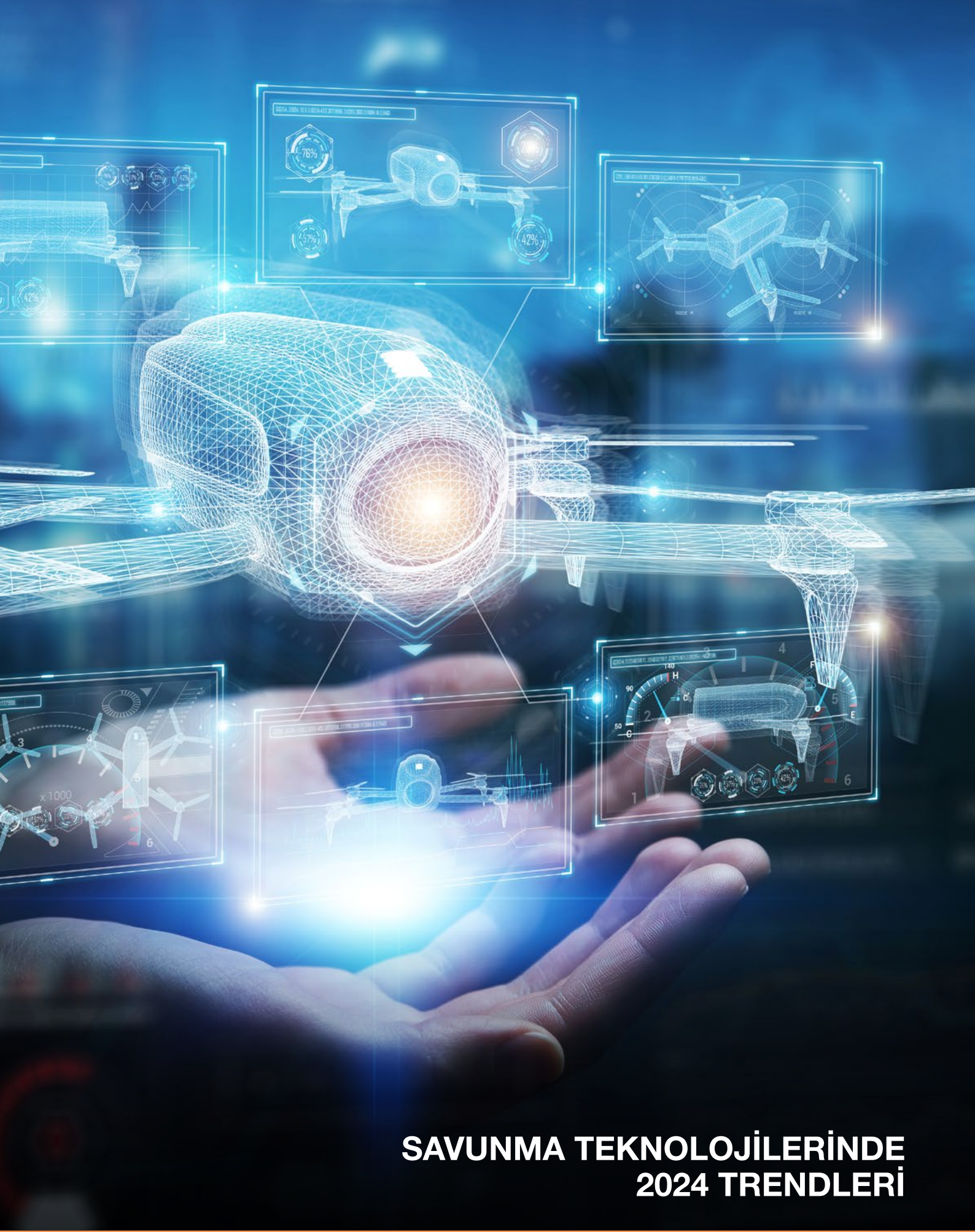

SAVUNMA TEKNOLOJİLERİNDE 2024 TRENDLERİ

TREND ANALİZİ MART 2024

thinktech
STM Teknolojik Düşünce Merkezi

STM ThinkTech

1. GİRİŞ

2023 yılında küresel jeopolitik sahnede, özellikle Rusya-Ukrayna Savaşı nedeniyle Doğu Avrupa'da devam eden tehditler ve İsrail'in Gazze saldırılarının gerginliği her geçen gün tırmandırdığı Ortadoğu'daki çatışmalar öne çıkmıştır.

Savaşların yıkıcı ve gayrıinsani boyutu bir yandan dünya toplumlarını tedirgin ederken, diğer yandan da küresel jeopolitik arenadaki gerilim ve olumsuz gelişmeler ülkeleri savunma ve askeri kapasitelerini gözden geçirme, geliştirme ve uluslararası rekabette öne geçirme çabalarına sevk etmiştir. Yaşanan olumsuzluklar ülkelerin bu çabalarının halk nezdinde olumlu karşılık bulmasına ve kamuoyunun savunma inovasyonuna yönelik destekleyici bir tavır almasına da yol açmaktadır. Örneğin, İngilizlerin yüzde 59'u savunma harcamalarının Gayri Safi Yurtiçi Hasılanın (GSYH) yüzde 2,5'ine çıkarılmasını desteklemektedir[1].

Ülkeler, olası bir çatışma durumunda potansiyel olarak kendilerine avantaj sağlayabilecek teknolojik çözümlere giderek daha fazla odaklanmaktadır. 2024 yılında savunma alanı teknolojik gelişmelerin ve etik zorlukların ilgi çekici bir birleşimine tanık olmaktadır. Bu dönüşüm savunma yeteneklerini yeniden şekillendirmekle kalmamakta, aynı zamanda savunma ve güvenliğin geleceği hakkında kritik soruları da gündeme getirmektedir. Örneğin, ABD Savunma Bakanlığı 2023 mali yılı bütçesinde araştırma ve geliştirme için 130,1 milyar dolarlık rekor bir bütçe ayırdığını duyurmuştur. ABD Savunma Bakanı Lloyd Austin, bütçedeki bu artışın nedenini şöyle açıklamaktadır: "İleri teknoloji, siber, uzay ve yapay zekâ konusundaki hazırlık seviyemizi yükseltme ihtiyacı duyuyoruz[2]."

Yaşanan gelişmeler, ülkeler açısından, tüm savunma alanlarında operasyonel avantaj sağlamak için yeni teknolojileri benimsemeyi hiç olmadığı kadar zorunlu hâle getirmiştir. Savunma ekosistemi ileri teknolojinin rehberliğinde yeniden şekillenirken, otomasyon ve siber programları birleştiren hibrid tekniklerin yükselişi, konvansiyonel savaşın zemin kaybetmesine neden olmaktadır. Bu çerçevede siber savaş, yapay zekâ ve robotik yeni savaş alanları olarak öne çıkmaktadır.

Analizimizde tüm bu gelişmelerden yola çıkarak, 2024 yılında savunma sanayiine yön vermesi beklenen teknoloji trendlerini ve bu trendler çerçevesinde yaşanması beklenen gelişmelerin neler olabileceğini inceledik.

2. 2024 YILINDA DA SIKÇA ANILACAK SAVUNMA TEKNOLOJİLERİ

2.1 Büyük Veri

Günümüzde büyük veri, "gelişen ve bozucu teknolojiler" kategorisinde değerlendirilmektedir. Artan dijitalleşme, yeni sensörlerin çoğalması, yeni iletişim modları, nesnelerin interneti ve sosyal medya, büyük verinin gelişimine önemli ölçüde katkıda bulunmuştur. Gelişmiş Veri Analitiği, bu tür büyük hacimli bilgileri anlamlandırmak ve görselleştirmek için gelişmiş analitik yöntemleri ifade

etmektedir. Bu teknikler, yapay zekâ, optimizasyon, modelleme ve simülasyon, insan faktörleri mühendisliği ve yöneylem araştırması dahil olmak üzere veri ve karar bilimlerindeki araştırma alanlarından alınan çeşitli yaklaşımları kapsamaktadır.

Dünya yalnızca 2022'de 94 zettabayt (ZB) veri oluşturmuş ve bu verilerin yüzde 80 ila 90'ı yapılandırılmamış durumdadır. Bu sayının her iki yılda bir, ikiye katlanması ve bu eğilim kontrol edilmeden devam ederse 2042 yılına kadar yılda yaklaşık 100.000 ZB'ye yükselmesi beklenmektedir. Yalnızca 2021 ve 2022'de oluşturulan veriler şimdiye kadar oluşturulmuş tüm verilerin yüzde 90'ını temsil etmektedir. 2020'de dünyanın bulut veri depolaması 6.800 exabyte iken (1000 Exabyte = 1 ZB), bunun 2025 yılına kadar 200 ZB'nin üzerine çıkması beklenmektedir. Tüm bu verilerin toplanması, iletilmesi ve depolanması gerekmekte, bu da bunları anlamlandırmaya yardımcı olacak enerji ve analitik araçlara yönelik artan bir talep yaratmaktadır.

Büyük veri, NATO'nun yetenekler yelpazesinde önemli bir stratejik bozucu olacak bir bilgi ve karar avantajı yaratma potansiyeline sahiptir. NATO'nun "Bilim ve Teknoloji Trendleri 2023-2043" raporuna göre veriler, "operasyonel verimliliğin artmasını, maliyetlerin düşmesini, lojistiğin iyileştirilmesini ve varlıkların gerçek zamanlı izlenmesini sağlayacak; aynı zamanda, stratejik, operasyonel, taktik ve kurumsal seviyelerde önemli ölçüde daha fazla durumsal farkındalık yaratacaktır. Bu uygulamalar, her düzeyde gelişmiş karar vermeyi desteklemek için tahmine dayalı analitiğin daha derin ve daha geniş bir şekilde uygulanmasına yol açacaktır[3]."

2.2 Hipersonik Sistemler

Hipersonik, ses hızının beş veya daha fazla katı (saatte 761 mil) hızda hareket eden herhangi bir nesneyi tanımlamaktadır. Temel hipersonik teknolojisi onlarca yıldır mevcut olmasına rağmen, gelişmiş hipersonik askeri sistemler yeni yeni test edilmekte ve piyasaya sürülmektedir. Bu yeni teknolojinin en dikkat çekici özelliği, hipersonik füzelerin alçak irtifalarda uçabilme ve havada manevra yapabilme yetenekleri sayesinde, mevcut füze savunma sistemleriyle takip edilmelerinin neredeyse imkânsız hâle gelmesidir[2].

Rusya, Çin ve Amerika Birleşik Devletleri (ABD), hem saldırı füzelerine hem de savunma sistemlerine odaklanarak kendi hipersonik silah sistemlerini kurmak için yarışmaktadırlar. Hipersonik füzeler, ilk kez 2022'nin Mart ayında Rusya tarafından Ukrayna'ya karşı kullanılmıştır[4].

2022'de hipersonik teknoloji araştırmalarına 3,8 milyar dolar ayıran ABD Savunma Bakanlığı, 2024'te 4,7 milyar dolar talep etmektedir. Ayrıca, ABD Savunma Bakanlığında balistik füzelere karşı katmanlı bir savunma sistemi geliştirilmesinden sorumlu olan Füze Savunma Ajansının (Missile Defense Agency) hipersonik savunma için 247,9 milyon dolarlık bir bütçesi bulunmaktadır. ABD'de özel şirketler de hipersonik teknoloji geliştirmek için yarışmaktadır. Bir start-up olan Hermeus, hipersonik hızda seyahat edebilen uzaktan kumandalı bir uçak geliştirmektedir[2].

Pentagon'un 14 kritik teknolojisinden biri olan hipersonik silahlar, muhtemel düşmanları caydırma yeteneği için gerekli görülmektedir. Kongre kısa süre önce, Füze Savunma Ajansının füze savunması aşamalarından olan Süzülme Aşaması Önleme programının, 2029 yılına kadar ilk operasyonel yeterliliğe ulaşmasını zorunlu kılmıştır. Ek olarak, Stratejik ve Uluslararası Çalışmalar Merkezi kısa süre önce, özellikle Çin ve Rusya gibi ülkelerle yoğunlaşan rekabet ışığında, füze tehditlerini engellemede ve ülkenin hipersonik füze savunma yeteneklerini artırmada gelişmiş sensör mimarilerinin önemini vurgulayan bir çalışma yayınlamıştır[5]. Hipersonik silahların muharebe ortamına etkisi konusunda NATO da araştırmalarını sürdürmektedir. Hipersonik yeteneklerin, öncelikli kara ve deniz hedeflerine karşı etkinliğini artırması hedeflenmektedir[3].

2.3 Yönlendirilmiş Enerji Silahları

Yönlendirilmiş enerji silahları, "konsantre elektromanyetik enerji, atomik veya atom altı parçacıklardan oluşan bir ışın üreten" teknolojiyi kullanmaktadır. Basit bir ifadeyle, yönlendirilmiş enerji silahları, elektrik enerjisini veya kimyasal enerjiyi odaklı şekilde hedefine ileterek, hedefe zarar vermektedir. Diğer silahların aksine, bu teknolojide mermi yoktur.

Yönlendirilmiş enerji silahlarının örnekleri, yüksek enerjili lazerler, yüksek güçlü mikrodalga cihazları ve parçacık ışınlı silahlardır. Bu tür silahların geliştirilmesi ilk olarak 2000'li yılların başında hız kazanmıştır. O tarihlerde bu silahlar istenen hedefe ulaşsalar da ağır ve hantal kalmıştır. Bununla birlikte, son yıllarda, yönlendirilmiş enerji silahları çok daha küçük ve daha hafif hâle gelmiştir. Yönlendirilmiş enerji silahları, sessiz ve çoğu durumda görünmezdir, aynı anda birden fazla hedefe saldırabilirler.

NATO'nun "Bilim ve Teknoloji Trendleri 2024-2043" raporuna göre, yönlendirilmiş enerji silahları olgunlaşmış ve talep küresel olarak artmıştır. Bu lazerler ve yüksek güçlü mikrodalga silahlar zaten savaş alanında yıkıcı bir güçtür ve önümüzdeki birkaç yıl içinde daha da yaygın olarak kullanılması beklenmektedir. Bahsekonu rapor, mevcut yönlendirilmiş enerji silahları küresel pazarının 14,3 milyar dolar olduğu ve 2027 yılına kadar 72,1 milyar dolara yükseleceği tahminlerine yer vermektedir. Bu büyüme, enerji depolama, yapay zekâ/makine öğrenmesi ve malzemelerdeki gelişmelerden kaynaklanmaktadır. Birçok yönlendirilmiş enerji silahları sistemi çalışır hâle gelmiş veya çok ileri Teknoloji Hazırlık Seviyelerinde bulunmaktadır.

ABD'nin önde gelen savunma şirketi Lockheed Martin kısa süre önce ABD donanması muhriplerine Yüksek Enerjili Lazer ve Entegre Gözetlemeli Optik Göz Kamaştırıcı (HELIOS) sistemini kurmuştur. Sistem, 2022'nin sonlarında USS Preble gemisinde ilk kez sahneye çıkmıştır. HELIOS, 60 kW'lık yönlendirilmiş enerjili bir lazerdir, ancak daha güçlü 100 ve 150 kW'lık lazerler de mevcuttur. ABD Savunma Bakanlığı, 2024'te 500 kW'lık lazerlerin ve 2030'da 1 MW'lık lazerlerin kullanıma sunulacağını öngörmektedir[2].

ABD Uzay Kuvvetleri de bu silahları "uzay hâkimiyeti" elde etmek için geliştirdiğini doğrulamış, ancak ayrıntıları açıklamaktan kaçınmıştır[2]. Raporlarda, Uzay Kuvvetlerinin geliştirilmekte olan üç lazer silahı olduğunu, ancak bu silahları kullanıma sokmaktan 20 yıl uzakta olabileceği belirtilmektedir.

2.4 Robotik ve Otonom Sistemler

Tüm dünyada orduların yapay zekâ ve robotik teknolojilerine verdiği önem artmaktadır. Robotik teknolojilerin öne çıkmasının nedenlerinin başında insan kayıpları riskini azaltırken askeri operasyonlarda verimliliği artırması gelmektedir[6].

Robotik ve otonom sistemler, esas olarak durumsal farkındalığın artması ve askerlerin fiziksel ve bilişsel iş yükünün azaltılması sayesinde askeri çatışmaları bir sonraki seviyeye taşımayı mümkün kıldığı için savunma sanayii için büyük bir potansiyele sahiptir. Hem karada hem de denizde kullanıldıkları için manevra özgürlüğünü kolaylaştırmaktadır[7].

Robotlar ve otonom sistemler, kara mayını temizleme, mühimmat imhası, arama kurtarma operasyonları veya denizaltı navigasyonu ve gözetiminde yardımcı olabilmektedir. Diğer yandan, dünyada, sürü hâlinde otonom bir şekilde görev yapacak olan İnsansız Hava Aracı (İHA) ile ilgili birçok proje yürütülmekte ve geleceğin harekât ortamında da kullanılacağı öngörülmektedir. Özellikle yapay zekâ, otonomi, nesnelerin interneti, bulut veri ve 5G gibi teknolojilerin yaygınlaşması ile sürü hâlinde otonom harekât icra edebilen İHA'lar geliştirilmeye başlanmıştır. Bu gelişmelere paralel olarak değişen harekât ortamında, sürü otonom İHA'lara sahip olan ordular icra edilecek harekâtlarda karar icra döngüsünü kısaltarak stratejik, operatif ve taktik seviyede çok büyük avantaj sağlayacaklardır[8]. Denizlerde insansız olarak otonom veya uzaktan kontrolle görev yapabilen deniz araçları her geçen gün daha da yaygınlaşmaktadır. Gelişen teknolojiler ışığında ilk savunma hattı, saldırı, keşif, denetim, gözlem ve araştırma başta olmak üzere birçok kullanım alanı kazanan bu araçlar, mürettebatlı deniz araçlarının güvenli bir mesafede operasyonlara katılmasına imkân vermektedir[9].

2024 yılında da adından sıkça söz ettirecek askeri robot pazarının 2025 yılına kadar yüzde 11 bileşik büyüme oranıyla 24,2 milyar dolara ulaşması beklenmektedir. Sadece ABD Savunma Bakanlığının 2021'de robotik platformlara ve teknolojilere 7,5 milyar dolar harcadığı bildirilmektedir. ABD'de hâlihazırda çalışan 20 robotik programı vardır[2].

Silahlı otonom robotların savaşlarda kullanımı daha yeni yeni şekillenmeye başlamakla birlikte, dünyanın dört bir yanında, Yeni Zelanda ve Avustralya Hükümeti de dahil olmak üzere birçok ülke özerk silah sistemlerine karşı çıkmaktadır. Ancak, ABD bu robotların yasaklanmasını desteklememektedir. Birçok ülke, uzaktan kumandalı bir insan tarafından çalıştırılan robotik silah sistemleri olan "man-in-the-loop" sistemlerini hâlihazırda kullanmaktadır[2].

NATO'ya göre robotik, tüm özerklik seviyelerini (tam insan kontrolü dahil) kapsayan sistemler tasarlama ve inşa etme çalışmasıdır. İnsansız araçlar, bir kişi tarafından uzaktan kontrol edilebilir veya göreve bağlı olarak otonom olarak hareket edebilir. Uygulamalar arasında ulaşılamayan alanlara erişim, sürekli gözetim, uzun süreli dayanıklılık, askerleri destekleyen robotlar, daha ucuz yetenekler ve otomatik lojistik teslimatlar yer almaktadır[3].

İşbirliğine dayalı özerklik, boyut, ağırlık, güç ve maliyetlerdeki azalmalar ve yerleşik yapay zekâdaki önemli iyileştirmeler, robotik ve otonom sistemleri operasyonlarda etkili bir kuvvet çarpanı hâline getirmiştir. Bu çabaların başarısı, ISTAR (İstihbarat, Gözetleme, Hedefleme ve Keşif) ve hassas saldırı platformlarının operasyonlarda giderek daha yaygın hâle gelmesiyle, platform özerkliğinin (örneğin insansız araçlar) artan kullanımında görülmektedir.

Operasyonlarda daha fazla yarı-özerk ve tam özerk sistemlere yönelme NATO'nun gelecekteki yeteneklerini önemli ölçüde genişleterek her askerin bir bölük, her geminin bir görev grubu ve her uçağın bir filo olarak hareket edeceği bir ortama dönüştürecektir. Robotik ve otonom sistemler geliştirme, öncelikle yüksek irtifa-uzun dayanıklılık (HALE), artan entegre yapay zekâ seviyeleri, karar hızı ve insan-makine faktörleri (örneğin, gerekli insan gözetimi ve karar vermeyi korurken genel insan-makine ekibinin/sisteminin nasıl daha etkili hâle getirileceği) gibi operasyonel ihtiyaçlar tarafından yönlendirilmektedir. "Bilim ve Teknoloji Trendleri 2024-2043" raporuna göre, hem NATO'ya hem de potansiyel düşmanlara yönelik operasyonel avantajlar göz önüne alındığında, özerk sistemlerin önümüzdeki 20 yıl içinde mevcut ve gelecekteki operasyonel yetenekleri önemli ölçüde ve giderek daha fazla geliştireceği, tehdit edeceği ve etkinleştireceği konusunda çok az şüphe vardır[3].

2.5 Yapay Zekâ

Savunma ve havacılık sektöründeki karar vericilerinin yüzde 86'sı, ülkelerinin savunma uygulamaları için yapay zekâyı benimsediğini belirtmektedir. Bu durum 2024 yılında da yapay zekâ uygulamalarının daha fazla gelişeceğine işaret etmektedir[1]. 2024'te kamu ve özel sektör kuruluşları, yapay zekâ sistemlerinin güvenli, sorumlu ve güvenilir olup olmadığını anlamaya daha fazla önem verdikçe, yapay zekâ standartları ve ortaya çıkan sertifikasyon rejimleri de sert bir şekilde etkilenecektir.

Savunma ve havacılık karar vericilerinin yüzde 86'sı, ülkelerinin savunma uygulamaları için yapay zekâyı benimsediğini söylemektedir. Bu da 2024'te bu alanın daha fazla gelişeceğine işaret etmektedir. Yapay zekânın daha fazla güven vermesi için, açıklanabilirlik, şeffaflık, kesinlik ve doğruluk gibi yönleriyle gelişmesi gerekmektedir. Bu güven var olduğu sürece, savunma topluluğunun en son tehditlere karşı koymak için yapay zekâ teknolojisini daha fazla kullanmasına yol açacaktır[1].

Yapay zekâ algoritmaları büyük miktarda veriyi işleyebilmekte ve gerçek zamanlı olarak bilinçli kararlar alabilmektedir. Hayatın birçok alanında olduğu gibi, bu da savaş alanında dönüşüm yaratacaktır[10].

Yapay zekâ, savunma sanayiinde orduyu eğitmek, gelişmiş silahlar üretmek, gözetleme yapmak ve siber

güvenlik sağlamak için kullanılmaktadır. Teknoloji, bazı askeri operasyonlar sırasında askerlerin yerini alabilmekte ve bu da asker kayıplarını en aza indirmektedir. Gerçek zamanlı veri analizi gerçekleştirerek ve bilinçli karar almayı mümkün kılarak komuta ve kontrol sistemlerini dönüştüren yapay zekâ; ekipman arızasını tahmin etme yeteneği sağlayan kestirimci bakım sağlamakta, ağ trafiğinin analiz edilmesi, güvenlik açıklarının tespit edilmesi ve siber saldırılara zamanında müdahale edilmesi sayesinde siber tehditleri tespit etmekte ve azaltmakta, yapay zekâ güdümlü simülasyonlar ve sanal ortamlar kullanılarak askeri personel eğitilebilmekte, istihbarat ve gözetlemede kullanılmakta ve karar almayı desteklemektedir. Yapay zekâ büyük miktarda veriyi işleme yeteneği sayesinde ordunun durumsal farkındalığını artırıcı etki yaratmaktadır. Tüm bu nedenlerle yapay zekâ, 2024'te de askeri operasyonların dönüşümünde, etkinliğinin ve verimliliğinin artırılmasında büyük bir role sahip olacaktır[7].

Avrupa Savunma Ajansının (European Defence Agency -EDA) "2040'ın Ötesinde AB Askeri Yeteneklerinin Geliştirilmesi" raporunda, yapay zekânın temel kullanım alanları arasında yer alan karar verme sürecine insan rolünün dahil edilmesi ve tanımlanması konusunun gelecekte yapay zekâ tartışmasını yönlendirecek faktörlerden biri olacağı vurgulanmaktadır. EDA'ya göre bu sistemler, yeterli insan-makine işbirliğine izin veren operasyonel modellerin geliştirilmesini gerektiren insan eylemini tamamlamalı ve onun yerine geçmemelidir[11].

2.6 Siber Güvenlik

Son yıllarda siber saldırılar giderek daha fazla fiili savaşa benzer hâle gelerek vatandaşları tehdit etmekte ve büyük aksaklıklara neden olmaktadır. Bilgisayar korsanları ve siber teröristler, diğer ülkeler için resmi sıfatlarla veya kendi başlarına hareket ederek, elektrik şebekeleri ve iletişim sistemleri gibi kritik altyapıları çökertme yeteneklerini göstermiştir. Örneğin, bir uzman, siber suçluların tüm ABD'nin elektrik şebekesini devre dışı bırakmak için yalnızca dokuz trafo merkezini devre dışı bırakmasının yeterli olduğunu belirtmektedir[2].

2024 yılında siber güvenlik, savunma sanayii alanındaki trendlerden biri olmaya devam edecektir. Dijital bağımlılık arttıkça hem saldırı hem de savunma amaçlı siber savaş yeteneklerinin önemi de artmaktadır. Örneğin, yapay zekâ, siber güvenlikte giderek daha fazla öne çıkmakta, tehdit algılama ve tehditlere müdahaleyi otomatikleştirip geliştirmektedir. Ancak, bu ilerleme adeta iki ucu keskin bir bıçaktır. Yapay zekâ savunma mekanizmalarını düzene sokarken, aynı zamanda siber tehditler için yeni yollar açmakta, yapay zekânın faydalarından yararlanmak ile kötüye kullanım potansiyeline karşı korunmak arasında dikkatli bir denge kurulmasını gerektirmektedir[6].

Siber güvenlik, Rusya-Ukrayna Savaşı'nda önemini ve vazgeçilmezliğini benzersiz biçimde kanıtlamıştır. Ukrayna'nın son iki yılda çeşitli ülke ve kuruluşlardan aldığı siber savunma desteği akışı kritik olmaya devam etmektedir. Güvenli ve esnek dijital teknoloji ve hizmetler, Ukrayna'nın uzun vadeli hedefinin merkezinde yer almaktadır. Bu nedenle uzmanlar; Ukrayna esnek, dijital olarak bağımlı bir ekonomi inşa etmeye çalışırken, 2024'te hem ulus devletleri hem de özel sektörü içeren yenilikçi ortaklıklar görülme ihtimaline işaret etmektedir[1].

Daha geniş bir açıdan bakıldığında, 2024'te dünya çapında önemli seçimler yapılacak ve 50'den fazla ülkede halk, seçim için sandığa gidecektir[12] ve bu da bilgi güvenliği konusuna dikkatleri çekecektir. Yapay zekâ tarafından oluşturulan içeriğin doğrulanması ve seçim sistemlerinin siber müdahaleye karşı güvence altına alınması, önümüzdeki yıl boyunca dünyanın en büyük seçmen kitlesine sahip ülkelerinin bazılarında büyük zorluklar yaratabilecektir[1].

Gartner, 2025 yılına kadar siber saldırganların insanlara zarar vermek veya onları öldürmek için operasyonel teknolojiyi silah hâline getireceğini tahmin etmektedir[13]. Tüm dünyada ordular siber saldırılara karşı savunmayı ve kendi saldırılarını başlatmayı amaçlayan çok sayıda personel ve kuruluşlar görevlendirmektedir. Örneğin ABD'de Deniz Piyadeleri kısa süre önce dört yeni siber odaklı pozisyonun kurulduğunu duyurmuştur. ABD ordusunun diğer kollarında da siber güvenlik konularına adanmış personel mevcuttur. ABD Siber Komutanlığı, 2017 yılında Birleşik Muharip Komutanlığı hâline getirilmiş ve hâlihazırda 6.000'den fazla askeri personel istihdam etmektedir[2].

2.7 Kuantum Sensörler

Klasik fizik yasalarıyla açıklanamayan olayları araştırarak bilimde devrim yaratan kuantum mekaniği, 20'nci yüzyılın başlarında atomların, fotonların ve atom altı parçaların davranışını inceleyen araştırmalardan doğmuştur. Kuantum teknolojileri günümüzde henüz geliştirilme aşamasında olsa da temel zorluklar anlama, yatırım ve uygulamaları tanımlama ihtiyacından kaynaklanmaktadır.

Kuantum teknolojileri savunmada yepyeni olanakların kapısını aralamaktadır. Kuantum teknolojileri denizaltı gemi hareketlerinin tam olarak anlaşılmasına izin vermekten kriptografiyi kırmaya ve daha fazlasına kadar birçok alanda dönüşümsel bir etkiye sahip olabilecektir[10]. Örneğin, kuantum mekaniği ilkelerine dayanan "kuantum sensörlerle", savunma operasyonlarının temel yönlerinin 2024'te devrim yaratması ve aşağıdakiler aracılığıyla bozucu avantaj sağlaması beklenmektedir[1]:

- Benzersiz doğruluk ve hassasiyet sayesinde gelişmiş tehdit algılama ve gözetleme, ordunun proaktif tehdit tespiti için çok önemli olan ortamdaki küçük değişiklikleri tespit etmesini sağlar.
- GPS'in olmadığı ortamlarda dahi güvenli navigasyon ve konumlandırma sağlar, personel için riski önemli ölçüde azaltır ve görev başarısını artırır.
- Gizli teknoloji karşı önlemleri; kuantum radar yetenekleri aracılığıyla küçük, gizli veya hipersonik nesneleri benzeri görülmemiş bir hassasiyetle tespit etmek ve izlemek için kuantum etkilerinden yararlanarak geleneksel radar sistemlerinin sınırlamalarını ele alabilecektir.

- Güvenli iletişim ve şifreleme; iletişim sırasında hassas askeri verilerin gizliliğini ve bütünlüğünü sağlamak için geniş bant dalga biçimlerini korumak için kalkan sağlayacaktır.
- Kuantum sensörlerinin savunmaya entegrasyonu, ordunun çeşitli cephelerdeki yeteneklerini güçlendirirken, sürekli gelişen bir ortamda ulusal güvenliğe önemli ölçüde katkıda bulunan stratejik bir sıçramayı yansıtmaktadır.

NATO, "Bilim ve Teknoloji Trendleri 2024-2043" raporuna göre tüm kuantum teknolojileri arasında sensörler en gelişmiş olanıdır ve atomik enerji seviyeleri, fotonik durumlar ve spinler gibi fiziksel niceliklerin hassas ölçümlerini mümkün kılmaktadır. Dahası, kuantum sensörleri, manyetik, elektrik ve yerçekimini mükemmel çözünürlüklerde haritalandırarak, önemli ölçüde artırılmış hassasiyetle klasik muadillerini büyük ölçüde aşabilmektedir. Bununla birlikte, SWaP-C (boyut, ağırlık, güç ve maliyet) zorlukları oldukça ciddidir ve bu tür sensörlerin sahaya yerleştirilmesini sınırlayacaktır. Rapora göre elektromanyetik, gravimetrik, görüntüleme, radar ve manyetik algılama alanlarında sensör geliştirmeleri devam etmektedir. Bu ilerlemeler özellikle kısa vadede denizde mayın tespiti ve ASW (denizaltı karşıtı savaş) açısından önemlidir. LiDAR (ışık algılama ve menzil), algılama yetenekleri için arzu edilen, uzun vadeli bir hedeftir; ancak yolda geliştirilen teknolojinin savunma açısından kısa vadeli faydalar sağlaması muhtemeldir[3].

2.8 Çok Alanlı Entegrasyon

Çok Alanlı Entegrasyon (Multi-Domain Integration -MDI), tüm dijital ekosisteme bir bütün olarak bakmakla ilgilidir. Savunma uzmanları 2024'te, beş savunma alanının (kara, hava, deniz, siber ve uzay) veri paylaşımı ve hassas işlemeye (edge processing) dayalı entegre bir kuvvete doğru ilerlediğini görmeyi beklediklerini ifade etmektedir. Kuvvetlerin etki alanlarının her birini platform odaklı olmaktan uzaklaştırmak ve itici güç olarak zamanında, eyleme geçirilebilir ve görev açısından kritik veri ve istihbarat ile hizmet odaklı bir mimari yaklaşımına taşımak hedefler arasındadır.

Bununla birlikte, bu tür bir ilerleme ancak Çok Alanlı Entegrasyon teknolojilerini uygulamak için hükümetlerin sektörler arası ve uluslararası işbirlikleri ve esnek standartlar oluşturması ile mümkündür. BAE Systems'in bir araştırmasında da savunma karar vericileri hem hükümetin (yüzde 58) hem de endüstrinin (yüzde 57) çok alanlı entegrasyon stratejilerinin geliştirilmesi ve uygulanması için kaynak sağlamada rol oynaması gerektiğini ifade etmiştir[1].

2.9 Askeri Nesnelerin İnterneti

Günümüzde "sivil hayatta" kullanımı gittikçe yaygınlaşmaya başlayan nesnelerin interneti kavramı, 1970'lerde askeri laboratuvarlarda askeri amaçlarla ortaya atılmıştı. ABD Savunma Bakanlığı İleri Araştırma Projeleri Kurumunun (DARPA) 1970'lerin sonlarında başlayan ve 1980'lerde devam eden dağıtık sensör ağları araştırma programı kapsamında geliştirilen ayakkabı kutusu boyutlarındaki sensörler, savaş meydanındaki tehditlerin tespiti amacıyla kullanılmıştı. Bu program çerçevesinde geliştirilen teknolojiler, sivil uygulama alanları bularak günümüzde kullanılan nesnelerin interneti ekosistemini oluşturmuştu. Şimdi bu çalışmalar orijinal amacına dönerek ve nesnelerin interneti bir kez daha savaş alanına taşınmaktadır[14].

Nesnelerin İnterneti'nin bir sınıfı olan Askeri Nesnelerin İnterneti (Internet of Military Things -IoMT), operasyonel yetenekleri ve muharebe operasyonlarını geliştirmek için çeşitli askeri varlıkların, cihazların ve birbirine bağlı varlıklardan oluşan karmaşık bir ağın internet ile entegrasyonunu içeren gelişen bir alandır[15].

Askeri nesnelerin interneti sistemlerinin belki de en önemli katkıları; yapay zekâ sistemleri ve veri analiz becerileriyle, insanlara ve cephedeki robotlara danışmanlık yapabilmesidir[14]. Askeri nesnelerin interneti, cihazların, teknolojilerin ve internetin birbirine bağlı bir ağı olması, otomasyonun artmasını kolaylaştırmakta, karar almayı geliştirmekte ve gerçek zamanlı veri paylaşımını güvence altına almaktadır. Bu da durumsal farkındalığı geliştirmekte ve daha hızlı ve etkili karar almayı kolaylaştırmaktadır. IoMT'nin 2024 yılı ve sonrasındaki gelişme ve uygulamalarının sensörlerin, araçların, robotların ve silahların entegrasyonunu içermesi beklenmektedir[7].

3. İLERİ TEKNOLOJİLERİN AVRUPA GÜVENLİK EKOSİSTEMİNDEKİ YANSIMASI

Jeopolitik değişimlerin ve teknolojik gelişmelerin damgasını vurduğu 2023 yılında, Rusya-Ukrayna Savaşı nedeniyle özellikle Avrupa'nın güvenlik ve savunma mimarisinin derin değişimler geçirmeye devam ettiği göze çarpmaktadır. Bu dönüşümler yalnızca Avrupa ülkelerinin stratejik önceliklerini etkilemekle kalmamış, aynı zamanda ordu ve dolayısıyla personel üzerinde de doğrudan etki yaratmıştır.

2023'te Avrupa ülkeleri, büyük güçler arasında artan gerilimler karşısında rollerini tanımlamakta zorlanırken, Rusya'nın Ukrayna'da devam eden işgali ve İsrail'in Gazze saldırıları, birleşik bir Avrupa tepkisine duyulan ihtiyacın altını çizerek güvenlik duruşlarının yeniden değerlendirilmesine yol açmıştır. 2023 Avrupa açısından aynı zamanda teknolojik gelişmelerin askeri yetenekleri yeniden tanımlamaya devam ettiği yıl olmuştur. Yapay zekâ, siber yetenekler ve uzay tabanlı teknolojiler, modern savunma yapılarının ve stratejilerinin ayrılmaz bir parçası hâline gelmiştir. Avrupa'da savunma kuvvetleri ve personelinin bu gelişmekte olan teknolojileri etkin bir şekilde kullanmak ve bunlara karşı savunma yapmak için uygun ekipmana ihtiyacı olacak ve kuvvetler buna göre eğitim ve öğretimden geçirilecektir. Askeri personel söz konusu olduğunda, daha bağımsız ve esnek bir Avrupa savunma duruşuna hazırlığı artırmak için eğitim ve

teçhizata daha fazla yatırım yapılması beklenmektedir[16].

2024'te özellikle Avrupa'da güvenlik ve savunmada teknoloji önceliğinin belirgin bir fark yaratacağı ortadadır. Analizimizin ikinci bölümünde yer verdiğimiz öne çıkan ve bunlara eklenecek başka teknolojilerin neleri değiştireceği Avrupa'da savunma ile ilgili kuruluşların ilk gündem maddeleri arasında yerini almıştır. Örneğin Avrupa Savunma Ajansı (European Defence Agency -EDA) 2023'ün Ekim ayında, savunmada uzun vadeli küresel, yetenek ve teknoloji eğilimlerinin etkisi hakkında derinlemesine bir analiz yayınlamıştır. "2040 Sonrasında AB Askeri Yeteneklerinin Geliştirilmesi ("Enhancing EU Military Capabilities beyond 2040)"[11] başlıklı analiz, önümüzdeki 20 yıl ve sonrasında yetenek gereksinimlerini ve teknolojik ilerlemeleri şekillendirecek gelecekteki temel eğilimleri tanımlamaktadır. AB üye devletlerinden uzmanlarla işbirliği içinde EDA, potansiyel düşmanlara karşı askeri avantajı korumak için çok önemli olan bir dizi uzun vadeli yetenek eğilimi belirlemiştir.

Yetenek Geliştirme Planının 2023 Uzun Vadeli Değerlendirmesinde belirlenen ana eğilimler arasında çoklu alan bağlantısı; neredeyse gerçek zamanlı olarak gelişmiş durumsal farkındalığa olanak tanıyan bilişsel üstünlük; gelecekteki silah sistemlerine karşı koyma yeteneği ve uzay tabanlı etkinleştirme ve operasyonel varlıklara daha fazla güvenme olarak öne çıkmaktadır.

Çalışmaya göre, gelişmekte olan bozucu teknolojiler (Emerging Disruptive Technologies-EDT), 2040 askeri gereksinimlerinin şekillendirilmesinde birincil rol oynayacaktır. EDA, gelecekteki savaş alanının bir parçası olarak dikkate alınması gereken olası askeri uygulamaları ve zorlukları tanımlamak için dokuz temel EDT'yi belirlemiş ve bunları yetenek geliştirme perspektifinden incelemiştir. EDT'lerden ortaya çıkan sistemlerin ve bunların kombinasyonlarının askeri bağlamda birden fazla uygulamaya sahip olması muhtemeldir. Otonom sistemler bu açıdan değerli bir örnektir, hâlihazırda askeri yeteneklere hızla dahil edilmekte ve bu sistemlerin önümüzdeki yıllarda hızlanması beklenmektedir. Hipersonik ve yönlendirilmiş enerji silahları gibi yeni bozucu silahlar, silahlı kuvvetler için yeni fırsatlar ve zorluklar getirecektir[17].

EDA'nın çalışması ile 2040 ve sonrasında stratejik bağlamı şekillendirecek ana faktörlerin bir analizi yapılmış ve kalıcı dijitalleşmenin savaşın karakterini önemli ölçüde etkileyeceği stratejik faktörlerle ilgili eğilimler belirlenmiştir. İklim değişikliği ve etkisi, gelecekteki operasyonel ortamları yeniden şekillendirecektir. Artan küresel rekabet, yanlış bilgilerin yayılması, yaşlanan nüfus, siber tehditler ve ekonomik faktörler, AB güvenliğinin geleceğini etkileyen temel unsurlar olarak belirlenmiştir.

EDA'nın Öngörü Tatbikatı ile yapay zekâ, 5G iletişim ağları, yazılım tabanlı muharebe sahası görüşü ve insansız sistemlerin yaygın kullanımı ile ilgili gelişmelerle savaş alanının yaygın olarak dijitalleşmesi, gelecekteki savunma yetenekleri için önemli bir fırsat ve tehdit olarak tanımlanmıştır[17].

4. SONUÇ

Rusya-Ukrayna Savaşı ve İsrail'in Gazze'de sürdürdüğü saldırıların yarattığı küresel tedirginlik, başta Avrupa olmak üzere tüm dünyada güvenlik kaygılarını artırmıştır. Bu nedenle ülkeler savunma ve askeri kapasitelerini geliştirmek için, 21'inci yüzyılda savaşların doğasını kökten değiştiren bozucu teknolojilere odaklanmıştır.

Savunma ekosistemi ileri teknolojinin rehberliğinde dönüşmekte; siber savaş, yapay zekâ ve robotik yeni savaş alanları olarak ön planda yer almaktadır. Bu çerçevede hipersonik sistemler ve yönlendirilmiş enerji silahları, kuantum sensörleri ve askeri nesnelerin interneti teknolojileri de savunma sanayiinde ezberbozan yeniliklerin ortaya çıktığı alanların başında gelmektedir.

Orduların savunmasının yanı sıra saldırı kapasitelerini de güçlendirecek teknoloji çözümleri önümüzdeki aylarda kritik öneme sahip olacaktır. Dünyanın önde gelen ülkeleri teknoloji yeniliklerini olabildiğince hızlı geliştirmek, test etmek ve uygulamak için yarışmaktadır.

Yapay zekâ ve insansız sistemlerin yaygın kullanımı ile ilgili gelişmelerle savaş alanının yaygın olarak dijitalleşmesi, gelecekteki savunma yetenekleri için tüm dünyada önemli bir fırsat ve tehdit olarak tanımlanmaktadır. İleri teknolojilerin savaş ve askeri operasyonlar üzerindeki potansiyel etkisi, gelişmiş durumsal farkındalık, personel için azaltılmış risk, artan verimlilik, gelişmiş hassasiyet, ölümcüllük ve siber savunmayı içermektedir. Yeni teknolojilerin muharebe sahasına ve askeri eğitime hızlı bir şekilde adaptasyonu güvenlik kaygılarının had safhaya çıktığı çağımızda tüm ülkeler için önde gelen savunma önceliğidir.

KAYNAKÇA

[1] *BAE Systems*, "The future is now: Top five defence technologies to watch in 2024",https://www.baesystems.com/en/digital/predictions-2024-top-five-defence-technologies-to-watch. (Erişim Tarihi: 19 Mart 2023)

[2] Howarth, Josh; (2024), "6 Military Technology Trends to Watch (2024-2027)", *Exploding Topics*, (24 Ocak 2024), https://explodingtopics.com/blog/military-technology-trends. (Erişim Tarihi: 19 Mart 2023)

[3] *NATO*, (2023), "Science & Technology Trends 2023-2043", (Mart 2023), https://www.nato.int/nato_static_fl2014/assets/pdf/2023/3/pdf/stt23-vol1.pdf. (Erişim Tarihi: 19 Mart 2023)

[4] *NTV*, (2022), "Rusya Ukrayna'da ilk kez hipersonik füze kullandı: Hançer", (19 Mart 2022), https://www.ntv.com.tr/galeri/dunya/rusya-ukraynada-ilk-kez-hipersonik-fuze-kullandi-hancer,iep-ENuUukiwjqn-_hKjHA. (Erişim Tarihi: 19 Mart 2023)

[5] Myatt, Summer; (2023), "5 Pentagon Defense Tech Priorities for 2024", *GOVCON WIRE*, (20 Aralık 2023), https://www.govconwire.com/2023/12/5-pentagon-defense-tech-priorities-for-2024/. (Erişim Tarihi: 19 Mart 2023)

[6] Shukla, Shalini; (2023), "Defence Technology Trends 2024: AI, space systems lead big shifts", *Tech Observer*, (18 Aralık 2023), https://techobserver.in/news/defence/defence-technology-trends-2024-ai-space-systems-lead-big-shifts-280863/. (Erişim Tarihi: 19 Mart 2023)

[7] Sokolova, Victoria; (2024), "Driving Digital Transformation in Aerospace & Defense: Technology Trends in 2024", (3 Ocak 2024), *epicflow*, https://www.epicflow.com/blog/driving-digital-transformation-in-aerospace-defense-recent-technology-trends/. (Erişim Tarihi: 19 Mart 2023)

[8] Kalınbacak, İmren; (2023), "SÜRÜ OTONOM İHA SİSTEMLERİNİN MUHAREBE SAHASINDA UYGULAMA TAKTİKLERİ VE GELİŞTİRİLEN YENİ TEKNOLOJİLER" *Savunma Bilimleri Dergisi*, https://dergipark.org.tr/tr/pub/khosbd/issue/77151/1162593. (Erişim Tarihi: 19 Mart 2023)

[9] *STM ThinkTech*, (2021), "İNSANSIZ DENİZ ARAÇLARININ GELECEĞİ VE KULLANIM KONSEPTLERİ III- İDA'ların Mevcut Durumu ve Küresel İDA Pazarının Gelişimi", (30 Haziran 2021), https://thinktech.stm.com.tr/tr/insansiz-deniz-araclarinin-gelecegi-ve-kullanim-konseptleri-iii-idalarin-mevcut-durumu-ve-kuresel-ida-pazarinin-gelisimi. (Erişim Tarihi: 19 Mart 2023)

[10] Daniels, Chris; (2023), "EMERGING TECHNOLOGIES SHAPING THE FUTURE OF DEFENSE OPERATIONS", *KARVE*, (30 Mayıs 2023), https://www.karveinternational.com/insights/emerging-technologies-shaping-the-future-of-defense-security-operations%20. (Erişim Tarihi: 19 Mart 2023)

[11] *European Defence Agency*, (2023), "ENHANCING EU MILITARY CAPABILITIES BEYOND 2040", (Eylül 2023), https://eda.europa.eu/docs/default-source/eda-publications/enhancing-eu-military-capabilities-beyond-2040.pdf. (Erişim Tarihi: 19 Mart 2023)

[12] Bag, Mustafa; (2024), "2024 yılında 50'den fazla ülkede halk, seçim için sandığa gidecek", *euronews*, (10 Ocak 2024), https://tr.euronews.com/2024/01/10/2024-yilinda-50den-fazla-ulkede-halk-secim-icin-sandiga-gidecek. (Erişim Tarihi: 19 Mart 2023)

[13] *Gartner*, (2021), "Gartner Predicts By 2025 Cyber Attackers Will Have Weaponized Operational Technology Environments to Successfully Harm or Kill Humans", (21 Temmuz 2021), https://www.gartner.com/en/newsroom/press-releases/2021-07-21-gartner-predicts-by-2025-cyber-attackers-will-have-we. (Erişim Tarihi: 19 Mart 2023)

[14] *STM ThinkTech*, (2018), "Savaş Nesnelerinin İnterneti", (13 Kasım 2018), https://thinktech.stm.com.tr/tr/savas-nesnelerinin-interneti. (Erişim Tarihi: 19 Mart 2023)

[15] *Taal Tech*, "5 Leading Trends in Internet of Military Things (IoMT)", https://www.taaltech.com/5-leading-trends-in-internet-of-military-things-iomt/. (Erişim Tarihi: 19 Mart 2023)

[16] *European Organisation of Military Associations and Trade Unions*, "European Security and Defence from 2023 to 2024", https://euromil.org/european-security-and-defence-from-2023-to-2024/. (Erişim Tarihi: 19 Mart 2023)

[17] *European Defence Agency*, (2023), "Beyond 2040 - EDA analysis warns on future warfare trends and technology imperatives for European defence", (23 Ekim 2023), https://eda.europa.eu/news-and-events/news/2023/10/23/beyond-2040---eda-analysis-warns-on-future-warfare-trends-and-technology-imperatives-for-european-defence. (Erişim Tarihi: 19 Mart 2023)

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