İÇİNDEKİLER

ÜNİTE 1: SAVUNMA TEKNOLOJİLERİNİN TEKNİK YÖNLERİ

1. Temel Kavramlar ve Terminoloji

Savunma teknolojilerinde kullanılan teknik terimler, alanı anlamak ve doğru analiz yapabilmek için bir "ortak dil" işlevi görür. Bu bölümde İHA/SİHA, elektronik harp, radar, savunma yazılımları ve balistik sistemler gibi kavramlar hem tanıtılacak hem de ulusal/uluslararası örneklerle açıklanacaktır.

1.1 İHA / SİHA (İnsansız Hava Aracı / Silahlı İnsansız Hava Aracı)

Tanım ve Önemi

İHA'lar, üzerinde insan bulunmadan, uzaktan kumanda ya da otonom sistemlerle görev yapan hava araçlarıdır. Savunmada devrim niteliğinde bir teknoloji olup, gözetleme, keşif, istihbarat toplama, hatta doğrudan hedef imha görevlerinde kullanılmaktadır.

Türleri

TÜR	ÖZELLİK	ÖRNEK
Mini / Mikro İHA2–5 kg	İHA2–5 kg, düşük irtifa, kısa süreli keşif	Kargu-2 (Türkiye)
Taktik İHA	50–500 kg, orta menzil, gözetleme	Bayraktar TB2
MALE (Medium Altitude Long Endurance)	24–48 saat havada kalış, orta-yüksek irtifa	ANKA-S
HALE (High Altitude Long Endurance)	30.000 ft üzeri, kıtalararası operasyon	Global Hawk (ABD)

Türkiye Örnekleri

Bayraktar TB2: Ukrayna-Rusya savaşında dünya gündemine oturdu, birçok ülkeye ihraç edildi.

Akıncı: Ağır mühimmat taşıyabilen ileri seviye SİHA.

ANKA-S: Uydu kontrollü, uzun menzilli keşif-gözetleme.

Küresel Örnekler

MQ-9 Reaper (ABD): Afganistan ve Irak'ta yoğun olarak kullanıldı.

Heron (İsrail): Uzun yıllar Türk Silahlı Kuvvetleri envanterinde de bulundu.

Stratejik Önemi

1.2 Elektronik Harp (EH) Sistemleri ve Radar Teknolojileri

Elektronik Harp Nedir?

Elektronik harp, modern savaşların en kritik unsurlarından biri hâline gelmiştir. Elektromanyetik dalgaların yönlendirilmesiyle iletişim sistemleri etkisiz bırakılabilir. Sinyal istihbaratı düşmanın haberleşmesini çözümlemeyi mümkün kılar. Elektronik karıştırma ise radar ve iletişim sistemlerini bozarak üstünlük sağlar. Bu alan, teknolojik gelişmelerle sürekli yenilenmektedir.

Temel Unsurlar

Elektronik Destek (ED):

- Düşman sinyallerini algılayarak varlığını tespit eder.
- Sinyallerin frekans, güç ve yön bilgilerini analiz eder.
- Elde edilen verilerle taktik ve stratejik istihbarat sağlar.

Elektronik Taarruz (ET):

- Radar ve haberleşme sistemlerini bozarak işlevsiz bırakır.
- Yanıltıcı sinyaller göndererek düşmanı yanlış yönlendirir.
- Elektronik altyapıyı hedef alarak operasyonel üstünlük kurar.

Elektronik Koruma (EK):

- Kendi haberleşme ve radar sistemlerini korur.
- Anti-jamming teknikleriyle karıştırmalara karşı önlem alır.
- İletişim ve sensör güvenliğini sürdürerek operasyon sürekliliğini sağlar.

Radar Teknolojileri

Radar sisteminin çalışma prensibi oldukça basittir. Sistem, bir verici aracılığıyla yüksek frekanslı elektromanyetik dalgalar yayar. Bu dalgalar, çevredeki nesnelere çarptıktan sonra geri yansır ve radarın alıcısı tarafından algılanır. Bu yansıyan sinyaller, radar sistemi tarafından işlenerek nesnenin uzaklığı, hızı ve yönü gibi veriler hesaplanır.

Radarların savunma stratejilerindeki önemi

Radar teknolojisi, askeri stratejilerde hem savunma hem de saldırı açısından kritik bir rol oynar. Radarlar, modern savaşın her aşamasında bilgi üstünlüğü sağlar; düşmanın konumunu, hızını, yönünü ve hareketlerini önceden tespit

ederek operatörlere büyük bir avantaj sunar. Bu sayede radar sistemleri, stratejik karar alma süreçlerini doğrudan etkileyen bir faktör haline gelmiştir.

ÖRNEKLER:

Klasik Radar: Döner anten, 2D görüntü.

AESA Radar (Active Electronically Scanned Array): Elektronik tarama yapar, aynı anda birden çok hedef izler.

Türkiye Örnekleri

ASELSAN KORAL: Elektronik harp sistemi, düşman radarlarını kör edebiliyor.

EIRS (Erken İhbar Radar Sistemi): Uzun menzilli AESA radar.

1.3 Savunma Yazılımları ve Balistik Sistemler

Savunma Sanayisinde Yazılımın Rolü

Modern savunma sistemleri, sadece donanımdan ibaret değildir; yüksek teknolojiye sahip yazılımlarla desteklenir. Yazılım, insansız hava araçlarından (İHA) komuta kontrol sistemlerine, radar teknolojilerinden siber güvenlik çözümlerine kadar geniş bir yelpazede kullanılmaktadır. Bu kapsamda savunma sanayisindeki yazılım uygulamalarının şu temel işlevleri vardır:

1. Gerçek Zamanlı Veri Analizi: Yazılımlar, saha verilerini gerçek zamanlı olarak analiz ederek karar alıcıların doğru hamleler yapmasını sağlar.

2. Simülasyon ve Eğitim Sistemleri: Savaş senaryolarının simüle edilmesi ve personel eğitimi için kullanılan yazılımlar, sahadaki performansı artırır.

3. Siber Güvenlik: Kritik savunma altyapılarının korunması için yazılımlar saldırılara karşı önleyici ve tepki verici çözümler sunar.

4. Otonom Sistemler: İHA'lar, kara araçları ve denizaltıların otonom olarak çalışmasını sağlayan algoritmalar bu yazılımların eseridir.

Balistik Sistemler

Balistik füze, başlangıçta bir roket motoru ile hız kazanan ve daha sonra yerçekiminin etkisiyle hedefe yönelen bir füze türüdür. İlk aşamada dik bir açıyla fırlatılır ve atmosferin dışına çıkar. Atmosferin dışında belirli bir yörünge izledikten sonra yerçekimi etkisiyle tekrar atmosfere girer ve hedefe ulaşır.

Bu yüzden "Balistik" terimi, füzenin kontrol dışı olarak yerçekimi etkisinde hareket ettiği yörüngeden gelir.

Bu füzeler genellikle nükleer, kimyasal, biyolojik veya konvansiyonel savaş başlıkları taşır.

Kıtalararası balistik füzeler (ICBM) gibi türler, 5.500 kilometreden fazla mesafeleri kat ederek, bir kıtadan diğerine saldırı yapma yeteneğine sahiptir.

Tür	Menzil Aralığı	Açıklama
Kısa Menzilli (SRBM)	300 – 1.000 km	Bölgesel hedeflere karşı kullanılır.
Orta Menzilli (MRBM)	1.000–3.000 km	Daha geniş coğrafyalara etki eder.
Uzun Menzilli (ICBM)	1.000–3.000 km	Kıtalar arası hedeflere ulaşabilir.

Balistik füzeler menzillerine göre sınıflandırılır. SRBM'ler kısa menzilli olup bölgesel tehditler için tercih edilir. MRBM'ler orta mesafeli stratejik hedeflere yöneliktir. ICBM'ler ise kıtalar arası atış kapasitesine sahiptir ve en yüksek menzile ulaşır.

Türkiye Örnekleri

HİSAR: Alçak ve orta irtifa hava savunma sistemi.

SİPER: Uzun menzilli hava savunma

SOM Füzesi: Uzun menzilli seyir füzesi.

2. Tehditler ve Zafiyetler

Günümüzün modern savunma teknolojileri her geçen gün gelişmekte, ancak buna paralel olarak karşılaştıkları tehditler ve zafiyetler de artmaktadır. Savunma sistemlerinin güvenilirliği yalnızca sahip olunan silah ve donanımın gücüyle değil, aynı zamanda bu sistemlerin elektronik harp, siber saldırılar ve asimetrik tehditlere karşı korunma kapasitesiyle belirlenir.En gelişmiş silahlar bile uygun önlemler alınmadığında düşük maliyetli yöntemlerle etkisiz hale getirilebilir. Bu nedenle modern savunma anlayışı, yalnızca güçlü silahlar geliştirmekten ibaret değildir; aynı zamanda bu silahların çok katmanlı bir güvenlik ağı içinde korunmasını da gerektirir.Özetle, savunma teknolojilerinin etkinliği, onların esnek, dayanıklı ve sürekli güncellenebilir olmasına bağlıdır. Yalnızca bu şekilde hızla değişen güvenlik ortamında caydırıcılık ve stratejik üstünlük korunabilir.

2.1 Siber Saldırı Türleri

Siber saldırılar, günümüzün en kritik askeri tehditlerinden biri haline gelmiştir. Geleneksel silahlı çatışmaların ötesinde, devletler artık rakiplerini zayıflatmak için öncelikle siber altyapıları hedef almaktadır. Enerji ağları, iletişim sistemleri, ulaşım hatları ve finansal altyapılar bu saldırıların başlıca hedefleri arasında yer alır. Bu nedenle siber güvenlik, modern savaş doktrinlerinde en az konvansiyonel savunma kadar stratejik bir önem taşımaktadır.

2.1.1 DDoS (Distributed Denial of Service)

Tanım: Bir sisteme aşırı miktarda trafik gönderilerek hizmet dışı bırakılmasıdır.

Örnek: Estonya (2007) siber saldırıları, kritik kamu kurumlarını günlerce felç etmiştir.

Askeri Etki: Komuta-kontrol merkezlerinin işleyişini durdurabilir, radar sistemlerini geçici olarak devre dışı bırakabilir.

2.1.2 Veri Sızdırma (Data Breach)

Tanım: Kritik askeri bilgilerin yetkisiz kişilerce ele geçirilmesidir.

Örnek: ABD’de Edward Snowden vakası, gizli NSA belgelerinin sızmasına yol açmıştır.

Türkiye Açısından Risk: Savunma projelerine ait Ar-Ge bilgilerinin çalınması, ulusal güvenlik açığı doğurur.

2.1.3 Zararlı Yazılım ve Casus Yazılımlar

Stuxnet (2010): İran'ın nükleer tesislerini hedef alan bu saldırı, savunma tarihinde en ünlü siber sabotajlardan biridir.

Etki: Fiziksel sistemlere zarar verebilir; radar, füze kontrol merkezlerini sabote edebilir.

2.2 Uydu ve İletişim Sistemlerine Yönelik Tehditler

Savunma operasyonları günümüzde büyük ölçüde uydu tabanlı iletişim ağlarına ve GPS sistemlerine bağımlı hale gelmiştir. Komuta-kontrol mekanizmalarının işlerliği, hedef tespiti, istihbarat paylaşımı, navigasyon ve silah sistemlerinin etkin kullanımı doğrudan bu altyapılara bağlıdır. Ancak bu teknolojik üstünlük, beraberinde yeni tehdit ve zafiyetleri de getirmektedir.

Sinyal Karıştırma (Jamming): Uydu sinyalleri düşman unsurlar tarafından kasıtlı olarak bozulabilir veya bastırılabilir. Bu durumda haberleşme kesintiye uğrar, askeri unsurlar koordinasyon yeteneklerini kaybeder ve özellikle insansız hava araçları gibi platformlar görev dışı kalabilir.

Sinyal Aldatma (Spoofing): Yanıltıcı sinyaller gönderilerek dronlar, füzeler ya da gemi ve uçak gibi unsurlar yanlış yönlendirilebilir. Böyle bir durumda yüksek teknolojiye sahip sistemler bile dost unsurlar için ciddi bir risk oluşturabilir.

Uyduya Fiziksel Saldırı: 2007 yılında Çin'in gerçekleştirdiği anti-uydu (ASAT) füzesi denemesi, bu tehdidin somut bir örneğidir. Uydu imhası yalnızca haberleşme ve gözlem kapasitesini felce uğratmakla kalmaz, aynı zamanda yörüngede oluşan enkaz diğer uydular için de ciddi bir tehdit haline gelir.

Türkiye açısından: Göktürk-1 ve Göktürk-2 gözlem uyduları ile Türksat haberleşme uyduları, ülkenin bağımsız istihbarat, keşif ve iletişim kapasitesini güçlendirmiştir. Ancak bu kazanımlar, uydu güvenliği sağlanmadığı takdirde stratejik bir kırılganlık noktası olmaya devam etmektedir. Türkiye'nin, yalnızca yeni uydular geliştirmesi değil; aynı zamanda bu uyduların siber saldırılara, elektronik harp girişimlerine ve anti-uydu tehditlerine karşı korunmasını sağlayacak savunma stratejileri oluşturması kritik önemdedir.

2.3 Yapay Zekâ Kaynaklı Operasyonel Hatalar

Yapay zekâ, savunma teknolojilerinde hedef tespiti, otonom sürü dron yönetimi, siber güvenlik tehdit analizleri gibi alanlarda kullanılmaktadır. Ancak bu teknoloji çift taraflı bir kılıçtır.

Yanlış Hedef Tanıma: Dost unsurların düşman olarak algılanması ("Friendly Fire").

Önyargılı Algoritmalar: Verilen eğitim verisi hatalı ise sistem yanlış kararlar alabilir.

Kontrol Kaybı: Otonom silah sistemlerinin insan müdahalesi olmadan karar alması, etik ve güvenlik sorunları doğurur.

Örnek: ABD ordusunun bazı testlerinde, yapay zekâ destekli dronların beklenmedik davranışlar göstererek "kendi kararlarını aldığı" rapor edilmiştir.

2.4 Türkiye'nin Karşı Karşıya Olduğu Zafiyetler

1. Yerli Yazılım Eksiklikleri

Türkiye, savunma sanayinde önemli ilerlemeler kaydetmiş olsa da, kritik yazılımlar konusunda hâlâ dışa bağımlılık oranı yüksektir. Özellikle radar, hava savunma sistemleri, komuta-kontrol yazılımları ve uydu işletim yazılımlarında yabancı kaynaklı çözümler kullanılmaktadır. Bu durum, sistemlerin güvenliği açısından risk oluşturmakta; olası bir kriz veya yaptırım durumunda

güncellemelerin kesilmesi ya da arka kapı (backdoor) yazılımlar yoluyla sistemlerin manipüle edilmesi ihtimalini doğurmaktadır.

Gelişim İçin:

Yerli yazılım ekosistemini güçlendirecek Ar-Ge yatırımlarının artırılması, üniversite-savunma sanayi iş birliklerinin genişletilmesi ve açık kaynak kodlu çözümlerin millî güvenlik perspektifiyle uyarlanması kritik önemdedir.

2. Uydu İletişimi

Türkiye, Göktürk ve Türksat uyduları ile gözlem ve haberleşme kapasitesini geliştirmiş olsa da, hâlen NATO altyapısına bağımlı olarak çalışmaktadır. Bu bağımlılık, savaş veya kriz anında uydu erişiminin kısıtlanması riskini doğurmaktadır. Ayrıca Türkiye'nin yörüngedeki uydu sayısı sınırlı olduğu için, küresel kapsama alanı ve sürekli iletişim sağlama kapasitesi de kısıtlıdır.

3. Siber Güvenlik Açıkları

Türkiye, son yıllarda siber güvenlik alanında kurumsal yapılar oluşturmuş olsa da, kamu kurumları ve özel sektör arasında hâlen koordinasyon eksiklikleri yaşanmaktadır. Bu durum zaman zaman veri sızıntılarına, kimlik bilgilerinin yasa dışı platformlarda paylaşılmasına ve kritik altyapıların hedef alınmasına yol açmaktadır. Özellikle enerji, ulaşım ve bankacılık sektörleri olası siber saldırılar karşısında yüksek risk taşımaktadır.

3. Kritik Altyapı ve Yerli Üretim

Savunma teknolojilerinde kritik altyapılar ve yerli üretim kapasitesi, ulusal güvenliğin temel taşlarıdır. Bir ülkenin dışa bağımlılığı ne kadar azsa, kriz ve savaş anlarında manevra kabiliyeti o kadar yüksek olur. Türkiye'nin son yıllarda savunma sanayinde elde ettiği ilerlemeler, bu stratejinin somut bir yansımasıdır.

3.1 Türkiye'nin Dışa Bağımlılığını Azaltma Stratejileri

Türkiye, 1974 Kıbrıs Barış Harekâtı sırasında uygulanan ABD silah ambargosundan sonra savunma alanında dışa bağımlılığın ne kadar büyük bir risk olduğunu tecrübe etmiştir. Bu nedenle son yıllarda stratejik olarak üç ana hedef belirlenmiştir:

1. Yerli Üretim Oranını Artırma

2000'lerin başında %20 seviyesinde olan yerli üretim oranı, 2023 itibarıyla %70'lere yaklaşmıştır.

2030 hedefi, %80–85 seviyesine ulaşmaktır.

2. Kritik Teknolojilerde Bağımsızlık

Motor, radar, uydu ve yazılım gibi alanlarda dışa bağımlılığı azaltmak.

İthal bileşenler yerine yerli mühendislik çözümleri geliştirmek.

3. İhracat Kapasitesini Artırma

Bayraktar TB2, Akıncı, T129 ATAK gibi ürünlerle Türkiye, 30'dan fazla ülkeye savunma teknolojisi ihraç etmektedir.

Savunma ihracat gelirleri 2022'de 4,4 milyar $ seviyesine ulaşmıştır.

3.2 ASELSAN, TUSAŞ ve ROKETSAN Örnekleri

ASELSAN (Askerî Elektronik Sanayi)

1975'te kurulmuştur.

Uzmanlık alanları: Radar, elektronik harp, haberleşme sistemleri, gece görüş teknolojileri.

Önemli Projeler:

AESA Radar geliştirme (hava savunma için kritik).

GÖKDENİZ yakın hava savunma sistemi.

Sahil güvenlik ve kara kuvvetleri için modern telsiz sistemleri.

TUSAŞ (Türk Havacılık ve Uzay Sanayii A.Ş.)

1984'te kurulmuştur.

Uzmanlık alanları: Uçak, helikopter, insansız hava araçları (UAV).

Önemli Projeler:

HÜRJET: Jet eğitim uçağı.

ATAK-2: Ağır taarruz helikopteri.

Milli Muharip Uçak (KAAN): Türkiye'nin 5. nesil savaş uçağı.

ROKETSAN

1988'de kurulmuştur.

Uzmanlık alanları: Füze ve roket sistemleri.

Önemli Projeler:

SOM seyir füzesi (F-16 ve milli uçaklarda kullanılıyor).

SUNGUR hava savunma füzesi.

UMTAS tanksavar füze sistemi.

Uzay roketleri ve uydu fırlatma projeleri.

3.3 Yerli Motor ve Radar Projeleri

Bir ülkenin savunma bağımsızlığında en kritik noktalarından biri motor teknolojileridir. Çünkü uçak, helikopter, İHA ve tanklar için motor geliştirmek son derece zorlu bir mühendislik alanıdır.

Yerli Motor Projeleri

TEI (TUSAŞ Motor Sanayii A.Ş.):

TS1400: ATAK helikopterleri için yerli turboşaft motor.

TEI-PD170: İnsansız hava araçlarında kullanılan dizel motor.

BATU motoru: Altay tankı için geliştirilmiş yerli motor.

Yerli Radar Projeleri

ASELSAN AESA Radar: Milli Muharip Uçak (KAAN) için geliştirilmektedir.

EIRS (Erken İhbar Radar Sistemi): Uzun menzilli hava savunma için tasarlanmıştır.

CENK-S Radar: Milli gemilere entegre edilen çok fonksiyonlu radar sistemi.

3.4 Stratejik Önemi

Yerli üretim, sadece ekonomik bir gereklilik değil, aynı zamanda stratejik bir güvenlik meselesidir.

Savaş ve Ambargo Riski: Dışa bağımlı ülkeler, kriz anlarında tedarik sıkıntısı yaşar.

Teknoloji Transferi: Yerli üretim sayesinde mühendislik bilgisi ülke içinde kalır.

İhracat Gücü: Savunma teknolojileri, uluslararası ilişkilerde stratejik bir koz haline gelir.

3.5 Türkiye’nin Yol Haritası

Kısa Vadeli Hedef: 2025’e kadar insansız hava, kara ve deniz sistemlerinde %75 yerli oranı.

Orta Vadeli Hedef: 2030’a kadar milli uçak, tank ve füzelerde tamamen yerli motor ve radar entegrasyonu.

Uzun Vadeli Hedef: 2040 sonrası için uzay tabanlı savunma sistemlerinde (uydu fırlatma, lazer silahları, hipersonik füzeler) bağımsız üretim kapasitesi.

4. Yeni Teknolojiler ve Savunma

Savunma teknolojilerinin geleceği, büyük ölçüde yeni nesil teknolojilerin entegrasyonuna bağlıdır. Yapay zekâdan kuantum bilgisayarlara, biyoteknolojiden uzay tabanlı sistemlere kadar geniş bir yelpazede gelişmeler, savunmanın doğasını köklü biçimde değiştirmektedir. Günümüzün savaş alanı sadece karada, denizde ve havada değil; siber uzayda ve uzayda da sürmektedir.

4.1 Yapay Zekâ ve Otonom Sistemler

Kullanım Alanları

İnsansız Hava Araçları (UAV): Hedef tespiti, rota belirleme, sürü halinde görev icrası.

Karar Destek Sistemleri: Komutanlara gerçek zamanlı veri analizi sunma.

Elektronik Harp: Düşman radarlarını yanıltma, siber saldırılarda otomatik savunma.

Örnekler

Bayraktar KIZILELMA: Yapay zekâ destekli insansız savaş uçağı.

Sürü Drone Teknolojisi: Onlarca mini İHA'nın eş zamanlı olarak koordineli görev yapabilmesi.

ABD ve Çin'deki Prototipler: Yapay zekâ ile savaş simülasyonlarında pilotları geçen otonom uçaklar.

4.2 Siber Güvenlik ve Siber Savaş

Savaşların önemli bir kısmı artık siber alanda yaşanmaktadır. Devletler, enerji santralleri, bankalar, haberleşme altyapısı gibi kritik hedeflere saldırılar düzenlemektedir.

Türkiye'nin Kapasitesi

Siber Komutanlık: Türk Silahlı Kuvvetleri bünyesinde kurulmuştur.

HAVELSAN Siber Güvenlik Çözümleri: Yerli yazılımlarla ağ güvenliği, tehdit tespiti.

Milli Yazılımlar: Ulusal işletim sistemleri ve şifreleme algoritmaları.

4.3 Kuantum Teknolojileri

Kuantum teknolojileri, kuantum mekaniğinin temel ilkelerinden (süperpozisyon, dolanıklık, belirsizlik ilkesi vb.) yararlanarak klasik teknolojilerin ötesinde yetenekler geliştirmeyi amaçlar. Savunma sanayiinde öne çıkan kullanım alanları şunlardır:

1. Kuantum Haberleşme

- Kuantum anahtar dağıtımı (QKD) sayesinde kırılamaz şifreleme sağlanır.
- Geleneksel şifreleme yöntemleri süper bilgisayarlar tarafından kırılabilirken, kuantum tabanlı iletişimde her müdahale fark edilir, bu da güvenliği üst seviyeye çıkarır.

2. Kuantum Radar Sistemleri

- Geleneksel radarların aksine, radar görünmezliği (stealth) teknolojilerini aşabilecek kapasiteye sahiptir.
- Kuantum dolanıklık ve foton tabanlı algılama teknikleri sayesinde düşük görünürlüklü uçaklar veya denizaltılar tespit edilebilir.

3. Kuantum Hesaplama

- Çok karmaşık askeri simülasyonlar, şifre kırma, malzeme bilimi ve yeni silah teknolojilerinin geliştirilmesi için kullanılabilir.
- Özellikle kriptoanaliz (mevcut şifrelerin kırılması) ve optimizasyon problemleri (lojistik, operasyon planlaması, rota belirleme) açısından devrimsel potansiyele sahiptir.

4. Kuantum Sensörler ve Navigasyon

- GPS bağımlılığını ortadan kaldırabilecek kuantum navigasyon sistemleri geliştirilmektedir.
- Bu sayede GPS sinyallerinin kesildiği ya da aldatıldığı (spoofing/jamming) ortamlarda bile hassas konumlama yapılabilir.

- Ayrıca denizaltı tespiti, yer altı yapıların haritalanması ve hassas füze yönlendirmesinde kullanılabilir.

5. Kuantum İstihbarat ve Elektronik Harp

- Kuantum tabanlı sensörler elektromanyetik spektrumda çok daha hassas ölçümler yapabilir.
- Bu, düşman iletişim trafiğinin tespiti, elektronik sinyal analizi ve yeni nesil elektronik harp kabiliyetleri anlamına gelir.

4.4 Uzay Tabanlı Sistemler

Uzay artık sadece bilimsel araştırmaların değil, savunma stratejilerinin de yeni sahnesi haline gelmiştir.

Uydu Teknolojileri: İstihbarat, haberleşme, GPS alternatifi milli sistemler.

Türkiye'nin Uyduları:

GÖKTÜRK-1 ve GÖKTÜRK-2: Yüksek çözünürlüklü görüntüleme.

TÜRKSAT serisi: Haberleşme.

İMECE: Yer gözlem uydusu.

Uzay Komutanlığı: ABD, Çin ve Rusya tarafından kurulmuş olup gelecekte Türkiye için de zorunlu bir adım olabilir.

4.5 Biyoteknoloji ve Savunma

Geleceğin savaşları yalnızca makinelerle değil, biyolojik unsurlarla da şekillenecektir.

Biyolojik Silahlar: Genetik olarak hedeflenmiş virüsler.

Asker Sağlığı: Genetik testlerle askerlerin dayanıklılığını artırma.

Biyosensörler: Savaş alanında kimyasal ve biyolojik tehditleri anında tespit etme.

4.6 Gelecek Perspektifi

Türkiye'nin bu teknolojilerde yol haritası:

- 2025: Yerli İHA/SİHA, füze ve elektronik harp sistemlerinde bölgesel üstünlük sağlamak.
- 2030: Milli muharip uçak (KAAN) ve uzay tabanlı savunma teknolojilerini aktif kullanıma sokmak.
- 2040: Otonom ve ileri teknolojiye dayalı savunma sistemleriyle küresel ölçekte ilk 5 ihracatçı ülke arasına girmek.

Genel Hedef Özeti: Türkiye'nin savunma sanayii, yerli ve millî üretimi artırarak dışa bağımlılığı azaltmayı, ileri teknoloji platformları (hava, kara, deniz, uzay) geliştirmeyi ve otonom–yapay zekâ tabanlı sistemlerle küresel ölçekte rekabetçi, ihracatçı bir güç olmayı hedeflemektedir.

5. KÜRESEL SAVUNMA AR-GE YAPILARI VE TÜRKİYE'NİN ROLÜ

5.1 Uluslararası İş Birlikleri

NATO DIANA Programı

NATO, savunma inovasyonunu hızlandırmak amacıyla 2022'de Defence Innovation Accelerator for the North Atlantic (DIANA) programını başlatmıştır. Bu program, müttefik ülkelerdeki girişimcilere ve teknoloji şirketlerine destek vererek yapay zekâ, kuantum teknolojileri, biyoteknoloji, yeni malzemeler ve enerji çözümleri gibi alanlarda inovatif çözümler geliştirmeyi hedeflemektedir. Türkiye de bu programda yer almakta olup, savunma start-up ekosisteminin NATO standartlarına uyum sağlamasında DIANA kritik bir rol üstlenmektedir.

EUROSAM Ortaklığı

Türkiye, özellikle uzun menzilli hava savunma sistemleri alanında Fransa ve İtalya ortaklığındaki EUROSAM konsorsiyumu ile iş birliği yapmaktadır. Bu çerçevede SAMP/T hava savunma sistemi üzerine ortak çalışmalar yürütülmüş, Türkiye'nin yerli hava savunma kabiliyetleri (SİPER projesi) bu tecrübelerle desteklenmiştir. Ancak Türkiye'nin Rusya'dan S-400 tedarik etmesi, bu iş birliğinde belirli gerilimler yaratmıştır.

ABD-Türkiye İş Birlikleri

Türkiye ile ABD arasındaki savunma Ar-Ge iş birlikleri tarihsel olarak önemli olmakla birlikte, son yıllarda sınırlı düzeyde kalmıştır. Türkiye'nin F-35 programından çıkarılması bu iş birliğini ciddi ölçüde zayıflatmıştır. Ancak hâlen F-16 modernizasyon projeleri, lojistik destek ve ortak eğitimler gibi alanlarda iş birliği devam etmektedir. Bunun yanında Türkiye'nin savunma sanayiinde bağımsızlık stratejisi, ABD'ye olan bağımlılığı azaltmayı hedeflemektedir.

5.2 Türkiye'de Savunma Ar-Ge Yapıları

TÜBİTAK-SAGE

Türkiye'nin en önemli savunma araştırma merkezlerinden biridir. SOM seyir füzesi, Gökdoğan ve Bozdoğan hava-hava füzeleri, Hassas güdüm kitleri (HGK, LGK) gibi kritik projelere öncülük etmiştir. TÜBİTAK-SAGE, mühimmat ve füze teknolojileri alanında Türkiye'nin dışa bağımlılığını azaltmada stratejik bir rol üstlenmektedir.

Savunma Sanayii Başkanlığı (SSB)

SSB, Türkiye'deki tüm savunma projelerinin planlanması, koordinasyonu ve finansmanında ana otoritedir. Alt yüklenici firmalar (ASELSAN, TUSAŞ, ROKETSAN, HAVELSAN vb.) SSB'nin yönlendirmesiyle projeler yürütmektedir. Ayrıca SSB, Milli Teknoloji Hamlesi ile Türkiye'nin kritik teknolojilerde yerlileşme ve bağımsızlaşma vizyonunu savunma sanayiine entegre etmiştir.

Üniversiteler ve Teknokentler

ODTÜ, İTÜ, Bilkent, YTÜ gibi üniversiteler savunma teknolojileri alanında önemli araştırma projeleri yürütmektedir. Teknopark İstanbul, ODTÜ Teknokent gibi yapılar, savunma girişimciliği için birer Ar-Ge merkezi haline gelmiştir.

5.3 Karşılaştırmalı Analiz

ÜLKE	Öne Çıkan Kuruluş	Teknoloji Alanı	Açıklama
ABD	DARPA	Yapay zekâ, robotik, hipersonik silahlar, siber güvenlik	Dünyanın en büyük savunma Ar-Ge bütçesine sahip. Pek çok yenilikçi teknoloji (internet, GPS vb.) DARPA'dan çıkmıştır.
İSRAİL	Rafael,IAI	Demir Kubbe, insansız sistemler, elektronik harp	Küçük ölçekli olmasına rağmen yüksek teknolojiye dayalı savunma ve katliam soykırım inovasyonunda öncü bir ülke.
RUSYA	Rostec	Elektronik harp, füze teknolojileri, hipersonik silahlar	Sovyet mirasına dayanarak güçlü bir savunma ekosistemine sahip; özellikle elektronik harp kabiliyetleriyle öne çıkıyor
TÜRKİYE	ASELSAN,TUSAŞ, ROJETSAN,HAVELSAN	İHA/SİHA, radar, füze, motor geliştirme	Son 20 yılda hızlı büyüme kaydetti. İHA/SİHA teknolojilerinde küresel liderlerden biri haline geldi.

5.4 Türkiye’nin Rolü ve Gelecek Perspektifi

Türkiye, son yıllarda yerli ve milli savunma sanayi vizyonu ile dışa bağımlılığı azaltma konusunda önemli ilerlemeler kaydetmiştir. İHA/SİHA alanında elde edilen başarılar, Bayraktar TB2 ve Akıncı gibi platformlarla uluslararası tanınırlık kazanmıştır. Ancak motor teknolojileri, uydu sistemleri, siber güvenlik ve kuantum teknolojileri gibi alanlarda hâlâ gelişime ihtiyaç vardır.

Güçlü Yönler:

- İHA/SİHA teknolojilerinde liderlik.
- ASELSAN, ROKETSAN, TUSAŞ gibi firmaların küresel ölçekte rekabet gücü.
- Genç ve dinamik mühendis kadrosu.

Zayıf Yönler:

- Kritik bileşenlerde (motor, çip, elektronik) dışa bağımlılık.
- Savunma yazılımlarında yerli alternatiflerin sınırlı olması.
- Uluslararası yaptırımlara açık olma durumu.

Öneriler:

1. Kritik Teknolojilerde Bağımsızlık: Motor, çip ve sensör teknolojilerinde yerlileşmeye öncelik verilmeli.
2. Kuantum ve Yapay Zekâ Yatırımları: Yeni nesil savunma teknolojilerine erken yatırım yapılmalı.
3. Uluslararası Konsorsiyumlar: Türkiye, NATO DIANA gibi platformlarda aktif rol alarak hem bilgi transferi hem de Ar-Ge iş birlikleri geliştirmeli.
4. Siber Güvenlik Ekosistemi: Ulusal siber savunma stratejisi daha kapsamlı hale getirilmeli.

ÜNİTE 2: Savunma Teknolojilerinin Etik Yönü

Savunma teknolojileri, günümüz modern dünyasında devletlerin güvenlik stratejilerinde belirleyici rol oynar. Bu teknolojiler küresel anlamda siyasi, ekonomik, diplomatik ve uluslararası ilişkileri dengeler. Savunma teknolojilerinin gelişimi, beraberinde yalnızca stratejik üstünlük ve güvenlik avantajları değil, aynı zamanda derin etik ikilemleri de getirmektedir. Savunma teknolojileri yalnızca askeri güç açısından değil; insan hakları, adalet ve etik sorumluluk çerçevesinden de değerlendirilmelidir.

1.Yapay Zekâ Destekli Silahlar: Kontrol Kimde?

Yapay zekâ destekli silahlar, gelişmiş algoritmalar sayesinde hedef tespiti, veri analizi ve operasyonel kararları hızlı bir şekilde gerçekleştirebilen sistemlerdir. Bu silahlar insan müdahalesine ihtiyaç duymadan çalışabilmesi açısından savunma anlamında hız, doğruluk ve operasyonel verimlilik sağlamaktadır. Bunun yanı sıra yapay zekâ destekli silahlar, insan kararını büyük ölçüde azaltarak hedef seçimi ve savunma süreçlerini otomatikleştirmektedir.

Yapay zekâ destekli silah uygulamaları etik çerçeveden incelendiğinde birçok tartışmaya açık husus barındırır. Bahsi geçen yapay zekâ uygulamalarında insan müdahalesi ve iradesi minimum konuma gelmektedir. Bu durum her ne kadar bir takım avantajlara yol açsa da etik açıdan bir sürü problem meydana getirmektedir. Örneğin karar mekanizmasının çoğu zaman yapay zekâ üzerinden gerçekleşmesi insanın vicdan ve ahlaki yargılarının savunma ve savaş anlamında etkisizleşmesine yol açar. Sivil ve asker ayrımı konusunda yapay zekâ çoğu zaman yeterli olmayabilir. Bu ayrımın olmaması uluslararası savaş hukukunu büyük oranda sekteye uğratır. Bu durumda sivillerin zarar görmesi kaçınılmaz hâle gelir. Hata oranı düşük olsa bile sonuçlar geri dönüşsüzdür. Bu gibi olumsuz durumlarda yargılanacak irade ve merci belirsizdir. Yapay zekâ

tarafından yapılan hamleler ve uygulamalar hangi irade tarafından gerçekleştirilmiştir? Bu belirsizlik hesap verebilirlik ilkesini zedeler.

1.1 İnsan-Makine Karar Verme Sınırı

Yapay zekâ destekli silah sistemleri, hedef tespitinden saldırı kararına kadar birçok aşamada insandan bağımsız hareket edebilmektedir. Bu durum, "ölümcül karar" denilebilecek düzeydeki kararların insan yerine makine tarafından verilmesi riskini doğurur. Etik açıdan, savaşta kimin yaşayıp kimin öleceğine bir algoritmanın karar vermesi, insan iradesini ve vicdanını devre dışı bırakmaktadır. Dolayısıyla tartışmalar, insan denetiminin hangi noktada mutlaka korunması gerektiği üzerinde yoğunlaşmaktadır.

1.2 Otonom Silahlarda Etik Sorumluluk

Otonom silahların en büyük sorunlarından biri, hatalı bir karar alındığında sorumluluğun kime ait olduğunun belirsiz olmasıdır. Bir sivil hedef vurulduğunda suç, sistemi geliştiren mühendise mi, onu kullanan askere mi, yoksa emri veren devlete mi yüklenmelidir? Karar alma sürecinin insandan çok makineye kayması, sorumluluğun dağılmasına ve hesap verebilirliğin ortadan kalkmasına yol açmaktadır. Bu durumda yargı süreci ve yargılanacak irade konusu zora düşmektedir.

Cenevre Sözleşmesi

Cenevre Sözleşmeleri, savaş zamanında sivillerin, yaralı askerlerin ve savaş esirlerinin korunmasını amaçlayan uluslararası anlaşmalardır. En temel ilke, savaşan tarafların masum sivillere zarar vermemesi ve onlara insani muamele göstermesidir. Günümüzde savunma teknolojilerinin hızla gelişmesi, bu sözleşmelerin uygulanmasını zorlaştırmakta, özellikle yapay zekâ destekli silahlar ve insansız hava araçları gibi araçların siviller üzerindeki etkisi tartışma konusu olmaktadır. Cenevre Sözleşmeleri, 1949'da kabul edilmiş ve ek protokollerle güçlendirilmiştir.

- **Örnek madde:** 1949 tarihli IV. Cenevre Sözleşmesi'nin 27. maddesi, sivillerin "her zaman insanca muamele görme hakkına sahip olduğunu" belirtir.

- **Örnek uygulama:** Sivillere yönelik toplu bombardımanlar veya sivil bölgelerin hedef alınması, bu maddeye aykırıdır. Ancak modern teknolojilerde, örneğin insansız hava araçlarının saldırılarında sivil kayıplar yaşandığında bu sözleşmenin ihlali tartışmaya açılmaktadır.

Uluslararası İnsancıl Hukuk

Uluslararası insancıl hukuk, savaşların kuralsız bir şekilde yürütülmesini engellemek için geliştirilmiş hukuk dalıdır. Bu hukuk, "orantılılık" ve "ayrım gözetme" ilkeleri üzerine kuruludur. Yani savaşta kullanılan araçlar yalnızca askeri hedeflere yönelmeli, siviller korunmalı ve gereksiz acıya yol açılmamalıdır. Yeni nesil savunma teknolojileri bu kurallara ne ölçüde uyuyor sorusu, etik açıdan en çok tartışılan konulardan biridir. UİH, Cenevre ve Lahey Sözleşmeleri gibi uluslararası belgelerden beslenir.

- **Örnek madde:** 1977 tarihli Ek Protokol I, 48. maddesinde "savaşan tarafların sivillerle savaşçıları ayırt etmek zorunda olduğunu" açıkça ifade eder.
- **Örnek uygulama:** Otonom silahların dost-düşman ayrımında hata yapması, bu ilkeyle çelişebilir. Çünkü yanlış hedeflemeler, savaşçı yerine sivillerin zarar görmesine yol açabilir.

2. Askeri Yapay Zekâ ve Karar Algoritmaları

Askeri yapay zekâ, savaşlarda karar alma süreçlerini hızlandırmak ve daha doğru hale getirmek için kullanılan bir teknolojidir. Bu teknoloji, büyük miktarda veriyi hızlı biçimde analiz ederek hedef tespiti, risk değerlendirmesi ve operasyon planlaması gibi birçok işlev görebilir. Karar algoritmaları ise, bu yapay zekâ sistemlerinin nasıl işlediğini belirleyen temel mekanizmalardır; yani hangi verilerin dikkate alınacağı, nasıl değerlendirileceği ve hangi koşullarda

eyleme geçileceği bu algoritmalar sayesinde belirlenir. Dolayısıyla askeri yapay zekâ ve karar algoritmaları, modern orduların etkinliğini artıran en kritik unsurlar arasında yer almaktadır.

2.1 Algoritmik Önyargılar

Algoritmik önyargılar, yapay zekânın kullandığı verilerden ya da yazılımın tasarımından kaynaklanan hatalı ve tek taraflı sonuçlardır. Bu durumda yapay zeka tamamen tarafsız çalışamaz. Çünkü yapay zekâ, insanlar tarafından hazırlanan verilerle eğitilir. Eğer bu veriler eksik, hatalı ya da tek taraflı olursa, yapay zekâ da aynı önyargıları taşır. Mesela bir sistem, daha önce gördüğü örneklere dayanarak bazı grupları yanlış tanıyabilir ya da belirli durumları hatalı değerlendirebilir. Bu yüzden algoritmik önyargılar, teknolojinin yanlış kararlar almasına ve adaletsiz sonuçlar ortaya çıkmasına yol açabilir.

Askeri yapay zekâda bu durum çok daha kritik hâle gelir çünkü kullanılan veriler eksik, yanlış ya da belli bir bakış açısıyla hazırlanmışsa, sistemin aldığı kararlar da adil olmayabilir. Örneğin, bir hedefi tanımlarken yapay zekâ yanlış veriler yüzünden sivil bir aracı düşman unsuru olarak algılayabilir. Bu da masum insanların zarar görmesine yol açabilir. Dolayısıyla algoritmik önyargılar, askeri yapay zekâda sadece teknik bir hata değil, doğrudan hayatı etkileyen bir risk anlamına gelir.Bu sistemin ortaya çıkardığı olumsuz vakalara örnekler verilebilir.

2.1.1 Lavender Sistemi

- Hamas’a ait hedefleri ve militanları belirlemek amacıyla geliştirilmiş bir yapay zekâ tabanlı sistemdir.
- Telefon konuşmaları, sosyal medya verileri ve hareketlilik bilgileri gibi dijital izleri analiz ederek potansiyel hedefleri sınıflandırır.
- İnsan analistler sistemi denetlese de karar süreci büyük oranda algoritmalara dayanmaktadır.

- Hatalı tespitler sivil kayıplara yol açabilmekte, bu da sistemin etik açıdan yoğun eleştiriler almasına neden olmaktadır.
- En çok tartışılan nokta, insan hayatını etkileyen bir kararın sorumluluğunun kimde olacağı sorusudur.

Lavender sistemi, savaşta özellikle düşmanla bağlantılı olduğu düşünülen kişileri hızlı bir şekilde belirlemeyi hedefler. Yani kısaca, asker ya da savaşla ilgili kişileri tespit ederek onları hedef göstermeye çalışır. Fakat bu sistem bazen yanlış kararlar verip sivilleri de "hedef" olarak tanıyabilir. Bu durumda masum insanların hayatı riske girer. Etik açıdan bakıldığında, sivillerin güvenliği savaş hukukunda en temel kuraldır. Ancak böyle bir teknoloji, hatalı işlediğinde insanların hayatını sayılara indirger ve insan haklarını ikinci plana atar.

2.1.2 Patriot Dost Ateşi Olayları

- Patriot hava savunma sistemleri, düşman uçaklarını ve füzelerini tespit edip vurmak için geliştirilmiştir.
- Ancak 2003 Irak Savaşı sırasında ciddi dost ateşi olaylarına yol açmıştır.
- Bir İngiliz savaş uçağı Patriot tarafından yanlışlıkla vurularak düşürülmüştür.
- Aynı dönemde bir Amerikan uçağı da benzer şekilde hedef alınmıştır.
- Bu hatalar, sistemin dost ve düşman hedeflerini ayırt etmede yanılabildiğini göstermiştir.
- Saniyeler içinde karar verilmesi gerektiğinde insan denetimi devre dışı kalabilmektedir.
- Makinelerin tek başına karar vermesi, büyük riskler doğurmuştur.
- Bu olaylar, teknolojik silahların güvenilirliği ve sorumluluk konularında etik tartışmaları gündeme getirmiştir.

Patriot dost ateşi olayları, askeri teknolojilerin her zaman hatasız çalışmadığını ve bu durumun ciddi sonuçlar doğurabileceğini göstermiştir. Bu tür vakalar, makinelerin verdiği kararların insan hayatını nasıl etkileyebileceğine dair etik tartışmaları gündeme getirmektedir. Bu durum, insan denetiminin ne kadar önemli olduğunu ve makinelerin verdiği kararların mutlaka etik ve hukuki çerçevede kontrol edilmesi gerektiğini ortaya koymuştur. Savaşta sorumluluk,

sadece teknolojiye değil, onu kullanan insanlara da aittir. Ve tüm denetimin teknolojiye bırakılması bazı durumlarda masum askerlerin hayatını riske atabilir, sorumluluğun kime ait olduğu konusunda belirsizlik yaratabilir ve savaşta insan haklarını zedeleyebilir.

2.2 Yapay Zekânın Savaş Hukukuna Etkisi

Yapay zekânın savaş alanında kullanılması, mevcut savaş hukukunu önemli ölçüde zorlayan yeni sorunlar ortaya çıkarmaktadır. Uluslararası insancıl hukuk, sivillerin korunmasını, orantılı güç kullanılmasını ve askeri hedeflerin açık biçimde ayırt edilmesini şart koşar. Ancak yapay zekâ destekli sistemler, kararlarını algoritmalara dayandırdığı için bu kurallara her zaman uygun davranmayabilir. Özellikle dost-düşman ayrımı, sivil kayıpların önlenmesi ve orantısız saldırıların engellenmesi gibi konularda hata riski oldukça yüksektir. Ayrıca, yapay zekânın yanlış bir karar vermesi durumunda sorumluluğun kime ait olacağı da belirsizdir; bu durum hesap verebilirlik ilkesini zayıflatır. Dolayısıyla yapay zekânın savaş hukukuna entegrasyonu, hem teknik hem de etik açıdan ciddi düzenlemeler ve uluslararası iş birliği gerektirmektedir.

3. Dijital Güvenlik ve Askeri Gözetim

Dijital güvenlik anlamında günümüzde savaşlar sadece sahada değil, dijital ortamda da gerçekleşiyor. Siber saldırılar, askeri iletişim sistemlerini, radarları, insansız araçları hatta devletlerin kritik altyapılarını hedef alabiliyor. Bu yüzden dijital güvenlik, modern ordular için en az fiziksel savunma kadar önemli hale

gelmiştir. Askeri yapay zekâ ve veri tabanlı teknolojiler ne kadar gelişirse gelişsin, bunların güvenliğini sağlamak ve siber tehditlere karşı korumak ulusal savunmanın temel bir parçası olarak görülmektedir.

Teknolojinin ilerlemesiyle birlikte askeri gözetim sistemleri de çok daha gelişmiş bir hâl aldı. Uydu takip sistemleri, insansız hava araçları ve yapay zekâ destekli izleme yazılımları sayesinde ordular, hem savaş bölgelerinde hem de sınır güvenliğinde sürekli gözetim yapabiliyor. Bu sistemler, operasyonlarda büyük avantaj sağlarken aynı zamanda veri toplama ve kişisel mahremiyet gibi konularda tartışmaları da beraberinde getiriyor. Dolayısıyla askeri gözetim, günümüzde yalnızca stratejik bir araç değil, aynı zamanda güvenlik ve özgürlük dengesi açısından da kritik bir mesele olarak öne çıkmaktadır.

3.1 Ulusal Güvenlik Adına Veri Erişimi

Ulusal güvenlik, devletlerin en temel önceliklerinden biridir ve bu güvenliği sağlamak için verilerin toplanması ve işlenmesi günümüzde büyük bir önem taşımaktadır. Özellikle askeri alanda iletişim kayıtları, konum verileri, dijital haberleşme ve sosyal medya aktiviteleri gibi bilgiler, potansiyel tehditlerin önceden tespit edilmesi için kullanılmaktadır. Ancak bu durum, bireylerin kişisel mahremiyeti ile devletin güvenlik ihtiyaçları arasında hassas bir denge kurulmasını zorunlu hale getirir. Devletler güvenliği sağlamak için geniş çapta veri erişimine ihtiyaç duysa da, bu erişimin sınırlarının belirlenmemesi etik sorunlara ve hak ihlallerine yol açabilir. Bu nedenle ulusal güvenlik adına veri erişimi, hem güvenlik hem de özgürlükler açısından dikkatle yönetilmesi gereken kritik bir konudur.

Ulusal güvenlik adına veri erişimi, sadece dış tehditleri değil, içerideki güvenlik risklerini de kontrol altına almak için kullanılmaktadır. Ordular ve güvenlik kurumları, siber saldırıları önlemek, terör faaliyetlerini izlemek ve kritik altyapıları korumak amacıyla geniş çaplı veri analizine başvurur. Büyük veri teknolojileri ve yapay zekâ, toplanan bu bilgileri işleyerek devletlere hızlı karar alma imkânı verir. Ancak veri erişiminin sınırları net çizilmediğinde, yalnızca güvenlik odaklı değil, toplumsal özgürlükleri etkileyen sonuçlar da doğabilir. Bu nedenle ulusal güvenlik gerekçesiyle yapılan veri toplama faaliyetlerinin şeffaf,

denetlenebilir ve hukuki çerçeveler içinde olması, hem güvenliği hem de demokratik hakları korumak açısından zorunludur.

3.2 Sivil Haklar ve İzleme Teknolojileri

Teknolojinin gelişmesiyle birlikte devletlerin kullandığı gözetim araçları çok daha güçlü hale geldi. Kamera sistemleri, yüz tanıma yazılımları, konum takibi ve çevrim içi veri analizi, güvenlik için büyük kolaylık sağlasa da sivil haklar açısından tartışmalı bir alan oluşturuyor. Çünkü bu teknolojiler, bireylerin özel hayatını ve özgürlüklerini doğrudan etkileyebiliyor. Ulusal güvenlik adına yapılan gözetim faaliyetleri, eğer denetimsiz şekilde kullanılırsa kişisel mahremiyetin ihlali ve ifade özgürlüğünün kısıtlanması gibi sorunlara yol açabilir. Bu nedenle izleme teknolojilerinin kullanımı, güvenliği sağlarken aynı zamanda temel hak ve özgürlükleri koruyacak dengeli bir çerçeveye oturtulmalıdır.

Sivil haklar ile izleme teknolojileri arasındaki tartışmaların en önemli noktalarından biri, bu uygulamaların güvenlik için olduğu veya özgürlüğü kısıtladığı ikilemidir. Devletler güvenliği sağlamak için geniş çaplı gözetim sistemleri kullanırken, bu durum halkın özgürlükleri kısıtlandığı ve özel alanlarına müdahale edildiği düşüncesine sahip olabilmelerine neden oluyor. Bu da toplumda özgürlük alanını daraltan bir “gözetim kültürü” oluşturuyor. Ayrıca, izleme teknolojilerinin sadece suçla mücadele için değil, siyasi muhalifleri veya belirli grupları kontrol altında tutmak amacıyla da kullanılabileceği endişesi vardır. Bu yüzden demokratik toplumlarda, gözetim teknolojilerinin kullanımına ilişkin bağımsız denetim mekanizmalarının bulunması büyük önem taşır. Aksi hâlde, teknolojik gözetim güvenliği artırmak yerine toplumda güvensizlik ve baskı ortamı yaratabilir. Bu gibi durumların örneği birçok ülkede ve birlikte görülmektedir.

Çin:

- **Teknoloji / Sistem:** Yüz tanıma ve sosyal kredi sistemi
- **Amaç:** Güvenlik ve düzen sağlama

- **Etik / Mahremiyet Sorunu:** İnsanların davranışlarının izlenmesi, ifade özgürlüğü ve özel yaşamın sınırlanması
  ABD:
- **Teknoloji / Sistem:** Kitlesel veri toplama (NSA)
- **Amaç:** Ulusal güvenlik
- **Etik / Mahremiyet Sorunu:** Telefon ve internet verilerinin izlenmesi, mahremiyetin ihlali
  Avrupa Birliği (AB):
- **Teknoloji / Sistem:** GDPR (Genel Veri Koruma Tüzüğü)
- **Amaç:** Veri güvenliği ve şeffaflık
- **Etik / Mahremiyet Sorunu:** Gözetim ve veri işleme faaliyetlerinde şeffaflık, özgürlük ve güvenlik dengesinin korunması

Güvenlik teknolojilerinin kullanımı, yalnızca teknik kapasiteyle sınırlı kalmamalı; aynı zamanda demokratik denetim mekanizmalarıyla kontrol altında tutulmalıdır. Çin ve ABD'deki uygulamalar, denetimsiz gözetim ve veri toplamanın mahremiyet ihlallerine yol açabileceğini gösteriyor. AB'deki GDPR gibi düzenlemeler ise, devletlerin ve kurumların bireylerin verilerini nasıl kullandığını şeffaf şekilde denetlemeye olanak tanıyor. Bu örnekler, güvenlik önlemlerinin demokratik ilkelerle uyumlu şekilde uygulanmasının önemini vurguluyor.

4. Devlet Destekli Siber Saldırılar ve Etik

Günümüzde devletler sadece kara, deniz ve hava gücüyle değil, aynı zamanda siber sahada da mücadele ediyor. Devlet destekli siber saldırılar; kritik altyapılara, bankacılık sistemlerine, haberleşme ağlarına ya da diğer devletlerin kurumlarına yönelik olarak yapılan dijital saldırıları kapsıyor. Bu saldırılar askeri ya da siyasi avantaj sağlamak için kullanılsa da, etik açıdan büyük tartışmalar doğuruyor. Çünkü siber saldırılar sadece devletleri değil, sıradan vatandaşların günlük yaşamını da etkileyebiliyor. Elektrik şebekesinin çökmesi, sağlık sisteminin felç olması ya da kişisel verilerin çalınması gibi sonuçlar, sivillerin güvenliğini doğrudan tehdit ediyor. Bu nedenle devlet destekli siber operasyonlar, ulusal güvenlik ile insan hakları arasındaki ince çizgide değerlendirilen önemli bir etik sorun haline gelmiştir.

Devlet destekli siber saldırılar, bir devletin kendi istihbarat kurumları ya da gizli ekipleri aracılığıyla başka ülkelere karşı düzenlediği dijital saldırılardır. Bu saldırıların amacı genellikle bilgi toplamak (casusluk), kritik sistemleri bozmak ya da saldırılan ülkenin güvenliğini zayıflatmak olur. Bazen bu saldırılar doğrudan fark edilmez, ama etkileri hem teknik hem de etik açıdan büyük olabilir. Bu saldırılar sadece devlet kurumlarını değil, masum sivilleri de etkileyebiliyor. Örneğin bir hastanenin sistemine yapılan saldırı, hastaların tedavisini engelleyebilir; bir banka sisteminin çökmesi ise milyonlarca insanın parasını riske atabilir. Yani devletler güvenlik adına böyle bir yöntem kullandığında, sivil halkın hakları ve güvenliği tehlikeye girmiş oluyor.

4.1 Rusya-Ukrayna Siber Çatışmaları

Rusya-Ukrayna siber çatışmaları, 2014'teki Kırım ilhakıyla başlayan ve 2022'deki tam ölçekli işgalle yoğunlaşan bir dijital savaş alanıdır. Rusya, Ukrayna'nın elektrik şebekeleri, bankacılık sistemleri ve devlet kurumlarını hedef alan siber saldırılar düzenlemiştir. Örneğin, 2015'te Ukrayna'daki elektrik santrallerine yapılan saldırılar, yüzbinlerce kişinin elektriksiz kalmasına yol açmıştır. 2022'de ise, Rus askeri istihbarat servisi GRU, Ukrayna'nın devlet ve askeri kurumlarına yönelik DDoS saldırıları başlatmıştır. Ayrıca, IsaacWiper adlı silme yazılımı kullanılarak kritik veriler hedef alınmıştır.

Bu siber çatışmalar, yalnızca askeri hedefleri değil, doğrudan sivilleri de etkilemiştir. Elektrik kesintileri, hastanelerin çalışmaması ve bankacılık sistemlerinin çökmesi gibi etkiler, sivil halkın yaşamını zorlaştırmıştır. Bu durum, siber savaşın etik sınırlarını zorlamaktadır. Bu gibi siber saldırılar, savaş hukukunun sivilleri koruma ilkesine ters düşüyor ve ciddi etik sorunlar ile karşı karşıya kalmaya sebep oluyor.

4.2 İsrail-İran Siber Gerilimi

İsrail ve İran arasındaki siber gerilim, gün geçtikçe Orta Doğu'nun en belirgin dijital çatışmalarından biri haline gelmiştir. Her iki ülke de siber savaş alanında önemli yeteneklere sahip olup, karşılıklı saldırılarla birbirlerinin kritik altyapılarını hedef almaktadır.

İran, özellikle MuddyWater ve APT34 gibi gruplarla tanınırken, İsrail'in en bilinen grubu Predatory Sparrow (Gonjeshke Darande) olarak bilinir. 2025 yılı

itibarıyla, bu gruplar arasında 450'den fazla siber saldırı gerçekleşmiştir. İran, İsrail'in bankacılık sistemlerine yönelik DDoS saldırıları ve veri sızıntıları gerçekleştirirken; İsrail, İran'ın enerji ve finans sektörlerine yönelik siber saldırılar düzenlemiştir. Örneğin, Haziran 2025'te Predatory Sparrow, İran'ın Bank Sepah'ına siber saldırı düzenleyerek verileri yok etmiş ve Nobitex adlı kripto borsasından 90 milyon doları çalmıştır. İran ise, İsrail'in su ve gaz altyapılarını hedef alarak kritik sistemlere zarar vermiştir.

Bu siber çatışmalar, yalnızca askeri hedefleri değil, sivil altyapıları da tehdit etmektedir. Elektrik şebekeleri, su temini ve bankacılık sistemleri gibi kritik hizmetler, bu dijital saldırılar nedeniyle aksayabilmektedir. Özellikle İran'ın merkezi sistemleri, siber saldırılara karşı daha savunmasız hale gelmiştir.

Sonuç olarak, İsrail ve İran arasındaki siber gerilim, dijital savaşın sınırlarını zorlamakta ve bölgesel güvenliği tehdit etmektedir. Her iki ülkenin de siber yetenekleri, geleneksel askeri güçle kıyaslanamayacak kadar etkili olabilir, bu da siber savaşın gelecekteki önemini vurgulamaktadır.

5. Bilgi Güvenliği ve Dezenformasyon

Bilgi güvenliği ve dezenformasyon, günümüz dijital dünyasında birbirine sıkı sıkıya bağlı konulardır. Bilgi güvenliği, kritik verilerin yetkisiz kişilerce ele geçirilmesini, değiştirilmesini veya silinmesini önlemeyi amaçlar. Dezenformasyon ise yanlış veya yanıltıcı bilgilerin kasıtlı olarak yayılmasıdır ve özellikle sosyal medya gibi hızlı bilgi akışı olan platformlarda hızla yayılabilir. Bu durum, devletler, kurumlar ve bireyler açısından ciddi tehditler oluşturur; çünkü yanlış bilgiler, kamuoyunu yanıltabilir, güvenliği zayıflatabilir ve karar alma süreçlerini bozabilir. Özellikle ulusal güvenlik bağlamında, siber saldırılar ve dezenformasyon kampanyaları birbirini besleyerek hem askeri hem de sivil alanlarda riskler yaratır.

5.1 Savaşta Bilgi Manipülasyonu

Savaşta bilgi manipülasyonu, düşmanı yanıltmak, kendi tarafın moralini yükseltmek veya kamuoyunu etkilemek amacıyla bilgilerin kasıtlı olarak

değiştirilmesi veya çarpıtılmasıdır. Bu tür stratejiler, sadece düşman askerlerini değil, sivil halkı da hedef alabilir. Sosyal medya, haber siteleri ve propaganda kanalları, bilgi manipülasyonunun en çok kullanıldığı alanlardır. Yanlış bilgiler, çatışma sırasında karar almayı zorlaştırabilir, güvenliği tehdit edebilir ve savaşın gidişatını etkileyebilir. Günümüzde dijital teknolojiler sayesinde bilgi manipülasyonu çok daha hızlı ve yaygın hâle gelmiştir, bu da etik ve güvenlik açısından ciddi sorunlar doğurur.

durum, hem askeri hem de sivil taraf için stratejik riskler oluşturuyor ve etik açıdan ciddi sorular ortaya çıkarıyor; çünkü gerçekler manipüle edilirken masum insanlar da zarar görebiliyor.

Örneğin, 2022'deki Rusya-Ukrayna savaşında her iki taraf da sosyal medyayı aktif şekilde kullandı. Ukrayna, Rus saldırılarının şiddetini ve kayıplarını vurgulayarak dünya kamuoyunun desteğini kazanmaya çalıştı. Öte yandan Rusya, kendi kayıplarını gizleyip başarılarını abartarak halkın moralini yüksek tutmaya çalıştı. Bu durum, bilgilerin taraflı şekilde sunulmasının savaşın algısını nasıl değiştirebileceğini gösteriyor ve bilgi manipülasyonunun hem askerleri hem de sivilleri etkileyebileceğini ortaya koyuyor.

5.2 Sosyal Medya Üzerinden Psikolojik Harp

Sosyal medya, günümüzde psikolojik harp için etkili bir araç hâline gelmiştir. Yanlış bilgiler, abartılmış haberler ve manipüle edilmiş görseller kullanılarak insanların korku, kaygı veya panik yaşaması sağlanabilir. Savaş dönemlerinde bu tür stratejiler, hem düşman askerlerin moralini bozmak hem de sivil halkı etkileyerek kamuoyunu yönlendirmek amacıyla kullanılır. Örneğin, bir çatışma bölgesinde abartılı kayıp haberleri veya tehdit mesajları yaymak, insanların kararlarını ve davranışlarını değiştirebilir. Bu durum, sosyal medyanın sadece bilgi paylaşım aracı olmadığını, aynı zamanda modern savaşlarda psikolojik bir silah olarak da kullanılabileceğini gösteriyor.

Bu duruma örnek olarak, 2014'te Ukrayna'da Kırım krizinde sosyal medya üzerinden çeşitli mesajlar ve videolar yayıldı. Rus yanlısı hesaplar, Ukrayna ordusunun başarısız olduğunu ve sivillerin tehlikede olduğunu gösteren abartılı

paylaşımlar yaptı. Bu paylaşımlar, halk arasında korku ve panik yaratmayı, moral çöküntüsü oluşturmayı hedefliyordu. Aynı zamanda karşı tarafın askerleri de bu dezenformasyondan etkilenerek karar almakta zorlanıyordu. Bu örnek, sosyal medyanın psikolojik harp için nasıl kullanılabileceğini net bir şekilde gösteriyor.

6. Gençlerin ve Sivil Toplumun Rolü

Gençler ve sivil toplum kuruluşları, modern savunma ve güvenlik konularında önemli bir rol oynar. Gençler, teknolojiye ve sosyal medyaya hâkimiyetleri sayesinde bilgiye hızlı ulaşabilir, farkındalık yaratabilir ve toplumsal tartışmalara katılabilir. Gençler ve sivil toplum, güvenlik ve savunma alanlarında yalnızca bilgi paylaşmakla kalmaz, aynı zamanda etik ve demokratik değerlerin korunmasına da katkı sağlar. Sivil toplum kuruluşları ise kamuoyunu bilinçlendirmek, etik meseleleri gündeme taşımak ve hükümet politikalarını denetlemek açısından kritik bir işlev görür. Özellikle savunma teknolojileri, bilgi güvenliği ve dijital etik konularında gençlerin ve STK'ların katkısı, daha şeffaf, bilinçli ve güvenli bir toplum inşa edilmesine yardımcı olur.

6.1 Askeri Teknolojilere Genç Bakış Açısı

Gençler, askeri teknolojilere bakış açısı bakımından hem yenilikçi hem de eleştirel bir perspektif sunar. Teknolojinin hızlı gelişimi ve dijitalleşmenin yaygınlaşması, gençlerin yapay zekâ, otonom silah sistemleri, siber güvenlik ve gözetim teknolojileri gibi alanlarda farkındalıklarını artırmıştır. Bu farkındalık, gençlerin yalnızca teknolojik yenilikleri takip etmekle kalmayıp, aynı zamanda bu teknolojilerin etik ve hukuki boyutlarını da değerlendirmelerini sağlar.

Örneğin, yapay zekâ destekli silahlar ve algoritmik karar sistemleri konusunda gençler, olası sivil kayıplar, etik sorumluluk ve hukuki düzenlemeler hakkında bilinçli tartışmalar yapabilir. Sosyal medya ve dijital platformlar aracılığıyla gençler, bu konuları daha geniş kitlelere ulaştırabilir, kamuoyunda etik kaygıları ve demokratik değerlerin korunmasını gündeme taşıyabilirler. Ayrıca, gençler sivil toplum kuruluşlarıyla iş birliği yaparak, savunma politikalarının şeffaf ve hesap verebilir olmasına katkı sağlayabilir. Bu bağlamda, genç bakış açısı askeri teknolojilerin yalnızca bir güç unsuru olarak görülmesini engeller; aynı zamanda

bu teknolojilerin etik, hukuki ve toplumsal sorumluluk boyutlarının da tartışılmasını sağlar ve toplumun bilinçli kararlar almasına yardımcı olur.

6.2 Sivil-Askeri İş Birliğinde Yeni Modeller

Sivil-askeri iş birliği, modern güvenlik ve savunma politikalarının etkinliği açısından giderek daha fazla önem kazanmaktadır. Geleneksel modelde sivil ve askeri aktörler arasındaki etkileşim sınırlı ve hiyerarşikken, günümüzde yeni iş birliği modelleri daha esnek, şeffaf ve karşılıklı faydaya dayalı yaklaşımları ön plana çıkarmaktadır. Bu modellerde, sivil toplum kuruluşları, akademik kurumlar ve teknoloji şirketleri, askeri planlama ve teknoloji geliştirme süreçlerine aktif olarak katılabilir. Böylece, askeri stratejiler sadece güvenlik hedefleriyle sınırlı kalmayıp, etik, hukuki ve toplumsal boyutlar göz önünde bulundurularak şekillendirilebilir. Özellikle yapay zekâ ve siber güvenlik alanlarında, sivil uzmanların katkısı, risk yönetimi ve etik sorumlulukların daha iyi anlaşılmasına yardımcı olur. Yeni iş birliği modelleri, aynı zamanda toplumun güvenlik süreçlerine dahil olmasını sağlayarak, savunma politikalarının demokratik denetime açık ve hesap verebilir olmasını destekler.

Sivil-askeri iş birliği, etik açıdan şeffaflık ve hesap verebilirlik açısından önem taşır. Sivil aktörlerin sürece dahil olması, askeri stratejilerin sadece güç odaklı değil, toplumsal değerler ve insan hakları gözetilerek planlanmasını sağlar. Böylece güvenlik politikaları, hem etik sorumlulukları hem de toplumsal meşruiyeti dikkate alarak şekillenir.

Firdevs Burak ve Elif Rana Durdu tarafından...

SORULAR

1- İnsansız hava araçlarının savaş alanında giderek artan rolü, devletlerin güvenlik politikalarını nasıl dönüştürüyor ?

2- Elektronik harp ve siber saldırılar gibi görünmez tehditler, klasik askeri caydırıcılık anlayışını hangi açılardan yetersiz bırakıyor olabilir?

3- Savunma sanayinde dışa bağımlılığın azaltılması sadece askeri bir mesele midir, yoksa ekonomik ve diplomatik boyutları da var mıdır?

4- Sürü drone ve yapay zekâ tabanlı sistemler, savaş alanında insan faktörünü hangi noktalarda geri plana itiyor ?

5- Kuantum teknolojilerinin (iletişim, radar, hesaplama) askeri alana girmesi, mevcut güç dengelerini nasıl sarsabilir?

6- Uzay ve biyoteknoloji tabanlı savunma yatırımları, uluslararası hukuk ve etik açısından hangi yeni tartışmaları gündeme getirecek?

7- Otonom silahların hata yapması durumunda sorumluluğun kimde olduğu konusundaki belirsizlik, uluslararası ilişkilerde hangi krizlere yol açabilir?

8- Ulusal güvenlik adına yapılan gözetim ve veri toplama, bireylerin temel özgürlükleri ile nasıl dengelenmeli ?

9- Devlet destekli siber saldırıların sivilleri doğrudan hedef alması, geleceğin savaş hukukunu nasıl şekillendirebilir?

10- Sosyal medya üzerinden yürütülen psikolojik harp kampanyaları, toplumların algısını ve kararlarını etkilemede konvansiyonel savaş kadar güçlü olabilir mi?

11- Gençlerin ve sivil toplumun savunma teknolojilerine dair getirdiği eleştirel bakış açısı, devlet politikalarında nasıl bir yenilenme sağlayabilir?