Savunma Bilimleri Dergisi, 20(2): 303-326 (2024)

SAVUNMA BİLİMLERİ DERGİSİ
The Journal of Defense Sciences

https://dergipark.org.tr/tr/pub/khosbd

Askeri Taktik Ağlarda Derin Makine Öğreniminin Etkisi

Impact of Deep Machine Learning on Military Tactical Networks

Fuat ÖZÇAKMAK*

ODTÜ, Sosyal Bilimler Enstitüsü, Bilim ve Teknoloji Politikası Çalışmaları (Teknoloji Yönetimi), Ankara,Türkiye

Makale Bilgisi

Derleme
Başvuru: 04.09.2023
Düzeltme: 27.02.2024
Kabul: 28.03.2024

Keywords

Deep Machine Learning
Military Tactical Networks
Artificial Intelligence
Military Communication
Deep Neural Networks

Anahtar Kelimeler

Derin Makine Öğrenimi
Askeri Taktik Ağlar
Yapay Zekâ
Askeri İletişim
Derin Sinir Ağları

Önemli Noktalar

Tarih boyunca önemli teknolojik ilerlemeler, askeri güçlerin daha verimli ve etkili olmasını sağlamıştır. Günümüzde yaşanan önemli teknolojik gelişmelerden biri olan yapay zekânın da askeri alanda sinerji yaratacak potansiyele sahip olduğu değerlendirilmektedir. Özellikle Vietnam savaşı sonrasında önemi artan ve geliştirilen askeri taktik ağların veri işleme ve iletme yetenekleri yapay zekâ ile desteklenecek kritik sahaların başında gelmektedir.

Grafiksel Özet

Özet

Askeri operasyonlar, her zaman strateji ve taktiklerin etkili bir şekilde kullanılmasını gerektirmektedir. Bu gerekliliğin şekil verdiği teknolojik ilerlemeler, günümüzde askeri güçlerin daha verimli ve etkili kullanılmasını sağlamaktadır. Derin makine öğrenimi gibi yapay zekâ yöntemleri, askeri stratejilerin geliştirilmesi ve uygulanmasında önemli bir rol oynamıştır. Bu stratejilerden biri de Askeri Taktik Ağların tüm harp alanında kullanılması sayesinde yaşanmaktadır. Ancak harp alanında Askeri Taktik Ağlar tarafından üretilen büyük verinin korelasyon yapılarak karar destek sistemlerine anlık bilgi aktarılması ve doğru kararları zamanında verebilmesi zor bir süreç olup, bu sürecin teknoloji desteği olmadan geliştirilemeyeceği aşikârdır. Bu noktada Yapay zekâ uygulamalarından biri olan Derin Makine Öğrenimini askeri taktik ağlar ile bütünleştirmek, daha hızlı ve isabetli tahminler sağlayabilecek, kısıtlamaları hafifletecek, askerler üzerindeki aşırı bilgi yüklemesini azaltacak ve ağ savunma stratejilerinin gelişimini sağlayacaktır.

Abstract

Military operations always require the effective use of strategy and tactics. Technological advances shaped by this necessity enable the more efficient and effective use of military forces today. Artificial intelligence (AI) methods such as deep machine learning (DML) have played an important role in the development and implementation of military strategies. One of these strategies is experienced through the use of Military Tactical Networks (MTN) in the entire battlefield. However, it is a difficult process to correlate the big data produced by MTN in the battlefield and transfer instant information to decision support systems and make the right decisions in a timely manner, and it is obvious that this process cannot be developed without technology support. At this point, integrating DML, one of the AI applications, with MTN will provide faster and more accurate predictions, alleviate restrictions, reduce information overload on soldiers and enable the development of network defense strategies.

*Corresponding author, e-mail: fuat.ozcakmak@tai.com.tr

DOI: 10.17134/khosbd.1355231

Elektronik/Online ISSN:1303-6831
Basılı/Printed ISSN:2148-1776

1. GİRİŞ (INTRODUCTION)

Askeri operasyonlar, her zaman strateji ve taktiklerin etkili bir şekilde kullanılmasını gerektirmektedir. Teknolojik ilerlemeler, askeri güçlerin daha verimli ve etkili olmasını sağlamıştır. Son yıllarda, Derin Makine Öğrenimi (DMÖ; Deep Machine Learning-DML) gibi yapay zekâ yöntemleri, askeri stratejilerin geliştirilmesi ve uygulanmasında önemli bir rol oynamıştır. Bu stratejilerden biri de Askeri Taktik Ağların (ATA; Military Tactical Networks-MTN) tüm harp alanında kullanılması sayesinde yaşanmaktadır. Bu ağlar, operasyonlar sırasında askeri birimler arasındaki iletişim ve bilgi alışverişinin omurgasını oluşturmaktadır. Günümüzün tüm modern ordularında kullanılan ve harekât konseptlerinin ayrılmaz bir parçası olan ATA'lar sahada kuvvetler arasında asimetrik güç etkisi yaratabilmektedir.

DMÖ, yapay sinir ağları ve derin öğrenme algoritmalarıyla çalışan bir alanı ifade eder. Büyük veri kümelerini analiz ederek desenleri ve ilişkileri tespit etmek için kullanılır [1]. Derin öğrenme modelleri, katmanlı yapısıyla karmaşık görevleri başarıyla yerine getirebilir ve insanların yapamayacağı kadar büyük veri kümelerini işleyebilir. Bu nedenle, askeri stratejilerin geliştirilmesinde ve optimize edilmesinde önemli bir araç haline gelmiştir.

DMÖ'nin temelini oluşturan derin ağlar, DMÖ için temel bir yapı taşıdır. Derin ağlar karmaşık veri kümelerinden otomatik olarak öğrenme yeteneği sağlar. Derin ağların, herhangi bir eğitimden önce bile sayısal duyarlılık sergileme yeteneği, sayısal bilgileri işlemek için doğuştan gelen bir kapasiteye sahip olduklarını gösterir [2]. Ayrıca, maruz kaldıkları aşamalı gelişimsel iyileştirme, öğrenmenin temel bir yönü olan öğrenme ortamının istatistiksel yapısına uyum sağlayabildiklerini göstermektedir. Genel olarak, bu bulgu, derin ağların yetenekleri ve farklı alanlardaki potansiyel uygulamaları hakkında değerli bilgiler sağlar [3].

Askeri operasyonlarda, hızlı ve doğru karar verilmesi hayati öneme sahiptir. Göztepe, Dizdaroğlu ve Sağıroğlu'na göre DMÖ, algoritmalarının gelişmesine paralel olarak yakın gelecekte operasyonel karar verme sürecini iyileştirmek için kullanılacaktır [4]. Buradan hareketle büyük veri analizi ve derin öğrenme algoritmalarının, düşman faaliyetlerini tahmin etmek, düşman hedeflerini belirlemek ve dost birliklerin hareketlerini optimize etmek gibi görevleri gerçekleştirebileceği söylenebilir. Örneğin, derin öğrenme modelleri, önceki askeri operasyonlardan elde edilen verileri kullanarak düşman stratejilerini ve davranışlarını analiz edebilecek ve gelecekteki operasyonlar için stratejik önerilerde bulunabilecektir.

DMÖ, nesne tanıma ve hedef tespiti konularında da önemli bir olgunluğa erişmiştir [5]. Askeri taktik ağlarında, düşman birliklerini veya tehdit oluşturan unsurları tespit etmek için görüntü veya video verileri iletilmektedir. Derin öğrenme modelleri, bu iletilen verileri analiz ederek düşman hedeflerini tespit etme, tanıma ve takip etme algoritmaları geliştirebilecek yeteneğe ulaşmışlardır. Bu da sahadaki birliklerin ve komuta kademelerinin daha isabetli kararlar almasını ve etkili bir şekilde hedef odaklı operasyonlar yapabilmelerini sağlayabilecektir.

DMÖ, askeri taktik ağlarında kullanılan özerk sistemlerin ve robotların geliştirilmesinde de

büyük bir rol oynar [6]. Örneğin, İnsansız Hava Araçları (İHA'lar) ve İnsansız Kara Araçları (İKA'lar), İnsansız Deniz Araçları (İDA'lar) derin öğrenme modellerini kullanarak çevrelerini algılayabilir, rotalarını optimize edebilir ve hedeflere yönelik saldırıları gerçekleştirebilir. Bu, askeri birliklerin risklerini azaltırken, operasyonel etkinliklerini artıracaktır.

Bu çalışmada, DMÖ'nin ATA'lardaki etkisi araştırılarak potansiyel uygulamaları ve faydaları incelenmiş, ayrıca askeri stratejilerin geliştirilmesinde ve optimize edilmesinde olası kullanım sahaları tespit edilmeye çalışılmıştır. Makalede, elde edilen veriler ışığında yapay zekâ uygulamalarının taktik ağlar ile bütünleştirilmesi sonucunda bu sistemlerin kullanıcılarına sağladığı faydalardaki değişim incelenmiştir. Bu kapsamda modern ordular tarafından kullanılmakta olan mevcut ATA kullanım konseptleri incelenmiş, DMÖ uygulaması ile geliştirilebilecek sahalar öngörülerek bu kapsamda yapılan literatür araştırmaları ile öngörüler karşılaştırılmıştır. NATO ülkelerince kullanılan Link-6, Link-7, Link-10, Link-11, Link-11, Link-16, Link-22, IJMS ve SADL [7] gibi taktik ağlarının konseptlerinin geliştirilmekte olan DMÖ yetenekleri ile birleştirilmesi sonucunda ortaya çıkabilecek değişikliklerin nasıl olabileceğine ilişkin değerlendirmeler yapılmıştır.

Mevcut literatürde konuya ilişkin yapılan çalışmalarda her ne kadar ATA'ların yapay zekâ uygulamaları ile birlikte kullanımına vurgu yapıldığı görülse de DMÖ etkisinin tüm yönleri ile analiz edildiği bir çalışmaya rastlanmamıştır. Bulunan kaynaklarda en fazla yapay zekanın komuta kontrol sistemlerine olan etkisi bulunmuş olup DMÖ ile askeri taktik linklerin bütünleştirilmesi konularına değinilmediği tespit edilmiştir [8]. Bu makalede günümüzde daha çok güvenli ve hızlı veri iletimi maksatlı kullanılan ATA'ların, içinde akan veri denizinin hangi fonksiyon alanlarına göre sınıflandırılması (nesnel konumlandırma, siber güvenlik, lojistik, hedef tanıma, asker sağlığı, eğitim, durumsal farkındalık) gerektiği ve DMÖ algoritmalarının etkisiyle bu alanlarda yaşanabilecek gelişmeler incelenmiştir.

Nitel analiz yöntemi ile ele alınan bu makalede, katmanlı yapısıyla karmaşık görevleri başarıyla yerine getirebilen Derin Öğrenme Modellerinin ATA'lara uyumlandırılması ile askeri operasyonlarda potansiyel gelişme sahaları, sorun sahaları ile ortaya konmuştur. ATA'ların DMÖ ile desteklenmesi durumunda bahsedilen sınıflar altında ayrı ayrı incelenmiş, ayrıca askeri stratejilerin geliştirilmesinde ve optimize edilmesinde olası kullanım sahaları tespit edilmeye çalışılmıştır.

Çalışma üç bölümden oluşmaktadır. İlk bölümde Askeri Taktik Ağların ne olduğu ve hangi maksatlar ile kullanıldığına ilişkin özet bilgi sunulmaktadır. İkinci bölümde DMÖ uygulamalarının tatbik edildiği alanların ATA yeteneklerine sağlayabileceği katkılar araştırılmış, bu kapsamda gelişen ve geliştirilmekte olan DMÖ algoritmaları ile; Nesne Konumlandırma, Siber Güvenlik, Lojistik, Hedef Değerlendirme, Sağlık, Eğitim ve Durumsal Farkındalık fonksiyon sahalarında ATA'lar ile beraber kullanımlarının yaratabileceği sinerji etkileri incelenmiştir. Son olarak DMÖ'nin, ATA'lara entegrasyonuna ilişkin aşılmasına ihtiyaç duyulan zorluklar

sıralanmış ve çalışmadaki temel bulgular üzerinden genel bir değerlendirme yapılarak çalışma sonlandırılmıştır.

2. ASKERİ TAKTİK AĞLARI ANLAMAK (UNDERSTANDING MILITARY TACTICAL NETWORKS)

Askeri taktik ağları, askeri harekatlarda kullanılan güvenli ses ve veri paylaşım sistemleridir. Bu ağlar, askeri birliklerin birbirleriyle, komuta merkezleriyle ve diğer kaynaklarla haberleşmesine olanak tanır. Amaçlarına göre tarihsel olarak gelişim gösteren bu ağlar ile günümüzde askeri birimler arasında taktik veya opreratif veri değişimleri, erken ihbar uyarıları, süreli veya sürekli yayınlar, silah sistemlerinin kontrolü, radar iz paylaşımları ve durumsal farkındalığı arttırıcı verilerin tek yönlü veya karşılıklı olarak paylaşımları yapılmaktadır [9].

Günümüz koşullarında kısıtlı operasyonlar da dâhil olmak üzere, tüm operasyon türlerinde bu verilerin anlık ve eksiksiz olarak komuta kademesine aktarılması, karar vericilerin en doğru kararı, en kısa sürede vermesini sağlamaya yardımcı olmaktadır. Bahse konu verilerin komuta kademelerine güvenli ve kesintisiz bir şekilde aktarılmasını sağlayan teknolojik sistemler ise Askeri Taktik Ağlar (ATA) olarak adlandırılmaktadırlar. ATA'ları, genellikle kablosuz iletişim teknolojileri, veri bağlantıları ve bilgi güvenliği protokolleri kullanarak oluşturulur. Bu ağlar, birliklerin sahadaki durumlarını takip etmelerini, koordinasyon sağlamalarını ve gerektiğinde hızlı kararlar almalarını sağlar. ATA'ları, genellikle saha tabanlı olan yerel ağlardan oluşur. Bu ağlar, askeri araçlar, taşınabilir cihazlar, sensörler ve diğer ekipmanlar arasında iletişim sağlar. Bu iletişim, ses, veri ve video gibi farklı türlerde verilerin aktarılmasını içermektedir [7].

ATA'lar, operasyonlar sırasında askeri birimler arasındaki iletişim ve bilgi alışverişinin omurgasını oluşturmaktadır. Kara, deniz, hava ve uzay dâhil olmak üzere farklı platformlar arasında gerçek zamanlı veri iletimi, durumsal farkındalık ve koordinasyon sağlarlar. ATA'lar içerdikleri teknolojiye bağlı olarak görüş içi veya görüş ötesi menzillerde haberleşebildikleri gibi zaman boyutunu da kullanarak haberleşme etkinliklerini arttırabilmektedirler.

Günümüzün tüm modern ordularında kullanılan ve harekât konseptlerinin ayrılmaz bir parçası olan ATA'lar, sahada kuvvetler arasında asimetrik güç etkisi yaratabilmektedir. Verileri en hızlı şekilde bilgiye dönüştüren ve kararları en kısa sürede birimlerine ulaştırabilen karar vericiler bu avantajı elde etmektedirler. Veriler mobil veya sabit konuşlu sensörlerden elde edilebilmektedir [10]. Söz konusu verileri sağlayabilecek örnek sistemleri ise şu şekilde sıralayabiliriz:

- Kara konuşlu Elektronik Sensörler (Sabit Hava Savunma Radarları, Mobil Hava Savunma Radarları, Elektronik Karıştırıcı Sistemler, Elektronik Algılayıcı ve Tespit Sistemleri, Optik ve Infra Red Kameralar, Pasif Radarlar, Hava Savunma Telsizleri, Dost-Düşman Tanımlama Sistemleri, Elektronik Destek/Taarruz Sistemleri)
- Uçan Elektronik Sensörler (Havadan Erken İhbar Uçakları, İnsansız Hava Araçları, Havadan Karıştırma Uçakları, Havadan Elektronik Destek/Taarruz Uçakları, Elektronik/Optik/Infra

Red Keşif Uçakları, Elektronik Algılayıcı ve Tespit Uçakları)

- Uzay Sistemleri (Keşif Uyduları, Haberleşme Uyduları, Radar Uyduları, Elektronik Destek Uyduları, Uzay ve Hava Savunma Uyduları)
- Silah Sistemleri (Akıllı ve Taktik Ağ bağlantılı her türlü mühimmat)
- Kara Konuşlu Silah Sistemleri (Hava Savunma Sistemleri, Füze Sistemleri, Zırhlı Birlikler, Mobil Komuta Kontrol Merkezleri
- Uçan Silah Sistemleri (Muharip Jet Uçaklar, Muharip Pervaneli Uçaklar, Muharip Helikopterler, Kargo Uçakları, Havadan Yakıt İkmal Uçakları, Genel Maksat/Arama Kurtarma Helikopterleri,
- Deniz Üstü Silah Sistemleri (Muharip Gemiler, Lojistik Destek Gemileri)
- Deniz Altı Silah Sistemleri (Muharip Denizaltılar)

Örnekleri çoğaltabileceğimiz bu sistemlerin bir arada uyum içerisinde çalışmasını sağlayabilmek ve doğru kararları zamanında verebilmek normal insan zekâsı ile yapılamayacağı aşikârdır. Çünkü dinamik olan bu sistemlerden akan veri büyüklüğü yüksek boyuttadır ve çok farklı alanlarda anlık olarak korale edilmesi için muhakkak yapay zekâ desteği gerektirmektedir [1]. Ayrıca bu harekât verilerinden daha fazlası da ilave olarak istihbarat, lojistik ve personel birimlerinden de gelmektedir. Elde edilen bu Büyük Verinin yapay zekâ algoritmaları ile işlenmesi ve karar tercihlerine dönüştürülmesi, birliklerini komuta eden karar vericilere büyük kolaylık sağlayacaktır.

DMÖ gibi bir başka yapay zekâ uygulaması olan Derin Sinir Ağları (DSA; Deep Neural Networks-DNN), görüntü ve ses gibi karmaşık, yüksek boyutlu veriler için özellikle uygun olan bir tür makine öğrenimi modelidir. Chjen ve arkadaşlarına göre katmanlı bir ağ savunma stratejisinin bir parçası olarak, gelen verileri sınıflandırmak ve potansiyel tehditleri tespit etmek için DSA sınıflandırma modelleri kullanılmaktadır [11]. Ancak, makine öğrenimi modellerinin kusursuz olmadığını ve yanlış pozitifler üretebileceğini veya ince anomalileri gözden kaçırabileceğini not etmek önemlidir. Bu nedenle, kapsamlı bir ağ savunma stratejisi için makine öğrenimi modellerinin yanı sıra güvenlik duvarları, erişim kontrolleri ve düzenli güvenlik denetimleri gibi diğer güvenlik önlemlerini dâhil etmek gerekmektedir [12].

Elde edilen bilgiler ışığında yapay zekâ uygulamalarından olan DMÖ ve DSA tekniklerinin askeri taktik ağlar ile bütünleştirilmesi ile, daha hızlı ve isabetli tahminler yapılabileceği, kısıtlamaları hafifletilebileceği, askerler üzerindeki aşırı bilgi yükünün azaltılabileceği ve siber savunma stratejilerinin güçlendirilebileceği söylenebilmektedir.

3. NESNE KONUMLANDIRMA KAPSAMINDA DMÖ UYGULAMALARI (APPLICATION OF DEEP MACHINE LEARNING IN OBJECT LOCATION)

DMÖ'nin ATA'lardaki en önemli uygulamalarından biri de nesne konumlandırmadır. Geleneksel olarak, denizde, karada ve havada nesne konumu için radar istasyonları, elektronik sorgulayıcılar ve uydular gibi yöntemler kullanılmaktadır. Ancak, bu yöntemler genellikle büyük miktarda veriyi etkili bir şekilde işleme gibi zorluklarla yol açmaktadır. Yapay sinir ağları gibi DMÖ algoritmaları da

nesnelerin hareketindeki anormallikleri analiz ederek ve tanımlayarak nesne konumlandırmayı iyileştirebilmektedir [13].

DMÖ teknolojilerinde, gerçekten de çeşitli araştırma alanlarında dikkate değer ilerlemeler yaşamıştır. Genellikle görüntü işlemede kullanılan ve girdi olarak görselleri alan bir derin öğrenme algoritması olan Evrişimli Sinir Ağlarının (ESA; Convolutional Neural Networks-CNN) sürekli gelişmesiyle, bilgisayar görüntü işleme teknikleri günümüzde yüksek performans ve doğruluk seviyelerine ulaşmış durumdadır. ESA'lar, görüntü sınıflandırma, nesne algılama ve görüntü bölümleme gibi bilgisayar destekli görsel analiz yeteneklerinde devrim yarattı demek yanlış olmayacaktır. İlave olarak, Bulanık ARTMAP ve Gauss Karışım Modeli gibi teknikler, belirlenmiş standartlardan herhangi bir sapmayı izlemek ve belirlemek için kullanılabilir [14]. Bu algoritmalar, sistemin önemli olmayan olayları algılayıp kullanmaz iken önemli olaylara dayalı kalıpları öğrenmesini ve yeni bilgi oluşumlarını güncellemesini sağlar.

Derin öğrenmenin ve ESA'ların hızlı gelişimi, aşağıdaki örnekler gibi çeşitli alanlarda bilgisayarla görüntü işleme uygulamalarını büyük ölçüde geliştirmiştir:

3.1 Yüz Tanıma

ESA'lar, yüz tanıma sistemlerinin doğruluğunu ve sağlamlığını önemli ölçüde iyileştirmiş ve en çok kullanılan derin öğrenme algoritmalarından birisi olmuştur [15]. Yapılan çalışmalarda ESA'ların Çok Katmanlı Algılayıcılar (Multilayer Perceptron) gibi birçok algoritmanın performansından daha yüksek bir performans sergiledikleri tespit edilmiştir [16,17]. ESA algoritmaları sayesinde bilgisayarlar yüz görüntülerinden ayırt edici özellikleri çıkarmayı öğrenebilmektedirler. Bu da bireylerin doğru bir şekilde tanımlanmasını ve doğrulanmasını sağlamaktadır [17]. Bu sayede ATA ile bütünleştirilmiş akıllı silah sistemlerinin ve mühimmatların hedeflerine doğrulukla yönlendirilmesinin sağlanabilmesi mümkün görülmektedir.

3.2 Nesne Tespiti

Daha Hızlı Bölgesel Temelli ESA ve You Only Look Once (YOLO) gibi ESA tabanlı nesne algılama yöntemleri, resimlerdeki veya videolardaki nesneleri belirleme ve yerelleştirme konusunda etkileyici sonuçlar elde edebilmektedir [5]. YOLO bir resimdeki nesneleri gerçek zamanlı olarak algılayan ve tanıyan bir algoritmadır. YOLO, ESA'nı kullanarak nesne tespitini bir regresyon problemi olarak gerçekleştirir. Bu algoritma, görüntülerdeki nesneleri tek bir geçişle tespit etme yeteneğiyle hızlı ve etkili bir yöntemdir. Ayrıca, YOLO tespit edilen nesnelerin sınıf ayrımlarını da sağlar. Bu tekniklerin otonom sürüş, gözetleme, medikal tanı/teşhis ve robotik gibi alanlarda önemli uygulamaları vardır [18].

Nesne tespiti; savunma (gözetleme), insan-bilgisayar etkileşimi, robotik ve ulaşım vb. birçok alanda uygulanmaktadır. Bu teknolojinin kullanıldığı alanlardan biri, sürekli gözetimdir. Sürekli gözetim için kullanılan sensörler, kısa bir süre içinde petabaytlarca görüntü verisi üretebilmektedir. Bu veriler, coğrafi verilere indirgenmekte ve mevcut senaryo hakkında net bir fikir edinmek için diğer verilerle entegre edilmektedir [6]. Bu süreç, ham görüntü

verilerinden insanlar, araçlar ve şüpheli nesneler gibi varlıkları izlemek için nesne konumunu içermektedir [19]. Bu teknoloji, güvenlik alanında kullanılan kamera sistemleri ve uzaktan izleme sistemleri gibi uygulamalarda yaygın olarak kullanılmaktadır. Bunun yanı sıra, askeri ulaşım alanında trafik akışını izlemek ve optimizasyon için kullanılabileceği değerlendirilmektedir.

3.3 Nesne Takibi

ESA'lar, nesne takip algoritmalarının geliştirilmesinde de önemli bir rol oynamıştır. Zaman içinde nesne özelliklerini öğrenip tahmin eden bu algoritmalar, nesneleri video karelerinde verimli bir şekilde izleyebilmekte ve onları gözetim ve video analizi gibi alanlarda kullanışlı hale gelmesini sağlamaktadır [20].

ESA'lar, görsel veriler üzerinde derin öğrenme yöntemlerini kullanarak nesne izleme uygulamalarına önemli katkılar sağlamaktadır [21]. Bu algoritmalar, video karelerindeki nesne özelliklerini zaman içinde öğrenmek ve tahmin etmek için derin öğrenmenin gücünü kullanmaktadır [22]. Bu sayede, gözetleme, video analizi ve diğer ilgili alanlarda çeşitli uygulamalar mümkün hale gelmektedir. ESA tabanlı nesne izleme algoritmaları, geleneksel yöntemlere kıyasla daha yüksek doğruluk ve sağlamlık sunmaktadır. Derin öğrenme teknikleri sayesinde, bu algoritmalar nesnelerin daha etkili bir şekilde izlenmesini sağlamakta ve karmaşık ortamlarda dahi iyi performans sergilemektedir. Bu özellikleri sayesinde, ESA tabanlı nesne izleme algoritmaları, modern bilgisayarlı görü sistemlerinde paha biçilmez araçlar olarak değerlendirilmektedir [21].

Bu gelişmeler, gözetleme, güvenlik, trafik kontrolü, otomatik sürüş, video analizi ve diğer birçok uygulama alanında önemli ilerlemelere yol açmaktadır. ESA'ların gücünü kullanan nesne izleme algoritmaları, gerçek zamanlı nesne takibi için daha etkili ve verimli çözümler sunmaktadır. Bu sayede, özellikle insansız askeri sistemler başta olmak üzere, operasyon alanı içerisinde bulunan tüm dost ve düşman unsurların hareketliliği takip edilebileceği gibi, düşman hareketlerinin hareketliliğinden niyetini tespit edip daha önceden tedbir alınabileceği değerlendirilmektedir.

3.4 Semantik Segmentasyon

Semantik Segmentasyon (Anlamsal Bölütleme), bir görüntüdeki piksel düzeyindeki objeleri algılayarak, farklı sınıflara ait nesnelerin bölgelerini çıkarmak için kullanılan bir görüntü işleme tekniğidir [23]. Tüm sınıfları ayrı ayrı gruplandırmak için, öncelikle bir öğrenme modeli kullanılması gerekmektedir. Bu model, görüntülerdeki farklı sınıflara ait nesnelerin özelliklerini öğrenerek, görüntüdeki pikselleri sınıflara ayırabilir [24]. Bu şekilde, bir görüntüdeki farklı sınıflara ait bölgeleri belirlemek mümkün olur. Anlamsal Bölütleme işlemi genellikle derin öğrenme veya yapay sinir ağlarıyla gerçekleştirilir. Bu yaklaşım, nesnelerin daha karmaşık yapılarını daha iyi tanımlayabilir ve doğru sınıflandırma yapabilir [25]. ESA'lar, bir görüntüdeki her piksele bir sınıf etiketi atamayı içeren anlamsal segmentasyonda devrim yaratmıştır. ESA'lardaki ilerlemeler gerçekten de yeni olasılıkların farkına varılmasını sağlamış ve bilgisayarlı görüntü işleme uygulamalarının performansını iyileştirerek sonuçta çeşitli

endüstrilere ve askeri faaliyet alanlarına fayda sağlamıştır.

Yukarıda bahsedilen örnek uygulamalardan da anlaşılacağı üzere derin öğrenmenin, veriye dayalı yaklaşımlardan öğrenmek için güçlü bir araç olduğu kanıtlanmıştır. Ayrıca manuel olarak tasarlanmış özelliklere duyulan ihtiyacı geride bıraktığını söylemek yanlış olmayacaktır. Büyük ölçekli veri kümelerinin mevcudiyeti gerçekten de derin öğrenmenin başarısında çok önemli bir rol oynadığı görülmektedir. Bu veri kümeleri, derin öğrenme modelleri için adeta yakıt görevi görerek anlamlı kalıpları etkili bir şekilde genelleştirmelerini ve çıkarmalarını sağlamaktadır. Derin öğrenme modelleri, çeşitli ve kapsamlı veri kümeleri üzerinde eğitim alarak verilerin karmaşık temsillerini öğrenebilir ve bu da görüntü tanıma, doğal dil işleme ve daha fazlası gibi çeşitli görevlerde performansın artmasına yol açabilmektedir. Verinin bol olması, daha iyi genelleştirmeye ve mühendislerin manuel olarak tasarlaması zor olabilecek iç görülü korelasyonlarını ve özelliklerini ortaya çıkarma potansiyeline olanak tanımaktadır [25].

Uygulama sayısı artmaya devam ettikçe, çeşitli ve zengin uygulama verilerinin birikimi de artmaktadır. Bu veriler, derin öğrenmenin daha da geliştirilmesi ve uygulanmasında çok önemli bir rol oynar. Ancak, verilerin kalitesinin derin öğrenme modellerinin etkinliği üzerinde önemli bir etkiye sahip olabileceğini not etmek önemlidir. DMÖ algoritmalarında kullanılan yüksek kaliteli, doğru şekilde etiketlenmiş veriler, daha güvenilir ve doğru sonuçlara katkıda bulunmaktadır [26].

Gerçek dünya verilerine ek olarak, sentetik verilerin entegrasyonunu dikkate almak, derin öğrenme için mevcut veri miktarını artırmak açısından da değerli olabilir. Sentetik veri oluşturma teknikleri, modelin gerçek dünya senaryolarındaki varyasyonları genelleştirme ve işleme yeteneğini daha da geliştirerek mevcut veri setini artırabilir. Bununla birlikte, sentetik verilerin istenen gerçek dünya senaryolarını doğru bir şekilde temsil etmesini sağlamak, optimum performans için çok önemlidir [27].

Özetle, ATA'lar ile bütünleştirilmesi sonucunda derin öğrenmeden elde edilecek büyük ölçekli verilerin mevcudiyeti ve bu verilerin kalitesi, derin öğrenmenin başarısı için çok önemli faktörlerdir. Ek olarak, harp simülasyonları, harp oyunları ve tatbikatlardan sağlanabilecek sentetik verilerin dâhil edilmesi, verilerin miktarını ve çeşitliliğini artırmak, böylece derin öğrenme modellerinin yeteneklerini geliştirmek için tamamlayıcı bir yaklaşım olarak düşünülebilir [28].

4. ASKERİ TAKTİK AĞLARDA SİBER GÜVENLİĞİN ARTIRILMASI (ENHANCING CYBERSECURITY OF MILITARY TACTICAL NETWORKS)

Askeri stratejilerde yapay zekâ uygulamalarının kullanımı, ATA'larda siber güvenlik açısından yeni zorluklar ortaya çıkarmaktadır. Yapay zekâ, siber saldırıların daha sofistike hale gelmesine ve savunma sistemlerinin bu saldırılara uyum sağlamasının zorlaşmasına neden olmaktadır. Bu noktada, Bistron ve Piotrowski tarafından yapay zekânın aynı zamanda askeri taktik ağlarda siber güvenliği artırmak için de güçlü bir araç olarak kullanılabileceği ifade edilmiştir [29].

Askeri taktik ağlarda siber güvenliğin artırılması, sürekli yenilik ve ortaya çıkan tehditlere uyum sağlamayı gerektiren sürekli bir çabadır [30].

Komuta merkezi hareketliliği, güvenli kablosuz iletişim, siber güvenlik önlemleri ve uç bilgi işlem, taktik ağların modernleştirilmesinde ve askeri operasyonların başarısının ve güvenliğinin sağlanmasında en önemli konuların başında gelmektedir.

Orduda kabloludan kablosuz iletişime geçiş süreci, gizli bilgilerin kablosuz ağlar üzerinden güvenli bir şekilde iletilmesinin zorluğuyla yavaş bir gelişim göstermektedir. Tarihsel olarak, sahadaki askerlerin Wi-Fi, Long-Term Evolution (LTE) ve diğer radyo türlerini kullanma yetenekleri, maliyet ve güvenlik izni gereklilikleri nedeniyle gizlilik dereceli verileri iletmek için sınırlıydı [31]. Zamanla gelişen ve yaygınlaşan ATA'lar siber saldırılara karşı savunmasız olduğundan, bu zorlukların üstesinden gelme fikri, siber güvenliği askeri operasyonlarda kritik bir endişe haline getirdi.

Bu endişenin giderilmesi, askeri operasyonların planlanması ve yönetilmesi için kritik öneme sahip olduğundan ATA'ların düşman saldırılarına karşı dayanıklı ve güvenli olması sağlanmalıdır. Bu noktada Sadiku ve arkadaşları, yapay zekânın, bilgisayar ağlarının siber güvenliğini artırmak için aşağıdaki şekillerde kullanılabileceğini belirtmektedir:

Saldırı Tespiti: Yapay zekâ, ağ trafiğini analiz ederek saldırıları tespit edebilir. Normal ağ trafiğinden sapmaları belirleyerek anormal aktiviteleri tanımlayabilir ve hızla yanıt verebilir. Bu, saldırıların erken aşamada tespit edilmesini ve etkilerinin azaltılmasını sağlar.

Davranış Analizi: Yapay zekâ, ağ içerisindeki kullanıcıların ve sistemlerin normal davranışlarını analiz edebilir. Kullanıcı davranışlarındaki anormallikleri tespit ederek içeriden gelen tehditleri belirleyebilir. Aynı zamanda sistemlerin normal çalışma şekillerini öğrenerek, potansiyel saldırıları önceden tahmin edebilir ve engelleyebilir.

Otomatik Savunma: Yapay zekâ, anlık veri analizi ve karar alma yetenekleriyle, siber saldırılara otomatik olarak tepki verebilir. Ağ dâhilinde saldırıları tespit edip engelleyebilir, savunma sistemlerini güçlendirebilir ve saldırılara uygun karşı önlemleri alabilir. Bu şekilde, ağları saldırılara karşı daha dirençli hale getirebilir.

Zayıflıkların Tespiti: Yapay zekâ, ağlardaki zayıflıkları tespit edebilir ve bunları düzeltmek için önlemler alabilir. Potansiyel güvenlik açıklarını belirleyerek savunma sistemlerinin iyileştirilmesini sağlayabilir. Bu da ağların saldırılara karşı daha güvenli hale gelmesini sağlar [32].

Bu yöntemlerin başarılı bir şekilde uygulanması sonucunda yapay zekâ ATA'larda siber güvenliğin artırılmasında önemli bir rol oynayacaktır. Siber güvenlik alanında yapay zekâ kullanımı, otonom saldırı tespitinde, tehdit analizinde ve savunma sistemlerinin güçlendirilmesinde büyük faydalar sağlayabilir. Aynı kapsamda Yanin, Ullah ve Katt araştırmalarında yapay zekânın, büyük veri analitiği ve makine öğrenme algoritmalarıyla donatılarak, anormal davranışları tespit etmek, saldırıları önlemek ve sistemleri güçlendirmek için öngörülerde bulunmak gibi görevleri yerine getirebildiğinden bahsetmişlerdir [33].

Benzer olarak Gökdemir ve Çalhan'da yapay zekâ gibi DMÖ de algoritmaları anormal ağ

davranışını algılayıp bunlara yanıt verebileceğini, potansiyel güvenlik açıklarını belirleyebileceğini ve siber tehditlere karşı proaktif olarak savunma yapabileceğini savunmuşlardır [34]. Bu algoritmalar sürekli olarak yeni verilerden öğrenerek ve gelişen saldırı tekniklerine uyum sağlayarak ATA'ların genel dayanıklılığını ve güvenliğini iyileştirebileceği değerlendirilmektedir.

Yapılan çalışmalar incelendiğinde saldırı tespiti, davranış analizi, otomatik savunma ve zayıflık tespiti gibi alanlarda yapay zekâ uygulamalarının kullanımının, normal bilgisayar ağlarının yanı sıra ATA'ları da saldırılara karşı daha dirençli hale getirebileceği söylenebilmektedir. Paralel olarak, yapay zekânın kullanımıyla birlikte yeni güvenlik zorluklarının ortaya çıkması, teknolojik sürecin doğal sonucu olarak karşımıza çıkmaktadır. Bu zorlukların üstesinden gelinmesi maksadıyla yapay zekâ tabanlı savunma sistemlerinin yanı sıra, siber saldırganların da yapay zekâ kullanabileceği göz önünde bulundurulması ve sürekli olarak güncellenen siber güvenlik politikalarıyla önlemler alınması faydalı olacaktır.

5. LOJİSTİK VE TAŞIMACILIK OPTİMİZASYONU (LOGISTICS AND TRANSPORTATION OPTIMIZATION)

Başarılı askeri operasyonlar için verimli lojistik ve nakliye çok önemlidir. Askeri tedarik zinciri yönetimi, askeri ürünlerin, parçaların ve hizmetlerin tedariki, üretimi, onarımı ve teslimatı gibi çeşitli işlevleri içerir. Araştırmalar öncelikli amacın, saldırı ve savunma silah sistemleri için zamanında ve uygun maliyetli desteğin sağlanması olduğunu göstermektedir [35]. Bu husus, alt tedarikçilerin, tedarikçilerin, onarım depolarının, dağıtım merkezlerinin, perakendecilerin yönetimini ve nihayetinde askeri üslere veya müşterilere/tüketicilere teslimatı içermektedir. Askeri tedarik zincirinin verimli yönetimi, askeri operasyonlarda hazırlık ve etkinliğin sürdürülmesi için çok önemlidir.

Askeri teçhizatın yedek parçalarının ihtiyaç duyulan yerde ve zamanda mevcut olmasını sağlamak için modern ordular, tipik olarak kapsamlı bir tedarik zinciri ve bakım sistemi izlemektedirler. Bu sistem, aşağıdakiler de dâhil olmak üzere birkaç temel bileşenleri içerir:

- *Envanter Yönetimi,*
- *Tahmin ve Planlama,*
- *Tedarik ve Üretim,*
- *Dağıtım ve Lojistik,*
- *Bakım ve Onarım,*

Orduların lojistik birimleri, bu bileşenleri bütünleştirerek, askeri operasyonları desteklemek için ihtiyaç duyulan yerde ve zamanda kullanılabilir olmalarını sağlamak için, yedek parçaların etkili bir tedarik zinciri içerisinde sürekliliğini sağlamaya uğraşmaktadırlar.

Abell makalesinde DMÖ algoritmaları, malların, mühimmatın ve birliklerin taşınmasını optimize ederek maliyetlerin düşmesine ve insanların operasyonel çabalarının azalmasına yol açabileceğinden bahsetmiştir. Makalesinin devamında ABD Kara Kuvvetleri'nin konu hakkında IBM firması ile yapmış olduğu anlaşmadan bahseden Abell, yapay zekâyı askeri ulaşım sistemlerine entegre edilmesi sayesinde, anormalliklerin hızla tespit edilebileceğini ve aksama süresini en aza indirmek ve operasyonel hazırlığı artırmak için bileşen arızalarının tahmin edilebileceğini belirtmiştir [36].

Ek olarak, makine öğrenimi algoritmaları kullanılarak da tedarik zinciri yönetimini, envanter kontrolünü ve rota planlamasını optimize etmek için geçmiş verileri analiz edebilir. Bu, daha etkili kaynak tahsisi sağlayabilir, gecikmeleri azaltabilir ve askeri lojistik ve nakliyede genel operasyonel verimliliği artırabilir.

Woschank ve arkadaşlarına göre yapay zekânın lojistik endüstrisinde kullanılması, gerçekten de verimliliği ve güvenliği iyileştirme potansiyeli göstermiştir. Makine öğrenimi ve tahmine dayalı analitik gibi yapay zekâ teknolojileri, karmaşık tedarik zinciri operasyonlarını analiz edip optimize ederek maliyetleri azaltabilir, gecikmeleri en aza indirebilir ve genel verimliliği artırabilir [37]. Bu bilgiler neticesinde, yapay zekâ destekli ATA'ların, envanter yönetimi, rota optimizasyonu ve lojistik operasyonları kolaylaştırmaya ve kaynak tahsisini iyileştirmeye yardımcı olan talep tahmini gibi çeşitli görevleri otomatik olarak yapabileceği değerlendirilmiştir. Ayrıca yapay zekâ destekli ATA'ların, lojistik sistemindeki güvenliği artırabileceği; hırsızlık, dolandırıcılık veya yetkisiz erişim gibi potansiyel risklerin erken tespit edilmesini sağlayarak anormallikleri gerçek zamanlı olarak aktif olarak izleyip tespit edebileceği; gelecekteki güvenlik ihlallerini önlemek için geçmiş verileri analiz ederek tedarik zinciri boyunca malların güvenliğini sağlayabileceği değerlendirilmiştir.

Yapay zekâ, lojistikte verimliliği ve güvenliği artırma potansiyelini göstermiş olsa da insan uzmanlığının ve gözetiminin çok önemli olduğunu belirtmek önemlidir. Yapay zekâ teknolojilerini insan kaynaklarıyla birleştirmek, problem çözme becerileri ve karmaşık durumlara uyum sağlama yeteneği kazandırdığından daha da iyi sonuçlara yol açabilir. Bu nedenle hem yapay zekâ yeteneklerini hem de insan becerilerini kullanan işbirlikçi bir yaklaşımın, lojistik endüstrisinde en uygun sonuçları vermesi muhtemeldir [38].

6. HEDEF TANIMA VE TEHDİT DEĞERLENDİRMESİ (TARGET RECOGNITION AND THREAT ASSESSMENT)

Doğru hedef tanıma ve tehdit değerlendirmesi, askeri operasyonlar için hayati öneme sahiptir. Makine öğrenimi algoritmaları, raporlar, haber akışları ve belgeler gibi çeşitli yapılandırılmamış bilgi kaynaklarını analiz ederek savunma kuvvetlerine değerli iç görüler ve durumsal farkındalık sağlayabilir [39].

Bu algoritmalar düşman örüntülerini tanımlayabilir, davranışını tahmin edebilir, görev yaklaşımlarını değerlendirebilir ve potansiyel güvenlik açıklarını tespit edebilirler. Askeri birimler, makine öğrenimi tekniklerinden yararlanarak veriye dayalı kararlar mekanizmaları geliştirebilir ve tehditleri etkili bir şekilde belirleme ve etkisiz hale getirme yeteneklerini geliştirebilirler.

İnsan ve yapay zekânın askeri operasyonlara entegrasyonu, savaşın etkinliğini ve verimliliğini artırma potansiyeline sahiptir. Hem insan hem de makine istihbaratının güçleri birleştiğinde, daha geniş bir senaryo yelpazesine sahip olunmakta ve gerekli istihbaratın istenilen zamanda ve yeterlilikte oluşturmak için ilgili birimler daha donanımlı hale gelmektedir [40]. Ancak, askeri operasyonlarda otonom teknolojilerin kullanımına ilişkin ele alınması gereken potansiyel etik hususlar da bulunmaktadır. Genel

olarak, yapay zekâ destekli akıllı ordunun gelecekteki gelişimi, teknolojik ilerlemeler ve politika kararları dâhil olmak üzere çeşitli karmaşık faktörlere bağlı olacağı söylenebilir.

Bir diğer DMÖ uygulaması olan Yapay Sinir Ağı (YSA; Artificial Neural Network-ANN), geleneksel teknikleri kullanarak üstesinden gelinmesi zor olan karmaşık bilgi işleme ve otonom kontrol problemlerini çözmek için büyük bir potansiyele sahiptir [41]. YSA'nın büyük miktarda veriden öğrenme ve uyarlama yeteneği, gerçek zamanlı işleme ve yanıt vermesini sağlayarak onu çeşitli askeri uygulamalar için umut verici bir araç haline getirmektedir. Bir yandan da YSA teknolojisi, askeri uygulamalar için güçlü araçlar sağlama potansiyeline sahiptir. Nöral ağlar, örüntü tanıma konusunda başarılı gelişmeler gösterirken, hedef tanıma ve izleme gibi uygulamalar için de uygun bir uygulama olarak karşımıza çıkmaktadır. Büyük veri kümelerinden öğrenme ve gerçek zamanlı olarak yeni durumlara uyum sağlama becerileri, bu sistemlerin doğruluğunu ve güvenilirliğini artırmaktadır.

İlave olarak, YSA'ları askeri operasyonlara gerçek zamanlı yönlendirme ve hassas seyrüsefer yaptırma konularında yüksek fayda sağlayabilmektedir [41]. Diğer konularda olduğu gibi, yapay zekânın askeri hedef tanımlama ve değerlendirilmesinde kullanımıyla ilgili etik ve yasal yükümlülükleri dikkate almak ve bu teknolojilerin sorumlu bir şekilde ve uygun sınırlar içinde kullanılmasını sağlamak önem arz etmektedir.

Askeri hedef tanıma ve izleme bağlamında YSA'ları, belirli askeri hedefleri veya ilgilenilen nesneleri belirlemek ve izlemek için eğitilebilecek yapıdadırlar. YSA'ları, görüntüler veya radar bilgileri gibi çok büyük miktarda sensör verisini analiz ederek, kalıpları tanımayı öğrenebilir ve gerçek zamanlı senaryolarda doğru tanımlamalar yapabilir. Ek olarak, YSA'ları gerçek zamanlı yönlendirme sistemlerinde kullanılabilir. Sinir ağları, girdileri sürekli olarak işleyerek ve çıktıları değişen koşullara göre ayarlayarak, İHA'lar veya diğer otonom araçlar gibi askeri varlıkların kontrol edilmesine ve yönlendirilmesine yardımcı olabileceği söylenebilir. Bu yeteneğin, karmaşık ortamlarda gezinme ve mevcut duruma dayalı olarak akıllı kararlar alma becerisini geliştirebileceği değerlendirilmektedir.

Mevcut araştırmalar, bir YSA türü olan derin öğrenme modellerinin, geleneksel makine öğrenimi algoritmalarına kıyasla tehdit algılama performansını gerçekten iyileştirebileceğini göstermiştir [42]. Bunun başlıca nedeni, derin öğrenme modellerinin, karmaşık kalıpları ve özellikleri ayıklamak için birbirine bağlı birden çok düğüm katmanından yararlanarak verilerin hiyerarşik temsillerini otomatik olarak öğrenme yeteneğidir. Sonuçta, derin öğrenme modellerinin performansının, eğitim verilerinin kalitesi, boyutu ve model mimarisi dâhil olmak üzere çeşitli faktörlere bağlı olduğunu not etmek önemlidir.

Bu bağlamda, YSA teknolojisi, çeşitli askeri uygulamalar için güçlü hesaplama araçları sağlama potansiyeline sahip olduğu söylenebilir. Bununla birlikte, etik çıkarımları göz önünde bulundurmak ve yanlış kullanımı veya istenmeyen sonuçları önlemek için uygun gözetimi sağlamak önemlidir.

7. SAVAŞ ALANINDA ASKER SAĞLIĞININ İYİLEŞTİRİLMESİ (IMPROVING BATTLEFIELD HEALTHCARE)

Savaş bölgelerinde, savaş alanı sağlık hizmetleri, askeri personelin refahını sağlamanın kritik bir yönüdür. Savaş, askerlerin hayatlarını riske atan zorlu bir ortamdır. Savaş koşullarında askerlerin sağlığı, savaş etkinliklerindeki başarıyı doğrudan etkileyen önemli bir faktördür. Savaş alanında askerlerin sağlığını korumak, savaşta üstünlük sağlamak için stratejik bir gereklilik haline gelmiştir. Bu nedenle, askerlerin sağlığına ve refahına odaklanmak, askeri operasyonların başarısı için hayati önem taşır. DMÖ, bu alanda önemli bir potansiyele sahiptir.

DMÖ savaşta askerlerin sağlığını artırmak için, çeşitli alanlarda önemli katkılar sağlayabilir. Örneğin, askeri personelin sağlık durumunu izlemek için giyilebilir cihazlar kullanarak DMÖ algoritmaları kullanılabilir. Bu cihazlar, askerin nabız, uyku düzeni, stres seviyeleri gibi önemli sağlık göstergelerini izleyebilir ve gerektiğinde askeri personelin sağlık durumu hakkında uyarılarda bulunabilir. Ayrıca, DMÖ, askerlerin yaralanma riskini tahmin etmek ve önleyici tedbirler almak için kullanılabilir. Geçmiş verileri analiz ederek, askerlerin yaralanma riski taşıdığı durumları belirleyebilir ve bu riskleri azaltmak için uygun önlemler alınabilir.

Gelişmiş teknolojiler, DMÖ ve ATA gibi yenilikçi araçlar, savaşta askerlerin sağlığını artırmak, savaş alanı sağlık hizmetlerini kolaylaştırmak ve askeri personelin refahını artırmak için önemli fırsatlar sunmaktadır. DMÖ, yapay zekâyı Robotik Cerrahi Sistemler, Robotik Yer Platformları ve diğer tıbbi teknolojilerle bütünleştirerek savaş alanı sağlık hizmetlerinin iyileştirilmesinde önemli bir rol oynayabilir. Panesar ve doktor arkadaşları yapay zekâ özellikli sistemlerin, cerrahi prosedürleri uzaktan destekleyerek ve gerçek zamanlı tıbbi analiz sağlayarak tıbbi müdahalelerin hızını ve doğruluğunu artırabileceğinden bahsetmişlerdir [43].

Bu sistemler ayrıca savaş alanında daha iyi sağlık hizmeti sağlamak için değerli bilgiler ve iç görüler toplamak üzere yaralı askerlerin tıbbi kayıtlarını da araştırır. Yapay zekâ desteği ile, büyük miktarda tıbbi veriyi analiz ederek yaralanmaları teşhis etmeye, tedavi seçenekleri önermeye ve hatta potansiyel olarak cerrahi prosedürlere yardımcı olmaya yardımcı olabilir. Savaş alanı sağlık hizmetlerinde büyük veri ve yapay zekânın bu entegrasyonu, tıbbi karar verme sürecini geliştirmeyi ve hasta sonuçlarını iyileştirmeyi amaçlamaktadır [44].

DMÖ'nin tıp alanına getirdiği gelişmeler göz önüne alındığında, DMÖ ile bütünleştirilmiş ATA'ların, savaş alanında sağlık hizmetlerinin etkin bir şekilde yönetilmesini kolaylaştıracağı rahatlıkla söylenebilecektir. Örneğin, taktik data linkleri, askeri personelin sağlık durumuyla ilgili verilerin gerçek zamanlı olarak sağlık personeline iletilmesini sağlayabilecektir. Bu sayede, sağlık personeli, sahada olan bir askerin acil tıbbi müdahaleye ihtiyacı olduğunu hızlı bir şekilde tespit edebilecek ve gerekli sağlık kaynaklarını yönlendirebilecektir. Ayrıca, bu geliştirilen ATA'lar, savaş alanında sağlık hizmetlerinin lojistik yönetimini kolaylaştıracaktır. Tıbbi malzeme ve ilaç stokları hakkında gerçek zamanlı bilgilere erişim sağlayarak, tıbbi kaynakların doğru bir şekilde

yönetilmesi ve ihtiyaç duyulan bölgelere zamanında ulaştırılması sağlanabilecektir.

DMÖ ve ATA'ların kullanımı, askeri personelin refahını artırmak için de büyük fırsatlar sunmaktadır. DMÖ, askeri personelin stres seviyelerini izleyebilir ve stres yönetimi konusunda önerilerde bulunabilir. Bunun yanı sıra, taktik data linkleri sayesinde askeri personel, aileleriyle daha sık ve güvenli iletişim kurabilir. Bu, askeri personelin moralini yükseltebilir ve psikolojik olarak daha sağlıklı bir ortamda çalışmalarını sağlayabilir. Ayrıca, taktik data linkleri, askeri personelin eğitim ihtiyaçlarını belirlemek ve kişiselleştirilmiş eğitim programları sunmak için kullanılabilir. Bu sayede, askeri personel daha iyi yetişmiş olacak ve savaşta daha başarılı olacaklardır.

Araştırmalar, DMÖ'nin, sağlık uzmanlarına karar vermede yardımcı olarak, teşhis doğruluğunu ve iş akışı verimliliğini artırarak ve klinik tahminleri ve hasta bakımını geliştirerek askeri personelin sağlık hizmetlerini iyileştirebileceğini göstermektedir [45-47].

8. SAVAŞ SİMÜLASYONU VE EĞİTİMİ (COMBAT SIMULATION AND TRAINING)

Simülasyon ve eğitim, askeri personelin muharebe senaryolarına hazırlanmasında çok önemli bir rol oynamaktadır. Askeri eğitim ve savaş simülasyonları, askeri personelin yeteneklerini ve karar alma becerilerini geliştirmek için kullanılmakta ve zayiatı ve riskleri minimize etmekte büyük fayda sağlamaktadır. Fawkes'in bildirisinde belirttiği gibi günümüzde, teknolojinin ilerlemesiyle birlikte DMÖ ve taktik data linkleri gibi yenilikçi teknolojilerin kullanılması, askeri eğitimlerin ve savaş simülasyonlarının etkinliğini artırmada büyük bir potansiyele sahiptir [48]. DMÖ, gerçekçi senaryolar oluşturarak, düşman davranışını taklit ederek ve kursiyerlere gerçek zamanlı geri bildirim sağlayarak savaş simülasyonunu ve eğitimini geliştirebilir. Bu algoritmalar, dinamik ve sürükleyici eğitim ortamları oluşturmak için geçmiş görev verileri ve gerçek zamanlı sensör girişi dâhil olmak üzere çok büyük miktarda veriyi analiz edebilir.

Makine öğreniminden yararlanan askeri eğitim programları, bireysel kursiyerlerin güçlü ve zayıf yönlerine uyum sağlayabilir, eğitim modüllerini kişiselleştirebilir ve eğitim sonuçlarını optimize edebilir. DMÖ destekli bu yeni program sayesinde, askeri personelin gerçek dünyadaki savaş durumlarına iyi hazırlanmasını sağlayarak daha verimli ve etkili eğitim sağlanabileceği değerlendirilmektedir. Yapılan araştırmalarda, DMÖ, askeri eğitimlerde simülasyon ve sanal gerçeklik gibi yenilikçi teknolojilerle birleştirildiğinde daha gerçekçi ve etkileşimli bir ortam yaratılmasına yardımcı olabileceği görülmüştür [49]. Askeri personel, simülasyonlar aracılığıyla gerçek savaş senaryolarını deneyimleyebilir ve karşılaşabilecekleri farklı durumlar hakkında pratik yapabilir. DMÖ algoritmaları, simülasyonlarda gerçekçi düşman davranışlarını modellere ve senaryolara entegre ederek daha etkili eğitimler sağlayabilir.

DMÖ desteği ile ATA'ların kullanılması, askeri eğitimlerin ve savaş simülasyonlarının etkinliğini artırmada büyük bir potansiyele sahiptir. DMÖ, askeri personelin büyük veri setlerini analiz etmelerine ve daha iyi kararlar almalarına yardımcı olabilir. Ayrıca, DMÖ algoritmaları, askeri eğitimlerde simülasyonlarla

birleştirildiğinde daha gerçekçi bir deneyim sağlayabilir. Taktik data linkleri ise birlikler arasında gerçek zamanlı iletişimi kolaylaştırarak koordinasyonu artırabilir ve DMÖ algoritmalarının veri analizini güçlendirebilir.

Ancak, bu yenilikçi teknolojilerin kullanımıyla ilgili bazı zorluklar da vardır. Özellikle, güvenlik ve gizlilik konuları dikkate alınmalı ve veri paylaşımı süreçleri sıkı bir şekilde yönetilmelidir. Ayrıca, DMÖ algoritmalarının doğruluğunu ve güvenilirliğini sağlamak için sürekli olarak eğitilmeleri ve iyileştirilmeleri gerekmektedir.

9. DURUMSAL FARKINDALIK VE TEHDİT İZLEME (SITUATIONAL AWARENESS AND THREAT MONITORING)

Askeri operasyonlar, hızla değişen savaş alanlarında etkili bir şekilde yönlendirilmek ve kontrol edilmek için güçlü bir durumsal farkındalık ve düşman tehdit izleme yeteneği gerektirmektedir. Bu ihtiyaçları karşılamak için gelişmiş teknolojilerin entegrasyonu kaçınılmaz hale gelmiştir. DMÖ ve ATA veri bağlantıları, askeri durumsal farkındalığı artırmak ve düşman tehditlerini izlemek için potansiyel olarak güçlü bir kombinasyon sunmaktadır.

ATA'lar, askeri platformlar ve birimler arasında iletişimi sağlayarak durumsal farkındalık ve tehdit izlenmesi konusunda gelişmiş silahlı kuvvetlerin omurgasını oluşturmaktadır [50]. Sabit ve hareketli platformlar arasında anlık veri paylaşımı yaparak birlikte çalışmayı kolaylaştırır. Ancak, verilerin anlamlı hale getirilmesi ve tehditlerin tanımlanması konusunda bu yeteneğin hâlâ geliştirilmesi gerekli kısımları mevcuttur. İşte bu noktada DMÖ devreye girmektedir. DMÖ, karmaşık veri kümelerini analiz etmek ve örüntüleri tanımak için algoritmalar kullanarak bilgisayar sistemlerinin eğitilmesini sağlar. Böylece veri bağlantıları aracılığıyla gelen veriler analiz edilerek düşman tehditleri hızlı ve hassas bir şekilde belirlenir.

DMÖ, büyük miktarda veriyi hızlı bir şekilde analiz edebilme yeteneği sayesinde askeri durumsal farkındalığı artırabilir. ATA aracılığıyla gelen veriler, DMÖ algoritmalarını besleyebilir ve anlamlı bilgilere dönüştürülebilir. Radar verileri, görüntüler, sinyal istihbaratı ve diğer sensör verileri DMÖ modelleriyle analiz edilebilir ve tehditlerin tespit edilmesi için kullanılabilir. DMÖ algoritmaları, taktik data linklerinden gelen verileri analiz ederek düşman birimlerin davranış modellerini tanıyabilir. Bu bilgi, askeri personelin stratejilerini ve taktiklerini daha iyi ayarlamalarına yardımcı olabilir. Ayrıca, DMÖ algoritmaları, derin ağların desteği ile, taktik data linklerindeki verileri gerçek zamanlı olarak izleyebilir ve olası tehditleri önceden tahmin ederek birimlerin proaktif bir şekilde tepki vermesini sağlayabilir. Bu sayede askeri birlikler, sahip oldukları verilere dayanarak daha hızlı ve daha doğru kararlar verebilir.

DMÖ algoritmaları, İstihbarat, Gözetleme ve Keşif (İGK; Intelligence Surveillance Reconnaissance-ISR) verilerini analiz ederek bu yetenekleri geliştirebilir. İHA'lar dâhil olmak üzere çeşitli kaynaklardan gelen İGK verilerini otonom olarak işleyip yorumlayan bu algoritmalar, düşman faaliyetleri hakkında gerçek zamanlı bilgiler sağlayabilir, potansiyel tehditleri belirleyebilir ve karar vermeye yardımcı olabilir. Ayrıca, yapay zekâ özellikli İHA'lar sınır bölgelerinde devriye gezebilir,

potansiyel tehditleri tespit edip izleyebilir ve müdahale ekiplerine ATA üzerinden değerli bilgiler iletebilir. Böylece, askeri üslerin güvenliği güçlendirilir ve askeri personelin savaşta ve uzak yerlerde güvenliği ile etkinliği artırılır.

DMÖ desteği ile ATA'ları düşman tehdit izleme kapasitesini de artırabilir. Derin öğrenme algoritmaları, belirli düşman tehditlerini tanımak ve tahmin etmek için eğitilebilir. Örneğin, düşman hava araçlarının tespiti veya düşman sinyal istihbaratının analizi gibi görevler, DMÖ teknikleriyle daha etkili bir şekilde gerçekleştirilebilir. Bu, dost birliklerin düşman faaliyetlerini daha iyi anlamalarını ve buna göre önlemler almalarını sağlar.

DSA'ları, askeri durumsal farkındalık ve düşman tehdit izleme konularında önemli bir rol oynayabilir. Bu ağlar, büyük miktarda veriyi analiz ederek örüntüleri ve ilişkileri tespit etme yeteneğine sahiptir. Askeri durumsal farkındalık, bir askeri birimin çevresindeki ortamı ve olayları anlama ve takip etme yeteneğini ifade eder. DSA'ları, birliklerin yerini belirleme, düşman hareketlerini izleme, hava durumu analizi gibi durumsal bilgileri işleyerek askeri birimlerin sahip olduğu bilgilerin analizini yapabilir ve bu sayede komutanlara daha doğru ve hızlı kararlar vermelerine yardımcı olabilir. DSA'ları, gözetleme sistemlerinden, uydu görüntülerinden, radar verilerinden ve diğer kaynaklardan gelen verileri analiz ederek düşman birimlerin yerlerini, aktivitelerini ve niyetlerini belirleyebilir. Bu bilgiler, askeri birimlerin stratejik planlamalarını ve müdahale stratejilerini geliştirmelerine yardımcı olabilir.

Derin bir sinir ağının, geleneksel makine öğrenimi yaklaşımına kıyasla, takviyelerin farklı özelliklerine ilişkin daha hızlı ve üstün tahminler sunabilmesi şaşırtıcı değildir. DSA'ları, girdi ve çıktı değişkenleri arasındaki karmaşık ilişkileri öğrenmek için daha büyük bir kapasiteye sahiptir, bu da onları yüksek derecede karmaşıklık içeren sorunları çözmek için ideal kılar. Geleneksel makine öğrenimi algoritmalarıyla karşılaştırıldığında derin öğrenme algoritmaları, verilerin daha soyut ve hiyerarşik temsillerini öğrenerek daha anlamlı özellikler çıkarmalarını mümkün kılar. Bu nedenle, DSA'larının bu durumda daha hızlı ve üstün tahminler sunabilmesi doğal olarak karşılanmaktadır [51].

10. ZORLUKLAR VE DEĞERLENDİRMELER (CHALLENGES AND CONSIDERATIONS)

DMÖ'nin, ATA'lara entegrasyonunda bir dizi zorluk ve karmaşıklık ortaya çıkabilir. İşte bu zorluklardan bazıları ve nasıl ele alınabilecekleri hakkında birkaç önemli nokta şu şekilde gruplanmaktadır:

Veri Sorunları: DMÖ, büyük miktarda etiketlenmiş veri gerektirmekte ancak ATA'lar genellikle sınırlı veriye sahip olmaktadır. Bu, eğitim için yeterli veri toplama ve etiketleme zorluğu yaratmaktadır. Bu sorunu aşmak için, yapay veri artırma teknikleri kullanılabilir veya benzer görevlerde daha fazla veri toplanabilir. Ancak bu noktada, doğru veri toplama yöntemleri ve veri setlerinin kalitesi büyük önem taşımaktadır. İlave olarak ATA'lar içerisinde iletilen gizlilik dereceli verilerin toplanıp üzerinde çalışılması güvenlik tedbirleri nedeni ile zorunlu prosedürlere maruz kalacak ve işlemlerin yavaş ilerlemesine neden olacaktır.

Güvenilirlik ve Güvenlik: Askeri sistemlerin güvenilirliği ve güvenliği hayati önem taşımaktadır. Veri gizliliği ve güvenliği gibi konular, bu teknolojilerin askeri uygulamalarında dikkate alınması gereken önemli faktörlerdir. DMÖ algoritmaları, yanlış kararlar verebilir veya saldırılara açık olabilir. Bu nedenle, bu algoritmaların güvenilirliği ve güvenliği, sıkı test ve doğrulama süreçleriyle sağlanmalıdır. Bu noktada belirli standartlar oluşturulmasının çok faydası olacaktır. Ayrıca, savunma mekanizmaları ve güçlü şifreleme yöntemleri kullanarak sistemleri korumak önemlidir.

İnsan-Faktörü: DMÖ, birçok askeri görevde insan faktörünün yerini alabilir veya onu tamamlayabilir. Ancak insan karar süreçleri ve zekâsı hala kritik öneme sahiptir. Bu nedenle, DMÖ algoritmalarının insanlarla etkileşim içinde çalışabilmesi ve insanların son kararı vermelerine olanak tanıması önemlidir. İnsanların DMÖ tarafından verilen kararları anlaması ve doğrulaması için şeffaflık ve açıklık sağlanmalıdır.

Etik ve Yasal Sorunlar: ATA'larda DMÖ kullanımıyla ilgili etik ve yasal sorunlar ortaya çıkabilir. Örneğin, savaş hukuku ve insan haklarıyla uyumlu olma, sivil hedeflerin korunması gibi konular dikkate alınmalıdır. Askeri birlikler ve komutanlar, DMÖ algoritmalarının kullanımını denetlemek ve etik kurallara uygunluğunu sağlamak için yönergeler ve politikalar geliştirmelidir.

Söz konusu zorluklara ilave olarak günümüz orduları ele alındığında yapay zekâ teknolojilerinin bütünleştirilmesi ve yaygın kullanıma verilebilmesi için dikkate alınması gereken üç zorluk vardır:

Modelde şeffaflık: Komutanların yapay zekâ sistemlerine olan güvenini kazanmak çok önemlidir. Hâlâ yapay zekâ tarafından sağlanan tavsiyeler, yorumlar ve yapay zekânın beslendiği algoritmanın gücü ile limitleri tam olarak açıklanamamaktadır.

Algoritmanın aktarılabilirliği: Algoritma, yalnızca belirli sorunlar için değil, tüm sorun türleri için uygulanabilir olmalıdır. Bir görevde kullanılan modellerin ile elde edilen algoritmayı diğer göreve aktarılması konusunda potansiyel sorunların yaşanabileceği değerlendirilmektedir.

Yetersiz eğitim verisi: Makine öğrenimi, yeterli miktarda eğitim verisine dayanmaktadır. Bu, yalnızca Denetimli Öğrenme (Supervised Learning) için etiketlenmiş verileri değil, aynı zamanda Takviyeli Öğrenme (Reinforcement Learning) için simülasyon verilerini de içerir. Bu tür verilerin mevcudiyeti askeri bağlamda bir zorluktur [44].

İşlem hızı ve karmaşıklık: Geçmiş bilgiler, elde edilen tecrübeler ve eğitim verileri ile beslenen DMÖ yazılımları verilerin yüksek oranda artması ve anlamlandırılacak verilerin daha fazla çeşitlenmesi neticesinde yüksek seviyede işlemci hızına ihtiyaç duyacaklardır. Zira verilerin çoğalmasının yanı sıra çeşitliliğinin de artması anlamlı sonuçlar çıkarmak konusunda algoritmalara büyük yük getirecektir. Artan ve karmaşıklaşan veriler oranında işlemci hızının artmaması neticesinde DMÖ tarafından zamanında istenilen verilerin sağlanamaması söz konusu olacaktır. Bu bağlamda işlemci hızına bağlı gelişmeler aynı paralelde değerlendirilmelidir.

Bu zorlukları aşmak için, ATA'lara DMÖ entegrasyonunda disiplinler üstü bir yaklaşım benimsenmelidir. Askeri personel, mühendisler, etik uzmanları ve hukukçular gibi farklı disiplinlerden uzmanlar bir araya gelerek bu zorlukları ele almalı ve uygun çözümler üretmelidir. Ayrıca, sürekli izleme, test ve geri bildirim süreçlerini de içeren sıkı bir takip mekanizması oluşturmak önemlidir.

11. SONUÇLAR (CONCLUSIONS)

DMÖ, askeri stratejilerin geliştirilmesi ve uygulanmasında önemli bir rol oynamaktadır. ATA'lar, bu teknolojik ilerlemeler sayesinde daha verimli ve etkili bir şekilde kullanılabilmektedir. Görülmüştür ki DMÖ, ATA'lar ile bütünleştirildiğinde, daha hızlı ve isabetli tahminler yapılmasını sağlayacak, kısıtlamaları hafifletecek, askerler üzerindeki bilgi yükünü azaltacak ve ağ savunma stratejilerini iyileştirecektir. Askeri operasyonlarda DMÖ ile geliştirilen modeller:

- Nesne konumlandırma,
- Siber güvenlik,
- Lojistik,
- Hedef tanıma,
- Tehdit değerlendirmesi,
- Asker sağlığının iyileştirilmesi,
- Simülasyon ve
- Durumsal farkındalık gibi alanlarda radikal değişiklikler sağlayabilecek potansiyele sahiptir.

Derin öğrenme modelleri, karmaşık görevleri başarıyla yerine getirebilen katmanlı yapısıyla askeri taktik ağlara uyumlandırılarak, operasyonlarda önemli bir avantaj sağlayabilecektir. Ancak, DMÖ ile askeri taktik ağlarının bütünleştirilmesi süreci, büyük veri korelasyonu ve doğru kararların zamanında verilmesi gibi zorluklar içermektedir. İnsan zekâsıyla bu sürecin gerçekleştirilmesi mümkün olmadığından, yapay zekâ bu noktada önemli bir rol oynamaktadır.

DMÖ'nin ATA'lara entegrasyonu, askeri operasyonlarda devrim yaratma potansiyeline sahiptir. Makine öğrenimi algoritmaları, nesne konumunu ve siber güvenliği iyileştirmeden lojistik ve nakliyeyi optimize etmeye kadar önemli avantajlar sunmaktadır. DMÖ, hedef tanımayı, savaş alanı sağlık hizmetlerini, savaş simülasyonu ve eğitimini ve durumsal farkındalığı iyileştirerek daha verimli ve etkili askeri yetenekler sağlar. Ancak, Yapay Zekânın askeri sektörde sorumlu ve güvenli bir şekilde konuşlandırılmasını sağlamak için zorlukların ve etik sonuçların dikkatli bir şekilde değerlendirilmesi gereklidir.

Yapay zekâ alanındaki gelişmeler, etkili askeri operasyonlara yönelik artan ihtiyaçla birlikte, DMÖ'ni ATA'lara entegre etmek konusunda kritik bir odak noktası haline gelmiş durumdadır [52].

Bulunan sonuçlar, derin öğrenme tekniklerinin;

- Güçlü öğrenme yeteneklerine sahip oldukları için operasyonel riski tahmin etmede etkili olduğunu,
- Derin öğrenme modellerinin diğer güçlü makine öğrenimi yöntemlerinden daha iyi performans gösterdiğini ve uygun ağ mimarilerinin tasarımı konusunda rehberlik sağlayabildiğini göstermektedir.

Bu bilgi, operasyonel risk tahmini için uygun tahmine dayalı modelleme tekniklerinin seçilmesi söz konusu olduğunda, risk yönetimi ve

risk azaltma açısından potansiyel faydalar sağlama konusunda gelecekteki karar verme sürecini geliştirmeye yardımcı olmaktadır [53].

DMÖ desteği ile kullanılan ATA'lar, savaşta kullanıldığında silahlı kuvvetlerin konvansiyonel gücünü arttırabilecek önemli bir potansiyele sahiptir. Yapılan araştırmalara ve bulunan makalelere göre fark yaratacak derecede gelişim görülebilecek bu potansiyel sahaları şu şekilde listelenebilir:

- ATA'ların görüş içi ve/veya görüş ötesi menziller haberleşme etkinliklerini arttırmak,
- Ağ savunma stratejilerini iyileştirmek,
- Nesne konumlandırma, tespit, takip yeteneklerini arttırmak,
- Askeri eğitimlerin ve savaş simülasyonlarının kalitesini ve etkinliğini artırmak,
- Askeri lojistiğin verimliliğini ve güvenliğini arttırmak,
- Hedef tanıma ve tehdit değerlendirme performansını arttırmak,
- Savaş alanında askeri personelin sağlık hizmetlerini iyileştirmek,
- Askeri personelin daha iyi kararlar almasına, daha gerçekçi eğitimler yapılmasına ve daha etkili bir şekilde koordinasyon sağlamasına yardımcı olmak,
- Askeri durumsal farkındalık ve düşman tehdit izleme yeteneklerini artırmak,
- Askeri birliklerin sahip oldukları verileri daha etkili bir şekilde analiz etmelerini ve tehditleri daha hızlı bir şekilde belirlemelerini sağlamak,
- Operasyonel karar verme sürecini iyileştirmek, nesne tanıma ve hedef tespiti yeteneklerini artırmak ve özerk sistemlerin performansını geliştirmek.

Sonuç olarak, DMÖ ile birlikte ATA'ların kullanımı, askeri operasyonlarda fark yaratacağı ve bir dizi alanı önemli ölçüde geliştireceği değerlendirilmiştir. Günümüzde gelinen noktada yapay zekâ teknolojisindeki devam eden ilerlemelerle, ATA'larda DMÖ'nin geleceği, savunma sektörü için büyük umut vaat etmektedir. Bu başarıldığında, yeni nesil askeri operasyonların gerçekleştirilebileceği söylenebilir.

Ancak, DMÖ'nin askeri operasyonlarda kullanımı, etik, güvenlik ve siber saldırı riskleri gibi çeşitli zorlukları da beraberinde getirmekte olduğu, veri gizliliği ve güvenlik gibi konuların dikkate alınması gerektiği hususları sürekli gündemde kalmalıdır. Bu nedenle, ATA temelli askeri stratejilerin geliştirilmesinde DMÖ kullanılırken dikkatli bir şekilde değerlendirme ve dengeleme yapılması önemlidir. DMÖ ve ATA veri bağlantılarının ancak doğru ve güvenli bir şekilde bütünleştirilmesi, askeri operasyonlarda üstünlük sağlayabilir ve askeri personelin güvenliklerini artırabilir. Yola çıkılırken bu bütünleştirme sürecinin zorlukları göz önüne alınmalı ve uygulamalar dikkatli bir şekilde yapılmalıdır. Ayrıca makine öğrenimi modellerinin kusursuz olmadığını ve yanlış pozitifler üretebileceğini veya ince anomalileri gözden kaçırabileceğini not etmek önemlidir.

TEŞEKKÜR (ACKNOWLEDGMENTS)

Bu araştırma hiçbir dış finansman almamıştır.

YAZAR KATKILARI (AUTHORSHIP CONTRIBUTION STATEMENT)

Fuat ÖZÇAKMAK: Kavramsal tasarım, araştırma, metodoloji, kaynaklar, görselleştirme,

yazma-taslak, yazma-gözden geçirme ve düzenleme.

ÇIKAR ÇATIŞMALARI (CONFLICTS OF INTEREST)

Yazar, herhangi bir çıkar çatışması olmadığını beyan eder.

KAYNAKLAR (REFERENCES)

[1] M. Atalay ve E. Çelik, "Büyük Veri Analizinde Yapay Zekâ ve Makine Öğrenmesi Uygulamaları- Artificial Intelligence and Machine Learning Applications in Big Data Analysis," Mehmet Akif Ersoy Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, cilt 9, no. 22, pp. 155-172, 2017. DOI: 10.20875/makusobed. 309727.

[2] S. Patel, "A Comprehensive Analysis of Convolutional Neural Network Models," International Journal of Advanced Science and Technology, cilt 29, no. 4, pp. 771-777, 2020., DOI: 10.1109/ICUE49301.2020.9307089

[3] A. Testolin, W. Y. Zou ve J. L. McClelland, "Numerosity discrimination in deep neural networks: Initial competence, developmental refinement and experience statistics," Developmental Science, cilt 23, no. 5, 24 January 2020. DOI: 10.1111/desc.12940

[4] K. Goztepe, V. Dizdaroğlu ve Ş. Sağıroğlu, "New directions in military and security studies: artificial intelligence and military decision making process," International Journal of Information Security Science, cilt 4, no. 2, pp. 69-80, 2015.

[5] N. Barışçı ve S. Sarıkaya, "Real-Time Multiple Objects Detection Using Yolo and Retinanet From Video and Camera," Uppsala-SWEDEN, 2019. DOI:10.56979/601/2023

[6] A. Yazici, Koyuncu Murat, S. A. Sert ve T. Yilmaz, "A Fusion-Based Framework for Wireless Multimedia Sensor Networks in Surveillance Applications," IEEE Access, cilt 7, pp. 88418-88434, 2019. DOI: 10.1109/ACCESS. 2019.2926206

[7] A. Stoica, D. Militaru, D. Moldoveanu ve A. Popa, "TACTICAL DATA LINK – FROM LINK 1 TO LINK 22," Sci. Bull. Mircea cel Batran Naval Acad, cilt 19, no. 2, pp. 316-322, 2016. DOI: 10.21279/1454-864x-16-i2-046.

[8] J. Schubert, J. Brynielsson, M. Nilsson ve P. Svenmarck, "Artificial Intelligence for Decision Support in Command and Control Systems," 23rd International Command and Control Research & Technology Symposium "Multi-Domain C2", 2018.

[9] N. Suri, G. Benincasa, R. Lenzi, M. Tortonesi, C. Stefanelli ve L. Sadler, "Exploring value-of-information-based approaches to support effective communications in tactical networks," IEEE Communications Magazine, cilt 53, no. 10, pp. 39-45, 2015. DOI: 10.1109/ MCOM.2015.7295461

[10] I. Ahmad, K. Shah ve S. Ullah, "Military Applications using Wireless Sensor Networks: A survey," International Journal of Engineering Science and Computing, cilt 6, no. 6, pp. 7039-7043, June 2016.

[11] L. Chen, S. Li, Q. Bai, J. Yang, J. Sanlong ve Miao Yanming, "Review of Image Classification Algorithms Based on Convolutional Neural Networks," Remote

Sensing, cilt 13, no. 22, p. 4712, 2012. DOI: 10.3390/rs13224712.

[12] J. Saxe ve K. Berlin, "Deep neural network based malware detection using two dimensional binary program features," 10th International Conference on Malicious and Unwanted Software (MALWARE), Fajardo, PR, USA, 2015. DOI:10.1109/MALWARE.2015.7413680.

[13] J. Romeo, "The coming of age of artificial intelligence," 20 April 2023. https://www.militaryaerospace.com/computers/article/14290944/artificial-intelligence-machine-learning. (01.06.2023).

[14] E. Granger, J. F. Connolly ve R. Sabourin, "A Comparison of Fuzzy ARTMAP and Gaussian ARTMAP Neural Networks for Incremental Learning," IEEE International Joint Conference on Neural Networks (IEEE World Congress on Computational Intelligence), Hong Kong, China, 2008. DOI: 10.1109/IJCNN.2008.4634267.

[15] M. Coşkun, A. Uçar, Ö. Yıldırım ve Y. Demir, "Face recognition based on convolutional neural network," Face recognition based on convolutional neural network, Kremenchuk, Ukraine, 2017. DOI: 10.1109/MEES.2017.8248937.

[16] S. Lawrence, L. Giles, A. C. Tsoi ve A. D. Back, "Face recognition: a convolutional neural-network approach," IEEE Transactions on Neural Networks, cilt 8, no. 1, pp. 98-113, January 1997. DOI: 10.1109/72.554195.

[17] P. Kamencay, M. Benco, T. Mizdos ve R. Radil, "A New Method for Face Recognition Using Convolutional Neural Network," Advances In Electrical And Electronic Engineering, cilt 15, no. 4, pp. 663-672, 2017. DOI:10.15598/aeee.v15i4.2389.

[18] J. Redmon, S. Divvala, R. Girshick ve A. Farhadi, "You Only Look Once: Unified, Real-Time Object Detection," IEEE Conference on Computer Vision and Pattern Recognition (CVPR), 2016. DOI:10.1109/CVPR.2016.91.

[19] Z. Feng, X. Zhu, L. Xu ve Y. Liu, "Research on Human Target Detection and Tracking Based on Artificial Intelligence Vision," IEEE Asia-Pacific Conference on Image Processing, Electronics and Computers (IPEC), Dalian, China, 2021. DOI:10.1109/IPEC51340.2021.9421306.

[20] A. Rohan, M. Rabah ve S.-H. Kim, "Convolutional Neural Network-Based Real-Time Object Detection and Tracking for Parrot AR Drone 2," IEEE Access, pp. 69575-69584, 2019. DOI:10.1109/ACCESS.2019.2919332.

[21] Y. Chen, X. Yang, B. Zhong, S. Pan, D. Chen ve H. Zhang, "CNNTracker: Online discriminative object tracking via deep convolutional neural network," Applied Soft Computing, cilt 38, pp. 1088-1098, 2016. DOI: 10.1016/j.asoc.2015.06.048.

[22] Y. Wang, X. Luo, L. Ding, S. Fu ve X. Wei, "Detection based visual tracking with convolutional neural network," Knowledge-Based Systems, cilt 175, pp. 62-71, 2019. DOI: 10.1016/j.knosys.2019.03.01.

[23] M. A. Demirtaş, "Derin Öğrenme Yöntemleri ile 3B Nokta Bulutlarının Semantik Segmentasyonuna Genel bir Bakış," Duzce University Journal of Science and Technology, cilt 11, no. 1, pp. 342-357, 2023. DOI: 10.29130/dubited.1004211.

[24] O. Güler ve İ. Yücedağ, "Derin Öğrenme İle El Hareketi Tanıma Üzerine Yapılan Çalışmaların İncelenmesi" 21. Akademik Bilişim konferansı., 2019.

[25] L. Zhang, Z. Sheng, Y. Li, Q. Sun, Y. Zhao ve D. Feng, "Image object detection and semantic segmentation based on convolutional neural network," Neural Comput & Applic, p. 1949–1958, 2020. DOI:10.1007/s00521-019-04491-4.

[26] M. Ren, W. Zeng, B. Yang ve R. Urtasun, "Learning to Reweight Examples for Robust Deep Learning," 35th International Conference on Machine Learning, Stockholm, Sweden, 2018.

[27] B. R. Kiran, I. Sobh, V. Talpaert, P. Mannion, A. A. A. Sallab, S. Yogamani ve P. Pérez, "Deep Reinforcement Learning for Autonomous Driving: A Survey," EEE Transactions on Intelligent Transportation Systems, cilt 23, no. 6, pp. 4909-4926, Haziran 2022. DOI: 10.1109/TITS.2021.3054625.

[28] X. Zhou, W. Gong, W. Fu ve F. Du, "Application of deep learning in object detection," 16th International Conference on Computer and Information Science (ICIS), Wuhan, China, 2017. DOI:10.1109/ICIS.2017. 7960069.

[29] M. Bistron ve Z. Piotrowski, "Artificial Intelligence Applications in Military Systems and Their Influence on Sense of Security of Citizens," Electronics, cilt 10, no. 7, p. 871, 2021. DOI:10.3390/electronics10070871.

[30] S. Joshi, A. Thakar ve C. Patel, "Applications of Machine Learning and Deep Learning in Securing Internet of Battlefield Things: A Futuristic Perspective," 10th International Conference on Computing for Sustainable Global Development (INDIACom), Delhi, India, 2023.

[31] P. F. Lamas, L. C. Ribas, A. M. Mendez ve J. C. Albar, "Evolving Military Bradband Wireless Communication Systems: WiMAX, LTE and WLAN," International Conferance on Military Communications and Information Systems (ICMCIS), Brüksel, Belçika, 2016. DOI: 10.1002/9781119892199.ch20

[32] M. N. Sadiku, O. I. Fagbohungbe ve S. M. Musa, "Artificial intelligence in cyber security," International Journal of Engineering Research and Advanced Technology, cilt 6, no. 5, pp. 1-7, 2020. DOI:10.1088/1742-6596/1964/4/042072

[33] M. M. Yamin, M. Ullah ve B. Katt, "Weaponized AI for cyber attacks," Journal of Information Security and Applications, cilt 57, 2021. DOI:10.1016/j.jisa.2020.102722

[34] A. Gökdemir ve A. Çalhan, "Deep learning and machine learning based anomaly detection in internet of things environments," Journal of the Faculty of Engineering and Architecture of Gazi University, cilt 37, no. 4, pp. 1945-1956, 2022. DOI: 10.17341/gazimmfd.962375

[35] D. Tsadikovich, E. Levner ve H. Tell, "AI-Based Integrated Scheduling of Production and Transportation Operations within Military Supply Chains," Advances in Artificial Intelligence: 9th Mexican International Conference on Artificial Intelligence, MICAI, Berlin, 2010. DOI: 10.1007/978-3-642-16761-4_19.

[36] N. Abell, "7 Key Military Applications of Machine Learning," 2 October 2020. https://medium.com/@nqabell89/7-key-military-

applications-of-machine-learning-9818dfa2ea86. (08.08.2023).

[37] M. Woschank, E. Rauch ve H. Zsifkovits, "A Review of Further Directions for Artificial Intelligence, Machine Learning, and Deep Learning in Smart Logistics," Sustainability, cilt 12, no. 9, p. 3760, 2020. DOI:10.3390/su12093760.

[38] S. C. Shu ve T. H. Xing, "Application of AI in Modern Logistics Systems," 11th International Conference on Information Technology in Medicine and Education (ITME), Wuyishan, Fujian, China, 2021. DOI:10.1109/ITME53901.2021.00015.

[39] C. Crosby, "Operationalizing Artificial Intelligence for Algorithmic Warfare," July-August 2020. https://www.armyupress.army.mil/Journals/Military-Review/English-Edition-Archives/July-August-2020/Crosby-Operationalizing-AI/. (09.08.2023).

[40] S. Fei-fei, Z. Zhi-Min, W. Yue-liang, X. Yang, Z. Fan ve N. Huan-sheng, "Application progress of artificial intelligence in military confrontation." Chinese journal of engineering, cilt 42, no. 9, pp. 1106-1118, 2020. DOI: 10.13374/j.issn2095-9389.2019.11.19.001.

[41] B. L. Yoon, "Artificial neural network technology," ACM SIGSMALL/PC Notes, vol. 15, no. 3, pp. 3-16, Agust 1989.

[42] S. Yuan ve X. Wu, "Deep learning for insider threat detection: Review, challenges and opportunities," Computers & Security, cilt 104, 2021. DOI: 10.1016/j.cose.2021.102221.

[43] S. Panesar, C. Yvonne, D. Chander, J. Morey, J. Fernandez-Miranda ve M. Kliot, "Artificial Intelligence and the Future of Surgical Robotics," Annals of surgery, cilt 270, no. 2, pp. 223-226, 2019. DOI:10.1097/SLA. 0000000000003262.

[44] Y. Zhang, Z. Dai, L. Zhang, Z. Wang, L. Chen ve Y. Zhou, "Application of Artificial Intelligence in Military: From Projects View," 6th International Conference on Big Data and Information Analytics (BigDIA), Shenzhen, China, 2020. DOI:10.1109/BigDIA51454.2020. 00026.

[45] S. Bhavya and A. S. Pillai, "Prediction Models in Healthcare Using Deep Learning," in Proceedings of the 11th International Conference on Soft Computing and Pattern Recognition (SoCPaR 2019), 2020. DOI: 10.1007/978-3-030-49345-5_21.

[46] O. S. Pianykh, S. Guitron, D. Parke, C. Zhang, P. Pandharipande, J. Brink ve D. Rosenthal, "Improving healthcare operations management with machine learning," Nature Machine Intelligence, cilt 5, no. 2, pp. 266-273, 18 May 2020. DOI:10.1038/s42256-020-0176-3.

[47] V. P. Gurupur, S. A. Kulkarni, X. Liu, U. Desai ve A. Nasir, "Analysing the power of deep learning techniques over the traditional methods using medicare utilisation and provider data," Journal of Experimental & Theoretical Artificial Intelligence, cilt 31, no. 1, pp. 99-115, 2018. DOI:10.1080/0952813X.2018.1518999

[48] A. J. Fawkes, "Developments in Artificial Intelligence: Opportunities and Challenges for Military Modeling and Simulation." 017 NATO M&S Symposium, 2017.

[49] C. Tsatsoulis, "A Review Of Artificial Intelligence In Simulation," ACM SIGART Bulletin, cilt 2, no. 1, p. 115–121, 1991. DOI: 10.1145/122388.106234

[50] J. L. Burbank, P. F. Chimento, B. K. Haberman ve W. T. Kasch, "Key Challenges of Military Tactical Networking and the Elusive Promise of MANET Technology," IEEE Communications Magazine, cilt 44, no. 11, pp. 39-45, November 2006. DOI: 10.1109/COM-M.2006.24815.

[51] M. A. Ali, Q. Guan, R. Umer, W. J. Cantwell ve T. Zhang, "Deep learning based semantic segmentation of μCT images for creating digital material twins of fibrous reinforcements," Composites Part A: Applied Science and Manufacturing, cilt 139, December 2020. DOI: 10.1016/j.compositesa.2020.106131.

[52] M. Bistron ve Z. Piotrowski, "Artificial Intelligence Applications in Military Systems and Their Influence on Sense of Security of Citizens," Electronics, cilt 10, no. 7, pp. 127-145, 2021. DOI:10.3390/electronics10070871.

[53] A. Kim, Y. Yang, S. Lessmann, T. Ma, M. -C. Sung ve J. E. Johnson, "Can deep learning predict risky retail investors? A case study in financial risk behavior forecasting," European Journal of Operational Research, cilt 283, no. 1, pp. 217-234, 16 May 2020. DOI:10.1002/isaf. 1532.