitim merkezleri yapıyoruz. Anahtar teslimden kastımız binasıyla, eğitim sistemleriyle simülatör eğitim merkezleri kuruyoruz yurt içinde ve dışında. Bunun haricinde eğitim sistemleri sunabiliyoruz, platforma özel olabilir, farklı özel amaçlı sistemler olabilir. Eğitim çözümleri ve ürünlerimiz var, paraşüt simülatörleri gibi, atış sistemleri gibi, farklı özel yine fonksiyonlara özel, sivil havacılık eğitim sistemleri yeni girdiğimiz bir alan. 8 yıldır bu alandayız. Dün ilk ihracatımızı gerçekleştirdik, bunun imza töreni oldu. Hindistan'a bir Airbus A320 simülatör ihracatı yaptık. Test ve eğitim sahaları konusunda ciddi bir tecrübemiz var. En çok ihracatını gerçekleştirdiğimiz iş kollarından bir tanesi. Pakistan, Güney Kore, Suudi Arabistan'da test ve eğitim sahalarımız var. Canlı simülasyon ciddi bir örnek olan bir kabiliyet, karar destek ve harp çözümlerinde de yine yurt içi ve yurt dışında projeler yaptık.

Yurt içinde yaptığımız simülatörlerin atıl zamanlarını değerlendirme amacıyla dost ve müttefik ülkelerden pilotlara eğitim satıyoruz. Buradan bir gelir elde edip silahlı kuvvetlerimize katkı sağlıyoruz. Kendi yaptığımız veya kendi yapmadığımız farklı eğitim sistemlerinin entegre lojistik destek hizmetlerini sağlıyoruz.

Buradaki yeni teknolojiler dediğim literatürde tarama yaptığınızda ortada görebileceğiniz teknolojiler. Bunların bazılarında biz Havelsan olarak birtakım çalışmalar ve projeler yapmaktayız. Bunlardan en bilindik olan Artırılmış Gerçeklik (AR), Karma Gerçeklik (XR) ve Sanal Gerçeklik (VR) teknolojileri. Bunlar özellikle yüksek sadakat seviyeli dış dünya ortamını modelleyerek, özellikle eğitim sistemlerinde gerçeğe çok yakın bir ortam sağlıyorlar. Bunlar eğitim sistemlerinde özellikle farkındalığı artırmak ve hızlı karar alma konusunda çok yardımcı oluyor. Eğitim alan personele VR teknolojisinde çatışma simülasyonları, oyun motorları da dahil olacak şekilde hizmetler sunuyoruz. Yurt içinde ve yurt dışında birtakım ürünlerle bu alandaki kabiliyetlerimizi sergiliyoruz.

XR teknolojisinde de gerçek ve sanal öğelerin aslında bir arada bulunduğu bir ortam oluşturuyoruz. Mesela tatbikat sırasında AR gözlüklerle birlikte gerçek kokpit içerisinde sanal dış dünya ile farklı bir ortam sunuyoruz. Buradaki teknolojiler daha teorik ve aynı zamanda yeni teknolojiler. Beyin bilgisayar arayüzleri, haptik teknolojiler gibi. Eğitim alan personelin beyin dalgalarının ölçülerek hangi eğitimlerin hangi aşamalarında stres seviyesinin yükseldiğini, bu stres yönetiminin nasıl yapılabileceğini algılamaya yarayan sistemler. Bunlar şu anda eğitim sistemlerinde son zamanlarda kullanılmaya başlayan sistemler oldu. Ama bu dalgaların, yani beyin dalgalarının algılanması için kullanılacak olan donanımlar çok karmaşık ve kullanıcı dostu olmayan donanımlar. Bu nedenle kullanımı zor oluyor, çok tercih edilmiyor ama spesifik, kişiye özel uyarlanabilir eğitim sistemleri özelinde kullanılabilecek olan sistemler olarak görüyoruz.

Haptik sistemler özellikle sanal ortamlarda bir takım duyu hislerini almak, önemli halde olabiliyor. Örneğin çatışma simülatörü veya kokpitteki pilotların hissetmesi gereken durumlar gibi. Vücudunuza giydiğiniz birtakım kıyafetlerle vurulma, dokunma, bir silahı gerçekçi hissetmenizi sağlayan sistemler bunlar. Gömülü eğitim sistemleri, artık en çok kullanılan sistemlerden biri. Özellikle simülatörler biliyorsunuz sadakat seviyeleri birtakım sertifikasyonlarla sağlanabiliyor

. Bir simülatörde alınan eğitim, hiçbir zaman gerçek bir platformda alınan eğitimin yerini tutmuyor. Çünkü gerçek platformda bu işin içerisinde stres var, birtakım. Özellikle harp zamanında, mesela dog fight (it dalaşı) esnasında vücudunuzun salgılamış olduğu birtakım hormonlar dolayısıyla karar verme yeteneğinizi etkileyen faktörler var. Bu nedenle gömülü eğitim sistemlerinde, yani gerçek platform üzerinde sanal bir eğitim alma konusu şu anda çok revaçta. Bu kapsamda Havelsan olarak biz de hem Kaan uçağının hem de Hürjet uçağının gömülü eğitim sistemini TUSAŞ'la birlikte geliştirmeye çalışıyoruz. IDEF fuarında da sürpriz bir sunumumuz olacak. Burada amaç sanal ortamda oluşturulan birtakım kuvvetlerin gerçek platformun içerisinde, örneğin bu bir uçaksa, tanksa bununla ilgili tehditlerin ekranlarda görülmesi. Elektro optik sistemlerinde bulunan sembolojilerin oluşturulması gibi düşünülebilir.

Özellikle yeni nesil uçaklarda çok kullanılan bir teknoloji de yapay zekâ. Bu eğitim sistemlerinin olmazsa olmazı. Özellikle performansı izlemek ve bu performansa yönelik de yapay zekâ tabanlı, insana daha yakın kararlar verebilen düşman unsurları gibi birtakım kabiliyetler bu tarz eğitim sistemlerinde ve simülasyon sistemlerinde önemli yer tutuyor. Dijital ikiz genelde platformların dijital ikizi diye biliyoruz ama artık biliyorsunuz dijital ikiz, gerçek bir sistemin dünyadaki bir sistemin davranışlarının ve performanslarının modellenerek dijital dünyaya aktarılması. Bu iş sadece platform bazında değil artık, askerlerin dijital ikizi veya sistemlerin, eğitim sistemlerinin veya kullanılan başka sistemlerin dijital ikizi olarak düşünüp bunların eğitim sistemlerine uyarlanması olarak görüyoruz.

Son dönemde gerçek zamanlı verilerle toplanan birtakım verilerin, özellikle yapay zekâyla da değerlendirilip, bunların eğitim planlamasındaki rolü konuşuluyor. Biyometrik geri bildirim sistemleri şu an da bu da çok yeni bir teknoloji. Özellikle askerlerin harp ortamında ve eğitim ortamında biyometrik verilerinin toplanarak analiz edilmesi. Yine yapay zekânın da işin içinde olduğu yazılımlarla bunların analiz edilerek yine kişiye özel eğitim konseptinin ortaya çıkması, bu kişiye özel eğitim yapılması. Artık günümüzde çok kullanılmaya başlandı. Eskiden eğitim sistemleri standarttı ve herkese aynı eğitimler veriliyordu, artık bu konseptten çıkıyor dünya.

Çünkü herkesin kabiliyeti, herkesin anlaması, herkesin eğitim ihtiyacı bir değil. Kişiye özel yaptığınız zaman bunu daha etkin ve daha maliyet etkin de bir eğitim sistemi kurabiliyorsunuz. Mesela çok yeni bir ifade, warfighter dijital twin, yani askerlerin dijital ikizi. Yani artık harp sahasındaki askerlerinizin sanal ortamda dijitalleştirilmesi, sanal dijitalleştirilmesi. Bunu da izlemeniz, bu kapsamda çok teorik şu anda literatürde de. Askerlerinizin performansını izleyebilirsiniz, harp alanındaki veya eğitimdeki durumları da kabiliyetlerini de buna göre planlayabilirsiniz.

Batte Space olarak adlandırılan hologram masası, sanal kum sanığı. Bunlar da artık dijital ortamda arttırılmış gerçeklik ve sanal gerçeklik gözlükleriyle, özellikle harp alanının eğitim ve dijitalleştirilmesi alanındaki teknolojiler. Aslında dünyaya baktığınız zaman bunun çok uygulaması var. Biz de de en son güncel teknolojilerle yeni eğitim merkezleri kuruluyor. Özellikle bir harp zamanında o kadar stres altında bir yaralıya müdahale etme, kritik önemde. Bu kapsamda tam da doğru zamanda doğru müdahaleyi yapmak, bunu çok kötü koşullar altında yapmak, baskı altında, ateş altında yapabilmek ve bunları doğru yapabilmek çok çok önemli. Bunu ölçen sistemler ve eğitim simülasyonları, dijital maketler var. Jandarma için bu kapsamda bir eğitim merkezi kuruldu.

Görsel artırma sistemi, özellikle askerimizin bir alana operasyon yapmadan önce bu alandaki, daha önce olmuş olayları gözlüğüne yansıtarak durumsal farkındalığının artırılması. Bunu eğitim platformlarında da kullanabiliyoruz. Özellikle yansıtılacak olan verinin ne olduğu, simülasyonlarla sağlanabiliyor. Bu gerçek harp alanında da kullanacak bir sistem olarak karşımıza çıkıyor.

Biz neler yaptık bu zamana kadar bu teknolojilerle. HRV ile mental iş yükü ölçümü projesi kapsamında aslında kalp atımları ile ilgili bir sinyal analizi yaptık. Bu sinyal analizini yaptığınız zaman birçok şeyi anlamlandırabiliyorsunuz. Jandarma havacılıkla bir çalışma yaptık bu kapsamda. Vücutlarına yerleştirilen birtakım sensörlerle özellikle görev esnasında ne gibi farklılıklar yaşıyorlar, hangi aktiviteyi sadece görev esnasında değil, aslında hangi aktiviteyi yaparken 24 saat içinde kalp grafiğinde değişiklikler oluyor.

Bunu da bir analiz yazılımıyla analiz ederek pilotlarımızın mental yüklerinin ne olduğunu, performanslarının, fiziksel performanslarının ne durumda olduğunu raporladık. Özellikle stresli görevlerde, komutanlara bir geri bildirim olarak sunduk.. Bunun bir sonraki adımı da bunun eğitim sistemlerinde yaygınlaştırılması ve daha küçük giyilebilir teknolojilerle uygulanması şeklindeydi

Genius 2.0 yine Savunma Sanayi Başkanlığımız ve ODTÜ MODSIMMER ile beraber gerçekleştirdiğimiz bir proje. Beyin dalgalarının ölçülerek pilotun bilişsel yükünün hesaplanıp bunu da eğitim sistemlerine, aktivitelerde, eğitim sırasında yaşadığı zorluklar, hangilerinde strese giriyor, hangi tepkileri veriyor gibi tepkileri ölçmek için gerçekleştirdiğimiz bir proje.

Five projesi ise simülasyonlarda, simülatörlerle uçmak gibi bir kabiliyet. Ama asıl önemli olan şey, taktik ortamın oluşturulması. Yani sadece simülatörlerle uçmak değil, aynı zamanda o taktik ortamda, bir takım düşman kuvvetlerinin ve farklı kuvvetlerin de içinde olduğu simülasyon ortamında sadakat seviyesini artırmak asıl amaç. Five ürünü, atak helikopteri simülatörü kapsamında gerçekleştirilen bir taktik ortam yazılımıydı, kural tabanlıydı.

Şu anda yapay zekâ tabanlı birtakım tekniklerle daha da akıllı hale getirildi. Şu anda bütün silahlı kuvvetlerimizin elindeki simülatörlerde bu ürün kullanılıyor.

Simülasyon dediğimizde gömülü eğitim sistemlerinde aslında bunu üç başlığa ayırıyoruz. Canlı, yapısal ve sanal olarak ayırıyoruz. Bu üç simülasyon tipini de gömülü eğitim sistemlerinde birleştiriyoruz. Yani gerçek platform üzerinde sanal varlıklarla bir simülasyon koşuyoruz. Bu da platform üzerinde fizyolojik etkileri de ön plana çıkartarak, onların da yaşanmasını sağlayarak gerçek harp ortamının kullanıcıya simüle edilmesi şeklinde geri dönüş sağlıyor. Kaan ve Hürjet'de de bu sistem kullanılacak.

Gelecek nesil eğitim konsepti sistemlerine baktığımızda, hava savunma sistemleri, bütün akıllı sistemler, karar destek sistemleri gibi bütün platformların simülatörlerle, gerçeğe yakın bir arazi alt yapısıyla, yani dış dünyaya sanal ortamda bağlanarak uçtan uca bir konsepte büründüğünü görüyoruz.

Şu anda dünyada da artık buna uygun birtakım entegrasyonların yapıldığını görüyoruz. Artık platformlar, gerçek savunma sistemleriyle entegre ediliyor, platformlar simülatlörlere bağlanıyor ve entegre ediliyor.

Bir harp alanı simüle edilerek gerçek bir harp içinde hissettiren gerçek platformlarla eğitim gündeme geliyor. Bir uçak için düşünülecek olursa, uçuş eğitiminden gerçek tehditlerin olduğu bir sahada atış ve kaçma manevra eğitimlerinin sağlanması, it dalaşı gibi durumlar için gerçek platform üzerinde en gerçeğe yakın sanal ortamlarla eğitim kabiliyeti sağlıyorsunuz. Bunlar uyarlanabilir eğitimler oluyor, eğitim planlamanızı istediğiniz gibi, aldığınız verileri de hesaba katarak uyarlama imkânı sunuyor. Maliyet etkinlik de bu sistemlerde önemli avantajlar sunuyor. Analitik, veriye dayanan sonuçlarla özellikle daha gerçekçi, daha iyi analiz ve gerçek verilerle, kuvvetin ne durumda daha iyi görebileceğiniz bir alt yapı oluşturulabiliyor.

Multi domain platform, yani müşterek çoklu alan kontrol sistemleri, sadece kara unsurlarının değil deniz ve hava kuvvetlerinin, diğer unsurların da bir arada olduğu bir eğitim ortamı gerçeği daha iyi yansıtacaktır. Buradaki en önemli konulardan bir tanesi de tabii ki gerçek harp ortamına hazır olma. Bu da eğitimle oluyor. Özellikle sadakat seviyesini artırdığınız zaman ve bu entegrasyonu uçtan uca sağladığınız zaman, personelinizi daha etkin bir şekilde harbe hazır hale getirmeniz mümkün olabilecek. Harp ortamının etkilerine baktığımız zamanda tüm seviyelerde özellikle erden tugay seviyesine kadar simülasyonlarla, simülatlörlerle bire bir harp ortamını tecrübe etmiş personel alt yapısı sağlanabilir. Özellikle bireyselleştirilmiş eğitimlerle eğitim planlarının yapılması, tam olarak hazırlanmış bir personel için çok önemli hale gelecektir. Kapsamlı eğitimlerle özellikle karşı kuvvetleri ve operasyon ortamını tanımak, bir yere operasyon yapmadan önce o operasyondaki ortama en yakın atmosferi sanal ortamda yaşatmak, sonucu etkileyecek ve daha etkili olacaktır.



Orhan Ertuğrul GÜÇLÜ
TÜBİTAK

Herkese merhaba, sunumunu yapacağımız kabiliyetimiz herkesi ilgilendiriyor. Çünkü biz Millî Savunma için Millî Ar-Ge diyoruz. Bizim temel motivasyonumuz özellikle eksik gördüğümüz noktalarda elimizdeki kabiliyetleri sektöre sunmak. Aslında S-Force'un temel dayandığı noktada geleceğin simülasyonu ve geleceğin savunma ortamı diyebiliriz. Bu noktaya nereden geldik, önce bir girizgâh yapayım. Tübitak Sage'nin 50 yıllık

geçmişi var, bir 25 yıllık da aslında mühimmatlar tarafından çok ciddi bir geçmişi var. Mühimmatlar tarafındaki geçmişimizin aslında temel dayandığı nokta, 25 yıl öncesinde de modelle kabiliyetimiz. ODTÜ'de bir güdüm kontrol laboratuvarı olarak kurulduk. Aslında bizim ilk çalışmalarımız modellemeye dayanıyor. Biz önce kağıtlar üzerinde çizimlerle başladı, sonra teknolojinin gelişmesiyle beraber sayısal ortama aktarıldı. Sonrasında da birtakım analizlerle sürecimizi hızlandırabilir olduk. Şimdi bir hava füzesinden örnek verelim. Göktuğ füze varyantları yapıyoruz hem görüş içi hem de görüş ötesi olmak üzere. Bunlara baktığımızda muadil olarak füzelerimizde eğitim 120 olarak geliyor, eğitim 120'nin sertifikaya olan versiyonu yaklaşık 780 atış sonrasında sertifikaya oldu. 780 füze atıldı. Göktuğ füzesinin ilk fazını kapatıyoruz, bu kapanışında ilk dayandığı noktada aslında biz benzetim geçmişimiz, modelleme simülasyon geçmişimiz geliyor.

Burada temel noktamız da şu. Biz 17-18 atışla Göktuğ füzesinin ilk fazını kapatabiliyoruz. Peki bunu nasıl yapıyoruz? İşte modelleme, simülasyon tarafındaki kabiliyetlerimiz. Modelleme simülasyon çok önemli. Çünkü maliyet etkin bir çözüm, dünya tarafından kabul görmüş ve herkesin kullanması durumunda, çok ciddi anlamda kendilerine fayda sağlayacağı bir yöntem. Evet eğitim teknolojilerimiz var, mühendislik tarafımız var, Havelsan'dan Mehmet Bey de bahsetti, özellikle Havelsan'ın yaptığı çok ciddi güzel çalışmalar var. Aslında ülkemizin maliyet etkin platform sistem, mühimmat geliştirmesinin önünü açıyor.

Bizim de aslında temel motivasyonumuz bu. Bu kadar az satış sayısı ile başarıya ulaşabilmemizdeki yegâne sebep bu. Çünkü o atıştan öncesinde, biz o mühimmatı gerçek ortamda, yani savaş ortamının dijital ikizi ortamda gerçekleştiriyoruz atışlarını. Aslında kandırıyoruz ve o mühimmatın algoritmalarını, o kartın içindeki algoritmaları çalıştırıyoruz. Çalışmasıyla bir orada hatalarımızı görebiliyoruz. Tabii ki çok geniş bir uzaydan bahsediyoruz, biz bunu daraltabiliriz. Ama her atışta da edindiğimiz bilgi birikimini, modelleme, simülasyon ortamına aktarabiliyoruz. İşte S-Force'un dayandığı nokta bu.

S-Force'da birçok kabiliyet var. Bir mühimmatı simülasyon ortamında gerçekten atıyormuş gibi kullanabiliyoruz, bir mühimmatı geliştirdik, artık birtakım algoritmalara ihtiyacımız var. Çünkü bir gemi görev grubuna şu anda seyir füzelerimizden, SOM'dan kaç tane atacağız, nasıl atacağız, hangi noktalardan bu mühimmatlar gelecek, bu mühimmatlar geldiğinde son noktada nasıl manevralar yapacak? Bu kısımlar çok kritik. İşte bu kısımları analiz edebildiğimiz ortam S-Force oluyor. Bütünleşik bir şekilde bütün testlerimizi yapabildiğimiz ortamın adı S-Force.

Uzun yıllardır kullanıyoruz, belli bir noktada belli kabiliyetleri dünya genelinde kullanılıyor ve yüzlerce, binlerce aslında lisansı oluşturulmuş bir yapıdan bahsediyoruz. Şimdi biraz detaylarına girelim, bu noktada S-Force nedir? S-Force'un açılımı Smart Framework for Operational Research Environment (Operasyonel Araştırmalar İçin Akıllı Muharebe Ortamı). Yani burada ne yapmaya çalışıyoruz, temelde merkezimizde operasyonel analiz var. Bir şeyin hangi sistem olursa olsun, hangi platform olursa olsun, hangi mühimmat olursa olsun, öncelikle operasyonel sahada etkinliğine bakıyoruz. Zaten temel dayandığımız nokta da burası. Savaş ortamının dijital ikizini oluşturuyoruz. Evet, simülasyon ortamlarımız var, taktik ortam benzetimimiz var, mühimmatlarımız uçuyor, hedefi vuruyor. Hedefte vurduğu değer üzerinden bir karar veriliyor, işte hedef yüzde bir birim zarar oluşturuldu, yüzde 50, yüzde 70 zarar oluşturuldu. Bunlar gerçekçi değil, bir dijital ikiz değil. Dijital ikiz dediğimiz şu, gerçekten bir savaş ortamında aynı durumu yaşasak, hedefteki tahribat, hedefe ulaşım, hedefe giderken sergilediği performans, seyir devam ederken hava savunma sistemleri tarafından yakalanıyor muyuz, görülüyor muyuz, görüldüğümüzde vuruluyor muyuz?

Bunu aslında analiz edebildiğimiz bir ortama ihtiyaç var. Operational Research'ın temel dayandığı iki değişken Survivability (Hayatta Kalma) ve Lethality (Ölümcüllük). Yani önce hayatta kalacağız, sonra da hedefi yok edeceğiz. Bunu analiz edebildiğimiz bir ortam burası. Peki amaç olarak geldiğimizde ilk olarak savaş ortamının dijital ikizi dedik, burası çok önemli, neden önemli? Savaş ortamının dijital ikizi çok geniş bir kavram. Biz neyi dijitalleştiriyoruz, hedef üzerindeki etkimizi, mühimmatlarımızın sayısı, kaç tane mühimmat attık, kaç tane mühim atmamız lazım, bir Arleigh Burke sınıfı destroyere kaç tane SOM füzesi atmamız lazım, tek bir gemiye kaç tane, SOM'la biz bu gemiyi vurabiliyor muyuz? Bunlar çok önemli noktalar. O yüzden bu ortamın hazırlanabiliyor olması gerekiyor ki analiz yapabilelim.

Diğer bir noktada karmaşık senaryolar oluşturma. Karmaşıklık buradaki aslında kilit nokta. Karmaşıklık seviyesini artırdıkça, aslında kompleksiteyi artırdıkça, neyi sağlıyorsunuz? Bir yandan gerçekçi bir ortama ulaşıyorsunuz ama bir yandan da aslında zor hesaplanan bir ortamı ortaya koyuyorsunuz. İşte Tübitak Sage'nin de bundan önceki geçmiş yıllardaki tecrübesini yansıttığı nokta burası. Bir simülasyon ortamımız var, modelleme kabiliyetimiz var. Farklı farklı çözünürlüklerde aynı ortamda yeri geliyor 2 bin tane unsur hesaplanabiliyor. Aynı ortamda yeni yine aynı ortamda çok yüksek çözünürlük modellerle 10-15 platformla tek bir bilgisayarda koşum olarak analiz yapabiliyoruz.

Etmen tabanlı görevler çok önemli. Çünkü siz savaş ortamında farklı farklı unsurlarınız var, her birini yönetemezsiniz. Ama onlar için bir takım kural dizileri tanımlamanız gerekiyor. İşte ben hava savunma sistemimde şu noktada görürsem ya da şu sinyal seviyesinde görürsem şu ateşlemeyi yapacağım. Bunu bir kural olarak tanımladınız, ortama koydunuz ve füze odaklı, platformunuz odaklı bir analize başlıyorsunuz. Ne yapıyorsunuz, ben füzemi şu noktadan attım, bu noktada dolaştı, hedefe ulaştı mı? Bu hava savunma sistemiyle, yani sizin burada mümkün olduğunca her türlü unsur için otomatik görev oluşturabilme kabiliyetiniz var. Ve önemli nokta bu. En başında da söyledik, operasyonel analiz ve karar destek operasyonel analiz sadece platformlar ortaya çıktıktan sonra yapılan bir analiz değil. Konsept çalışmaları, doktrinler kapsamında da kavram çalışmaları bu ortamlarda yapılır.

Oturumun teması geleceğin askeri. Peki geleceğin askeri nasıl olmalı? Geleceğin askeri nasıl olmalı sorusunun cevabını vereceğimiz ortam da burası oluyor. Yani hangi kabiliyetleri olmalı, hangi sistemler üzerinde olmalı. İşte diyelim ki lazer silahıyla zarar görmesin, başka silahlarla zarar görmesin, termobarik silahların etkisi minimum olsun gibi tüm olmasını istediğiniz özellikleri analiz edebileceğiniz nokta burası. Eğitim ve personel geliştirme noktasına baktığımız zaman temel odaklandığımız nokta, hava, kara, deniz, her bir kuvvetimiz kendi bazında çok güçlü. Buraya tek bir şekilde vuruşunuzda iyi etki oluşturabiliyorsunuz, ama bu üç kuvvetin bir arada aslında organizasyonu çok daha önemli burada. Biz de mevcut karar vericilerimizin bu ortamda müşterek harekât yapabilme kabiliyeti konusunda kendilerini yetiştirmelerini istiyoruz, bu ortamı hazırlıyoruz. Belirli alt yapılar var, yurt dışından temin edilen yazılımlar var. Ama temelinde modelleme eksikliği var, yani sahanın dijital ikizi yok. Orada bir takım olasılık tanımlamalar yapılıyor, yapılan tanımlamalarla analizler yapılıyor. Mevcut kabiliyetimizin etkisini göremiyoruz. S-Force bu noktaya geliyor. Savunma Sanayi'nde inovasyon, geleceğin askeri konseptinde de gelecekte ne olmalı, gelecekte nasıl bir savaş ortamı bizi bekliyor sorusu var. Biz, S-Force ile su altından uzaya kadar bütün unsurların modellenenebildiği bir ortam oluşturmuş oluyoruz. Gelecekte nasıl bir ortam olacak? Uzayda uydularımız mevcut kalabilecek mi? GPS kesildi, mühimmatlarımızın etkisi ne olacak? Bir yeri hedefliyoruz, 5 mühimmatla imha edeceğimizi düşünüyoruz, GPS'imizi kaybettik ne olacak? Yeni sistemler gerekiyor mu? Bunları analiz edebiliyor olmamız gerekiyor.

Peki getireceği faydalar? Stratejik karar alma yeteneği. Şimdi bir platform geliştiriyorsunuz. Çok önemli bir platform, ülkenin geleceğini belirleyecek bir platform. Bunda diyorsunuz ki bütün teknolojiler olsun, şu kabiliyetler olsun, bunlar olsun. Bir bakıyorsunuz ki o platform yapılamaz hale geliyor. Peki bu platform ne zaman hizmet edecek? 20 yıl sonrasında. 20 yıl sonrasında hizmet edecek bu platformda gerçekten bu sistemler böyle mi olmalı? 20 yıl sonrasında bunlar kabiliyet mi? Bunları analiz etmek gerekiyor. Bunları analiz ettiğiniz zaman karar vericinin önüne şunu koyuyorsunuz; ben bir platform yapacağım, benim sınırlarım bunlar. Şunlardan birkaçını seçip bu havuzu doldurman gerekiyor. Özellikle hava platformu üreticileri için çok önemli bir kavram.

Operasyonel verimlilik, evet platformlar ortaya çıktı, müşterek harekât yapacağız ya da birleşik harekât yapacağız. Bu birleşik harekatta diyelim ki bir noktaya hava saldırısı düzenlenecek. Bu hava saldırısında gerçekten F-16 platformu mu, Kaan mı gitmeli, insansız hava araçlarıyla bunu yapabiliyor muyuz? Çünkü maliyet etkin çözüm, en önemli çözümdür. Bakın bu konuda en iyi ülke aslında İngiltere. Bu işi çok iyi yapıyorlar. Özellikle II. Dünya Savaşı'nda Almanya'nın sahip olduğu hava gücünün daha azına sahip olmalarına rağmen Almanları kendi hava sahalarına sokmadılar. Çok ciddi taktikler geliştirdiler ve hangi noktada hangi güçlerini konuşlandırmak gerektiğini çok iyi biliyorlardı. Aslında bizim sahip olmamız gereken kabiliyet bu. Buna sahip olduğumuz zaman sonrasında aslında elimizdeki gücü tekil olarak çok güçlüyüz, belli platformlarda çok iyi platformlarımız var ama bunu birleştirdiğimiz zaman nasıl bir kuvvet çarpanı ortaya çıkıyor bunu bilmemiz gerekiyor.

Modelleme ve simülasyonun maliyet tasarrufu zaten ortada. Bunun için ülkemizde binlerce çalışanı olan bir savunma sanayi şirketimiz var. Bu teknolojinin ne kadar etkin olduğunu ne kadar önemli olduğunu ve ne kadar fayda sağladığını görüyoruz. Bir de savaş ortamı var, bazı platformlarımızı savaş ortamında etkinliğini görebiliyoruz. Savaş ortamında etkinliği görmeyelim, dijital ikizin ortamında görelim, gerçek etkinliğini orada görelim, algoritmaları geliştirelim, daha az kayıplarımız olur. Daha az insansız hava aracı düşer, daha az mühimmat sarfiyatı olur. Önemli olan da bu. Güvenlik ve ulusal savunma konusunda da hava, kara ve deniz kuvvetimiz çok güçlü ve bunları birleştirdiğimizde üç katından çok çok fazla güç elde edeceğiz, daha büyük bir güç çarpanı olacak. İnovasyon ve platform geliştirme bizim çok faydalandığımız bir durum. Biz hangi mühimmatları geliştirmeliyiz? 20 yıl sonra nasıl bir ortam olacak? Mesela Göktuğ füze varyantlarından bahsettik, mesela 20 yıl sonrası için ben size bir öngörü söyleyeyim, İHA'lardan atılan hava savunma füzeleri çok daha önemli olacak. Özellikle küçük İHA'lardan, TB2'den, TB3'ten. Bu kısım çok önemli. Bunu nasıl elde ettik? Çünkü dünyanın trendine bakabiliyorsunuz, ülkelerin sahip olduğu kabiliyetlere bakabiliyorsunuz. Bir dost ülkemiz F-35 son seviye platformu alıyor, biz alamıyoruz, ne yapacağız diyoruz. Halbuki 20 yıl sonrasında çok çok daha farklı senaryolar var. Bunu çalışabiliyor olmak gerek. Temel konumuzun da bu olması gerekiyor.

Büyük veri analizi ve sürdürülebilirlik konusunda da bir takım tekil senaryolar oluşturuyoruz. Tekil senaryolar oluşturduktan sonra konsept senaryolar oluşturuyoruz. Bunu arka planda yığın koşuma gönderiyoruz. O senaryo üzerindeki belli başlı parametreleri değiştirerek, düşman unsurunun sahip olduğu füze sayısını ya da füzenin hızlarını ya da sizin savunma konuşlanmanızdaki bazı unsurları gibi belirli koşulları değiştirerek milyonlarca konseptte senaryonun koşulunu alıyorsunuz arka planda. Bu da size aslında büyük bir veri elde etme imkânı sunuyor. Büyük veri ve sentetik veri ama dijital ikiz üzerine oluşturulmuş bir sentetik veri. Çok kıymetli, bu da sizin aslında sürdürülebilirliğiniz yönünde size büyük bir kapı açıyor.

S-Force'a bakıldığında içinde 5 adet komponent var. Sensör, kinematiks, taktik ortam benzetici, yeni koşum tarafları, sfate dediğimiz dünyada yüzlerce kullanıcısı binlerce lisansı oluşturulmuş bir yapı. Burada eski kabiliyetlerine bakarak, içerisindeki modeller artık elimizde bir istihbarat verisi var. O veriyi eşleyebileceğimiz seviyeye getirilmiş durumda. Birçok görev yazabiliyorsunuz, harp oyunu konsepti yapabiliyorsunuz.

Harp oyununda önemli nokta, sizin savaş ortamını mümkün olduğu kadar gerçekçi oluşturabilmeniz. Bunu yapabildiğiniz sürece aslında doğru bilgiler görüyorsunuz. Bir dog fight durumunda, bir hava angajmanında, özellikle görüş içi angajmanda füzenizin çokluğu önem arz ediyor. Füzenizin hızından ziyade, menzilden ziyade, kaç tane füze taşıdığınız önem arz ediyor. Sabit kanatlı uçaklardan deniz unsurlarına bütün sistemleri modelleri modelleyebiliyorsunuz, farklı farklı çözünürlüklerde. Benim elimde bu platformu tanımlayacak 5 tane parametre var, burada tanımlayabilirsiniz. Ortamın esnekliği de buradan geliyor. Aynı senaryo içerisinde farklı farklı unsurları çalıştırarak analiz yapabiliyorsunuz. Simülatör entegrasyonu yapılabilir. Özellikle pilot gerçek bir savaş ortamında bir hava savunma sistemine karşı angajman yapabiliyor mu, pilotun ona karşı etkinliği nasıl, hava savunma sisteminin attığı füzeden kaçınabilir mi? Bunları analiz edebiliyor. Çünkü gerçekçi bir ortam var. Orada tek başına platformun modeli, sistemi yeterli değil. Yerdeki sistemler de çok önemli. Onları nasıl tanımladığınız çok önemli. Onları nasıl tanımladığınız çok önemli. Platform geliştirirken özellikle yerdeki sistemi bilmek gerekiyor. Diyelim ki füze menzilimiz 100 km, hızı da 4 mach, gelen füzenin.

Bunun 100-120 km ya da 4,5 mach hız da çalışmalısınız ki, geleceğin ortamını gözlemleyebilesiniz. S-Force aslında bir ürün gamı ve birden fazla ürünü var. Temel olarak taktik ortam benzetici, bizim dijital ikizi oluşturduğumuz, içerisindeki modellerin elimizdeki bilgilerle bu sahne ortamında gerçekçi tanımlayabildiğimiz orta SFate. Bunun altında sensör modellemesi detaylı. Sensörden kastımız optik sistemler, radar sistemler, diğer sistemler, hepsini tanımlayabilirsiniz burada. Kinematik, önemli bir konu ve bizim 30-35 yıllık modelleme kabiliyetimizden geliyor. Farklı farklı çözünürlüklerde platformları burada tanımlayabiliyorsunuz. Hava, kara, deniz aracı, füzeler gibi.

Vision 3D, bir sahne ortamı oluşturdu, gerçekte nasıl görünüyor? Konsept senaryoyu oluşturan kullanıcı gerçeğe yakın sahne ortamını görmek istiyor. S-Craft ürünüyle de konsept senaryonun bazı değişkenlerini değiştirerek milyonlarca koşup kararlılık, duyarlılık ve ödünleşme analizlerini yapabiliyorsunuz. S-Sensör, kendi içinde bir radar modeli var ya da optik sistemi var. Bunların kendi algoritmalarının olması gerekiyor. Görüntü işleme algoritmaları olmalı. Ben bunları farklı ortamlarda geliştirdim. S-Sensör ile algoritmalarınızı tam olarak entegre edebiliyorsunuz. Bu da sizin algoritmalarınızı tam olarak test edebilmenizi sağlıyor.

S-Kinematics, içerideki modellerin güdüm algoritmalarının çalışmasını sağlıyor. Bir takım algoritma çalışmak istiyorsanız bunu yapabiliyorsunuz. S-Vision3D gece görüşü, infrared görüntü, farklı farklı görüntüleri oluşturma imkânınız var. S-TDL taktik data link işlevi görüyor. Dünyada bir takım özellikle bu tarz yazılım ürünlerini ortaya koyan firmalar var. Ama dünyada bir kullanıcının ihtiyaç duyabileceği bütün sistemleri içerisinde barındıran bir tane bile çözüm yok. Taktik data link çalışması hiçbir simülasyon ürününün içerisinde entegre edilmiş bir şekilde son kullanıcıya ulaştırılabilir bir noktada yok. Burada taktik data link emülatörü veya gerçek taktik data link ile bağlanabiliyor.

S-RT DEVKİT ise Göktuğ füzesinde verdiğimiz, 700-800 tane füze atmamızı engelleyen bölüm. 700-800 tane atmak demek 700-800 milyon dolar demek. Bunun temelinde SRT-DEVKİT ile oluşturduğumuz gerçek zamanlı o kartların dış dünyadan ihtiyaç duyduğu verileri ortaya koyabilmektir. Linux ortamında çalışır. S-FATE ile birlikte çalışır, S-FATE sahne ortamını oluşturur.

SRT-DEVKİT ise o kartın ihtiyaç duyduğu IMU, GPS simülatörü gibi farklı farklı simülatörleri kullanarak dış dünyadan ihtiyaç duyduğu verileri oluşturmalarını sağlar. S-FTA taktik ortam benzeticiyiz, gelişmiş taktik ortam benzeticiyiz. Smart Frame Work Advanced Tactical Engine bizim için önemli, çünkü içerisindeki modellerin artık gerçek seviyesi dijital ikiz seviyesinde.

S-Craft ile yığın koşumu alabiliyoruz. Tekil senaryoda duyarlılık, kararlılık, ödünleşme analizlerini yapacaksınız. Sensör, mümkün olduğunca kullanıcının her türlü elindeki parametreyi tanımlayabilmek için kullanılabilir. Bu altyapı Aselsan'da, Tutaş'ta ve diğer ortamlarda da bu kabiliyetle kullanılıyor. Kendi sistemini, kendi etkinliğini yapabilecek şekilde parametrelerin tanımlanabilir olması çok önemli. Radar tarafına geldiğimiz zaman anten, anten paternini, radar statülerini, parametrelerini, PRF değerini dahil tanımlamak ister. Çünkü anten üreticisi bunları tanımlayıp sistemin etkinliğine bakacak, hatta kendi modelini entegre edip algoritmasını test edecek gerçek savaş ortamında. Yine jammer parametreleri olarak baktığımız zaman bu da önemli. Normalde mevcutta jammerda birçok kabiliyet var, sistemler, kabiliyetler var. Ama jammer dediğimiz zaman kullanıcı bunu DRFM mi, Repeater mi, noise jamming mi yapacak, bunu tanımlayabilir ve bununla ilgili parametreleri de tanımlayabilir olması gerekiyor.

Kinematic tarafı zaten 25-30 yıllık bir geçmiş. Biz 2000 unsurlu bir senaryoda hangi seviyede bir model oluşturmam gerekiyor, hangi seviyede bir model oluşturmam gerekiyor, hangi seviyede modellerle bu senaryoyu koşturam gerektiriyor, kinematic ve 30 yıllık birikimin getirdiği cevap burada oluyor. Taktik datalink, biz bu yapıyı işbirlikçi yapıda tutuyoruz. Havelsan, Milsoft ve Simsoft gibi firmalarla kabiliyetlerimizi birleştirelim istiyoruz. Bizim temel pazarımız kendi kuvvetlerimiz, buradaki savunma sanayimiz değil. Temel nokta bunun yurt dışı kullanılabilirliğini artırmak. Yurt dışında ne kadar çok kullanılırsa, o kadar çok bize bir şekilde veri akışı olur, bilgi akışı olur. Biz bunca zaman bu sistemleri kullanırken diyorduk ki, X noktasına bu nasıl yapılır, şu nasıl yapılır? Aslında birtakım bilgiler veriyorsunuz farkında olmadan. Ama bunu kendi içinizde yaptığınız zaman ve yurt dışındaki kullanıcının kullanımına sunduğunuz zaman artık sorular size gelmeye başlıyor. Bu da çok kritik bir nokta.



Dr. Osman Gazi GÜÇLÜTÜRK
GALATASARAY ÜNİVERSİTESİ

Öncelikle merhabalar. Galatasaray Üniversitesi Hukuk Fakültesi'nde Bilişim ve Teknoloji Hukuku alanında doktora üyesi olarak görev yapıyorum. Teknoloji, regülasyon ve politikaları çalışıyorum. Hukukun bildiğiniz gibi çok farklı alanları var. Birazdan değineceğim, silahlı çatışma hukuku, aslında bir nevi şahsına münhasır bir alan ve bunlarla ilgili bazı

hususlardan bahsedeceğim ben size. Temelde ekranda yapay zekâya ilişkin bir vurgu görüyorsunuz ya da insan makine etkileşimine ilişkin bir vurgu görüyorsunuz. Bunun sebebi aslında genel bugün konuşulan diğer hususlarla bağlamak ama ben hukuka yönelik birkaç kavramsal açıdan da kavramsal incelemeden de bahsedeceğim. Şöyle bir planım var konuşmam süresince; aslında kavramsal bir açıklama, sonrasında yapay zekânın özellikle bu kavram bakımından ölümcül otonom silahlar ya da Little Autonomous Weapon Systems diye İngilizceden aslında çevirdiğimiz silahlar için önemi. Ve asıl işin hukuk kısmı ve bugünkü oturumdaki diğer konulara bağlayan bunun insan gözetimi, eğitim kısmıyla alakalı değerlendirmeleri var. Ben buraya bir sıfıncı bölüm eklemek istiyorum, şöyle bir şey bir giriş yapacağım şimdi. Ben burada çıkıp size bir hukukçu olarak aslında birçok kamudaki tecrübelerime dayanırsa, olduğunu düşündüğüm şekilde size bu işin nasıl yapılamayacağını anlatacağımı söyleyebilirdim.

Ama hukuk size bir işin nasıl yapılamayacağını anlatma mesleği değil öyle bir eğilim öyle bir yaygınlık olduğunu görüyoruz bir sürü sektörde. Belki akademide de bu iş böyle fakat hukukun aslında birden fazla olayı var. Bizim tarih yazıcılığının oldukça aşına olduğu bir ifade var; kanla kazandığını kalemle kaybetmek diye. Aslında uluslararası hukuktaki yaklaşım biraz bunun olmasını engellemek için var. Hukuk, ulusal hukuklarda sistemler biraz daha farklı. Merkezi bir kural koyucunun var kurallara uymadığında bu kuralları gelip size zorlayabilecek uymanızı sağlayabilecek bazı mekanizmalar var. Devletin icra mekanizmaları, kolluk kuvvetleri gibi.

Uluslararası hukuk biraz daha farklı ve savunma sanayine girdiğimizde iş, hiçbir devlet, bu sadece bizimle alakalı değil bu çok işin doğası gereği olan bir şey, hiçbir devlet kendi elini kolunu kendi savunma sistemini kendi Millî güvenliğini kendi kurallarıyla bağlamak istemediğinden ulusal hukukun aslında çok fazla temas etmediği bir alanda kalıyoruz. Bunun artısı eksisi var, ayrıca bahsedeceğim özel sektörü çok kötü etkileyebilir düzenlemeler ve nihayetinde özel sektör arasından kamuya geçişleri ve belli bir teknoloji gelişimi inovasyonu kısıtlayabilir. Ama asıl mesele ve konuşacağımız bütün hususlar burada biraz Uluslararası Hukuk altında olacak. Burada yapılan şey aslında, daha önceki oturumlarda farklı muharebe sistemlerinden farklı yeni tip savaşlardan bahsedildi. Burada yeni bir savaş var ve biz buna Warfare'e evrilmiş bir şekilde Low Fair diyoruz. Uluslararası hukuktaki aslında hukuk mücadelesi 'neyi yapamazsınız, neyi yapabilirsiniz değil, neyi nasıl yaparsanız o işten galip çıkarsınız' şeklinde ilerliyor. Bunun tabii çok bariz birkaç tane örneği var. Uluslararası hukukun şımarık çocukları dediğimiz bazı devletler var, bunu artık herkesin bu şekilde atıf yaptığı. Mesela kendinize şunu soruyor olabilirsiniz, hukuk diye bir şey var ama aslında işe yaramıyor. Çünkü bu devletlere hiçbir şekilde etki edemiyor, bunu yapmanın yolları var.

Devletlerin karşı karşıya gelmesinde galip çıkmanın yolları var ya da bir şey kötü giderse ki, zaten hukuk gibi genelde bazı meslekler böyledir, sadece kötü giderse işler karşınıza çıkar ya da kötü gideceğini düşünerek muhatap olursunuz. Daha tatsızdır, yani öyle bir şey olduğunda aslında sizin kendinizi korumanızı sağlayacak mekanizmalar vardır. Bunların hepsine birazdan değineceğim, şimdi sunumun içeriğine girelim zamanımızı kaybetmeden.

İlk olarak ölümcül otonom sistem ölümcül otonom silah sistemleri diye bir kavram var ve bu kavram aslında sandığımız gibi yeni bir kavram değil. Eski oldukça eski bir kavram, çünkü otonom kavramı aslında bizim zamana bağlı değiştirdiğimiz bir kavram. Stanford'un yapay zekâ ile ilgili bir araştırmasında çok güzel şekilde ifade edilen şöyle bir şey söylüyorlar, otonomi de benzer bir kavram; 'Biz yapay zekâ derken aslında o ana kadar görmediğimiz ve o ana kadar insanın yaptığını düşündüğümüz bir şeyi yerine getiren bir kavramı düşünüyoruz ve ona yapay zekâ etiketini yapııştırıyoruz.

Sonra bu normalleşiyor yayılıyor ve yapay zekâ demeyi bırakıyoruz, sonra bir sonraki yeni şeye yapay zekâ demeye başlıyoruz.’ Otonom da otonomide de biz aslında bunu biraz yaptık. Otomasyonla otonomi arasındaki çizginin gerçekten belirginleşme, gerçekten belirsizleşmesi çok yakın bir tarih. Ondan önce aslında arada böyle neydi, belirsiz belirsiz bir çizgi vardı ve içeriğinin nasıl doldurulacağını çok bilmiyorduk.

Ama neden önemli otonomik kavramı hukukçular için? Çünkü hepimiz aslında az çok tahmin ediyoruz hukukçu olmasak bile, sistemlerin, kuralların aslında bir sonuç bağlayabilmesi için, size bir şey zorlayabilmesi için sizin onu bilerek yaptığınızı ya da yapmanız gereken şeyi yapmayarak ona sebep olduğunuzu ortaya koyması lazım. Biz buna nedensellik bağı diyoruz. Eğer ortada otonom bir sistem varsa, otonom bir silah varsa, dolayısıyla kontrol eden kişinin aslında kontrolü çok etkisiz kaldıysa veya yeterince müdahale edemiyorsa o zaman aslında bu bağlar kopabiliyor. Dolayısıyla otonom dendiği zaman, otonomi dediği zaman hukuk sistemleri afalliyor. Çünkü ulusal uluslararası hiç fark etmez hukuk sistemleri aslında belli bir kontrol mekanizması üstüne kurulu. Bunu çektiğiniz zaman ortalık cidden karışıyor, yani ulusal hukuklarda işte kusursuz sorumluluk dediğimiz rejimler var nükleer santral kurarsanız içinde bir şey olursa bundan mesela sorumlu oluyorsunuz. Siz bir şey yapmamış olsanız, her şeyi düzgün yapmış olsanız bile ama devlet mekanizmaları daha farklı işliyor. Uluslararası hukukun etkisi burada devreye girecek. İkincisi ölümcül ifadesinin, ‘Little’ ifadesinin neyi karşılamadığı da çok belli değil. Çünkü aslında her olay uluslararası hukuk seviyesine taşınıp da hatta çatışma seviyesine, yani insancıl hukuk seviyesi var, insan hakları hukuku var. Eğer bir savaş ortamından bahsediyorsak, artık insan hakları yerini büyük ölçüde insancıl hukuka bırakıyor. Çünkü savaş ortamında dahi insan haklarının geçerli olduğunu, temel hakların korunduğunu söylüyoruz ama bir de bunun yanında yepyeni ve gerçekten biraz kaotik bir alan giriyor. Silahlı çatışma hukuku ve silahlı çatışma hukukunda ortada artık gerçekten bazı ipler kopmuş, iki tarafta birbirine zarar verme dur durumunda, bir şeyler yapılacak, bunu engellememiz mümkün değil. Ve kim ne derse desin bir şeyler olacak. Artık orada zararı minimize etmeye, tarafları kontrol etmeye, belli bir uzlaşma bulmaya, odaklanmaya çalışıyoruz.

Ölümcül, o zaman neredeyse her tarafta karşımıza çıkıyor böyle kavramsal etkiler, kavramsal sıkıntılar yaşıyoruz ama bugünkü oturumlarla, yeni silah, yeni savaş ve yeni askerle ilgili olarak en bağlantılı kısmı buradaki insan mekanizmasının rolü. Yani sistemi ne kadar otonomlaştırdık ve üzerine ne koyduğumuzda biz insanı hala kontrol edilebilir seviyede bıraktık ya da bırakmadık. Bunları aslında incelemek gerekecek. Bir tane tanım var, Uluslararası Kızılhaç Komitesi'nin (ICRC) ve diyor ki, "Ölümcül otonom silah sistemi kritik işlevlerinde otonomi sahibi olan, insan müdahalesi olmaksızın arama, tespit, tanımlama ve izleme gibi faaliyetlerle hedef seçebilen ve engelleme, güç kullanma, etkisiz hale getirme, zarar verme veya yok etme gibi saldırı adımlarını gerçekleştirebilen sistemlerdir». Uluslararası alanda çok fazla bu alanda çalışma yapıyorlar ve uluslararası dokümanlara da giriyor bu tanım. 'kritik işlevlerinde otonomi sahibi olmaktan ve insan müdahalesi olmamasından' bahsediyor. Tanım içerisinde böyle bir ifade var ve devamında aslında böyle kendi başına işlevler gerçekleştirmeden bahsediyor, hedefi bulma, tespit etme, belki etkileşime geçme gibi hususlar var.

Burada iki şeyi birbirinden ayırmak gerekiyor, aslında çok konuşuldu ama hukukçular açısından bizim bakış açımızı çok etkiliyor bu ve aslında sorumluluk bakımından da çok etkiliyor. Kullanıcı, operatör, devlet bakımından da yine çok etkileyecek. Destek sistemleri dediğimiz, daha önce de atıf yapılan sistemlerde doğrudan mekanizmayı biz aslında sistemin kendisine bırakmıyoruz. Bazı kararların kolaylaştırılmasında kendisine yer veriyoruz ama nihai etkileşimi insan kararına bırakıyoruz. Sistemlerin büyük bir kısmının bu olduğunu söylemek, şu an için oyunun kuralı bu. Arka planda neler oluyor, nasıl silahlar, nasıl teknikler deneniyor, zaten dediğimiz gibi bunları her zaman görmek mümkün değil. Ama bunu yapmadığınız zaman bazı düzenlemelere takılıyorsunuz ve çok risk aldığınıza dair bir sürü sorun ortaya çıkıyor. Milimetrik zamanlamaların, karar mekanizmalarının, o döngünün daha hızlı tamamlanmasının artık çok daha fazla kayba sebep olabileceği zamanlara geldiğinizde, çıkıp burada, 'Hayır, asla otonom mekanizmalara izin vermeyeceğiz, olması mümkün değil, daima başında orada bir insan tutmalıyız' demek çok doğru bir yaklaşım değil. Bunun birkaç tane sebebi var.

Bir, kayıplarınız çok daha büyük olabilir. Çünkü artık bu dronlar başta olmak üzere işte gördüğümüz o çok daha hızlı otonomi seviyesi yüksek veya uzaktan kontrol seviyesi yüksek araçlarla yapılan artık konvansiyonel parçası saydığımız savaşlarda en ufak beklemenin, tereddüdün etkisi de çok ağır olabilir.

İkincisi, siz bu kadar kompleks yapılan içerisine sözde bir insan faktörü koyduğunuzda, aslında orada, bu karar çok etkili ve gerçek olmuyor. Diyorsunuz ki, 'Tamam, nihai olarak vur emrini sen vereceksin', ama orada bir tane karar destek sistemi var. Ve bana diyor ki, 'Şu an en doğru zaman ya da şurası en doğru konum, burası en doğru hedef'. Ben zaten o anki, yani zaten simülasyon dünyasında bunun kararını vermeye çalışırsanız, bu gerçekte ne kadar etkilidir o ayrı, çünkü hiçbir gerçekçi, gerçek değildir, orada çok ciddi bir risk var. Ama savaşın kendi içerisinde bu kararını vermesini istemek bir insandan, çok ciddi bir insan kaynağı gerektiriyor. Bu sefer bu kadar müthiş silahları bu kadar konvansiyonel kurallarla kullanmak için, aslında var olup olmadığını bilmediğimiz ya da varsa da sayıları çok az derecede tecrübeli ve soğukkanlı insanlara ihtiyacımız var demek oluyor, bu da çok riskli bir yatırım. Çok riskli bir nokta, dolayısıyla tanıımı yapmalı mıyız, yapmamalı mıyız, tanımın içerisindeki unsurları nereye getirmeliyiz, bu başlı başına zaten ayrı bir sorun bizim için.

Peki yapay zekânın buradaki öne ne? Dediğim gibi aslında yapay zekâ şart değil otonomi için. Çünkü otonomi dediğimiz sistemin içeriğinin aslında gerçekten tek başına karar veriyor olmasının gerekip gerekmediği de bir tartışmalı. Tanımın içerisindeki ifadeler zaten farklı. Deterministik karar mekanizmalarını otonomiye sahip karar mekanizması tanıma altına sokabilirsiniz.

Hukukun oyunu biraz budur, yani kelimelerle oyun oynamaz, hukukta zaten mesleğin icabıdır, yapılabilir. Onun haricinde yapay zekâ olduğunda zaten insan müdahalesinin etkisi değişecek. Dolayısıyla bütün bu konuştuklarımızın sınırları gittikçe belirsizleşecek ve son bir şey daha var. Kontrolden bahsedeceğiz, eğitimden bahsedeceğiz, bunu ama ortaya koymak ve gerçekten kontrolün sağlanıp sağlanmadığını iddia etmek çok çok zor.

Çünkü hem eğitim süreçleri değişecek dediğim gibi, hem sistem komplike hale geldiği için artık eğitilmiş olan personellerin de zaten yeni bir eğitimden geçmesi veya anlama kapasitesinin değişmesi gerekecek. Belki artık bir tane mühimmatı kullanmak için ya da tek bir operasyon yapmak için çok daha fazla insana ihtiyacınız olacak. Çünkü teknik bir tarafı var. Üçüncüsü insanı oraya koysanız bile az önce söylediğim gibi etkisinin ne olacağını bilmiyoruz.

Peki bunlar bizi nereye götürüyor o zaman? Bir adım daha ilerleyeceğiz ve şimdi hukukun silah bu düzenlemeleri, yani hukukun bu silahlara bu sistemlere bakışından bahsedeceğiz.

Birincisi burada hukuki yaklaşımın neden önemli olduğu önemli ve ayrı bir tartışma konusu. Bir sürü risk var otonom silahlarda. Bunların bir kere otonomluk, otonomi seviyesinin değişikliğine göre operatörün bulunup bulunmaması, kontroldeki insanın etkisi, uzaklığı gibi bir sürü mesele konuşuluyor. Ama şöyle güzel deneyler var, bunların bazıları düşünce deneyi, bazıları gerçek yapılan deneyler. Bir insan, bir operatör çatışma ortamına ne kadar uzaksa, insan hayatına dair o kadar marjinal kararlar verebiliyor. Buna yabancılaşıma deniyor. Otonom sistemlerde çok ciddi bir yabancılaşıma riski var. Aynı şekilde ortamı görememe, etkileyememe, bilgilerini kullanama riski var. Yani bütün sistemin olayı, askeri, insanı ve konvansiyonel kuvvetleri oradan çekip başka bir savaş alanına iletirmek ve o şekilde mücadelede üstünlük sağlamak üzerine kurulu. Bunların hepsi bizi farklı noktalara farklı risklere getiriyor ve dediğim gibi, ulusal ve uluslararası hukukta aslında iki farklı yaklaşım görüyoruz. Çünkü ulusal hukuklar devletin elini, kolunu, kendisi bağlamak istemediği için bu sistemlerde çok fazla müdahale etmiyorlar. Mesela bizim kişisel verilerin korunması kanunumuz var ama çok güzel bir 28. Maddesi var, açıkça Millî güvenliğe ilişkin veri işlemlerini kapsam dışı bırakıyor, doğası bu normalde de bu.

Avrupa Birliği'nde yapay zekâ sistemine ilişkin şu an dünyanın tamamını etkileyecek bir tüzük var, yürürlüğe girdi ama henüz uygulanmaya başlamadı. Tabii ki diyor ki, Millî güvenliğe, ulusal sistemler ve savunma sanayine ilişkin uygulamalar bunun dışındadır.

Çünkü kimse, hiçbir devlet aslında bunu istemiyor. O zaman burada ne olacak? Uluslararası Hukuk devreye girecek. Uluslararası Hukuk nasıl bir yapı? İmza atılan bir yapı, devletlerin taraf olduğu bir yapı. Ama taraf olmasalar da bazı kurallarla bağlı oldukları, yine de böyle garip arada nüansı olan da bir yapı ve burada biz en çok örgütleri görüyoruz. Birleşmiş Milletler'i görüyoruz, NATO'yu görüyoruz, Avrupa Konseyi'ni görüyoruz. Şimdi bunlar bazı raporlar yayınlıyorlar, özellikle NATO'nun bu ciddi operasyon çalışmaları var.

İşte bu karar alma mekanizmalarına ilişkin durumları var. Amerika'nın kendi içinde yayınladığı, bakın şu önlemler alınmalı, bunları yapmalısınız gibi bir sürü yine ek unsur görüyoruz. Ama nihayetinde bunu acaba biz bunu sahada uygulatabilir miyiz? Bu çok önemli bir sorun haline geliyor. Çünkü, bizim yine ülkemizde var ama uluslararası hukukta da var olan bir şey var, kuralı koymak başka bir şey uygulamak başka bir şey. Dolayısıyla burada dikkat edilmesi gereken şey, aslında olay savaşa gittiğinde, devletlerin nihayetinde birbirlerine güç kullanmaya başlayacağı için, normalde yasaktır ama olmadığını söylememiz imkânsız, güç kullanmaya başladığında ya da konu bir ulusal güvenlik konusu halinde geldiğinde neler yapmanız gerekiyor ki, yüzde 100 güvende kalmalısınız. Zaten yüzde 100 hukuka uygun kalmanız mümkün olmayacak. Yüzde 100 aman kimse kimseyi öldürmesin, yapay zekâ çok güzel kullanılsın, her şey kontrol edilsin demeniz zaten mümkün olmayacak. Ne yapmalısınız ki, buradaki olayı, riski minimize edelim, nasıl eğitimler verelim, nasıl simülasyonlar yapalım, insanlarla nasıl temas edelim, personeli nasıl kuralım gibi soruları sormak gerekiyor.

Burada bir de silahların hukuki incelemesine ilişkin ayrı bir husus var. Şimdi yeni bir şey söylüyormuş gibi olacağım ama aslında bu da çok eski Cenevre sözleşmesinden kaynaklanan bir ek protokolün maddesi. O zamanlar bu öngörüldüğü için uluslararası hukuk çok hızlı değişen bir sistem değil zaten, çok detaylı hususlar haricinde şu deniyor; 'Yeni bir sistem geliştiriyorsanız, bunun içerisinde şunlara bakacaksınız bunlara dikkat edeceksiniz'. Aslında nihayetinde silahlı çatışmalar hukukun içeriğinde olayın, biraz orman kanununa döneceğinin herkes farkında. Dolayısıyla mekanizmalar ona göre kuruluyor, yapay zekânın buraya getiriliyor olması bize bir sürü dikkat edilmesi gereken risk koyuyor.

Evet, ama yapmamız gereken şey hala aynı, iş oraya geldiğinde devleti korumak, ulusal güvenliği korumak, insancıl hukuk ilkelerine, insan haklarının bazı kısımları devre dışı kalıyor, insancıl hukuk ilkelerine uygun bir şekilde oradan minimum zararlar ile ilerlemek oluyor.

Peki burada insan gözetiminin etkisi ne o zaman? Nelerden bahsettik, insan gözetiminde bir kere en önemli şey, anlamlı kontrol denen bir husus. Anlamlı kontrol de öyle, sadece başına bir adam koyduk demekle olmuyor. Çok ciddi eğitim vereceksiniz demek oluyor, çok ciddi sahayı göstereceksiniz demek oluyor. Ama en çok konuşulan şey, güvenilirlik, yani bu sisteme güvenmeniz gerekiyor, sistemin sırtınızı yaslayabileceğiniz bir sistem olması gerekiyor. Bu ne demek? Bu sistem 3 gün sonra dönüp sizin askerinizi saldırmayacak, size saldırmayacak ya da aynı zamanda hem can kaybederken hem zaten kötü bir şey yaşarken, bir de üstüne kan kaybetmeyeceksiniz. Ayrıca itibar kaybı, ayrıca maddi kayıplara uğramayacak.

Bunların hepsine dikkat edebilecek bazı mekanizmalar getirmek gerekiyor ve burada simülasyon sistemlerine ilişkin önemli raporlar, önemli sistemler var. Ama simülasyon sistemleri, mesela İngiltere örneği verildi, İngiltere'nin özellikle silahlı yapay zekânın kullanıldığı sistemlere ilişkin düzenlemelerin tartışıldığı bir meclis oturumunda, çok sık söylenen bir şey vardı; 'İstediğiniz şeyi simüle edebilirsiniz asla gerçek ortamı olduğu gibi simüle edemezsiniz.' Nihayetinde dönüp dolaşıp aslında hem insanlara ek yük getiren hem de konvansiyonel sistemleri korumamız gereken bir yere geliyoruz.

Şunu özellikle söylemek istiyorum, önemli olarak önemli bir şekilde ortaya koyulan bir kaygı ve bilgisayar başında yaşayan bir dönem insanı olarak aslında anlayabiliyorum da. Sistemlerin ve simülasyon sistemlerinin, üç boyutlu sistemlerin ve teknik ortamların, sanal ortamların aşırı derecede fazla bir insan üzerinde uygulanması durumunda, o insanın hem bir yalancı güvene sahip olma riski var, hem de gerçeklik algısının bozulma ihtimalleri var. Ve simülasyon sistemlerini kurarken, aynı zamanda eğer gerçek dünya etkileşimlerini korumazsanız, çok gerçekçi sistemler yaparsanız, o çok gerçekçi sistemler yaparsanız, bu çok gerçekçi sistemler gerçek, gerçekçilik algısını bozuyor. Ve bununla ilgili de bir sürü araştırma var.

Dolayısıyla çok garip bir yerde duruyoruz. İnsanları öldürüp, gerçek savaş alanı oluşturup, insanları öldürüp zarar veremeyiz ama en iyi sandığımız teknolojiler de bizi gerçeğe hazırlamayabilir. Çok ikilemli bir yerde kalıyoruz. Bunun tek ikilemli yolu, ortak bir çözüm üretmek, iki tarafa da giden bir yaklaşım benimsemek. Sadece teknolojiyi ilerletmek değil, onun yerine ikisini birden hem eğitim verip hem de konvansiyonel sistemlerdeki insan eğitim katkısını azaltmamaya çalışmak. Anlamlı kontrol kavramı var, burada da hedefe ve hedefin bulunduğu bölgeye ilişkin detaylı bilgi ve bağlam hakimiyeti önemli.

Örneğin, hedefle etkileşim gerçekleşirse ortaya çıkabilecek olumsuz durumları öngörme ve beklenmedik durumlarda oluşabilecek zararları azaltabilecek önlemleri alabilme konusu önemli. İnsanların etkileşimde planlamadan sona kadar sürekli aktif olarak sürece dahil olması ve etkileşimi hızlıca tamamen durdurmanın ya da en azından yavaşlatmanın mümkün olması gibi durumlar da önemli olacak.

Şurada ilginç bir şey var, yapay zekâ sistemlerine ilişkin düzenlemeleri kim yazıyor dersiniz tanıyorum, biliyorum ama hala bunların yazılması beni şaşırtıyor. Anlamlı kontrolün unsurları arasında etkin bir şekilde sistemi kapatmak diye bir şey var. Buna 'kill switch', bizim her yerde gördüğümüz kırmızı butonu eklemek gibi bir durum var. Bunu gerçekçi bulmuyorum, hukukçu olarak bile gerçekçi bulmuyorum. Mühendisleri zaten bu düzenlemelerle çoğunlukla dalga geçiyorlar.

Sistemin anlamlı bir şekilde sona erdirilmesi bazı durumlarda yarardan çok zarar sağlayabilir. Sistemin kapatılması veya zararlı unsurların eline geçmeden önce kendini yok etmesi apayrı mesele. Ama buradaki tartışmaların önemli olduğunu ve bence biraz düzenlemelerle yanlış yere gittiğini de söylemek isterim.

Eğitim ilişkin kısma son bir kez daha değineceğim. Burada eğitimin önem ve etkilerinde aslında birden fazla şey var. Burada ahkam kesecek insan değilim ama burada bahsettiğimiz artık zarar verilen kişi, zarara uğrayacak kişi, zarara uğrayacak şey asker.

Yıllarca ortaya konulmuş bir emek, eğitim ve nihayetinde ulusal güvenlik. Dolayısıyla burada hukukçular olarak aslında az önce söylediğim yabancılaşmayı bence düzenlemeyi yapan insanlar da yaşıyor, politika yapımcılar, hukuk yapımcılar da yaşıyor. Çünkü kağıt üzerinde, 'Aman siz yeter ki devletin başına bela açmayın, sorumluluğa sıkıntı getirmeyin, bunlara dikkat edin' demek, aslında saha alanında uygulanamaz kuralların oluşmasına sebep olabiliyor. Bunun tek bir çözümü var, böyle kuralların oluşturulmasında, her türlü alandan uzmanları bir araya getirmek. Bu bazı alanlarda yapılan bir şey, bazı alanlarda ise maalesef yapılan bir şey değil. Eğitimin içeriğiyle ilgili önemli hususlar var. Silah yetkinliği sistemi dediğimiz, silahı nasıl kullanacağını bilmek bir şey ama onun haricinde psikolojik etkenler en fazla tartışılan, en fazla eleştirilen ve en zor öğretileceği düşünülen konular. Çünkü o ortama girmeden daha önce söylendi, etkisini bilmeniz gerçekten zor. Ve dahası neyin yanlış gidebileceğini bilecek, anlayabilecek insanlara ihtiyacınız var. Simülasyonun aslında bir dizayn problemi bu. Simülasyonda çalıştığınızda bütün faktörleri bildiğiniz varsayımıyla hareket ediyorsunuz. Bu da çok eleştiriliyor. Çözümü ne? Çözümü bilmiyorum ben de gerçekten. Ama eleştirinin çok yerli yerinde olduğunu ve buna ilişkin bir sürü çalışma yapıldığını da görüyoruz. Ama nasıl çözülebilecek, ne yapılacak artık orası da ayrı bir sorun diye düşünüyorum.

Beni dinlediğiniz için teşekkür ederim.

SORU : Ceza hukukunda, cezai ehliyet dediğimiz, aklın olması gerektiğine dair bir hüküm vardır, 'deliler yargılanamaz.' Gibi. Yapay zekâ özelinde, insan kendi eğittiği bir sisteme, cezai uygulama yetkisi mi getiriyor? Yani ben operatörüm, emir komuta zincirinde bunu kullandım, ama yapay zekâ kararı referans alındı. Sonuç ne olur?

CEVAP: Burada yine ulusal ve uluslararası hukuku ayırmam lazım. Yani bu böyle uluslararası bir krize dönüşmezse, eğer sadece bireysel içeride bir sorumluluk olayı olarak kalırsa, o zaman orada da aslında bizim iç hukuktaki nedensellik bağımız, burada eğer bütün mekanik sistem bu şekilde kurgulanmışsa, atılması gereken bütün adımlar atılmışsa, yani bunlar sonuçta protokollerle, rehberlerle, güvenlik mekanizmalarıyla, kilitlerle çalışan sistemler, öyle ortaya direk bırakılmıyor.

Bu silsile uygulanmışsa, hepsi yapılmasına rağmen bir sorun çıkmışsa orada artık doğrudan personele ilişkin bir sorumluluk düzenlemesi çıkmayacağını afaki söyleyebilirim. Çok afaki konuşuyorum, çünkü olayın içerisinde küçük bir detay olur, hoca şöyle demişti gibi bir referansa düşmek istemiyorum. Asıl sorun uluslararası hukuk kısmında oluyor. Uluslararası hukukta sorumluluk çok daha farklı bir yerden işliyor. Devleti bir davranışın atfedilmesi dediğimiz bir şey var, devletler kolay kolay bağlanmaz, devletler yetkilisiyle, başkanlar veya bakanlarla bağlanırlar. Bunun haricinde mesela bir terörist örgüt, bir insan topluluğu, acaba bir şey yaparsa bu devlete atfedilebilir mi? Orada çok ciddi kurallar var, devlet eğitim verdi mi, silah sağladı mı, buna göz yumdu mu, mevcut işletilmesi gereken mekanizmaları işletti mi, işletmedi mi bunlara bakılıyor. Dolayısıyla, yani eğitim yapılmadıysa, önlem alınmadıysa, bu devletin de sorumluluğunu tetikleyecek. Ama her şey yolunda yapılmışsa bile, uluslararası hukukta yine başka bir şey var. Nihayetinde siz bunu en tepeden askeri mekanizmalardan kullanmayı tercih ettiniz, yine sorumluluk ortaya çıkabilir de. Burası şu an gelişen bir alan. Uluslararası hukuk kapsamında, Birleşmiş Milletler 'de bu alanda ciddi çalışmalar yapılıyor. Kararların çoğunda Türkiye'nin imzasını görmüyorum. Bu bilinçli bir çekinme mi, yoksa dahil mi değiliz onu bilmiyorum. Çünkü temsilcimiz var. Ama uluslararası hukuk kısmında bir sıkıntı var, ulusal hukukta da sorunun çözülmesine ilişkin kurallarımız var. Ama böyle bir şey olursa, uygulamayı sorarsanız, dürüst olmak gerekirse, mahkemenin önüne çok çıkabileceğini düşünüyorum.

Bağlayıcı bir şey söylemek istemiyorum, yarın 'böyle demiştiniz' durumuna düşmek istemem ama görüşümü paylaşıyorum. Çünkü çok fazla gizlilik kararı var. Bunu da doğru buluyorum bur arada. Ancak illaki ileride bazı mekanizmalar çıkacaktır, ilerleyecektir, ileride uluslararası soruşturmalar da işleyecektir ama orası biraz daha askeriye ve savunma sanayinin farklı bir alan olmasının sonucunu yaşayacak.

II. GÜN BEŞİNCİ OTURUM – YENİ SAVAŞ
TEMA:
Güvenli Teknoloji ve Ulusal Hassasiyetler

OTURUM KONUSU:
Teknolojide Gizlilik, Güvenlik ve Rekabet

OTURUM TEMALARI:

Veri Şifreleme
Siber Ağ Güvenliği
Bilgi Gizliliği ve Güvenlik Açıkları
Siber Tehditler
Elektronik Harp

X. OTURUM ÖZETİ

Günümüzde sokaktaki insandan askeri birliklere kadar her türlü iletişimin temelinde teknolojinin ve uydu-internet alt yapılarının bulunduğu hatırlatılırken, siber savaş yöntemlerinin topyekûn uygulanması halinde en büyük problemlerin iletişimde yaşanabileceği, GSM operatörlerinin ve televizyonların etkisiz kalacağı, bahsedilen otonom sistemlerin alt yapılarının etkileneceği bir durumun söz konusu olacağına dikkat çekildi. Özellikle askeri sistemlere sızmaların 2013 yılından bu yana yaşandığı yönündeki bilgiler paylaşılırken, yanıltma, sahte sinyal ve sahte veri ile yapay zekânın aldatılması gibi kritik konularda da siber güvenlik önlemlerinin önemi aktarıldı. Birbiriyle haberleşerek çalışan askeri sistemler zincirinde bir halkada meydana gelecek problemin tüm sistemi etkileyebileceği, işlemciden, donanıma, donanım tabanlı vektörle, tedarik-bakım sistemi dahil her türlü aşamadaki riskin sistem güvenliğinde dikkate alınması gerekliliği kaydedildi.

Türkiye'nin yapay zekâ alanında kendi dil modelini geliştirmenin Millî güvenlik perspektifinden bir yaklaşım gerektirdiği, her türlü istihbarat örgütünün yapay zekâyı kullandığı, siber güvenlik alanında etkin kullanıldığı ve dünya ülkelerinde bu konunun ulusal strateji boyutuyla ele alındığı örnekleriyle paylaşıldı. Yerli yapay zekâ çözümleri geliştirilmenin yanında 'yapay zekâ güvenliği stratejisi' konusunun da acil bir konu olarak ele alınması gerektiği, oluşturulacak yapay zekâ güvenlik stratejisinin de acil olarak askeri ve istihbarat sistemlerinin yapay zekâ güvenliğine entegre edilmesi talebinde bulunuldu. Yapay zekâ gelişim sürecinde denetim ve güvenlik testlerinin de acilen hayata geçirilmesi ve siber güvenlik firmalarıyla araştırma merkezlerinin iş birliğinin sağlanması gerekliliği paylaşıldı. Savunma sanayinde 'siber güvenlik' kültürünün oluşturulmasının ve çok basit uygulamalarla tedbirler alınabileceğinin de ifade edildiği oturumda, siber güvenlik alanındaki savaşı konvansiyonel savaştan ayıran en önemli fark için ilginç bir ifade kullanıldı: "Siber güvenlik tarafındaki savaşı fark ettiğiniz anda aslında o savaş bitmiştir. Çünkü, kişi istediği şeyi almıştır, götürmüştür veya istediği zararı vermiştir."



Hamdi ERKAN
ASELSAN
MODERATÖR

Merhabalar, bu iki günlük güzel etkinliğin son oturumu bize kaldı. Oturum son ama konu oldukça kritik bir konu. Oturumun teması Güvenli Teknoloji ve Millî Hassasiyetler. Geleceğin Askeri kavramı ile güvenli teknoloji kavramı birbirinden ayıramayan kavramlar. Güvenli teknoloji sadece bir inovasyon meselesi değil, aynı zamanda egemenliğimizi, bağımsızlığımızı, toplumsal bütünlüğümüzü

sürdürebilmemiz için kritik bir sorumluluktur. Bu panelde konunun uzmanlarından veri şifreleme, ağ güvenliği, bilgi gizliliği, güvenlik açıkları, hacker tehditleri, backdoor açıkları gibi önemli konuları hem mevcut durumları, hem de geleceğe dair perspektifleriyle dinleyeceğiz. Katılımınız için teşekkür ediyorum, son oturumdaki sabrınız için de teşekkür ediyorum. Panelimizin verimli geçmesini diliyorum.



Regaip KURT
HAVELSAN

Hoş geldiniz, iki gündür burada savunma sanayi alanında özellikle konvansiyonel savaşın uygulanması konusunda son teknolojiler, modern teknolojiler tanıtıldı. Konvansiyonel savaş ve konvansiyonel savaşlarda kullanılacak yöntemler ile kullanılacak teknolojiler anlatıldı. Buradaki teknolojiler, büyük ihtimalle, inşallah görmeyiz ama bir gün olası bir savaşta

kullanılacak, ülkemizi, milletimizi ve kurumlarımızı korumak için kullanacağımız teknolojiler. Eğer bu teknolojileri kullanacağımız bir savaş olursa, bu savaşı büyük ihtimalle haberlerden duyarsınız. Çünkü topyekûn bir savaş halidir. Fakat bir gün topyekûn bir siber savaş haline geçerse bunu haberlerden duyamazsınız. Çünkü haber kanalları size hizmet veremez durumda olurlar, telefonunuza bakmak isterseniz ne olup bittiğini anlamak için, GSM operatörünün size hizmet veremediğini görürsünüz. Çünkü o zaman da siber saldırılar

saldırıları yapılmıştır ve bu saldırılar sonucunda GSM operatörleri size hizmet veremez duruma gelmiştir.

Havelsan 'da çalışan siber güvenlik uzmanları olarak bizler, normal özel şirketlerde çalışan, siber güvenlik uzmanlarının yöneldiği alanlara yönelmiyoruz. Ya savaş hallerinde kullanmak üzere teknolojiler üretiyoruz ya da askeri teknolojilerin güvenliğini sağlamak için çalışıyoruz. Burada anlatılan bütün teknolojiler, gemilerimiz, uçaklarımız, füzelerimiz, yazılımlarımız, tamamı bizim kontrollerimizden geçerek, siber anlamda güvenli oldukları doğrulanarak hizmete alınıyorlar. Ve bunların testleri gerçekleştiriliyor. Fakat son zamanlarda artık bizim klasik yöntemlerle yaptığımız sızma testleri de yeterli olmamaya başladığı için yeni bir doktrin geliştirmeye başladık, yeni yöntemler geliştirmeye başladık. Bu yöntemler hem ülkemizde hem de NATO'da kullanılabilecek birtakım araçları içeriyor. Bugün ben bu araçları sizlere anlatacağım. Bizim yaptığımız faaliyetler genellikle sürekli kırmızı takım hizmetleri ve sızma hizmetlerinden oluşuyor. En başta bunlar var. Siber güvenlik eğitimleri düzenliyoruz, CTF ve Cyber Range platformları hazırlıyoruz, NATO'daki siber güvenlik tatbikatlarına etkin olarak katılım sağlıyoruz.

Locked Shields, komuta zinciri içinde olan bir tatbikat değil, hem de CWIX tarafında 2024'te gözlemci statüsündeydik, bu yıl TSK'nın siber gücü olarak oraya katılım sağlayacağız ekip olarak. Ve biryandan da kullandığımız araçları geliştirebilmek, teknolojiyi ilerletebilmek amacıyla yapay zekâ çalışmalarını yaparken, bilimsel anlamda ve pratik anlamda da bir şeyler yapmaya çalışıyoruz. Bunları birleştiriyoruz.

Askeri terminolojiden aldığımız bir ölüm zincirimiz var bizim, Cyber Kill Chain dediğimiz. Bu Lockheed Martin tarafından geliştirildi. Ve siber güvenlikte veya siber saldırılarda kullanılan bir yöntem bu. En başta bilgi toplama aşamasıyla başlayıp silahlanmaya, o silahın dağıtılmasına, açıklıkların sömürülmesine ve daha sonra da gerekli aksiyonların geliştirilmesine kadar giden bir süreç bu. Bu süreç aslında orduda kullanılan bir yöntem fakat biz yaptığımız çalışmalarda bu ölüm zincirinin bazı yerlerde yeterli olmadığını gördüğümüz için yeni bir ölüm zinciri geliştirdik. Yine askeri terminolojiden alınma ölüm zinciri. Bizim geliştirdiğimiz 'Sürekli Otomatize Kırmızı Takım Hizmeti ve Sızma Testi' dediğimiz ve sürekli

geliştirdiğimiz bir yöntem var, bununla sızma testleri arasında bir fark var.

Sızma testleri yaparken biz aslında bir sistemi belirli bir zaman aralığında sistem açıklarını test etmeye yöneliriz. Fakat zamanımız kısıtlı olduğu için hem o sistemde tespit edilmemiş açıklar kalabilir, hem bu bilinen zaman aralığından dolayı örneğin bir kurumun ağında test yapıyorsak, kurumun personeli bizim orada olduğumuzu bildiği için normalde davrandığından daha sıkı davranarak önlemler alabilir. Hem klasik bir yaklaşım olduğu için bulabileceği, gösterebileceği şeyler bellidir. Hem de bilinen zafiyetlere daha çok odaklanır. 'Zero Day' dediğimiz, o güne kadar bilinmeyen sıfıncı gün açıklarının araştırılmasını içermek ve tek seferlik bir zaman dilimini kapsar. Tek seferlik zaman diliminde bir kuruma test yaptığınız zaman sadece o zaman aralığındaki açıklıkları bulabilirsiniz. Fakat o test bittikten bir gün sonra yeni bir açıklık ortaya çıkabilir ve bu açıklık o kurumu tehdit edebilir, hayati sonuçları olabilir bu açıklarında.

Aslında anlatacağımız şeyler de genellikle bu yeni savaşın, yeni dünyanın ve yeni ortamın nasıl şekillendiğini bizlere açıklayacak. Fakat 'Sürekli Otomatize Kırmızı Takım Hizmeti ve Sızma Testi' dediğimiz hizmette biz kurumlara farklı şekillerde hizmet vermeye başladık. Sınırlı süreli ya da belirli süreli anlaşmalarla daha uzun süreli testler yapmaya başladık. Burada zaman geniş olduğu için açıklıkların gözden kaçma ihtimali de çok düştü. SOC dediğimiz, kurumların aslında mavi takımları, kurumları korumaya çalışan takımlar artık daha dikkatli davranmak zorundalar. Modern bir yaklaşım geliştirdik. Böylece SOC takımları da burada dikkatli oldukları için siber saldırının bizden mi geldiğini, başka yerden mi geldiğini bilmedikleri için her gelen alarma dikkatli bir şekilde bakmak zorunda oluyorlar. Bir örnek vereyim, yaklaşık 20 gün önce bir kurumla toplantı yapıyorduk. Yaptığımız toplantılarda geçen yıl kurumlarının işte belirli bir şekilde telefonla aranıp bazı personellerinin bilgisine ulaşıp, hesaplarına girildiğini söylediler. O hesaplara girenler bizlerdik ama üst kurumları o hizmetleri aldıkları için kendilerinin haberleri yoktu, başka şekilde kritik verilere erişildiğini söylediler. Başka bir zaman diliminde de o verileri alanlar bizlerdik ama onlar bizim olduğumuzu bilmiyorlardı. O kurumuz SOC'si, yani mavi takımı o kurumu korumakla yükümlü olan ekip, bunu bilmediği için daima böyle şeylere karşı daha dikkatli oluyor.

Modern bir yaklaşım sergiliyoruz dedik ve mavi takımları bunları bilmediği için de eğitiyor. Bu hizmette kurumun yazılımlarına veya sistemlerine yönelik, sıfıncı gün saldırıları da deniyor, yani o kurumun sistemlerinde daha önce hiç bilinmeyen bir açıklık varsa, uzmanlar tarafından bu açıklıklar test edilip, o bilinmeyen açıklıkların da ortaya çıkması sağlanıyor ve bu sürekli olarak yapılıyor. Dolayısıyla belirli bir zaman diliminde olmadığı için devam edebiliyoruz kurumu korumaya sürekli olarak. Bütün askeri sistemler birbirine bağlı çalışıyor. Dolayısıyla bu askeri sistemlerin tamamında güvenliğin sağlanması lazım.

Güvenliğin sağlanması için burada yetkilendirmenin doğru yapılması lazım, kimlik doğrulamasının yapılması lazım, şifrelemenin olması ve çalışması lazım. Bunlar görev kritik sistemler olduğu için sürekli çalışabilir durumda olması lazım ve bunların korunması için de siber güvenlik anlamında dayanıklı olması lazım. Gemilerde EKDİS deniler, haritalarının çizilmesini sağlayan sistemden bir örnek verebilirim. Normalde bir gemi karadan 10-15 kilometre açıldıktan sonra dünyayla bağlantısı kalmaz. Eğer TAFİCS gibi bir ağı bağlı değilse, uydu bağlantısı yoksa geminin karayla herhangi bir bağlantısı yoktur. Kendi içinde bir dünyadır. Bu örneği verme sebebim şu, normalde kendi içinde bir dünya olan, karayla bağlantısı olmayan bir sistemi hackleyemeyeceğinizi düşünürsünüz. Gemilere bu anlamda yönelen en büyük tehdit GPS saldırıları diye düşünülüyor. Ama EKDİS sisteminin haritaları, aslında tamamen dış dünyaya açık, internete açık bir sistemden güncelleniyor. Askeri sistemler için belki bu geçerli değil ama sivil sistemlerde ve sivil sistemlerin de büyük çoğunluğunda bu tarz haritalar kullanılıyor. Bu haritalama sistemleri özelinde FTP sunucusunda yaptığımız testler sonucunda, geminin haritasının güncellendiği sistemi, tamamen yetkili bir şekilde haritaları değiştirebilecek şekilde erişim sağladığımızı görüyoruz. Gemi karada bu sistemi güncelledikten sonra denize açılırsa, tamamen o haritaya bağlı olduğu için, denizin ortasında güncelleyemeyeceği için bu değiştirilmiş haritaya bağlı olmak zorunda. Karadan 10-15 kilometre açılmış, karayla hiç bağlantısı olmayan sistem bile hacklenebilir.

Gemi çok kapalı bir sistem olduğu için bu örneği veriyorum. Aslında hacklenmez diye bir şey yok askeri sistem olduğu için, çok güvenli gibi duruyor. Fakat tedarik zincirlerinden de kaynaklı bazı saldırılar, askeri sistemler de dahil bazı sistemleri

etkileyebiliyor. Çünkü bazen yüzde 100 yerli üretim yapamıyoruz, bir şekilde dışarıdan da bazen bir şeyler almak zorundayız. Bunlar işlemciler, donanım, donanım tabanlı vektörler de olabilir. Bunların içerisinde açıklar da olabilir veya diğer sistemlerde olabilir. Bizim geliştirdiğimiz Amerikan Hava Kuvvetleri'nden alınma bir sistem. F2T2EA dediğimiz bir sistem bu. Amerikan Hava Kuvvetleri'nde bir general olan Ronald R. Fogleman'ın bir sözü var, "21. Yüzyılın ilk çeyreğinde, dünya yüzeyinde hareket eden her şeyi bulmak, düzeltmek veya izlemek ve hedeflemek mümkün olacak" diyor. Hava Kuvvetleri için bir doktrin geliştirmiş. Biz de yeni kill chain sistemimizde bu doktrini baz aldık. Çünkü eğer dünya üzerinde hareket eden bir şeyi 10 dakikadan kısa bir sürede bulup yok edebiliyorsanız, internet üzerinde hareket eden şeyi de 10 dakikadan kısa sürede bulabilmeniz lazım. Bulamıyorsanız eğer, başka birisi mutlaka bulur. Dolayısıyla biz kurumlara hizmet verirken, bir kurumun varlıklarının üzerinde açıklık varsa, 10 dakikadan kısa sürede bunu bulalım ve o açıklığı kuruma bildirelim istiyoruz. Bazı yerlerde siber yoğunluklu ve kinetik yoğunluklu çatışmalar var. Bazı yerlerde ordular şehre girmeden önce siber saldırılar gerçekleştirildi, bazı yerlerde de fiziksel saldırıların ardından siber saldırılar gerçekleşti.

Yani tamamen orduyu, fiziksel savaşı destekleyecek nitelikte bir savaş ortamı var. Bu savaş ortamı da yeni savaşçıların olmasını gerektiriyor. İki ay önce Lübnan'da patlayan çağrı cihazları da az önce söylediğim ve tedarik zincirinden kaynaklanan bir zafiyet dolayısıyla yapılabildi. Size ürünü ya da bir yazılımı tedarik eden firma hedef alınırsa, sizin doğrudan hedef alınmanız yerine sizin sistemlerinizin de zarar görebileceği bir açık oluşabilir.

Bir de APT dediğimiz "Gelişmiş sürekli tehdit" durumları var, bunlar sistemlere erişim sağlarken farklı şekillerde çalışıyor, motivasyonları farklı. Örneğin Rusya'nın Ukrayna'ya yaptığı saldırılarda yıkıcı saldırılar görüyoruz, yöntemleri genellikle yıkıcı. Devlet destekli hacker grupları genellikle girdikleri sistemlere zarar verirler, Kuzey Kore'nin devlet destekli grupları genellikle küresel ekonomik sistemden para çekmek için uğraşırlar. Çünkü Kuzey Kore'nin kendi sistemi küresel ekonomik sisteme uygun değil, entegre olmaya müsait değil. Buradan kaybettikleri maddi desteği, diğer taraftan kazanmaya çalışırlar.

En tehlikeli olan Çin. Çin tarafında şöyle bir şey var; Çin devlet destekli gruplarının yaptığı her şey Çin'in ulusal stratejik çıkarlarıyla paralel olarak ilerliyor. Dolayısıyla girdikleri sistemlerde ne doğrudan zarar vermeye çalışıyorlar ne de sistemlerde olduklarını belli ediyorlar. Ta ki Çin'in ulusal amaçları onların belirli bir hareket tarzı veya ilerleme göstermesini gerektirene kadar.

NSA hacker denilen bir grup var, Shadow Brokers, NSA'nin kendisini hackleyip bazı dosyaları şifreli almışlardı ve bunları GitHub'da internete açık olarak koymuşlardı. Başta kimse NSA'nin hacklenebileceğini ve oradan veri alabileceğini düşünmedi. Fakat bir başka deepweb grubunda bu dosyanın parolası paylaşılmış, içindeki dosyaların gerçekten NSA'nin geliştirdiği siber silahlar olduğu anlaşıldı ve NSA'nin gerçekten hacklendiği ortaya çıktı. Bu siber silahlar, daha sonra 2017'de ortaya çıkacak, MS17-010 denilen bir zafiyetin aslında kullanıldığını gösteren siber silahlardı, NSA'nin dünya üzerindeki bütün Windows bilgisayarlara girmesini sağlayan bir sistemdi bu. Açıklık hala bazı sistemlerde durabiliyor, çünkü o sistemleri güncelleme imkanımız yok. Kritik olduğu için.

NATO ne yapıyor bu konuda? Active Cyber Defence (Aktif Siber Savunma) denilen bir strateji geliştiriyor. Aktif siber savunma dediğimiz savunmacı orantılı ve uluslararası hukuka saygılı olarak size yönelmiş siber saldırılara nasıl cevap vereceğinizi söylüyor. Bu siber saldırılara cevap verebilmek için de nasıl bir yol izlemeniz gerektiğini anlatmaya çalışıyor. Respond don't retribute dediği kısım, intikam almayıp, cevap verin dediği kısım. İkisi arasında ne fark var?

Saldırgan bir tutum izleyecekseniz, eğer sadece size yönelmiş bir tehdit durumunda, bu saldırgan tutumu izleyin ve sadece size yönelen tehdide bu saldırıyı yapın. Onun dışında üçüncü ülkelerin yargı alanlarına girecek, üçüncü grupların yargı alanlarına girecek şeylerden kaçının diyorlar. 2014 yılında Galler zirvesinde, 5. Maddede "NATO ülkelerinden birisine bir siber saldırı düzenlenirse bu bütün ülkelere düzenlenmiş sayılacaktır" deniyordu. 2014'teki Galler Zirvesi'nde NATO dedi ki, "Eğer fiziksel silahla eşdeğer zarar verecek bir siber saldırı düzenlenirse, bu da artık bütün NATO ülkelerine düzenlenmiş sayılır ve buna göre önlem alınır" denildi. 2016'da da siber, uzay, artık kara, hava ve deniz kuvvetlerinin yanında bir çatışma alanı olarak belirlendi ve burada artık çalışmalar yapılmaya başlandı. Bizim yaptığımız şeyler de aslında bu NATO'nun yaptıklarının,

Yaptıklarının veya gruplarının yaptıklarının birleştirilmesi ve kendimiz için bir alt yapı oluşturmak. Bunun için NATO tatbikatlarında bazen hedef geliştirme, ön çalışma gibi şeyler yapıyoruz. Locked Shields tarafında hem hedef geliştirme tarafında hem Blue Team tarafında hem Red Team hem de Green Team tarafında çalışıyoruz. Red Team'i Locked Shields tarafında çalışmamızın şöyle bir sebebi var; NATO genellikle savunmacı bir yaklaşım izliyor. Savunmacı bir yaklaşım izlediği için, siber silah geliştirilmesine ya da saldırgan araçlar geliştirilmesine doğrudan sıcak bakmıyor. Ama Locked Shields NATO'nun komuta kontrol kademesinin altında olan bir yer değil. Dolayısıyla burada bilimsel geliştirme, araştırma, yazılım geliştirmesi yapabiliyorsunuz. Burada böyle bir imkânımız olduğu için burada kendi Continuous Automadet Red Team' yazılımımızı geliştirip kullanabiliyoruz.

Cycon tarafında 'AB2F: AI-Based Battlenet Framework for Continuous Red Teaming in Cyber Operation - AB2F: Siber Operasyonda Sürekli Kırmızı Ekip Oluşturma için AI Tabanlı Muharebe Ağı Çerçevesi' bir yapı geliştiriyoruz. Bu da bizim Continuous Red Team'da yani saldırı yapmak için kullandığımız framework'de kullandığımız araçların yazılımlarının bilimsel alt yapısını oluşturuyor. Artık bu çalışmalar tamamlandıktan sonra da uygulama ve test alanı olarak gerçek ortamların kullanılabilmesi amacıyla CWIX (Koalisyon Savaşçısı Birlikte Çalışabilirlik Tatbikatı) tatbikatında gidip orada gerçekten bir Red Team egzersizi yapıyoruz bu yazılımları kullanarak. Aslında sızma testleri gibi şeyler veya APT grupların yaptığı şeyler, birbirleri ile oyun teorisi bağlamında karşılaştırılabilir.

Oyun teorisinde sonlu oyunlar ve sonsuz oyunlar vardır. Sonsuz oyunların özelliği şudur; oyuncular sürekli oyunda kalmaya çalışırlar. O oyundan çıkmadıkları müddetçe başarılıdırlar. Sonlu oyunlarda ise oyuncular kazanmaya çalışırlar, bir şey elde etmeye çalışırlar. Biz aslında siber güvenlik uzmanları olarak özellikle kurumları korumaya çalıştığımızda, sonlu oyunlar oynamaya meyilliyiz. Kurumlar da sonlu oyunlar oynamaya meyilli, fakat sonlu oyun oynayan kurumlar da kişiler de günün sonunda kaybetmeye mahkumlar, sonsuz oyunlar oynayanlarda. Aslında devlet destekli hacker grupları olabilir, bir yandan finansal amaçlı finansal güdümlü hacker grupları olabilir, suç örgütleri olabilir, bunların tek amacı oyunda kalmak ve bir şekilde o oyunu oynamak. Dolayısıyla buradaki yapı aslında devletlerle terör örgütlerinin çatışmasına

benzetilebilir. Devletler oyunu kazanmak isterler, terör örgütleri ise oyunun içinde kalmak isterler. Dolayısıyla gayri nizami harbe karşı başarılı olması, bir devletin çok zordur.

Yazılım, planlamayı ve yönlendirmeyi yapıyor, aynı zamanda bu planlama ve yönlendirme sonucunda çalışan, küçük yazılım parçaları halinde saldırıları da gerçekleştiriyor. Fakat bu saldırılar, yazılımın doğrudan kendi içinde tanımlı olan saldırılar değil, bu saldırıları sizi belirli bir formatta yazılıma tanımlamanız gerekiyor. Bu tanımlandıktan sonra hem ekip içinde bilgi aktarımı sağlanıyor, hem de birisi ayrıldığı zaman o tecrübeyi kaybetmemiş oluyorsunuz, tecrübe aktarımını sağlamış oluyorsunuz. İkinci olarak eğer siz bu aktarımı yapabiliyorsanız, yaptığınız şeyi çok daha iyi anlıyorsunuz, çok daha iyi kavriyor ve bir sonraki aşamaya geçebiliyorsunuz. Yazılım da daha sonra bu saldırıların tamamını otomatize edip, belirli aralıklarla bu saldırıları gerçekleştiriyor. Planlamayı ve yönlendirmeyi yaptıktan sonra 'Card Workflow Engine' denilen tarafa gönderiyoruz biz bir hedefi. Hedef olarak vereceğiniz şeyin sadece bir kurumun tek bir domaininin olması yeterli, herhangi başka bir şeye gerek yok. Bu domaini verdikten sonra o kurumun internet üzerinden ulaşılabilen bütün varlıklarını çıkartabiliyoruz. Veya bir iç ağ kurduysanız, iç ağda yazılımın kurulu olduğu, ulaşabildiği bütün her yerdeki varlıkları teker teker çıkartıyor. Bu varlıkları çıkarttıktan sonra, varlıklar bu arada planlamaları yapıldıktan sonra slave'lere gönderiyor. Slaver bilgi toplamayı yapıyor, bilgi toplama yaptıktan sonra bizim collaboration framework'ümüz var, o da ayrı bir yazılım. O yazılım aslında bu bilgileri işleyip veri tabanlarına kaydediyor ve zenginleştiriyor.

Bir kurumun bütün varlıkları ve o varlıkların alt varlıklarıyla birlikte bizim veri tabanlarımızda duruyor. Oralarda da aslında zafiyet analizi ve üretimi yapılıyor. 10 dakikadan kısa sürede bir kurumun üzerinde bir zafiyet çıkarsa onu bulmamız lazım demiştik, işte bizim veri tabanımızda bütün varlıklar detaylı bir halde tutulduğu için yeni bir zafiyet çıkarsa 10 dakikadan kısa sürede onu tespit ediyoruz ve o kuruma doğrudan bilgi gönderebiliyoruz. İşin biraz daha otomatize yapılan kısmı burada, analiz ve üretim kısımlarında operatör ve yapay zekâ birlikte çalışıyor ve LLM denilen modellerden destek alarak zenginleştiriyor veya yeniden kullanıma açıyoruz. Daha sonra dağıtım ve kullanım tarafında da yeniden gelen veri işleniyor ve orada zenginleştirilerek yeniden analizler gerçekleştiriliyor.

Bunun için de kullandığımız yöntem Black Dagger Black Chart denilen yöntem bizim yazılımımız ve Lockheed Martin'in Software Factory sistemi.

Bu bilgi aktarımı veya işlerin hızlanması açısından 3 yıllık bir anlaşma imzalanıyor Amerikan Savunma Bakanlığı ile. Bu anlaşmayla 3 yılda üretilmesi gereken kasklar 1,5 yılda üretiliyor. Böyle olunca Lockheed Martin'e dava açılıyor neden madem 1,5 yılda bitirebiliyordunuz da 3 yıllık süre verdiniz diye. Aslında, F16'lerden kalma bilgilerini birleştirerek, Software Factory sistemini kurarak 1,5 yılda bunu yapabildiklerini görüyorlar. Bu sistemi kendi yazılımımızla da entegre ederek, biz de orada sistemin çok hızlı çalışmasını sağlıyoruz. Buradaki sistem zaten tamamen dağıtık çalışıyor, dünyanın her yerinden IP alıyor ve sınırsız bir IP havuzu var.

Ölçeklenebilir bir yapı sunuyor sistem, tüm görevler bir kullanıcı arayüzü ve paralel çalışmayı destekleyen bir otomasyonla çalışıyor. Tek bir görev veya birden fazla görev için gerekli olan bir alt yapıya sahip, deneyimlerin aktarımıyla bilgi birikimini de sağlıyor sistem.

Teşekkür ediyorum.



Dr. Celal ERBAY
Millî İSTİHBARAT AKADEMİSİ
(MİA)

Öncelikle emeği geçen herkesi ve katılımcılarımızı selamlıyoruz. Son iki günde özellikle yapay zekâ konusunda oldukça bilgilendirici güzel sunumlar yapıldı. Biliyorsunuz özellikle yapay zekâ teknolojileri, Amerikalı büyük firmaların şu an hegemonyasında ama Avrupa Birliği 24 dili de kapsayacak şekilde yeni bir yapay zekâ modelini ilan etti. Ben özellikle baktım, Türkçe tabii ki yok bu

dillerin arasında, büyük oranda İngilizcenin yer aldığı bir dil modeli. Aslında buradan şuna gelmemiz gerekiyor, Amerikalı firmalar, Amerikalı istihbarat örgütlerini besleyebilir. Avrupalı bu gelişmeler de Avrupa istihbarat örgütlerini besleyecek. Bizim de gelecekte kendi dil modellerimizi geliştirmemizin ne kadar önemli olduğunu aslında buradan görebiliriz.

İki gündür yapılan sunumlarda aslında bu yönde bir ihtiyaç olduğunu net bir şekilde diğer konuşmacılar da ifade ettiler. Ben de benzer bir yaklaşım sunarak, bunu yaparken nelere dikkat etmemiz gerektiği konusunda sizleri bilgilendirmek istiyorum. Biraz daha yapay zekânın istihbarat ve güvenlik alanlarındaki kritik rolünü de gündeme alarak Millî Güvenlik perspektifinden genel hatlarıyla konuyu analiz edeceğim.

Değerli katılımcılar, yapay zekâ bildiğiniz gibi son yıllarda, özellikle istihbarat toplama ve ulusal güvenlik alanlarında önemli bir dönüşüm sağlamıştır. Bu dönüşümü de özellikle CIA ve NSI gibi istihbarat kuruluşları da hızlı bir şekilde benimsemişlerdir. CIA, yapay zekâyâ yaptığı yatırımlarla veri işleme ve istihbarat toplama süreçlerinde çok önemli gelişmeler göstermektedir. 1982 yılında, dikkatinizi çekmek isterim, 1982 yılında yazdıkları, hazırladıkları ve 2012 yılında gizliliği kaldırılan belgelerine göre, ilk yapay zekâ alanındaki yatırımlarını yapmasından bu yana, yapay zekâ teknolojilerini stratejik operasyonlarında kilit bir şekilde kullanmaktadır. Bu raporlarında yapay zekâyı takım arkadaşı olarak tanımlamaktadır. Özellikle açık kaynaklardan gelen devasa veri yığınlarını analiz etmek için Generative Üretken Yapay Zekâ teknolojilerini kullanmaktadırlar.

CIA'nın yapay zekâ direktörü bu teknolojilerin ajansın veri analizi hızını yüzde 50 oranında artırdığını açıklamıştır. Yine NSI yapay zekâyı özellikle siber güvenlik, enformasyonla mücadele gibi alanlarda aktif bir şekilde kullanmaktadır. Burada da yapay zekâ uzmanlarının belirttiğine göre siber saldırıları tespit etme ve yanıtlama süreçlerini yüzde 30 oranında artırdığı ifade edilmektedir. Kullandıkları yapay zekâ tabanlı çözümler, siber tehditlerin daha erken aşamalarda tespit edilmesini ve engellemesini sağlamaktadır. NSI, ayrıca yapay zekâ teknolojilerini seçim güvenliği ve dış aktörlerin dezenformasyon kampanyalarını izlemek için de aktif şekilde kullanmaktadır.

Çin'e geldiğimiz zaman, onlar yapay zekâyı ulusal güvenlik stratejilerinin merkezine yerleştirmişler, bu teknolojiyi siber güvenlikten askeri operasyonlara kadar çok geniş bir yelpazede kullanmaktadırlar. 2017 yılında yayınladıkları yeni nesil yapay zekâ geliştirme planına göre, 2030 yılına kadar dünyanın en büyük yapay zekâ merkezi olmayı hedeflemektedirler. Bu plana göre yapay zekâ, sadece kendi ekonomik kalkınmaları açısından değil, aynı zamanda ulusal güvenlik açısından da kritik bir teknoloji olacağını göstermektedir. Burada en dikkat çekici noktalardan biri de NSI'de olduğu gibi Çin'in de siber güvenlik alanında bunu kullanması. Çin İstihbarat Teşkilatı, yani Minister of State Security (MSS), yapay zekâyı siber saldırıları erken tespit etmek, verileri manipüle etmekten korumak ve tehditlere hızlı yanıt vermek için kullanmaktadır.

Yine geliştirdikleri yapay zekâ tabanlı yüz tanıma sistemlerini kamu güvenliğini sağlamak ve potansiyel tehditleri hızlı bir şekilde tespit etmek için yaygın bir şekilde kullanmaktadır. Açık kaynaklarda belirtildiği için ben de ifade edeceğim, özellikle Pekin'de konsoloslukların bulunduğu binada kameralara entegre edilen yapay zekâ sistemleriyle, daha doğrusu konsolosluklarda çalışan çalışanların analiz edilmesiyle, özellikle bir CIA grubunun ifşa edildiği açık kaynaklarda görülmektedir. Bu aslında Çin'in geldiği noktayı bize göstermektedir. Yine istihbarat teşkilatının dışında askeri operasyonlarda da çok aktif bir şekilde kullanmaktadırlar.

Çin Halk Kurtuluş Ordusu, yapay zekâ destekli silah sistemleri geliştirmekte ve bu sistemler hedef tespiti ve saldırıları, daha doğru ve hızlı bir şekilde yönlendirmek için aktif bir şekilde kullanılmaktadır.

Yapay zekâ, siber güvenlik alanında saldırı yöntemlerine de çok büyük yenilikler getirmiştir, etkinliklerini oldukça artırmıştır. Yapay zekâ tabanlı hackleme saldırı süreçlerini hızlandırarak, burada yine altını çizmek istiyorum, düşük teknik bilgiye sahip bireylerin bile etkili saldırılar gerçekleştirmesine olanak tanımaktadır. Yapay zekâ saldırıları, nasıl kullanıldığı ve bu süreçlerin aşamaları keşif, erişim sağlama, etki ve veri hırsızlığı, ayrıcalık yükseltme ve yatay hareket, savunmalardan kaçınma gibi aşamalarla gerçekleşmektedir. İlk aşama keşif aşaması, burada saldırganlar hedef sistem hakkında bilgi toplar, yapay zekâ ise açık kaynakları ve internetteki çeşitli platformları çok hızlı bir şekilde tarayarak çok değerli verileri saldırganlara sunabilir. Özellikle kişisel bilgileri, e-posta adreslerini ve güvenlik açığını tespit etmek için aktif bir şekilde kullanılır.

İkinci aşama erişim sağlama aşaması, burada yapay zekâ kimlik avı saldırısı, yani fishing gibi yöntemlerle sahte e-postalar ve mesajlar oluşturur, sahte içeriklerle kullanıcıları kandırarak şifreler ve kimlik bilgileri gibi hassas verilere rahatlıkla erişebilir. Yine yapay zekâ destekli deepfake teknolojileri, sahte video ve ses içerikleri üreterek hedef kişilerin kimlik doğrulamalarını geçmelerine yardımcı olur. Üçüncü aşama ise ayrıcalık yükseltme aşaması, burada saldırganlar elde ettikleri erişimi kullanarak sistemde daha fazla yetki kazanmak için yine yapay zekâ araçlarını kullanmaktadır. Burada yapay zekâ gerekli komutları ve yönlendirmeleri oluşturur. Böylece saldırganlar sistemde derinlemesine rahatlıkla hareket edebilirler. Dördüncü aşama yani etki aşaması. Özellikle fidye yazılımları gibi saldırıları daha hızlı ve etkili hale getirebilir. Yapay zekâ teknolojileri dosyaları şifreleyip fidye taleplerini daha geniş kitleye ulaştırabilir. Son olarak savunmalardan kaçınma. Bu da oldukça kritik biliyorsunuz. Bu tür sitemlerde yapay zekâ araçları, zararlı yazılımların tespit edilmesini engellemek için sürekli olarak kendisini dönüştüren polimorfik zararlı yazılımlar oluşturur ve bu da saldırganların siber güvenlik sistemlerinden rahatlıkla kaçmasına yardımcı olur. Bu anlamda kullanılan yapay zekâ araçlarından bazıları WormGPT, FraudGPT, Poison FPT, AutoGPT, FreedomGPT, ChaosGPT, White Rabbit NeoAI gibi yazılımlar.

Araştırdıkça daha fazla yapay zekâ aracı bulabilirsiniz. Bunlardan örneğin WormGPT, bu tür saldırganlara sınırsız içerik oluşturma imkânı tanır, güvenlik filtrelerinden kazçınmalarını mümkün kılar. Yine AutoGPT, FreedomGPT gibi yazılımlar bu süreçlerde siber saldırganlara yardımcı olur. Mesela FraudGPT siber suçlar için sahte sayfalar, kötü amaçlı yazılımlar, siber saldırı araçları üretebilir. Bu tür toollar yazılımlara belirli telegram kanallarından eriştirilebilir. Yani çok da public, halka açık bir şekilde dağıtılmıyor. Özellikle deepfake dediğimiz deep web dediğimiz kısımda, alanda bu tür toollar kullanıma sunulmaktadır. Genel olarak bu tür araçlar hackerların hedefleri manipüle etmelerini, zararlı yazılımlar üretmelerini ve siber saldırıları daha hızlı ve etkili bir şekilde gerçekleştirmelerine olanak tanır.

Örnekleriyle de gördüğümüz şekilde yapay zekâ modelleri artık oldukça kritik bir öneme haiz, ülkemiz açısından da aynı şekilde olacak. Ve açıkçası belki burada Savunma Sanayi ve İstihbarat alanlarında öncelikle böle bir yapay zekâ modelinin geliştirilmesi gerekmektedir. Ve bunun geliştirilmesi aşamasında oldukça dikkatli olmalıyız. Yapay zekâ yaşam döngüsü geliştirme, devreye alma, tasarım ve bakım aşamalarından ve alt bileşenlerinden oluşuyor. Bunun her aşamasında oldukça dikkatli olmak zorundayız ve bu döngünün her aşamasında olabilecek potansiyel riskleri ve zafiyetlerin nasıl istismar edilebileceğini göstermek istiyorum.

Yapay zekâ yaşam döngüsünün ilk aşaması olan tasarım aşamasında güvenlik mimarisinin eksikliği, saldırganların sisteme zararlı veri enjekte etmesine neden olabilir. Bu dediğimiz, bahsettiğimiz poisoning data (yapay zekâ zehirlenmesi) kullanarak yapay zekâyı eğitim sürecinde yanlış bilgiler verilebilir ve bu durum sonuçları etkileyebilir. Bu da aslında bizim gelecekte kullanma noktasında askeri ve istihbarat sistemlerinde hatalı istihbarat raporları, askeri operasyonların başarısızlığı veya gözetim verilerinin manipüle edilmesi gibi çok ciddi sonuçlara yol açabilir. İkinci aşama geliştirme aşaması, burada güvenlik açıkları ortaya çıkabilmektedir. Sistemlerin sürekli izlenmesi ve bu aşamada güvensiz kod yazımı, yetersiz erişim kontrolleri ve kötü yapılandırılmış modeller, saldırganların sistemi manipüle etmesine olanak tanıyabilir. Üçüncü aşama devreye alınma aşaması.

Burada da yine güvenlik açıkları ortaya çıkabilmektedir. Güvensiz API uç noktaları, bulut hizmetlerindeki yanlış yapılandırmalar ve yetersiz şifreleme, yapay zekânın uygulama ortamlarında manipülasyona ve saldırılara uğramasına yol açabilir. Özellikle insansız hava araçları gibi sistemlerde eğer bu tür açıklar varsa saldırganlar seyir rotalarını değiştirebilir veya sistemlerin kontrolünü ele geçirebilir. Son aşama bakım aşaması. Burada da güvenlik açısından kritik bir süreç var. Sistemlerin sürekli izlenmesi ve güncellenmesi gerekmektedir. Yine güvenlik yamalarının, gerekli güvenlik yamalarının zamanında yapılması gerekmektedir.

Özellikle siber güvenlik uygulamalarında yapay zekâ destekli savunma sistemlerinin bakımının ihmal edilmesi, sistemlerin saldırılara karşı daha savunmasız hale gelmesine yol açabilir. Özetlemek gerekirse yapay zekânın güvenlik zafiyetleri, yaşam döngüsündeki her aşamada farklı tehditlere yol açabilmektedir. Yapay zekâ modeli oluşturma sürecinde, yapay zekâ yaşam döngüsündeki tüm bu açıklar hem güvenlik uzmanlarının hem de teknoloji geliştiricilerinin dikkat etmesi gereken temel unsurlardır.

Ülkemizde eğer bir yapay zekâ modeli geliştireceksek, ki bu oldukça kritik ve acil bir konu. Özellikle son gelişmelerden sonra. Burada nelere dikkat etmeliyiz, bunları da özetlemek isterim. Ülkemizin aslında temelinde, bunun önemini yine vurgulamak istiyorum, yerli yapay zekâ teknolojilerinin geliştirilmesi gerekmektedir, bu oldukça bir konudur. Yapay zekâ alanında dışa bağımlılığı azaltmak için yerli çözümler oldukça önemli. Yerli yapay zekâ çözümleri, burada bizim güvenliği kontrol altında tutmamızı sağlayacak en önemli maddelerden bir tanesidir.

Yine özellikle vurgulamak istiyorum, Türkiye'nin savunma sanayinde yerli yapay zekâ çözümlerinin entegrasyonu, ulusal güvenlik açığını azaltarak daha sağlam bir savunma kapasitesi oluşturulmasını sağlayacaktır. Yine Türkiye'nin yapay zekâ güvenliği stratejisi, bizim biliyorsunuz yapay zekâ konusunda bir yol haritamız var, siber güvenlik konusunda bir yol haritamız var, aslında yapay zekâ güvenliği stratejisini de oluşturmamız gerekiyor. Eğer böyle bir dil modeli geliştirecekseniz, zekâ güvenliği stratejisini de oluşturmak büyük bir örnek arz etmektedir.

Ve eğer bu güvenlik stratejisini oluşturacaksak, özellikle askeri ve istihbarat sistemlerini yapay zekâ güvenliğine entegre ederek başlamalıyız. Yapay zekâ askeri ve istihbarat alanlarında büyük veri analizi, siber savunma, terörle mücadele gibi kritik görevlerde birçok çalışmayı hızlandırabilir ve çok da fayda sağlayabilir. Ancak tabi ki bu sistemlerin başlangıçtan itibaren güvenli bir şekilde tasarlanması ve güvenlik protokollerinin en baştan uygulanması önem arz etmektedir. Bir diğer önemli konu ise açıklanabilir yapay zekâ konusu.

Bu teknolojiye yatırım yapılması gerekmektedir. Yapay zekâ sistemlerinde karşılaşılan en büyük güvenlik zafiyetlerinden biri karar alma süreçlerinin şeffaf olmamasıdır. Aslında bu yüzden Türkiye olarak ülkemiz olarak ulusal güvenlik sistemlerinde kullanılacak olan yapay zekânın açıklanabilir olmasına özen gösterilmelidir. Bu şekilde yapay zekâ sistemlerinin nasıl çalıştığı ve hangi verilerle karar aldığını şeffaf bir şekilde ortaya koyarak yapay zekânın doğruluğunu arttırmış oluruz.

Son olarak da yapay zekâ sistemlerinde sürekli denetim ve güvenlik testlerinin yapılması gerekmektedir. Bunun da aslında bizim stratejimizin önemli maddelerinden biri olması gerekmektedir. Bu noktada ülkemizde çalışan siber güvenlik firmaları ve araştırma merkezleriyle iş birliği yapılarak penetrasyon testleri ve sürekli izleme sistemleriyle birlikte yapay zekânın dayanıklılığını artırmak önemli bir konudur.

Özetlemek gerekirse, yapay zekâ ulusal güvenlik alanında çok önemli fırsatlar sunmakta, fakat bu fırsatlar aynı zamanda bazı riskleri de beraberinde getirmektedir. Dünyada önde gelen CIA, NSI ve MSS gibi önde gelen istihbarat kurumları, bu dönüşüme hızlı bir şekilde adapte oldular. Yapay zekâyı aktif bir şekilde uzun yıllardır kullanıyorlar. Avrupa Birliği de bu yolda ciddi bir adım atmış durumda ve sırada açıkçası bizim de hızlı bir şekilde böyle bir dil modeliyle bu konuları ön plana çıkartarak askeri ve istihbarat alanlarında bunları kullanmamız gerekmektedir. Ben açıkçası yapay zekâ teknolojilerinin geleceğin güvenlik tehditlerine karşı hazırlıklı olmak için bugünden güçlü politikalar ve stratejiler gerektirdiğini ifade ederek sunumumu bitirmek istiyorum.

Saygılarımla.



Bülent ARSAL
STM

Teşekkürler sağ olun. Öncelikle hepinize ayrı ayrı teşekkür ediyorum. panelin son sunumu. Ama hem kendi tecrübelerimden hem de basit ama etkili neler yapılabilir, yöntemler neler, bunlardan bahsedeceğim. Aslında temelinde siber güvenlik tatbikatlarından bahsediyor olacağım. Daha önceki panelde simülasyon ortamlarına dair

bilgiler verilmişti. Bunun aslında biraz siber güvenlik tarafındaki durumu konuşmuş olacağız.

Ben yaklaşık 2,5 yıldır savunma sanayi de çalışıyorum. Daha önce Bilgi ve Teknolojileri Kurumu (BTK) bünyesindeki USOM'un başkanlığı görevini yapıyordum. Orası tamamen telekomünikasyon, iletişim haberleşme ve tamamen odağı siber güvenlik. Bu tarafta tamamen savunma sanayi. Şunu fark ettim, savunma sanayinde siber güvenlik biraz geriden geliyor, önceliği biraz geride. Gerçekten çok önemli yapıyoruz, SiHA'lar var, gemilerimiz var, uçaklarımız var. Bunların fiziksel bir karşılığı var hepimizde, bunlar genelde sistem olarak yapılıyor ve mümkün olduğu kadar dışarıya açık değil. Dost düşman tanıyor, onlara göre dizayn ediliyor ve siber güvenlik biraz daha geride kalıyor. Ancak, hepimizin de takip ettiği gibi artık normal IT sistemleriyle, bunun içine yazılımı da simülasyonu da bahsedebiliriz, uygulamaları da bahsedebiliriz. Ancak bunların hepsi artık savunma sanayinde bir üretimle çok yakınlaştı. Aslına bakarsanız hepsinin temelinde insan var.

Ben siber güvenliğe başlayalı 20 yıl oldu, 20 yıl önce başladığım en büyük sorun parolaydı. İlk geldiğim günden beri parolaydı, şu anda bakarsanız yine en büyük problem yine parola. Şimdi düşünün bir kişiye ben şifreleri versem, bir adminin parolasını elime geçirdiğimde, aslında ben gerçekten çok büyük bir iş yapmış oluyorum. Yani şunu demek istiyorum, aslında biz bazı basit uygulamalarla ve hayatımıza bir kültür olarak siber güvenliği ekleyebilirsek, çoğu saldırılardan çok rahat bir şekilde kurtulabiliriz. Şimdi biraz savunma güvenlik ve aslında siber savaşla, yani 5. Boyut olarak adlandırılan siber uzayla ve bir savaş alanı olarak tabir edilen siber güvenlik tarafındaki savaşla normal konvansiyonel savaş arasında çok

büyük bir fark var. Şöyle ki, siber güvenlik tarafındaki savaşı fark ettiğiniz anda o artık bitmiştir. Çünkü, kişi istediği şeyi almıştır, götürmüştür. Siz farkına bile varmazsınız ama konvansiyonel savaşta ne var, hatta ilan ediliyor, ben şu ülkeye savaş açtım. Veya bir tane füze gönderiliyor savaşın başladığı net olarak belli. Ama siber güvenlik dünyasında bu mümkün değil. Eğer siz fark ettiyseniz en basitinden kendi kullandığınız telefonunuz, bilgisayarınız, orada bir hareket fark ettiğinizde bilirsiniz ki oraya biri girmiş. Belki bilgileri çalmış ve götürmüş, iş işten geçmiştir. Siz artık bunu tespit etmek için uğraşırsınız. Bunun haricinde önemli bir fark daha var.

Bir önceki oturumda hukuktan bahsedildi, hukuk tarafında uluslararası hukuk hukuktan bahsedildi. Savaş, siber savaş, Çinli APT grupları, Rus, Kuzey ve İran hackerlerinden bahsedildi. Ama hiçbir zaman bunlar kanıtlanamayan, hangi sistemlerle yaptı, ne zaman yaptı, nasıl yaptı kesinlikle belli değil. Yani kendi mutlaka açıklayanlar vardı, işte İsrail çağrı cihazları konusunda bunu kendi açıkladı. Ama bunun kanıtlarına dair herhangi bir geriye yönelik bir iz bulunması çok mümkün değil. Çünkü çok kompleks, çok fazla bileşen içeren saldırılar bunlar. Dolayısıyla birbirinden çok büyük farkı var.

Siber güvenlik tarafındaki, aslında bakarsanız buradaki dinamikler çok farklı. Eğer siz normal konvansiyonel savaşta gibi savunma sanayindeki gibi bakarsanız siber güvenlik tarafına, zaten aslında bakarsanız bir adım gerideyiz. Bunu aslında çözebilmeniz çok kolay yöntemi var, tatbikatlar diyeceğim aslında ama yeterince önem veriliyor mu orası tartışılabilir. İşte ne adımları var, çeşitlerinden senaryolarından, takımlardan, yurt içi ve yurt dışı tatbikatlar var. Aslında STM Cyber Range hizmeti var. Amacım da işi biraz basitleştirebilmek. Az önce dediğim gibi parola, aslında hepimiz için çok basit bir kavram. Ama çok büyük şeylere sebep oluyor. Burada da tatbikatlar aslında görünürde çok önem verilmiyor. Benim katıldığım tatbikatlar haricinde Locked Shields hariç genelde angarya iş gibi bakılıyor tabiri caizse. Ancak ister masa başında olsun ister operasyonel tatbikatlar olsun, bunlar bizim çalışma kültürümüzü, iş yerindeki kültürümüzü ve savunma sanayindeki kültürü etkiliyor. Ve biz bu kültürü kazandığımız sürece, aslında bu konuda biraz daha fazla başarılı olabiliriz diye düşünüyorum.

Şimdi tatbikata baktığımızda bize aslında ne kazandırıyor? Bir kendi içimizde kendimiz bireysel olarak da kurum olarak da bütün şirket ve aslında bütün ülke olarak da bize bir kültür kazandırıyor. Bakış açımızı değiştiriyor. Neler var adımlarında? Bunlar ilk önce bir planlamayla başlıyor, her şey sonuçta bir planlamayla başlayacak. Burada ben neye yönelik bir tatbikat yapacağım? Çünkü siber güvenlik alanı çok geniş bir alanı kapsıyor. OT sistemler var, savunma sanayindeki sistemler var, IT sistemler, bulut sistemler, yapay zekâ var. Bu tarafta bir planlama lazım. Burada da kapsamı çok karmaşık tutmak bize bir şey katmayabilir, daha odaklı, mümkün olduğu kadar herkese bir şey kazandıracak bir kapsamda başlayıp, bununla ilgili yöntemlere uygun senaryoları hazırlıyoruz. Daha sonra aslında tatbikatı uygulamaya geçiyoruz. Bununla ilgili süreç senaryolarda neler varsa, onları başlatıyoruz, atakları yapıyoruz, karşılıklı olarak savaşıyoruz. Devamında bunun sonucundaki bir raporlama çıkıyor, bu raporlama kapsamında da ben artık kendi tarafında neler güçlü, neler zayıf bunları çıkarıp bir raporlama yapıyorum. Açık, yani zayıf yönlerimi geliştirmek için veya güçlü yönlerimi daha da geliştirebilmek için eğitim sağlıyorum. Aslında bakarsanız çok basit, belki şuna benzetiyorum ben bunu. Avrupa'da European Cyber Resilience Act (Avrupa Siber Dayanıklılık Yasası) yayınlandı. Bu da yürürlüğe girecek Avrupa Birliği'nde. Oradaki toplamda 12-13 tane madde var ve şunu diyor aslında; tüm dijital unsur içeren ürünler için orada iki kısma da ayrılıyor. Dijital unsur içeren her ürünü kapsıyor, onlar içinde 12-13 temel maddeler var. Aslında hepimizin bildiği çok basit maddeler. Neler onlar? Mesela güncellemelerinizi yapın diyor, bilinen açıkları sistemler barındırmamasın diyor. Normalde günlük hayatımızda da almamız gereken önlemler. Yapılması uygulanması çok kolay. Ama bunun size sürekliliğini sağlayıp ve işsel olarak bizim hayatımıza girmesi gerekiyor. Biraz önce de söylediğim gibi, atak öğrenildiyse iş işten geçmiştir. Biz bununla karşılaşmamak için sürekli tetikte olmalıyız. Siber güvenlik tarafında çalışan kişiler bilir, eğer norma şartlar altında işler iyi gidiyorsa, sistemler çalışıyorsa, siber güvenlik personellerinin belki adı bile bilinmez. Ama bir sorun olsun, bir sistem kesilsin veya bir tane atak yenmiş olsun, o zaman ilk başta siber güvenlikten sorumlu kişi çağırılır. Ve orada öğrenilir kim olduğu. Bu da aslında bunu engellemek için yöntemlerden bir tanesi. Ben hem kurum kültürü hem kendi yaşantımız olarak bunu kendi iç işleyişimize eklememiz gerekiyor.

Siber güvenliğin üç temel unsuru var, gizlilik, erişebilirlik, bütünlük. Ama tatbikat tarafında insan, süreç ve teknoloji var. Çok ayrıntılı sistemlerimiz ve yazılımlarımız var, ama süreç ve insan kısmında eksiğiz.

Savunma sanayi tarafında benim de tecrübe ettiğim çok fazla sürecimiz var, bu süreçler yazılı ve uyuluyor, uyulmaya çalışılıyor. Ama diğer tarafta kamu sektöründe veya özel sektörde bu kadar süreç yok. Geçenlerde takip etmişsinizdir, Rusya uzaktan Amerika'da bir kuruma uzaktan kablosuz saldırı yapıyor. Bunu nasıl yapıyor, ilk önce o kuruma yakın kablosuz ağ alanında olabilecek bir tane kurum ve şirketlere saldırıyor, onları ele geçiriyor, oranın bilgisayarından karşı tarafın kablosuz ağına dahil olduğu için oraya saldırıyor. Dolayısıyla kablosuz ağ deyip de ya benim kablosuz ağımdan buraya saldırılamaz, bu şekilde Rusya gelemmez, buraya ne olacak demek çok mantıklı olmuyor. Aynı şey savunma sanayi için de geçerli, hepimiz bilgisayar, iç ve dış ağ kullanıyoruz ama birleştikleri noktalar var. Stuxnet bunun yıllar önce gösterilmiş bir örneği aslında. Şu an olmadığına dair hiçbirimizin garantisi yok. Diğer üçüncü fark ise şu, siber güvenlik tarafındaki saldırılarda şu an olup olmadığına dair bir garantimiz yok. Şu dakikada olup olmadığını söyleyemeyiz, ya da biz saldırıyor muyuz bunu da söyleyemeyiz. Belki 6 ay geçiyor, bir sene geçiyor, artık saldırgan işini bitirmiş çıkmış ondan sonra sesini duyuruyor.

Tatbikat çeşitlerine devam edersek teknik simülasyonlar var, tamamen uygulamaya özel, ilgili kuruma özel, savunma sanayine özel, enerji, sağlık gibi sektörler için özel. Bunlar oradaki daha çok sistemleri, teknik cihazları, yazılımları kullanıp hazırlanıyor ve daha çok oradaki insan yeteneklerini ve süreçleri takip ediyor, onları kontrol ediyor. Kurumların da kişilerin de o zamanki resimleri çıkıyor. Siber saldırı olurken, olduğunda, olduktan sonra nasıl bir süreç işletiyorum, benim oradaki personelim nasıl bir tepki veriyor, ben buradan ne kadar az zararla çıkarım. Diğer de masa başı teorik uygulama. Bu da tamamen aslında süreçlerimizin gerçekten düzgün işleyip işlemediğini gösteren bir tatbikat.

Daha çok masa başı teorik uygulamalar biraz önemsenmiyor. Neler var senaryolarda, üçe ayırabiliriz. Ağ alt yapısıyla senaryolar var. IT/OT, bulut ağ mimarisi, oltalama, aktif dizin saldırıları, iç ve dış tehditler, izleme ve tespit etme, ağ güvenliği ve Ddos saldırıları gibi.

Tamamen ihtiyaca yönelik tatbikat yapılabilir. Hatırlarsanız dünyanın en büyük Ddos saldırılarından bir tanesi DNS alt yapılarına yapılan saldırıydı. Amazon, Twitter gibi sistemler bile zarar gördüler. Zararlı yazılımla ilgili kısımlar var. Bir tarafı donanımda düşünebilirsiniz. Hepimizin bildiği fidye, komuta kontrol merkezi, bot yazılımlar, malware analizi, keylogger, trojan, webshell gibi ya da uygulama güvenlik zafiyetleri, açıklarıyla ilgili saldırılar var. En önemlilerinden biri de siber güvenlik zafiyetleri ve açıklarıyla alakalı olanlar. Çünkü çok fazla sistemimiz var, çok fazla teknoloji kullanıyoruz ve bunların gerçekten güncel olup olmadığını, burada zafiyet olup olmadığını, bunların kapatılıp kapatılmadığını takip etmek çok kolay iş değil. Bunun için ayrıca ciddi tatbikatlar yapılması uygun oluyor.

Diğeri de yine önemli bir kısım. Aslında yönetim süreçleriyle ilgili senaryolar var. Hem bizim bir olay olduğunda mutlaka bunun bir kanuni yaptırımı olabiliyor, yurt dışından olabilir, yurt izinden olabilir. KVKK ile ilgili veri ihlal bildirimi varsa bir işlem sürecimiz olmalı. Bir saldırı olup olmamasını zamanında tespit edebilmek için bunların uygulaması, tehdit istihbaratı ile ilgili saldırıyı engellemekle ilgili senaryolar var. İletişim kanalları ayrı bir husus, çünkü bunun uygun bir şekilde bir repütasyon kaybı olmaması için ilgili yerlere aktarılması gerekiyor. Tatbikat takımları var, kırmızı takım aslında saldırabilmek, ele geçirmek için her türlü yöntemi kullanan kısım. Savaşta her şey mübahtır deyip bildiği her şeyi kullanan taraf. Mavi takım da tamamen 'Çanakkale Geçilmez' noktasında savunmaya çalışan, her türlü tedbiri almaya çalışan, bütün analizleri yapan kısım. Yani bunlar karşılıklı burada hem kendi yeteneklerini ölçüyor hem de kurumun o konudaki gerçekten dayanıklılığını ölçmeye çalışıyor. Yurt içi ve yurt dışındaki tatbikatlar var.

NATO her yıl düzenli tatbikatlar yapıyor. En önemlisi Locked Shields, NATO Siber Komutanlığı tarafından koordine ediliyor. Buraya bir sürü kamu kurumu, özel sektörden destek olunuyor. Aynı şekilde NATO tarafına da destek olunuyor. Yurt içi tatbikatlarının ayrı bir önemi var. USOM tarafından düzenleniyor, yurt içi farklı sektörler farklı olacak şekilde Finans sektörü, enerji sektörüne ayrı, yurt dışıyla birlikte eş zamanlı tatbikatlar da var. Buranın biraz farkı, saldıran takım genelde USOM kendi oluyor, diğerleri bir sistemi kendisine yapılmış sistemi savunmaya çalışıyorlar

Burada vurgulamak istediğim nokta, bizim gerçekten basit bazı tedbirlerle çoğu siber saldırıları engelleyebileceğimiz ve buradaki gerçekten farklı bir dinamizme sahip olan siber güvenlik dünyasında gereken tedbirleri almanın önemi.

Bizim STM tarafında da bir Cyber Range hizmetimiz başladı. Burada dört farklı kısmımız var. Çok basit olarak akademi kısmımız var, senaryo kısmımız var, Laboratuvar kısmımız var ve Cyber Range alanımız var. Amacımız, tamamen ilgili kurumun, şirketin, savunma tarafındaki şirketlerin kendi akademi tarafında eğitim, personel kalitesini ve yetkinliğini arttırmak. Üç farklı aşamada oluyor, ilk girenler, orta ve üst seviyede. Ve bunlar takip edilip rehberlik yapılıyor. Diğer senaryolar. Senaryoları geliştirip ilgili kişinin saldırgan gibi, hacker gibi düşünmesini sağlayabilecek, onların bakış açısını kazandırabilecek, onların yetkin olabileceği senaryolar var. Farklı yetkinlik seviyelerine uygun, güncel ve sürükleyici pratik senaryolar bunlar. Laboratuvarlar var, bir konuda uzmanlaşmak isteyebiliriz. Örneğin savunma sanayindeki bir ürün tarafındaki bir cihazda uzmanlaşmak isteyebilirsiniz. Oradan da onunla ilgili bir laboratuvar oluşturup orada sonuna kadar bu konuda yetkinliği kazandıracak bir kısım oluşturuyoruz. Diğer de Cyber Range alanı, aslında bütün akademi, senaryolar ve laboratuvarları birleştirip, bir araya getirip, kırmızı ve mavi takımı bir araya getirdiğimiz ve karşılıklı olarak onların birbiriyle mücadelesini izlediğimiz bir sitemimiz var. Böylece biz Cyber Range tarafıyla beraber bütün şirketlerin, bütün kurumların, TSK'nın, savunma sanayinin siber güvenlik alanında farklı bir dinamizme sahip siber güvenlik alanında yetkinliklerini artırmayı hedefliyoruz. En azından siber güvenlik tarafında, örneğin pager olayı gibi son zamanlarda yaşadığımız saldırılar gibi olaylarda en az zararı görmek, mümkün olan en erken zamanda tespit ederek gerekli tedbirleri almak ve bu noktaya gelmeden gerekli güvenlik tedbirlerini almak arzusundayız. Çünkü siber güvenliğin asıl önemli kısmı ben hacklenmeyeceğim kısmı değil, en kısa zamanda ben bunu nasıl tespit ederim, en az zararı nasıl görürüm şeklinde yaklaşımla bu tarafta kendi etkinliğimizi artırmak için çalışmamız gerekiyor. STM olarak da bunun için her türlü hizmeti sağlamaya çalışıyoruz.

Teşekkür ederim.



Çağlar AKMAN - HAVELSAN - CENGAVER SUNUMU

Merhaba, Havelsan'ın geleceğin askeri konsepti olan Cengaver'i canlı demoyla anlatacağım sizlere.

İlk olarak Dijital Birlik ne anlama geliyor? Dijital askerin ne tür ihtiyaçları olduğuna dair adımlardan geçtikten sonra Havelsan'ın dijital asker konseptinden ne anladığını Cengaver ismiyle size ne sunduğunu anlatacağım, aktaracağım, devamında da gerçek demomuzu yapacağız.

Dijital Birlik konsepti ile başladığımızda ilk olarak anlaşılması gereken aslında 'entegre akıllı tümleşik bir ağ'. Bu ağ içinde sensör ve network ile başlayan durumlar, her bir sensörün sağa sola yerleştirilmiş statik sensörlerden artık kognitiv varlıklar olarak bizlerin üstünde giyilebilir sensörler ya da robotik teknolojisinin üstüne yerleşmiş perception ya da etrafı algılamayı sağlayacak yapıya sahip heterojen sensörlerden değil de aktüatörlerinde olduğu, etrafa müdahale edebildiği bir birlik anlamamız gerekiyor. Şu anda yaptığım tanım mühendislik tarafında kaldı, bunun askeri jargonu yoktu. Dijital birlik dediğimize, biraz önce kurduğum mimari yapının içine geleneksel askeri yetkinlikleri, stratejiyi, geleneksel askeri bakış açısında birleştirdiğimizde 'Dijital Birlik' konsepti ortaya

çıkmiş oluyor. Dört tane hiyerarşik bloğa ayırabiliriz. ADHOC network (geçici kablosuz iletişim ağı) bu işin olmazsa olmazı. Çünkü hareketli birimlerden oluşuyor, sahada kendi kendine karar alan bağımsız küçük gruplardan tutun da geniş taburlara kadar çeşitli birimlerin olduğu ve bunları da artık destekleyen insan birimlerinin yanı sıra otonom sistemler var. Devamında, sahaya indirilmiş askerimiz, 'Digital Soldier, Future Soldier veya Dismounted Soldier' olarak adlandırabilirsiniz.

Otonom araçlar, insansız hava, kara, deniz araçları üçüncü, durumsal farklılık resminin oluşmasını sağlayan teknolojiler ise dördüncü bölümü oluşturuyor. Bütün bu özellikleri dijital birlik olarak eline alıyor dijital asker konsepti. Aslında en uç birim burada geleneksel askeri taktiklerin teknolojiyle birleştiği bir birim. Burada yapılması planlanan şey, askerin kendisinin etkinliğini, kendisinin durumsal farkındalığını artırarak daha etkin, daha efektif kararlar alması.

Tüm bu ihtiyaçlar için Havelsan'ın vizyonunu yansıtan ürünümüzün ismi 'Cengâver.' Şimdi gerçek bir Cengâver askerimiz üzerinde anlatımımıza devam edeceğiz. Sağlık ve aktivite verilerini, lokasyonu alabileceğiniz akıllı saat, gerçek zamanlı görüntü akış desteği sağlayan başlık ve gözlük, iletişim kulaklık ve mikrofonu, giyilebilir sensörler ve işlemciler, durumsal farkındalığın artırılması temel hedefiyle tasarlanan taktiksel ve taşıyabilir DOOB sistemi, eklenebilir .

Ve üzerinde taşıdığı karmaşık teknolojik birimlerle rafine bilginin kendisine ulaşmasıyla çevresinde ne olup ne bittiğini algılayabilen, ürettiği bilgiyi hem takım içinde arkadaşlarıyla veya diğer takım elemanlarıyla paylaşabilir sistem çözümü kurmaktan bahsediyoruz.

Dijital askerin ihtiyaçları, gereksinimleri neler olabilir? Başlığına geçelim, ilk olarak çevresel sensörler. Alışık olduğumuz, etrafa konan, etrafa yerleştirilmiş alan, KBRN gibi tehditleri algılayabilecek, etraftaki tehditleri algılayabilecek, atış tespit sensörleri bulunuyor. Bu örnekler çeşitlendirilebilir ve bu dijital askerin bir parçasıdır. Burada operasyonel konseptte uygun olarak, uygun ekibin sensör çözümünü giyilebilir teknolojilerle eklememiz gerekiyor. Batarya ve kablosuz haberleşme teknolojisinin gelişmesiyle daha çok verinin çok hızlı bir şekilde bir merkezden başka bir yere iletilebilir gerçeği ve giyilebilir teknolojinin de geliştiğini düşünürsek, dijital askerin bir parçası olduğunu görebiliyorsunuz.

Yoksa bir ağaç süslemesi gibi her yerinden sensörler sarkıyor olacak gibi bir durum yok. Çoklukta değil, yoklukta, en az malzemeye maksimum durumsal farkındalık bilgisinin edinilmesi gerekliliği en önemli hedeflerimizden. Bu ilk iki basamakta yönetilemeyen bir kompleksi kullanıcının takmak istemediği bir çözüme yönelmiyoruz. Komünikasyonun efektif, etkin bir haberleşme için uygun bant genişliğinde, uygun bir şekilde verinin hem bir takım hem de merkezle paylaşılmasını hedefliyoruz.

Dijital birliğin konsepti olan otonom cihazlarla etkileşimli bir şekilde bu bilgilerin birleştirilmesi, eş zamanlı bilgi alabilmek, nihayetinde karar destek çıkacak ortaya. Havelsan olarak harbiye ismiyle geliştirdiğimiz komuta kontrol sistemi, DOOB ürün ağacı gibi ürünlerimizi de entegre ederek taktik sahadan operasyonel ve stratejik seviyeye kadar karar destek ve durumsal farkındalık resmini sağlamaya çalışıyoruz sistem üzerinden.

Son bileşeni ise fiziksel güvenliğin yanı sıra siber güvenlik olarak özetleyebiliriz. Bunu Havelsan'ın geliştirdiği ürünlerle lego gibi, yapboz gibi ele alabiliriz. İstedığınız kısım silinsin, yenisini veya gerekli olanı ekleyin gibi. Unutulmaması gereken şey, personelin taşımayacak kadar ağırlığı üstüne yükleyemeyecek olmamız.

Konu sadece ağırlık değil, biz 30 kiloyu geçmeyecek, 72 saat çalışacak, 36 saat çalışacak gibi talepler olabilir. Bu yeterli değil, son kullanıcılarla mühendisler bir araya geldiğinde ölçülebilir metrikler üzerinden konuştuğumuz için bu şekilde söylüyoruz. Gereksinim olarak tanımlayabiliriz ama günün sonunda insanın bunu kullanacağını unutmamamız gerekiyor. 'Hareket kuvveti ve yeteneği' olan 'motility' hedefimiz, 'hareketlilik' anlamındaki 'mobility' değil. Yani hareketliliği engellemek. Kolunun, bacağının herhangi bir sensörden dolayı rahatsız olmaması lazım, hareket esnekliğini engellememesi gerek. O yüzden istenilen her özellik eklenebilir ama ihtiyaca yönelik ve huzurunu, konforunu da özellikle operasyonunun verimliliğini bozmayacak bir ürün çıkarmalıyız.

İlk önce dijital birliğin olmazsa olmaz omurgası iletişim ve haberleşme. Burada hedefimiz 'neredesin, nasılsın, iyi misin?' gibi mesela çocuklarımız için sorduğumuz sorunun cevabına benzetilebilir. Biz de insanı sensöre çevirdikten sonra, haberleşme ağıyla bir iletişim ağına, networke bağlıyoruz.

Geleneksel olarak GPS dış mekanlarda çalışıyor ama kapalı ortamlara girdiğimizde hazır çözümler var geçmişten gelen bluetooth, wi-fi ile ilgili çözümler bulunmaktaydı. Havelsan olarak geçtiğimiz sene 8 tane patent aldığımız yazılımlarımız ve protokollerimizde 8 tane patent ultra geniş bant tabanlı bir bağıl konumlandırma, görelî konumlandırma çözümümüz bulunmaktadır. Hem daha önce girilmiş hem de daha önce girilmemiş ortamlarda hassas konumlama yapabiliyoruz. Bu bilgiye 'neredesin' cevabıyla saatten ulaşıyoruz. Çocuklarda bulunan kalp atışı, kandaki oksijen seviyesi, sıcaklık seviyesi gibi bilgilerin yanı sıra koşuyor mu, yürüyor mu, bayıldı mı, öne mi düştü, sağa mı düştü, vücudunda beklenmedik bir kalp ritmi artışı var mı gibi. Bu bir klinik saat değil, bu bir sağlık saati. İstenilen bilgilerin, bilgilerin artırılmasının konulacak sensör sayısına bağılı olduğunu tekrar belirtmeliyim.

Peki bilgileri topladık da ne yaptık? Bunu demomuzla da anlatalım. Sahada bulunan askerin elinde ister cep telefonu ister tablet olabilir, ara yüz üzerinden kendisinin durumunu, çevresindekilerin durumunu, tehditlerin durumunu gösterebileceği bir yazılımımız var. Günün sonunda bu asker sahada olsaydı sadece telsizi ve saati olacaktı. Eğer komutan daha fazla bilgi istiyorsa, uzaktaki karargâha görüntü aktarımı için gözlüğü de olabilir. Ortada bir masa varmış gibi, komutan sahadaki tüm personelin gerçek zamanlı olarak konumunu takip edebilecek, sağlık durumunu takip edebilecek, üzerindeki kamera ile otonom çalışan sistemlerle de birleştirilen görüntü ve verileri elde edebilecek. Artırılmış gerçeklik ve karma gerçeklik içeren grafiklerle de verilerin gerçekliği ve gerçekliğe yakınlığı desteklenecek. Bu arada dron ise kilit ekip elemanını takip edebiliyor. Dron onu belirli bir açıdan takip edebilir.

SORU: Sahnedeki askerimiz genç. Örneğin 2000 doğumlu bir askerimiz Windows yazılımını kullanarak doğmuş olacaktı, sanal gözlüğü takan komutan ise 40-50 yaşlarında, onun emir alacağı ise belki daha ileri yaşlarda. Burada X, Y ve Z nesli gibi üç farklı kuşaktan bahsediyoruz. Android, DOS, Sanal gözlük gibi farklı kuşak teknolojilerden bahsediyoruz. Bu teknolojilerde nesil farkı nasıl aşılacak? Bir de sunumunuz yazılım odaklıydı, donanım tarafında ABD'nin başlatıp iptal ettiği ve yeniden açtığı IVAS projesi var. Buradaki en önemli husus elektronik

harp ve savaş ortamına uygun, dayanıklı donanım üretimi ve hacimli miktarda üretimiyle ilgili konulardaki önerinizi öğrenebilir miyim?

CEVAP: Sürekli olarak sensörler, elde edilen bilgiler, mühendis ve son kullanıcı vurguları yapmıştım. Bizim niyetimiz, biz böyle şeyler yapıyoruz, yapabiliyoruz değil? Biz taktiksel ve geleneksel olarak militer taktikleri öğretemeyiz, onlar bize öğretecek. Onlara yeni oyuncak vermek de değil hedefimiz. İhtiyaç olduğunu bildiğimiz bilgi ve donanımı sağlayacak tekniklerle geliyoruz. Yoksa biz istediği kadar farklı sensör koyar, projecikler ekleyerek yapıp göz boyayabilirdik. Daha renkli bir sunum da yapabilirdik. O yüzden de basit sorularla anlattık, 'neredesiniz' ve 'nasılsınız' gibi cümlelerle anlattık. Bu sistem bütün askerlere konulacak mı? Yerine konulamayacak, özel kuvvetler, özel harekât, eğitiminin, maliyetinin zor olduğu personele konulabilir belki. Yani şu anda bu teknolojiler yoktu da askeriye eksik miydi? Hayır değildi, yani bunlar olmadan önce çok daha sıkıntısı mı var, hayır.

Biz burada diyoruz ki, siz zaten bu ihtiyaçları telsizle, yazışmalarla alıyorsunuz. Biz bunu hızlandırıyoruz. Bir de sizin zaten kognitif olarak asistan veriyoruz. Asistan kalkıp da komutana komutanlığı öğretmeye kalkmayacak ya da yeni doktrin yazmayacak. Biz teknolojilerle neler yapılabileceğini gösteriyoruz, o isterse yazılı olarak da tekrar alıp okuyabilir. Gözlük olmak zorunda mı? Değil. Sahadan gereken değerli ve işe yaradığı bilinen bilginin toplama şekli değişmeyecek, biz de bunu hızlandırıyoruz. Durumsal farkındalık konusunu savunma sanayii askere öğretmedi, asker durumsal farkındalık ontolojisini savunma sanayiye öğretti. Biz onlara uyuyoruz. Biz de onlardan öğrenmiş olduğumuz ve sınırlarını çizdikleri şeyleri teknolojiyle nasıl daha kullanılır hale getireceğimizi sunuyoruz.

Donanım konusunda ise, yazılım olmadan telefon alır mısınız? Donanım olmadan da yazılımı bir yere koyamayız. Donanım önemli ama yazılımlar, uygulamalar, işlevsellikler olmazsa donanım da değersiz. Donanım üretim kısmı dünyada oturmuş durumda. Donanımın kullanışlı tasarımı için de çok büyük yatırımlar gerekiyor. Biz hiçbir şekilde donanım referanslamıyoruz. Bizim Havelsan olarak patentli algoritma

ve yazılımlarımız var. A, B, C, D, E firmaları da bu işlere uygun donanımlar üretebiliyor, biz yazılımı entegre edebiliriz diyoruz. Havelsan'ın büyük vizyonu yazılım ve algoritmaya odaklanmak. Cengâver, teknolojilerin her aşamasının eklenmesiyle tek-er bazında, Komuta ve Kontrol konseptinde görev ve yetkilerin tek askerden en üst düzey karar vericiye kadar tanımlandığı, stratejik planlamanın yapıldığı, planların taktik ve tek asker seviyesine iletilmesini sağlayacak iletişim altyapısının sağlandığı ve tüm seviyelerde durumsal farkındalığın sağlandığı bir "sistemler sistemi" olarak geliştirilmesi hedeflenmektedir. Benzerleriyle karşılaştırıldığında sensör sayısı, gerçek zamanlı veri iletimi ve konumlandırma özellikleriyle üstünlük sağlamaktadır.

SORULAR ÜZERİNE EK TEKNİK AÇIKLAMALAR:

- Sistem, topografik veya harita bilgisi yoksa, ilk girilen ortamlarda konumsal bilgi sağlayacak. Mağara ve benzeri ortamlar için anlık haritalama yapan teknolojiler kullanıyoruz lidar ve farklı sensörlerle. Sağlıkla ilgili klinik değil, operasyonel sağlık verilerini alıyoruz.
- Sağlık ve kondisyon ile ilgili verilerde kliniksel sağlık değil, operasyonel sağlık verileri öncelikli. Ancak bu verilerin kapsamı genişletilebilir.
- Bir Tabur, Tugay veya er bazında her türlü özellik, veri aktarımı ve özellikler karar vericilerin taleplerine göre değiştirilebilir.
- Avrupa Birliği projesi bitirdik yakınlarda. Haziran 2024'te Brüksel'de teslim ettik. Dijital Birlik kapsamında benzer bir sistemi, üst düzey sorumlulara özel askerlere bu sistemleri teslim ettik.



KAPANIŞ KONUŞMASI

Semih DEMİRTOKA – HAVELSAN

Değerli katılımcılar, kıymetli misafirlerimiz,

İki gün süren Future Soldier – Geleceğin askeri etkinliğimiz boyunca burada son derece değerli paneller gerçekleştirildi, değerli bilgiler paylaşıldı. Benim de Hibrit Teknolojiler ve Çoklu Alan Operasyonları panelinde panelist olarak katkıda bulunma fırsatım oldu. Görüşlerimizi paylaşma, sizlerden güzel sorular alma şansını, imkanını yakalamış olduk. Yeni Dünya, Yeni Savaş ve Yeni Savaşçı konuları çerçevesinde geleceğin askeri ve teknolojileri konuşuldu. Biraz önceki panelde bu değişim dönüşümün yönetimiyle ilgili bir atıfta bulunulmuştu. Aslında bu geleceğin askeri konusu teknolojik olmakla birlikte, bizim zihniyetimizin değişmesi gereken, devamlı, yenilikçi ya da işte yıkıcı diye tabir edilen, moda tabirle kullanayım, yıkıcı denilen konularda devamlı nasıl geliştirme yapılabilir, bunun arayışı içerisine girmek gerekiyor. Ben de o anlamda, bu konferansı bu bağlamda değerli buluyorum. Savunma sanayi burada, hepiniz savunma sanayi çalışanları ya da ilgililerisiniz, diğer sektörlerde de olmakla birlikte özellikle bizim sektörün heyecan veren, diğer sektörlerde de rekabetçilik var, bence bizim sektörde heyecanlı tutan, diri tutan, siz bir tedbir geliştiriyorsunuz, karşı taraf bir karşı tedbir geliştiriyor, sizin onun karşı tedbirine karşı bir tedbir almanız gerekiyor. Dolayısıyla devamlı bir yarış içerisindeyiz, yüksek hızda akan bir nehrin içerisindeyiz, hayatta kalmaya çalışıyorsunuz. Hatta daha önemlisi lider olmaya çalışıyorsunuz. Dolayısıyla bu bağlamda ben bu Future Soldier – Geleceğin Askeri konferansını değerli buluyorum.

Kapanış konuşması için aslında SASAD Yönetim Kurulu Başkan vekilimiz ve Havelsan Genel Müdürümüz Dr. Mehmet Akif NACAR Bey katılacaktı. Ama Hindistan'da Havelsan'ın ilk sivil simülatör ihracat başarısını yakaladık, onunla ilgili sözleşmeyi imzalamak için Hindistan'a gitti. Buraya yetişemediği için de beni gönderdi. Ben tekrar katılımlarınız için teşekkür ediyorum.

Bir sonraki etkinlikte görüşmek üzere, iyi çalışmalar.

DEĞERLENDİRME VE SONUÇ BÖLÜMÜ

DEĞERLENDİRME

GELECEĞİN ASKERİ TEKNOLOJİLERİ VE SEKTÖRE DAİR

YAPAY ZEKÂNIN ÖNERİLERİ

SONUÇ

DEĞERLENDİRME



- Yapay zekânın askeri sistemlerde ve teknolojilerde kullanımı artacaktır.
- Yapay zekânın temel aracı ve gerçekten en iyi olduğu şey, veriyi parçalayabilmesi ve verileri analiz edebilmesi olarak sunulurken, günümüzdeki dönemde hayatımızda ve askeriyede en büyük katkısının analitik kolaylaştırıcı merkezli olarak ele alınması gerektiği ifade edilmiştir. Günümüzde henüz yapay zekânın ilk adımlarını attığı ve asıl gerçekliğinin hissedileceği yakın gelecek için hazırlıkların hızlandırılması önerilmektedir.

- Savaşlarda bilgi operasyonları ve bilgi operasyonu ile yıkımın en eski strateji olduğu ve tarihsel süreçte yöntemlerinin değiştiği hatırlatılırken, yapay zekânın da ölçeklenebilir ve ölçülebilir son nesil bilgi operasyon aracı olduğu tanımına da yer verilmiştir.
- Geleceğin savaş ortamında haberleşme, komuta kontrolü, iletişim bilgisayarları, istihbarat, keşif, gözetim ve hedef tespiti yeteneklerinin yapay zekâ uygulamalarının ilk hedefi olacağı yönünde ortak görüş hakimdir.
- Yapay zekânın, yakın gelecekte strateji oluşturma, düzenleme ve tamamlama süreçleriyle savunmanın üretkenliğini dönüştürecek, askeri kabiliyetleri değiştirecek öngörülmektedir.
- Çin, Rusya, Hindistan, Amerika gibi ülkelerin yapay zekâ teknolojilerini otonom ve robotik teknolojilerde özellikle otonom sürüler alanında ve elektronik harpte kullanımında önceliklendireceği düşünülmektedir. Yapay zekânın askeri ve stratejik rekabet üzerinde belirgin bir rol üstlenmesi beklenmektedir.
- Amerika'nın yapay zekâ algoritmasıyla jet uçurabildiğini ve özerk olarak 8 farklı görevi yerine getirebilmesi yapay zekânın doğum aşamasında yapabildikleri olarak tanımlandı. Yapay zekânın insan beyninden daha hızlı çalışması dolayısıyla, bu tür bir teknoloji ile büyüyen özerkliği, endüstriye ve insan kaynağına nasıl entegre edebileceğimizin iyi kurgulanması gerekliliği paylaşıldı.
- Yapay zekâ destekli askeri yeteneklerin, hız, konum ve öldürücülüğü artırarak teknolojik askeri kabiliyetlerin etkisini artıracakı düşünülmektedir.
- "Rakibin geliştirdiği bir teknolojide geride kalmak, olası felaketlerin önünü açmaktır" prensibiyle gelişen her teknolojiye ilgi gösterilmesi tavsiye edilmektedir.
- Yapay zekânın yakın dönemde, kendi kendine öğrenen ve yorumlayan askeri sistemler üzerinde denenebileceği ön görülmektedir. Ve düşmanca tutumu anlayarak tepki vermesi üzerine eğitilmeye başlandığı kaydedilmektedir.

- Yapay zekânın kullanımı, bilgi üstünlüğünün derecesini belirleyecek faktör olarak görülmektedir.
- Yapay zekânın verilen veriyi taklit etmek olduğu, orijinal bir şey bulmak yerine verilerden yorum yaptığı da unutulmamalı. Dolayısıyla yapay zekânın tam anlamıyla sonuç vereceği eğitim süreçlerine kadar kontrol ve optimizasyon sağlayan algoritmalarla geliştirilecek yöntemler de tavsiye edilmektedir. İnsan geri beslemeli, karar alacak veya tavsiye de bulunacak opsiyonların geliştirilmesine de önem verilmesinin kritik kararlar da ve iş verimliliğinde katkı sağlayacağı düşünülmektedir. Bu yönde yazılımlar, projeler ve çalışmalara yapay zekânın gelişimi sürecinde öncelik verilebilir.
- Blockchain teknolojisinin büyük veri süreçlerinde kuantum teknolojileriyle birleşerek güvenli bir veri alt yapısı sunacağı düşünülmektedir.
- Siber saldırılar dijital ve fiziksel dünyanın kusursuz entegrasyonu olarak savaşları etkileyecek doktrinlerin kaynağı olabilecektir.
- Kuantum haberleşme teknolojileri yakın geleceğin farkı belirleyen ve sistemleri güvenli kılan şifreleme sistemi olacaktır. Uyum kadar bu konuda tedbirlerin geliştirilmesi de öncelikli konular arasında olmalıdır.
- Kuantum sensörler, biyoteknoloji ve nanoteknoloji alanları hızla gelişecektir. Bu yönde gelecek projeksiyonlarına ve yatırımlara ihtiyaç vardır.
- İnsansız hava araçlarının ve otonom uçakların hava hakimiyetindeki etkisi artarak devam edecektir.
- Yapay zekâ destekli otonom görev tamamlayabilme özellikleri, elektronik harp karşısında önemli bir avantaj sağlayacak faktör olarak nitelendirilmektedir.
- Yapay zekâ da dahil, tüm teknolojilerde geliştiren ve teknolojiye yön veren olmak gerekmektedir. Özellikle kritik teknolojilerde ortak iş birliği modelleriyle yatırım teşvik edilmelidir.

- İnsansız kara ve deniz araçları, robot köpekler savaş alanlarında küçük robot savaşlarının ilk işaretleri olarak kabul edilirken, 10-20 yıllık süreçte orta ve büyük robotların önce lojistik, devamında ise aktif savaş personeli olarak sahaya inmesi öngörülmektedir.
- Sürü halinde hareket eden otonom hava, kara ve deniz araçları yakın gelecekte savaş alanlarında çok daha fazla etkin olmaya başlayacaktır. Otonom askeri teknolojiler ile geleneksel savaş teknolojilerinin bütünleşmiş operasyon konseptlerinin suni çatışmalarla gerçek sahalarda bir süre daha test edileceği düşünülmektedir.
- Alçak yörünge uydularının öneminin artacağı öngörülmektedir. Elon Musk'ın Starlink uydu teknolojilerinin Rusya-Ukrayna arasındaki çatışmada üstlendiği görevler, bu öngörüğü desteklemektedir. Önümüzdeki yıllarda, yakın yörünge, ay ve dünya yörüngesinde uzay rekabeti ve savaşlarının başlayabileceği düşünülmektedir.
- Keşif, gözetleme, istihbarat ve casus uydular kadar, bunları kullanarak çalışan sistemler için savunma sistemlerinin geliştirilmesi, füzelerin de elektronik harp özellikleri kazanmasına yönelik çalışmaların önem kazanacağı ifade edilmektedir.
- Sinyal bozucu sistemler, hedef yanıltıcı sistemler yapay zekâ ile farklı bir boyut kazanacaktır. Dijital ikiz konusu, elektronik harp alanının önemli savaş doktrinleri arasında elektronik bir manipülasyon yöntemi olarak öngörülmektedir.
- Sahada manevra kabiliyetini ve lojistiği etkileyen araç ve sistemler, düşman tarafından tespiti engelleyen teknolojilerin gelişimine ve bu alanda yeni ürünlere ihtiyaç bulunmaktadır.
- Büyük veriden elde edilen analiz sonuçlarından durumsal farkındalığı artıracak görsellerin üretilmesi, operasyon anında ve eğitimlerde süreçlere katkı sağlayacaktır.

DEĞERLENDİRME



- TEK-ER'in kıyafetlerinde vücut ısısının düzenlenmesi, kızılötesi ışınlara karşı önlem, kullanacağı teknik cihazlar için düşük enerji kullanımı ve hareketten ve çevresel faktörlerden enerji üretimi sağlayan sistem entegrasyonu çalışmaları dünyada yaygın olarak yapılmaktadır.
- Dış iskelet sistemleriyle askerlerin yük taşımaya katkı, dayanıklılık, güç ve hareketliliğe yönelik sistem entegrasyonları önem kazanmaktadır.
- İletişim ve istihbaratın yanı sıra, askerin hedef olmasını engelleyecek veya olası tehditleri bertaraf ederek en az seviyede zarar görmesini sağlayacak kıyafet ve teknoloji çalışmalarına önem verilmesi önerilmektedir.
- En iyi sistemlere de sahip olsanız, neyi ne zaman kullanacağınızı belirleyemezseniz sonucu garanti edemezsiniz. Beyin ve yetenekli insan, tüm teknolojik gelişmelere rağmen uzun süre etkisini kaybetmeyecek.

- Teknolojik gelişimlerin tüm dünyadaki askerlerin fiziksel hareket etkinliklerini kısıtladığı, teknolojiyle birlikte gelişen yeni tür rahatsızlıkların oluşabileceği öngörülmektedir.
- Özellikle otonom ve robotik sistemleri kullanacak, masa başında görev yapacak personelin, uzun süre dikkat gerektiren bu tarz teknolojileri kumanda edecek personellerin psikolojik ve fizyolojik olarak yeni nesil eğitim programlarına tabi tutulmaları tavsiye edilmektedir.
- Sahada teknolojik ekipmanlarla veya mobil yüklerle görev yapan personelin kritik durumlardaki reaksiyon sürati durumu özellikle inceleme konularından biri olmalıdır. Ayrıca kuvvet, sürat ve dayanıklılık dengesi boyutuyla teknoloji üretimi ve kullanımına yönelik çalışmalar önerilmektedir.
- Rusların Asurlular döneminden kalma tekniklerle dronlara karşı tanklarını korumak için geliştirdikleri zırhlar, eski ile yeninin yenilebileceği ve insan aklının savaştaki yerinin göstergesi olarak kabul görmektedir.
- Teknolojide yaşanabilecek kesintileri de öngörerek, geleneksel savaş yöntemlerinden tamamen vazgeçilmemesi ve bu konuda ihtiyatlı olunması tavsiye edilmektedir. Geleneksel yöntemlerle gelişen teknolojilerin birleşiminin, savaş teknolojilerinin gelişim döneminin en önemli boyutu olarak kabul görmektedir.
- Güncel teknolojileri yakalayan insanlar veya şirketler, vekil aktör olarak savaşlarda önemli rol üstlenecektir. Starlink, X, Facebook'un ve Microsoft gibi firmaların Ukrayna-Rusya savaşındaki pozisyonları bunun belirtileri olarak kabul edilmektedir.
- Simülasyon sistemlerinin eğitimde farkındalığı artırma ve hızlı karar alma konusundaki önemi artıyor. Özellikle, gerçeğe en yakın harp ortamlarındaki tatbikatlar, yeni teknolojilere uyum süreçlerini hızlandırmaktadır.

- Deepfake ve sosyal medya savaşlarının bir sonraki versiyonunun duygu ve hislerin de analiz edilerek sonuçlara eklendiği, zihin okuma evresine ilerlemesi beklenmektedir. Konvansiyonel harpte sosyal medya yazılımı, VR gözlük ve neuralink gibi teknolojilerin oynadığı rolü artırması ve bu sürecin oluşmasına zemin hazırlaması beklenmektedir.
- Şirketlerin, askeri birliklerin, organizasyonların yapay zekâ ve yeni nesil savaş teknolojilerini etkin kullanımı için yeni yapılanmalara gitmelerinin gerekliliğine dikkat çekilmektedir. Özellikle eğitim alanında ve eğitilmiş personel konusunda hızlı çalışmalar yapılması gerekliliği ifade edilmiştir.
- Gelecekte düşmanın hangi gerçeğiyle başa çıkmak zorunda olduğumuzu tahmin etmenin daha zor olduğu bir dönem başlamaktadır. Çok fazla dinamik içinde, çok hızlı reaksiyonların gerekeceği savaş ve çatışma ortamları öngörülmektedir.
- Analiz, bireysel ve teknoloji gelişiminin en önemli unsuru olarak kabul edilmektedir. Bu noktada personelin ve sunulan teknolojinin yeteneklerinin, performansının, sınırlarının ve gelişmenin temeli olarak kabul edilirken, tüm süreçlerde analiz merkezli hareket ve üretim tarzına ihtiyaç duyulmaktadır.
- Siber güvenlik, hibrit hareket, insansız kara ve deniz araçları ile otonom sistemler, simülasyon, sanal gerçeklik gibi tüm konularda zekâ, analitik beceri, psikolojik dayanıklılık, hızlı ve doğru karar verebilme konularında yeterlilik ve insan yönetimi de kuvvet çarpanı statüsü kazanacak potansiyele sahiptir.
- Çok sayıda farklı otonom veya bilgisayar tabanlı sistemin ulaştıracağı veriyi işleyecek, değerlendirecek ve karar verecek teknik alt yapı kadar, insan kabiliyetine de ihtiyaç duyulacağı ifade edilmektedir.

GELECEĞİN ASKERİ TEKNOLOJİLERİ VE SEKTÖRE DAİR



317
MİLYAR
\$

ABD merkezli Top 100'deki 41 şirket, 317 milyar dolar silah geliri kaydetti. Bu rakam, Top 100'ün toplam silah gelirlerinin yarısı ve 2022'ye göre yüzde 2,5 daha fazla. 2018'den bu yana, Top 100'deki ilk 41 ABD şirketinden 30'u 2023'te silah gelirlerini artırdı.



133
MİLYAR
\$

Avrupa merkezli 27 ilk 100 şirketin (Rusya hariç) toplam silah gelirleri 2023 yılında 133 milyar dolara ulaştı. Bu, 2022'ye göre sadece yüzde 0,2 daha fazlaydı ve dünya bölgeleri arasında en küçük artışı temsil ediyordu.



103
MİLYAR
\$

Çin merkezli Top 100'deki dokuz şirket, yavaşlayan bir ekonominin ortasında 2019'dan bu yana silah gelirlerinde en küçük yıllık yüzdelik artışını (+%0,7) gördü. 2023'teki toplam silah gelirleri 103 milyar dolara ulaştı.



6,7
MİLYAR
\$

İlk 100'deki üç Hintli şirketin toplam silah geliri %5,8 artışla 6,7 milyar dolara çıktı. Çıktı.



2,2
MİLYAR
\$

Nükleer savaş başlıkları tasarlayan, üreten ve bakımını yapan Birleşik Krallık Atom Silahları Kurumu (AWE), Top 100'deki Birleşik Krallık şirketleri arasında silah gelirlerinde yıllık bazda en büyük yüzdelik artışı (+%16) kaydederek 2,2 milyar dolara ulaştı.

YAPAY ZEKÂNIN ÖNERİLERİ

“

Türkiye’de savunma sanayisine yatırım yapmak, hem stratejik açıdan önemli hem de büyüme potansiyeli olan bir alandır. Dünyadaki trendleri ve Türkiye’nin mevcut savunma sanayi altyapısını dikkate alarak şu alanlar üzerinde durabilirsiniz:



İnsansız hava araçları (İHA), deniz araçları (İDA) ve kara araçları (İKA) artık modern orduların temel unsurları. Özellikle otonomi seviyelerinin artmasıyla insansız sistemlere olan talep hızla büyüyor.

Yapay zekâ (AI), sensör füzyonu ve büyük veri analizi, hem operasyonel etkinliği artırmak hem de karar verme süreçlerini hızlandırmak için kritik önemde. Savaşlar artık yalnızca fiziksel sahada değil, siber ortamda da yapılıyor. Kritik altyapıları koruma, saldırı tespit ve önleme sistemleri büyük önem taşıyor.



Lazer silahları, hedeflere hassas müdahale ve düşük maliyetli mühimmat sunması nedeniyle geleceğin teknolojisi olarak görülüyor. Dayanıklı, hafif ve düşük maliyetli malzemeler, hem askerî ekipmanlar hem de zırh sistemleri için kritik.

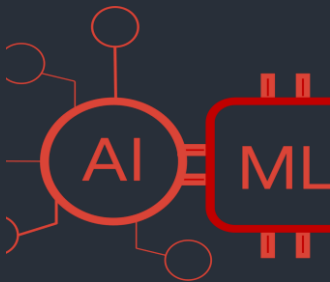
”

GELECEĞİN ASKERİ TEKNOLOJİLERİ VE SEKTÖRE DAİR



Deloitte'nin 23 Ekim'de yayınladığı 2025 öngörüsüne göre 2022'deki 59 ülkenin savaş durumu dolayısıyla yaptığı harcamaların etkisinin 2025'te de devam etmesi bekleniyor ve yapay zekâdan ve gelişmiş hava hareketliliğinden (AAM) insansız sistemlere kadar birçok teknolojinin geniş tabanlı operasyonel hale gelme potansiyeli var. Geçtiğimiz yıl boyunca, yapay zekâ görünüşte her yerde bulunur hale geldi ve bu da sektördeki şirketlerin teknolojiyle giderek daha fazla rahatladığını gösteriyor. 2025'te yapay zekânın satış sonrası hizmetleri geliştirmek ve tedarik zincirini optimize etmek gibi çeşitli alanlarda ilerlemeyi hızlandırmaya yardımcı olması muhtemel.

Geçtiğimiz yıl hava yolculuğundaki canlanma, yeni uçaklara olan talebi önemli ölçüde artırdı. Havacılık ve savunma şirketleri tedarik zincirinde kalite zorlukları ve azalan filo mevcudiyetiyle karşı karşıya kaldıkça, mevcut ticari uçakların ömrünü uzatma çağrısı büyüyor. Uçakların operasyonel ömrünü uzatmanın bir yolu etkili bakım, onarım ve revizyondan (MRO) geçer. Bu nedenle şirketler, daha fazla verimlilik ve maliyet etkinliği ihtiyacını karşılamak için dijital teknolojileri entegre etmek gibi değer fırsatlarını, gelişmiş MRO hizmetleriyle belirliyor.



Deloitte'un yakın zamanda yaptığı bir ankete göre, havacılık ve savunma sektöründen katılımcıların %81'i yapay zekâ ve makine öğrenimi (AI/ML) teknolojisini halihazırda kullandıklarını veya kullanmayı planladıklarını bildirdi. Satış sonrası şirketlerinden gelen yanıtlar da AI/ML, üretken AI ve genişletilmiş gerçekliğin önümüzdeki bir ila üç yıl için ana odak teknolojileri olduğunu belirtti.

GELECEĞİN ASKERİ TEKNOLOJİLERİ VE SEKTÖRE DAİR



Amerika merkezli Uzay Vakfı'na göre, küresel uzay ekonomisi 2023 yılında 570 milyar ABD dolarına ulaşarak, bir önceki yıla göre %7,4'lük bir artış gösterdi (öngörülen beş yıllık bileşik yıllık büyüme oranı %7,3'e paralel olarak), bu artışın başlıca nedeni ticari sektördür. Özellikle konumlandırma, gezinme ve zamanlama (PNT) alt sektörü, 445 milyar ABD doları tutarındaki ticari toplamın yaklaşık %47'sini (209 milyar ABD doları) oluşturdu. Bu pazarın 2035 yılına kadar %155 büyümesi bekleniyor ve önümüzdeki yıl ana odak noktası olabilir. Tedarik zinciri yönetiminden ulaştırmaya kadar sektörlerdeki şirketlerin konum tabanlı hizmetler için PNT teknolojilerine güvenmeye devam etmesi muhtemeldir.

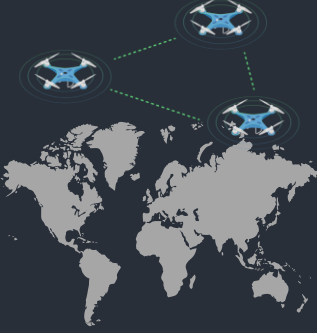
ABD'nin 2025 mali yılı savunma bütçesi talebi, Savunma Üretim Yasası Satın Almaları ve Endüstriyel Taban Analizi ve Sürdürülebilirlik programlarından yararlanarak savunma sanayi tabanını güçlendirmek için stratejik alanlara yatırım yapmaya devam eden Amerika Birleşik Devletleri Savunma Bakanlığı (DoD) odağını yansıtmaktadır.

Bu programların toplam bütçe talebi 1,5 milyar ABD dolarıdır. Bu arada, 2025 mali yılı bütçe talebinin 163,4 milyon ABD doları, termal koruma ve katı roket motor teknolojileri için teslim süresi ve alt kademe 1 tedarikçi sorunlarını ele almak üzere hipersonik araştırma ve geliştirme çalışmalarına tahsis edilmiştir.



Katı yakıtlı roket motorları için bu öncelik füze teknolojisinden uzay alanındaki gereksinimlere kadar uzanmaktadır. Aslında, katı yakıtlı roket motorlarına odaklanmak yeni bir şey değil, ticari faaliyetlerin artmasına katkıda bulunan büyüyen bir eğilimin devamıdır. Sadece geçen yıl, Kara Kuvvetleri, Deniz Kuvvetleri ve Hava Kuvvetleri büyük katı yakıtlı roketler geliştirmek için çalışan yeni pazar katılımcılarına 100 milyon ABD dolarından fazla yatırım yaptı. Sadece son iki yılda, havacılık ve savunma endüstrisinde bir dizi yüksek profilli anlaşma yapıldı: Bir ABD ana yüklenicisi, Amerika Birleşik Devletleri'ndeki iki katı yakıtlı roket motoru sağlayıcısından birini satın aldı ve iki ana yüklenici büyük miktarlarda roket üretmek için stratejik bir anlaşma imzaladı.

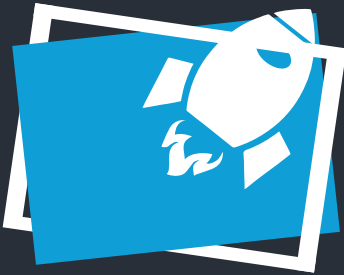
GELECEĞİN ASKERİ TEKNOLOJİLERİ VE SEKTÖRE DAİR



Jeopolitik gerginlikler savunma harcamalarının mevcut ve öngörülen odağının çoğuna katkıda bulunuyor. Bu etki hiçbir yerde insansız sistemler (diğer adıyla dron) pazarından daha belirgin değildir. Bir yıl önce, bazı tahminler 2023 küresel askeri dron pazarını 20,21 milyar ABD doları kadar yüksek olarak değerlendirmişti. İnsansız sistemler için hız muhtemelen 2025'te odakta kalacak.

2025 mali yılı DoD bütçe talebi, hava gücü için ayrılan 61,2 milyar ABD dolarının bir kısmını MQ-4 Triton ve MQ-25 Stingray gibi insansız hava araçları sistemlerine tahsis ediyor.

Ticari cephede, operatörler insansız hava sistemleri için inşaat, emlak, altyapı, petrol ve gaz, tarım ve lojistik gibi çeşitli endüstrilerde uygulamalar buluyor. ABD havacılık endüstrisi için çığır açıcı bir kararla, Federal Havacılık İdaresi artık Dallas bölgesindeki birden fazla ticari operatör için eş zamanlı görüş hattının ötesinde uçuşlara izin verecek. Bu, yabancı yapımı insansız hava araçlarına yönelik olası yaptırımlara ek olarak, insansız hava sistemlerinde daha fazla büyüme için zemin hazırlayabilir.



Son on yılda, füze ve mühimmatla ilgili tedarik ve Ar-Ge için DoD bütçe talepleri %340 artarak 2015 mali yılındaki 9 milyar ABD dolarından 2024 mali yılında 30,6 milyar ABD dolarına ulaştı. Bu işaretler, sektörün 2025 yılına kadar küresel katı roket pazarında büyümeye devam etmesini bekleyebileceğini gösteriyor.

Büyük ölçüde elektrikli dikey kalkış ve iniş (eVTOL) uçaklarına odaklanan gelişmiş hava hareketliliği (AAM) endüstrisi son yıllarda ilgi ve yatırım gördü. Profesyonel yatırımcılar, 1,787 trilyon ABD dolarından fazla yönetim altındaki varlıktan (AUM) sorumlu yönetici grubunun %93'ünün eVTOL sektörüne ilgi göstermesiyle AAM'nin potansiyeline giderek daha fazla ilgi gösteriyor. eVTOL uçakları, elektrikli tahrik sistemleri sayesinde muadillerine kıyasla daha sessiz ve daha çevre dostudur ve sıfır operasyonel emisyonu neden olur. Bu sistemler kargo taşımacılığı ve askeri uygulamalar için değerlendirilirken, en büyük değer teklifi muhtemelen kentsel hava hareketliliği yolcu pazarındadır.

GELECEĞİN ASKERİ TEKNOLOJİLERİ VE SEKTÖRE DAİR



Havacılık ve savunma endüstrisi için 2025 yılı "operasyonelleştirme" kelimesiyle tanımlanabilir. Endüstri, dijital teknolojilerdeki gelişmeler, stratejik yatırımlar ve işgücü geliştirme ve tedarik zinciri görünürlüğüne yenilenen odaklanma ile desteklenen sürekli bir dönüşüm yaşıyor. Yetenekten tedarik zinciri fırsatlarına, havacılık ve savunma şirketleri, endüstrinin kalıcı sorunlarından bazılarını ele almak için dijital teknolojileri ve yapay zekâyı entegre etmek için çalışıyor.



Satış sonrası hizmetlerde, öngörücü bakım için AI uygulamaları iyi bilinir hale geldi, ancak önde gelen havacılık ve savunma şirketleri muhtemelen AI çözümlerini MRO değerlendirmelerine yönelik daha bütünsel bir yaklaşıma dahil edecektir. Benzer şekilde, endüstri liderlerinin tedarik zinciri görünürlüğü için dijital uygulamalarını, parça ve işgücü kıtlığından parçaların kalitesi ve güvenilirliğiyle ilgili endişelere kadar uzanan sorunları çözmek için geliştirmelerini bekliyoruz. İş gücünde, sıkıntı gerçektir ve öncülerin yeteneğe üretimle aynı ilgiyi göstermeleri beklenmektedir. Yeni ürünler alanında, endüstrinin ticari ortamlarda gelişmiş hava hareketliliği ve insansız sistemlerin operasyonel uçuşu yoluyla kendilerini farklılaştıran birkaç kilit oyuncu görmesi muhtemeldir. Sektör genelindeki büyümenin her adımda temel alınan teknolojiyle devam etmesi muhtemeldir. Sektör genelinde uygulanan sayısız teknoloji, şirketler için çok sayıda fırsat sunmaktadır; bu fırsatlar hem marjları hem de gelecek için yenilikleri yönlendirmeye ve önlerindeki fırsatları yakalamaya yardımcı olabilir.

GELECEĞİN ASKERİ TEKNOLOJİLERİ VE SEKTÖRE DAİR

PwC'ye 2025 yılı ve önümüzdeki üç yıl için havacılık ve savunma sektöründe göre başlıca eğilimler şöyle:

Portföy yeniden şekillendirme: Ortaya çıkan teknolojiye olan talep ve yeni katılımcılardan gelen artan rekabet, büyük oyuncular stratejilerini yeniden düşünmeye yöneltti. Operasyonları basitleştirmek için temel olmayan varlıkları elden çıkarmayı, temel yeterlilikleri modernize etmek için sermayeyi birleştirmeyi ve risk sermayesi destekli girişimleri satın alarak inovasyonu sürdürmeyi düşünüyorlar.

Jeopolitik baskılar: Avrupa, Avustralya ve Güney Kore'deki artan savunma bütçeleri sektör büyümesini önemli ölçüde etkiledi. Avrupa ülkeleri, özellikle NATO üyeleri, Ukrayna'daki çatışma nedeniyle harcamalarını artırdı. Avustralya, Avustralya, Birleşik Krallık ve ABD arasındaki üçlü bir güvenlik ortaklığı olan AUKUS gibi Hint-Pasifik güvenlik öncelikleri ve girişimleriyle uyumlu olarak savunma yatırımlarını artırdı. Benzer şekilde, Güney Kore, füze savunması ve ileri teknolojiye odaklanarak bölgesel tehditlere karşı savunma bütçesini artırdı. ABD'de, yeni yönetimin iç odaklı bir şekilde savunma harcamalarını artırmaya devam etmesi bekleniyor.

Ortaklıklar ve ortak girişimler (JV'ler): Sektör, geleneksel satın almalar yerine JV'leri giderek daha fazla tercih ediyor. Bu değişim, JV'lerin daha az karmaşık olması, daha az düzenleyici engelle sahip olması ve risklere karşı daha fazla koruma sağlaması nedeniyle. JV'ler ayrıca satın alma yoluyla elde edilen inovasyon yoluyla gelişmiş yeteneklerin geliştirilmesini destekler.



GELECEĞİN ASKERİ TEKNOLOJİLERİ VE SEKTÖRE DAİR

Uzay sektöründe stratejik genişleme: Uzay sektöründeki birleşme ve satın alma faaliyetleri, uydu tabanlı iletişim, savunma yetenekleri ve alçak Dünya yörüngesi (LEO) altyapısına yönelik artan taleple birlikte artış gösterdi. Şirketler, ulusal güvenlik ve ticari önceliklerle uyumlu olarak, otonom uydu ağlarında ve yörünge içi hizmetlerinde uçtan uca yetenekler kurmak için giderek daha fazla başkalarını satın alıyor. Ek olarak, özel sektörün yeni yönetim üzerindeki etkisi, uzayı stratejik bir varlık olarak yükseltebilir, daha fazla yatırım ve inovasyonu teşvik edebilir ve sektörün daha fazla konsolidasyonuna yol açabilir.

Ticari konsolidasyon: Yoğunlaşan rekabet ve operasyonel verimsizlikler, küçük ve orta ölçekli havacılık şirketlerini stratejik konsolidasyona yönlendiriyor. Daha büyük oyuncular, özellikle dar gövdeli uçaklar ve satış sonrası hizmetler gibi yüksek talepli segmentlerde kritik tedarik zinciri yeteneklerini güvence altına almak, üretim darboğazlarını azaltmak ve ölçek ekonomisi elde etmek için M&A'dan yararlanıyor.

Tedarik zincirlerinde bağlantıyı artırmaya yönelik önemli bir eğilim görüyoruz — hem şirket içinde hem de şirket duvarlarının ötesinde. Sonuç, artık tedarik zinciri boyunca sürekli olarak erişilebilen bir veri zenginliğidir. Sonuç olarak, bu, ortakların ilgili bilgilere neredeyse gerçek zamanlı ve eş zamanlı erişebildiği tedarik zinciri ekosistemlerine yol açıyor — böylece kararlar gerçekten olan bitene göre optimize edilebilir ve bilgilendirilebilir.



GELECEĞİN ASKERİ TEKNOLOJİLERİ VE SEKTÖRE DAİR



Askeri robotlar ve otonom sistemleri üzerine bir araştırma yayınlayan Alliedmarketresearch ise, yapay zekâ tabanlı robotlara ilginin kimyasal, biyolojik, radyolojik ve nükleer (KBRN) saldırı risklerinin bulunduğu bölge ve ülkelerde talebin 2030 yılına kadar artacağı öngörüsünü paylaşıyor. İnsansız otonom sistemlerde güvenilirlik, donanım ve yazılım performansı ile bakım hizmetlerini sağlayabilen firmaların kalıcı olabileceği vurgusu yapılan araştırmada, kurtarma ve lojistik ihtiyaçlar dolayısıyla insansız kara araçlarına olan ihtiyacın artacağı vurgulanıyor. Araştırma 2030 yılına kadar çok sayıda ülkenin insansız helikopter ve otonom silahlı kara sistemleri için bütçe ayırdığı bilgisini paylaşırken, sadece Amerika'da bu alanda 30'dan fazla projenin testlerinin sürdüğünü öngörüyor. Ayrıca, tank kategorisindeki insansız kara araçlarının da 5 yıllık süreçte hızlı büyüme göstermesi bekleniyor.



Teknolojideki sektörel dönüşümleri şirketlere raporlayan IMARC araştırma şirketi de operasyonel verimliliklerin askeri alanlardaki artışıyla ve siber güvenlik çözümleriyle sistemlerin birleştirilmesiyle piyasadaki güçlü büyümenin artacağı yönünde tahminini yayınladı. Afet müdahalesi, kolluk kuvvetleri ve arama kurtarma operasyonları alanlarında da yeni bir pazar oluşacağı öngörüsünü paylaşan IMARC, çeşitli arazi türlerine uygun biyoteknoloji taşıyıcı robotlar veya insansız araçların özellikle tüneller, mağara ve mesken alanlarındaki kullanımının birkaç yılda hızla büyüyeceğine dair verilere yer verdi. Şirkete göre, insan makine iş birliğinin yanı sıra yapay zekâ birleşimi ile pazar 2032'ye kadar 31.8 milyar doları aşacak.



Futuremarketresearch şirketi, robotik ve otonom sistemler (RAS) pazarının 2030 yılına kadar 27.5 milyar dolara çıkacağını öngörüyor. Taktik mekanik teknoloji ve yapay zekâ otonomisinin de sektörün oyuncularını değiştireceği tahminini paylaşan araştırma grubu, insansız hava sistemlerinin tanklar ve gemiler gibi zırhlılara karşı etkisinin gelişeceğini, insansız kara sistemlerinin de personel güvenliği ve taktik açısından ön plana alınacağı tahminini yapıyor.

GELECEĞİN ASKERİ TEKNOLOJİLERİ VE SEKTÖRE DAİR

STATZON

Araştırma şirketlerinden Statzon küresel askeri robot pazarının 2030 yılına kadar 42.6 milyar dolar olarak tahmin ederken, yapay zekâ, otomasyon ve savaş alanında insan kayıplarını azaltarak yüksek riskli görevler gerçekleştiren sistemlerin istikrarlı büyümesini göstereceğine dikkat çekiyor. Yapay zekâ ve büyük verideki gelişmelerin askeri robotların verimliliğini ve özerkliğini artırarak muharebe senaryolarında daha yetenekli kılacağı belirtilen araştırmada, özellikle bomba imha, yaralı tahliyesi, ön cephe gözetleme görevleri gibi kabiliyetlerinin rekabette önemli olacağını kaydediyor.



Şirketlerin tahminlerinde en önemli pazarlar sırasıyla Kuzey Amerika, Ortadoğu, ve Afrika, Avrupa, Asya Pasifik ve Güney Amerika olacak. Şirketlerin raporlarında dijital alt yapıya artan bağımlılık ve siber alandaki artan tehditler haberleşme ve iletişimi, uydu teknolojilerini kapsayan telekomünikasyon içerikli üreticilerin de önem kazanacağını vurguluyor. Dünya genelinde hükümetlerin güvenli ağlar, sağlam şifreleme sistemleri, tehdit istihbaratı, siber yanıt mekanizmaları dahil olmak üzere gelişmiş siber savunma yeteneklerine daha fazla yatırım yaptığı, orta vadede de yapay zekâ ve nesnelerin interneti (IoT) yatırımlarının büyüyeceği, sağlam siber savunmalara olan ihtiyaç doğrultusunda da siber segmentin hızlı bir büyüme göstereceğini belirtiyor. 2024'de yaklaşık 27 milyar dolar olan askeri uydu pazar büyüklüğünün 2029 yılına kadar 40 milyar doları aşması bekleniyor.

FORTUNE BUSINESS INSIGHTS

Fortune Business Insights, LEO, MEGO, GEO alanında bu rakamı 30 milyar doların üzerinde öngörürken teknolojiye hızlı değişimin ve küp uydularda oluşabilecek yeni oyuncuların büyümeyi hızlandırabileceği yorumunu da öngörülerinde paylaşıyor. Uydulardan elde edilen görüntülerin analizinde kullanılacak yapay zekâ uygulamalarının ve bu uygulamaların askeri otonom sistemlere entegre edilmesinin de yeni bir sektör oluşturduğunu belirten Fortune Business Insights, askeri iletişimdeki en büyük büyümenin C3ISR yetenekli küçük uydularda olacağı tahmininde bulunuyor.

GELECEĞİN ASKERİ TEKNOLOJİLERİ VE SEKTÖRE DAİR

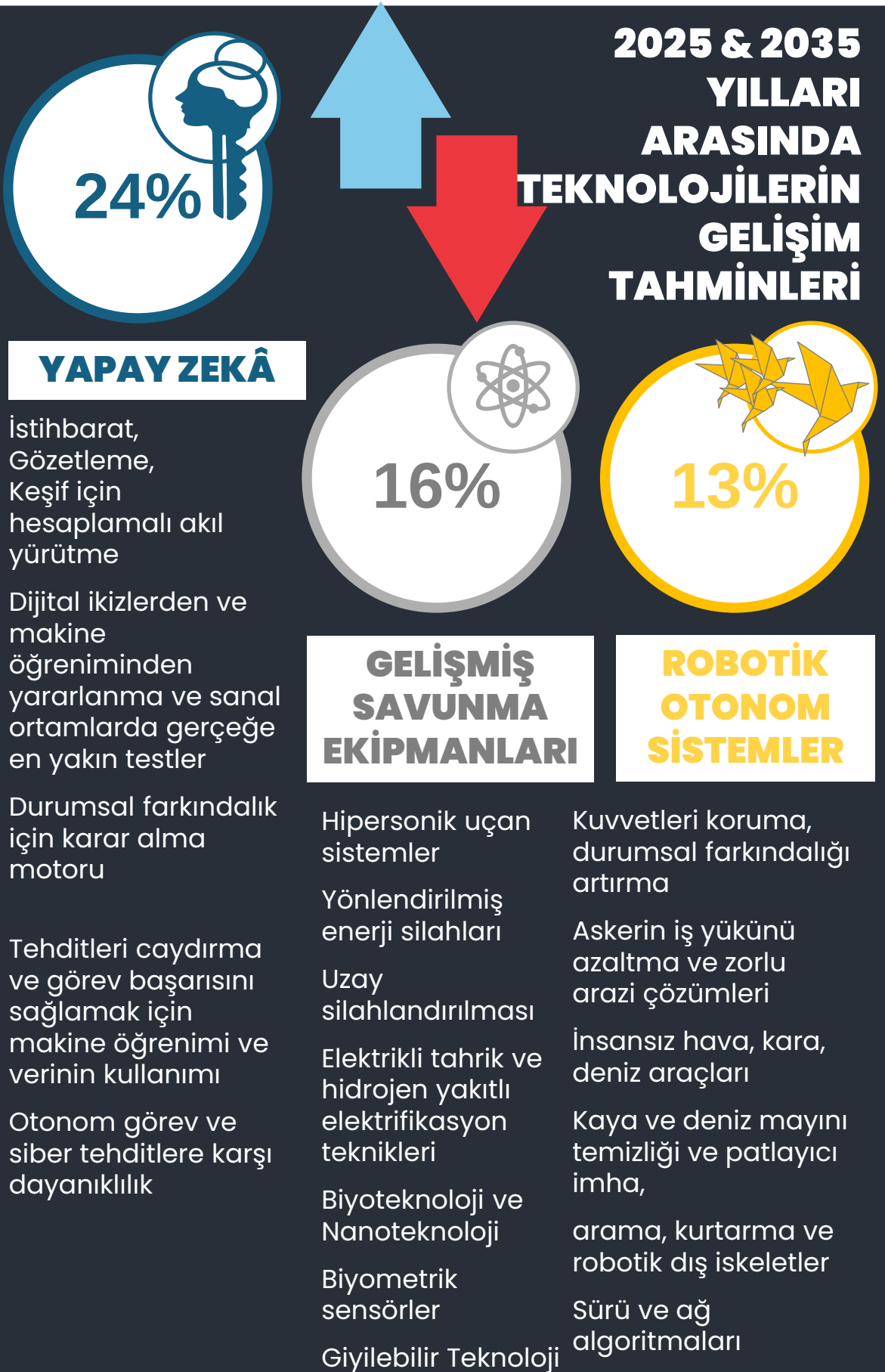


Global Market Insight 2024'de küresel askeri uydu pazarının 30.3 milyar dolarlık bir değere sahip olduğunu belirtirken, küçük uydu pazarıyla marketin 2032 yılında 73.3 milyar dolara ulaşabileceğine dair büyük bir projeksiyon sunuyor. 1000 kilo üstü uydular 2023 yılında 19 milyar dolarlık bir gelirle küresel pazara hakim olurken, pazarın en büyük oyuncuları Raytheon, Northrop Gruman ve Airbus. Savunma operasyonlarının optimize edilmesi, lojistiğin düzene sokulması, bilgi paylaşımının iyileştirilmesi ve birlikte çalışabilirliği sağlamak için yapay zekâ, makine öğrenimi ve büyük veri analitiğine yönelik ürünlere ve çözümlere talep 5 yılda hızla artacak. Özellikle Çin ve Amerika arasında savunma platformları, sistemleri ve teknolojilerine yapılan hızlı teknolojik ilerlemeler ve yatırımlar da pazarın hızlı büyümesindeki en önemli etken olacak.

Marketandmarkets ve Futuremarketresearch patlama ve hırsızlık risklerine rağmen mühimmat stoğuna da büyük talep olduğunu, 2028 yılında akıllı mühimmat teknolojileriyle market değerinin 2028'e kadar 33-35 milyar dolar market değerine ulaşmasını öngörüyor. Büyümede en büyük ve en hızlı büyümenin havacılık alanında olacağı yönünde de veriler mevcut.



Araştırma şirketleri, savunma sanayinde 2028 yılında beklenen 2.5 trilyon dolarlık bütçe tahmininin 2024 yılında gerçekleştiği, 2023 ile 2024 arasındaki harcama büyümesinin yüzde 4.9 olduğu değerlendirmesini paylaşıyorlar. Şirketlere göre, özellikle yapay zekâ, uydu ve uzay teknolojilerindeki gelişmeler ve jeopolitik gelişmelere göre yıllık büyümenin yüzde 3-7 oranında olabileceği yönündeki tahminler abartılı değil.



IOT

9%

**ASKERİ
NESNELERİN
İTERNETİ**

Gemiler, uçaklar, tanklar, insansız hava araçları, askerleri ve operasyon üstlerini tutarlı ve güvenli bir ağa bağlama

Bilişim, yapay zekâ ve 5G&6G teknolojileriyle çalışan sistemlerin entegrasyonu

Biyometrik verilerle iç görüleri artırma ve çevresel izleme

Siber saldırılara karşı savunmasızlık endişesini giderme ve rakip sistemleri etkisiz hale getirme,

Bilgi kayıplarını önleme ve sistemlere zarar verme teknolojileri

Yapay zekâyı yanıltma operasyonları

KBRN merkezlerine yönelik siber tehditler

Savunma ve müdahale yeteneklerini bir arada tutma

9%

**SİBER
SAVAŞ VE
ELEKTRONİK
HARP**



9%

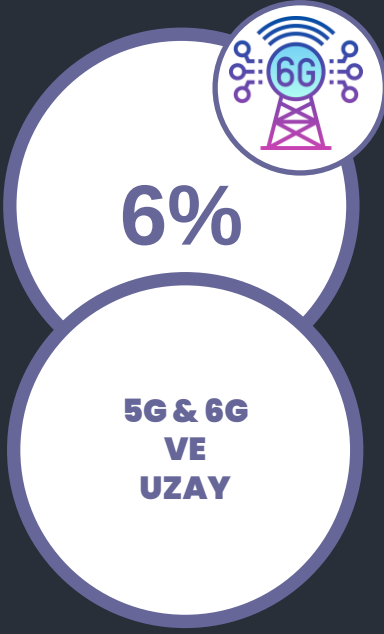
**SÜRÜKLEYİCİ
TEKNOLOJİLER**

Tekrarlanabilir ve esnek deneyim ortamları oluşturmak

Gerçeğe en yakın sanal ortamlarda eğitim ve görev provaları ile uyumlu çalışmayı sağlamak

AR, VR, XR, MR gibi tüm teknolojilerle personeli göreve en hazır hale getirme

Geliştirilen ve üretilen sistemlerin sanal ortamlarda başarı, dayanıklılık, enerji, kuvvet, etki ve MRO gibi faktörlerinin gerçek koşullara en yakın şekilde test edilmesini sağlayan sanal ortamlar



5G&6G ile hiper bileşik bağlantı ve güvenli veri alt yapısı

Büyük miktarda verinin uzak sensörlere ve silahlara aktarılmasını sağlayan, yoğun, dayanıklı savaş alanı alt yapısı

İnsansız sistemlerin tüm alt yapısı için uzaktan kontrol ve kesintisiz bağlantı alt yapısı

WiGL (Havada ağ tabanlı kablosuz şarj ve loMT enerji desteği, kablosuz vericilerle enerji üretimi)

Askeri operasyonlarda zamanında ve uygun bilgi akışını sağlayacak teknik alt yapı

Uzaydan kontrol edilen ve yakın yörünge hakimiyeti, mikro dalga, uydu savar füze ve teknoloji, kinetik enerji, nükleer füze teknolojileri

Teknoloji kullanımıyla daha yoğunlaşacak bilginin ve analizinde ve simülasyonlarda kullanılacak bilişim alt yapısı

Gelen verilerin etkili şekilde yorumlanması

Analitik, hız ile güvenli ve verimli veri akışı için kuantum teknolojileri

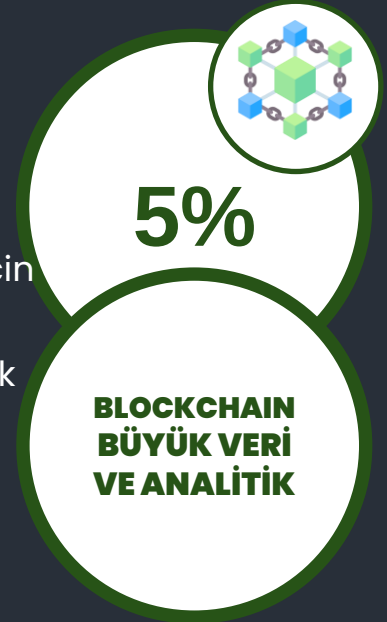
Kuantum şifreleme, hesaplama, kriptografik analiz ve sensör tabanlı gizli tespiti

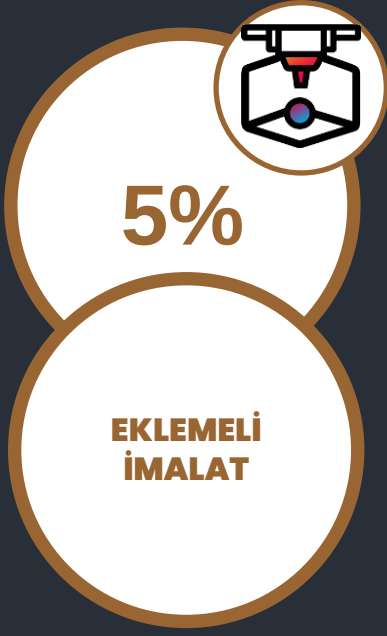
Kuantum mekaniği ve kuantum tabanlı güçlü elektronik sistem ürünleri

İnsansız araçların manevra, tahrip ve tespitine yönelik analitik çalışmalar

Gizli askeri bilgilerin korunması ve siber tehdit önlemleri için blockchain alt yapısı

Veri analitiği ile yapay zekâyı birleştiren blockchain projeleri





Hız, kapasite ve yakıt tüketiminde performansın iyileştirilmesi gibi konular, ağırlığı azaltan dayanıklı üretimler

3D baskı teknolojileri gibi yeni tasarım mühendisliği ürünleri

Zırh, kendi kendine ısınan giysiler ve mühimmat için yeni kombinasyon sağlayan ürünler

Geçici parça üretimi, onarım, malzeme işleme ve yerinde montaja yönelik girişimler

Mobil mikro parça üretimi

Mikrodalga ve termal sistemler

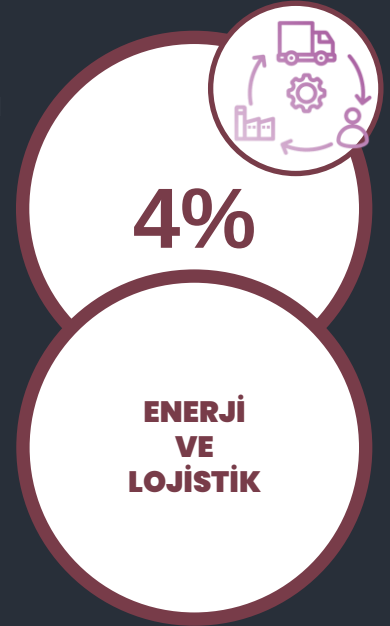
Robotik ve otonom sistemlerin uzun süre dayanıklılığını sağlayacak hafif veya yerinde üretim sağlayan çözümler

Hızı artırıcı ve yerinde çözüm üreten, kolay taşınabilir onarım ve tedarik yöntemleri

Düşük ısı ve tespiti geciktirici ürünler

Operasyonel lojistik süreçleri kolaylaştıracak ve enerji verimliliğini artıracak projeler

Artan operasyonel karmaşıklıklarda riski düşüren ve kısıtlamaları indirgeyen enerji ve lojistik süreçleri



Veriler Startus Insight'ın, dünya çapında kurulan ve 4,7 milyondan fazla start-up çalışmalarının SaaS tabanlı yapay zekâ desteğiyle yaptığı araştırmadan alınmıştır.



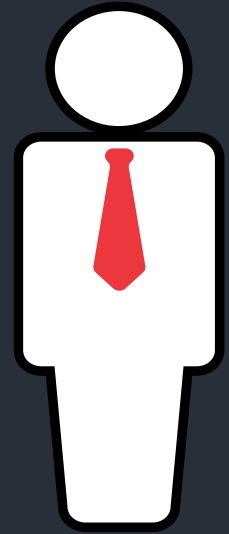
Startus Insight, yeni askeri teknolojiler kapsamında kamu ile test edilen 1036 projenin hangi alanlarda olduğunu ve hangi alanların uzun süreli desteklendiğini inceleyerek ilk 10 savunma ve bilişim sektörü projesini incelemiştir.

Startus Insight, yeni askeri teknolojiler kapsamında kamu ile test edilen 1036 projenin hangi alanlarda olduğunu ve hangi alanların uzun süreli desteklendiğini inceleyerek ilk 10 savunma ve bilişim sektörü projesini incelemiştir.

Çalışmaların İsrail, İngiltere ve Amerika'da yoğunlaştığı, Hindistan, Almanya, Fransa, Birleşik Arap Emirlikleri'nde yoğunlaştığı görülürken, Anduril, GeoSite, Epirus, Hermeus, Rebellion, Raven, Delfex, Geofabrika, Taekion gibi start-up projeleri de değerlendirmede yer almaktadır.

2025-2030 yılları arasında yukarıdaki alanlarda ürünleşmelerin hızlanacağı ve bundan sonraki 20 yıllık savunma sanayi rekabetine de bu teknolojilerdeki çalışmaların yön vereceği yorumu paylaşılmıştır

Hava Savunma Sistemlerinin dünyada %6,56'lık bir büyüme gösterdiği vurgulanan araştırmada, büyümenin, hava tehditlerine yönelik artan küresel vurguyu ve gelen tehditleri tespit etmek, izlemek ve etkisiz hale getirmek için sofistike sistemlere olan ihtiyacı vurguladığına dikkat çekildi. Ayrıca ülkelerin sektördeki bu gelişim hava sahası güvenliği, füze savunması ve radar sistemlerine verdiği öncelik olarak kabul edildi. öncelik verdiğini göstermektedir. Proaktif Siber Güvenlik , 320 şirket ve 26.000'den fazla çalışanı ile geçen yıl 2600'den fazla yeni çalışanın eklenmesiyle desteklenen bir diğer kritik eğilimi işaret ediyor. Bu, %4,17'lik yıllık büyüme oranına yansıyor. Bu eğilim, siber güvenlikte önleyici önlemlere doğru kayan odağı vurguluyor.



YAPAY ZEKÂNIN ÖNERİLERİ



Türkiye, özellikle otonom silah sistemleri ve insansız hava araçları gibi alanlarda küresel ölçekte rekabet edebilir bir noktadadır. Ancak kuantum teknolojileri ve blockchain gibi alanlarda daha fazla yatırım ve uzun vadeli stratejilere ihtiyaç duyulmaktadır. Türkiye'nin güçlü yönleri ve hızla büyüyen savunma sanayisi, gelecekte daha da ileri bir konum elde etmesini sağlayabilir.

Türkiye, konumunu güçlendirmek için teknoloji transferi, yerel ekosistemlerin gelişimi için kolaylaştırıcı ve teşvik edici önlemler ile ulusal stratejiler ile bu avantajların uzun vadeli etkilerini görecektir. Bu noktada şu noktalarda önlemler alınabilir:

Ar-Ge yatırımları artırılabilir, teknoloji transferleriyle anlaşmalar artırılarak bilgi ve deneyim birikimi hızlanabilir ve anlaşmalarla teknolojiye erişim sağlanabilir.

Üniversite-Sanayi iş birlikleri artırılarak, akademisyenler ve öğrenciler projelere dahil edilebilir. Akademik araştırmalar start-up projelere dahil edilebilir, bilginin sanayileşmesi için alanlar oluşturulabilir. Kuantum, fizik, yapay zekâ, siber güvenlik ve blockchain gibi alanlarda lisans ve lisans üstü programlar geliştirilmelidir.



Yetenekli insan kaynağı, ulusal ve işbirliklerinin artırılması, bölgesel ittifaklar, uluslararası Ar-Ge fonlarıyla işbirliği, ulusal eko sisteminin kurulması gibi adımlar süreçleri hızlandırabilir. Güçlü bir vizyon ve koordinasyonla mevcut alt yapının harekete geçirilmesi mümkündür.

YAPAY ZEKÂNIN ÖNERİLERİ

“Türkiye, özellikle otonom silah sistemleri ve insansız hava araçları gibi alanlarda küresel ölçekte rekabet edebilir bir noktadadır. Ancak kuantum teknolojileri ve blockchain gibi alanlarda daha fazla yatırım ve uzun vadeli stratejilere ihtiyaç duyulmaktadır. Türkiye'nin güçlü yönleri ve hızla büyüyen savunma sanayisi, gelecekte daha da ileri bir konum elde etmesini sağlayabilir.”

Hedef:
Teknolojik altyapıyı
güçlendirmek ve
temel kapasiteleri artırmak.

Kuluçka merkezlerinde Millî güvenlik ve askeri hassasiyetler kapsamında ürünleştirme ve insan kaynağı geliştirme için Millî programlar uygulanması, Blockchain tabanlı tedarik zinciri yönetim sistemi ve siber güvenlik sisteminin gerçek ortamlarından önce test edilmesi

Mevcut yeteneklerle hedef teknolojiler arasında pilot projeler başlatılması ve geliştirilmesi ile akademik projelere fırsat tanınması

Ar-Ge ve
İnovasyon
Yatırımları

SONUÇ

İki gün süren organizasyonda, üretim, yatırım ve modernizasyon yaklaşımlarının, 5-10 yıllık yakın gelecek, 10-25 yıl orta dönem ve 25-50 yıllık uzun sürdürülebilir yaşam döngüsü projeksiyonlarıyla ele alınması gerekliliğine dikkat çekilmiştir. Hassas ve kritik donanımların üretimi noktasında özel sektörün ve devlet kurumlarının iş birliğinin önemi vurgulanarak, akademik çalışmaların ürüne dönüştürülmesinde koordinasyonun 'Millî seferberlik' yaklaşımıyla yapılması gerekliliği ifade edilmiştir.

Yapay zekânın istihbarat analizi, karar destek araçları, savaş taktikleri gelişimi, simülasyon ve hedef tespiti gibi alanlarda öncelikle kullanılacağı öngörülmekte, tüm ülkelerin otonom sürüler ve elektronik harp özelinde yapay zekâ çalışmaları yaptığı düşünülmektedir. Yapay zekânın, yakın gelecekte savaş stratejisi oluşturulması, düzenleme ve tamamlama yönüyle de etkisini artırması beklenmektedir.

Uydu ve telekomünikasyon sistemlerinin geleceğin savaş ortamlarında ve elektronik harpte vazgeçilmez olacağı, bu boyutuyla da hem hedef hem de avantaj olarak kritik önemini artıracığı vurgulanmaktadır. Otonom ve robotik sistemler, akıllı mühimmatlar ve hipersonik füze, 5. Ve 6. nesil savaş uçakları gibi hava, kara, deniz, siber ve uzay teknolojilerinin müşterek çalışacağı ortamlarda yerli ürünlerinin önemini daha da artıracığına dikkat çekilmiştir. Tüm bu birleşik sistemlerin çok sayıda farklı platformdan alacağı veriler en hassas konu olarak önceliklendirilirken, verilerin işlemesinin önemi ve bu veri yönetimi için kritik barındırma, analiz ve güvenlik tedbirleri kritik konular olarak ön plana çıkmıştır. İletişim ve veri değerlendirme aşamalarında 'yapay zekâ', 'büyük veri', 'nesnelerin interneti', 'otonom ve robotik sistemler', 'elektronik harp' gibi konu başlıklarında siber güvenlik hassasiyeti ön plana çıkmış ve bu alandaki yatırımların önemi ortak kaygı olarak dile getirilmiştir.

Deepfake (derin sahtecilik) ile başlayan sürecin dijital ikiz ve sahte sinyal üretimi boyutuyla, siber saldırıların da yapay zekâya sahte veri üretimiyle önemli savaş çarpanı olacağı öngörülerinde bulunmaktadır. Geleceğin savaşlarında komuta ve kontrol sistemlerinin elektronik harp ve siber saldırılarda ilk hedef olacağı kaygısı paylaşılmıştır.

Askeri donanım kullanımını durduran, azaltan veya hedef saptıran siber saldırılar, modern askeri kuvvetlerin görevlerini geçici de olsa yerine getirememesi riski taşımakta, zaiyat ve fiziksel hasara da sebep olabilecek kapsam taşımaktadır. Radyo frekansı merkezli elektronik harp ve siber alan, bilgi üstünlüğünü elde etmek ve komuta-kontrol ağlarını etkisizleştirmek için birleşik silah yaklaşımına entegre bir alan olarak görülmektedir. Bu noktada gerek verilerin işlenmesi ve korunması gerek elektronik harp ve siber harp alanlarında güvenli, hızlı iletişim ağlarının oluşturulması için, blockchain ve kuantum teknolojilerinin dikkatle takip edilmesi ve geliştirilmesi tavsiye edilmiştir. Bu teknolojilerin güvenli veri alt yapısı ve büyük veri analizinde temel sistemler olacağı, bu alandaki yatırımların da önemli olacağı kaydedilmiştir. Kuantum algılama ve hesaplama, uzay tabanlı sensörler ve yedekli iletişim ağları da geleceğin askeri teknolojik sistemleri için önemli alanlar olarak dikkat çekmektedir.

Savunma sektöründe kullanılan sistemlerin temelindeki çip ve sensör teknolojilerinin yerli üretimi noktasındaki dışa bağımlılığın azaltılmasının olağanüstü durumlarda oluşabilecek risklerin bertaraf edilmesinde Millî menfaatler açısından önemi hatırlatılmıştır.

Future Soldier – Geleceğin Askeri teknolojileri eğiliminde donanım, yazılım, siber güvenlik alanlarının ön plana çıktığı, bilişim teknolojileri merkezli çalışmalarda sağlam, farklı ve yenilikçi ürün odaklı üretimin yanı sıra, mobiliteye uyumlu ve teknik destek sağlayan daha uzun menzilli, daha hızlı, daha iyi iletişim sağlayan ürünleşmenin de küresel rekabette önemli olduğu değerlendirilmektedir.

Yeni teknolojilerin, uygulama ve kombinasyonlarının teknolojilerin kendisi kadar önemli olarak görülürken, geleceğin askeri teknolojilerinde iletişim kurma, operasyonları yönetme biçimleri, oluşturacakları hasar ve etkinin oranı, özerklikleri ve sürdürülebilirlikleri de yeni nesil teknolojinin temel bileşenleri olarak görülmektedir.

Uzaktan savaş için makine ve teknik alt yapıya güven geleceğin savaş ortamları için en temel kaygıları oluştururken, gerçek zamanlı tespit ve takibi kolaylaştıran, bilgi akışını hızlandıran, caydıran, önleyen veya yanıltan teknolojiler, manevra alanı ve kabiliyetini artıran, dayanıklılığın belirleyici olduğu yetenekler, daha ucuz sensörler ve büyük veri analitiğinin birleşimi, uzun menzil, gelişmiş imha potansiyeli ve nokta atışı sağlayan ürünler savunma alanındaki rekabet alanlarını oluşturacaktır.

Lazer, mikrodalga ve yönlendirilmiş enerji silahları, hipersonik silah sistemleri, enerji üretimi, depolama ve ikmal çözümleri, kitle imha silahları, sürü hava, kara, deniz sistemleri ve karşı önlemler, makine öğrenme algoritmaları, dayanıklı-hafif verimli-yenilikçi malzeme ile üretim teknikleri, mikroelektronik, gelecek nesil kablosuz teknolojiler (FutureG), robot teknolojileri, hızlı hücum ve bölge savunmasına yönelik çözümler teknoloji merkezli savaşın önemli dinamikleri arasında kabul edilmektedir.

TEK-ER özelinde vücut korumaya yönelik tedbirler, kızılötesi ışınlar ve tespiti önlemeye yönelik teknolojiler, yük almak ve hareket kabiliyetine destek sağlayacak dış iskelet sistemleri, kullanılacak elektronik sistemler için mobil enerji üretimi, istihbarat ve iletişiminin sürekliliği, dronlara karşı geliştirilen zırhlar, saha ve masa başındaki personelin teknolojik gelişimlere fiziksel ve psikolojik uyum eğitimleri, simülasyon eğitimlerinin gerçekliğe yakınlığı ve farklı senaryolarla eğitim metotları, zekâ ve analitik becerili personel sayısına duyulacak ihtiyaç da en önemli konular olarak ön plana çıkmıştır.

Ürünlerin uzun ömürlü ve verimli kullanılabilmesi açısından 'lojistik destek analizi' sürecinin tasarım aşamasıyla birlikte başlamasının gerekliliği, aksi durumda ürünlerin ciddi maliyetler getirebileceği veya operasyonel riskler oluşturabileceği, bu konunun kritik konu olarak değerlendirilmesi gerektiği kaydedilmiştir.

Sistemler, kavramlar ve yetenekler, gerçek bir düşmana karşı uzun süreli bir çatışmada test edilene kadar, geleceğin savaşlarına dair tahminler yapılabilir. Bu 'Future Soldier – Geleceğin Askeri 2024' organizasyonu değerlendirmelerinin savunma sanayi paydaşlarına fikirden tasarıma, üretimden pazarlamaya ve markalaşmaya giden yolda bir rehber olacağına inanıyoruz.

Saygılarımızla

SASAD

