T.C.

İNÖNÜ ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

YAPAY ZEKÂNIN SİBER TERÖRİZM ÜZERİNDEKİ ETKİSİ

YÜKSEK LİSANS TEZİ

DANIŞMAN

Dr. Öğr. Üyesi Emin GİTMEZ

HAZIRLAYAN

Cumali Cem DOĞAN

MALATYA-2025

T.C.

İNÖNÜ ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

YAPAY ZEKÂNIN SİBER TERÖRİZM ÜZERİNDEKİ ETKİSİ

YÜKSEK LİSANS TEZİ

HAZIRLAYAN

Cumali Cem DOĞAN

DANIŞMAN

Dr. Öğr. Üyesi Emin GİTMEZ

MALATYA-2025

ONUR SÖZÜ

Yüksek lisans tezi olarak sunduğum "**Yapay Zekânın Siber Terörizm Üzerindeki Etkisi**" başlıklı bu çalışma, İnönü Üniversitesi Sosyal Bilimler Enstitüsü Tez Yazım Yönergesi'ne uygun olarak hazırlanmış olup; tezimin akademik ve etik kurallara uygun olarak hazırlandığını, kullanılan kaynakların kaynakçada belirtilenlerden oluştuğunu ve bu eserlerin hepsine de atıfta bulunduğumu belirtir, aksi bir durum halinde aleyhime doğabilecek tüm hak kayıplarını kabullendiğimi beyan ederim**.**

Cumali Cem DOĞAN

ÖNSÖZ

Yapay zekânın siber terörizm üzerindeki etkilerini incelemek amacıyla hazırlanan bu tezin tamamlanma süreci hem dünyaya hem de teknolojiye olan bakış açımı derinden etkileyen zorluklarla geçmiştir. 06 Şubat 2023 tarihinde meydana gelen yıkıcı depremler, benim de dahil olduğum sayısız hayatı derinden etkilemiş ve böylesi afetleri önceden öngörüp etkilerini hafifletebilecek yenilikçi çözümlere duyulan ihtiyacı açığa çıkarmıştır. Bu noktada yapay zekânın benzersiz yetenekleri sayesinde sismik veriler analiz edilerek depremler öngörebilir ve deprem bölgelerinde yaşayanlar için bir umut ışığı olabilir. Yine bu süreçte kanser hastalığına yakalanarak yedi ay mücadele ettikten sonra Temmuz 2024'de vefat eden babam yetişememiş olsa da yapay zekânın erken tanı ve kişiselleştirilmiş tedavi konularındaki yetenekleri, sağlık sonuçlarını dönüştürebilecek, sayısız birey ve ailenin acısını hafifletebilecek güçtedir. Yapay zekâ, bir taraftan insan yaşamına dair umut vadederken diğer taraftan kötüye kullanımı nedeniyle insan yaşamını tehdit etme potansiyeli düşündürücü ve üzücüdür.

Öncelikle kendileri de depremi yaşamış olmalarına rağmen, çalışmam süresince bana yol gösteren, desteğini esirgemeyen ve akademik çalışmamdan kopmamamı sağlayan tez danışmanım Dr. Öğr. Üyesi Emin GİTMEZ'e ve yüksek lisans eğitimim boyunca bilgisini, tecrübesini ve desteğini esirgemeyen değerli hocam Doç. Dr. Osman AĞIR'a en derin teşekkürlerimi sunarım. Çalışmam sırasında beni bilgi ve tecrübeleriyle yönlendiren, telefonlarımı hiç cevapsız bırakmayan ve bana sabır gösteren değerli arkadaşlarım Doç. Dr. Mehmet ALTUĞ'a ve Dr. Fatih PEHLİVAN'a, bu yolculuğa birlikte başladığımız ve tez yazım sürecinde birbirimize sürekli destek olduğumuz değerli dostum M.Kemal AYCAN'a, göstermiş oldukları anlayıştan dolayı mesai arkadaşlarıma, kızım Vuslat DOĞAN'a, oğlum C.Gürsel DOĞAN'a ve yaşadığım tüm zorlu zamanlarda olduğu gibi bu zorlu dönemde de yanımda olan en büyük destekçim sevgili eşim Esra DOĞAN'a sonsuz teşekkürlerimi sunuyorum. Bu tez çalışmasını rahmetli babam C. Gürsel DOĞAN'a ve 06 Şubat 2023 tarihinde meydana gelen depremde hayatını kaybeden yurttaşlarıma ithaf ediyorum.

Cumali Cem DOĞAN

Malatya-2025

ÖZET

YAPAY ZEKÂNIN SİBER TERÖRİZM ÜZERİNDEKİ ETKİSİ

Cumali Cem DOĞAN

Yüksek Lisans Tezi

Danışmanı: Dr. Öğr. Üyesi Emin GİTMEZ

İnönü Üniversitesi Sosyal Bilimler Enstitüsü

Siyaset Bilimi ve Kamu Yönetimi Anabilim Dalı, Güvenlik ve Terör Bilim Dalı

Bu çalışma, yapay zekâ (YZ) teknolojilerinin siber terörizmde nasıl kullanıldığını incelemektedir. Çalışmanın temel amacı, YZ'nin terör grupları tarafından propaganda, finansman, örgüte yeni üye kazandırma, siber ve fiziksel saldırılar gibi alanlarda nasıl kullanıldığını ortaya koymak ve oluşturduğu riskleri değerlendirmektir. Çalışmanın verileri alanyazın taraması, uluslararası raporlar ve somut olay analizleri yoluyla elde edilmiştir. Çalışmada yapay zekâ kavramı ve tarihçesi üzerinde durulmuş, yapay zekânın kullanıldığı teknolojilerden Nesnelerin İnterneti, Blokzincir, Robotik ve Otonom Sistemler, Akıllı Şehirler ve İnsansız Hava Araçları gibi konular araştırma kapsamında incelenmiştir. Daha sonra terör, terörizm kavramları, siber uzay ve siber saldırı yöntemleri ele alınmış, yapay zekâ teknolojilerinin terörist gruplar tarafından nasıl kullanıldığı ayrıntılı olarak incelenmiş, yapay zekâ destekli propaganda, dezenformasyon ve radikalleşme faaliyetleri, terörizmin finansman süreçlerindeki rolü, siber ve fiziksel saldırı teknikleri analiz edilmiştir. Bulgular, YZ'nin özellikle üretken yapay zekâ (GenAI), deepfake teknolojisi ve otomatik botlar aracılığıyla terör örgütlerinin propaganda ve örgüte yeni üye kazandırma stratejilerini güçlendirdiği, terörizm finansmanına araç sağladığı, siber ve fiziksel saldırı yöntemlerinin geliştirdiğini göstermektedir. Sonuç olarak, YZ teknolojilerinin terörist gruplar tarafından kullanımı; dezenformasyon kampanyaları, siber saldırılar ve İHA tabanlı fiziksel saldırılar gibi geniş bir tehdit yelpazesi oluşturmaktadır. Bu teknolojilerin kötüye kullanımını önlemek amacıyla, devletlerin YZ teknolojilerinin geliştirilmesi ve kullanılmasına yönelik

düzenlemeler oluşturması, YZ'nin potansiyel riskleri hakkında farkındalık oluşturacak eğitimlerin düzenlenmesi, uluslararası iş birliğinin artırılması, siber güvenlik politikalarının güçlendirilmesi gerekmektedir.

Anahtar Kelimeler: Yapay Zekâ, Siber Terörizm, Siber Saldırı, İnsansız Hava Araçları, Deepfake, Kripto Para, Propaganda.

ABSTRACT

The Impact of Artificial Intelligence on Cyber Terrorism

This study examines how artificial intelligence (AI) technologies are used in cyber terrorism. The main purpose of the study is to reveal how AI is used by terrorist groups in areas such as propaganda, financing, recruitment, cyber and physical attacks and to evaluate the risks it poses. The data of this study were obtained from literature review, international reports and case studies. In the study, the concept of artificial intelligence and its history were emphasised, and topics such as the Internet of Things, Blockchain, Robotics and Autonomous Systems, Smart Cities and Unmanned Aerial Vehicles were examined within the scope of the research, Then, the concepts of terrorism, terrorism, cyberspace and cyber-attack methods were discussed; how artificial intelligence technologies are used by terrorist groups was examined in detail; and artificial intelligence-supported propaganda, disinformation and radicalisation activities, the role of terrorism in financing processes, cyber and physical attack techniques were analysed. The findings show that AI, especially generative artificial intelligence (GenAI), strengthens terrorist organisations' propaganda and recruitment strategies through deepfake technology and automated bots, and that it provides tools for terrorism financing, and develops cyber and physical attack methods. As a result, the use of AI technologies by terrorist groups poses a wide range of threats, from disinformation campaigns to cyber attacks and UAV-based physical attacks. In order to prevent the misuse of these technologies, governments should establish regulations for the development and use of AI technologies, organise trainings to raise awareness about the potential risks of AI, increase international cooperation, and strengthen cyber security policies.

Key Words: Artificial Intelligence, Cyber Terrorism, Cyber Attack, Unmanned Aerial Vehicles, Deepfake, Cryptocurrency, Propaganda.

İÇİNDEKİLER

TABLOLAR LİSTESİ

KISALTMALAR LİSTESİ

TVZ : Türkiye Zekâ Vakfı

YZ : Yapay Zekâ

ABD : Amerika Birleşik Devletleri

ANI : Dar Yapay Zekâ

ASI : Süper Yapay Zekâ

AGI : Genel Yapay Zekâ

ML : Makine Öğrenmesi

DL : Derin Öğrenme

NLP : Doğal Dil İşleme

CV : Bilgisayar Görüşü

IoT : Nesnelerin İnterneti

RFID : Radyo Frekanslı Tanımlama

AIoT : Nesnelerin Yapay Zekâsı

İHA : İnsansız Hava Aracı

UAB : Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı

WEF : Dünya Ekonomik Forumu

DoS : Hizmet Dışı Bırakma

DDoS : Dağıtık Hizmet Dışı Bırakma

SQL : Yapısal Sorgu Dili

FBI : Amerikan Federal Soruşturma Bürosu

NATO : Kuzey Atlantik Konseyi

UNCCT : Birleşmiş Milletler Terörle Mücadele Merkezi

UNICRI : Birleşmiş Milletler Bölgelerarası Suç ve Adalet Enstitüsü

IŞİD : Irak ve Şam İslam Devleti

GenAI : Üretken Yapay Zekâ

GAN : Üretken Çelişkili Ağlar

FETÖ : Fethullahçı Terör Örgütü

AWS : Otonom Silah Sistemleri

SİHA : Silahlı İnsansız Hava Araçlarının

BM : Birleşmiş Milletler

UNOCT : Birleşmiş Milletler Terörle Mücadele Ofisi

CAR : Çatışma Silahlanma Araştırması

CAPTCHA : Bilgisayarları ve İnsanları Ayrı Algılamak İçin Tamamen Otomatik Kamu Turing Testi

ŞEKİLLER LİSTESİ

1. GİRİŞ

Teknolojik gelişmelerin hayatımızın her alanına nüfuz ettiği günümüzde, yapay zekâ (YZ) ve siber terörizm küresel güvenlik ve toplumsal düzen açısından önemli tartışma konuları haline gelmiştir. Özellikle son yirmi yılda dijital teknolojilerin hızlı gelişimi, devletler ile insanlar arasındaki etkileşim biçimlerini dönüştürmekte, bununla birlikte yeni tehdit alanlarını da beraberinde getirmektedir. Bu tehdit alanlarından biri de terörizmdir. Terörizm tarih boyunca toplumları etkileyen ve uluslararası güvenliği tehdit eden bir olgu olarak varlığını sürdürmektedir. Terörizmin geleneksel sınırlarını aşarak dijital dünyaya taşınması, siber uzayın bir mücadele alanı haline gelmesine sebep olmuştur. Siber terörizm, terör örgütlerinin ideolojilerini yayma ve örgüte yeni üye kazandırma da yeni stratejiler geliştirmelerine olanak tanımaktadır. Ayrıca ekonomik kalkınmayı engellemekten devletlerin kritik alt yapı ve tesislerini hedef almaya, insanların kişisel güvenliğini tehdit etmeye kadar geniş bir yelpazede etkili olabilmektedir. Yapay zekâ teknolojisinin sunmuş olduğu yetenekler ise bu bağlamda hem büyük fırsatlar hem de ciddi riskler yaratmaktadır.

Günümüzde teknolojik dönüşümün merkezinde yer alan yapa zekâ; büyük verilerin analizi, doğal dil işleme, yüz tanıma ve bağımsız karar alma gibi yetenekleriyle sağlık, savunma ve ekonomik alanlarda benzersiz bir verimlilik ve katkı sunmaktadır. Yapay zekânın dönüştürücü etkisi, tıpta erken teşhis yöntemleri, endüstride otomasyon sistemleri, eğitim ve öğretimde kişiselleştirilmiş öğrenme platformları ve savunma sistemleri uygulamalarına kadar geniş bir yelpazeye yayılsa da aynı zamanda kötü niyetli aktörlerin elinde yıkıcı bir silah haline dönüşebilmektedir (Blauth vd., 2022:77110).

Yapay zekâ teknolojilerinin terörist faaliyetlerde kullanımı, bu grupların propaganda, radikalleşme, finansman sağlama, saldırı yeteneklerinin geliştirilmesi ve operasyonel koordinasyon gibi alanlarda etkinliğini artırmaktadır. Yapay zekânın kötüye kullanımı, bireylerin ve devletlerin güvenliğini tehdit eden ciddi bir sorun olarak karşımıza çıkmaktadır. Bu bağlamda, YZ yalnızca terörizm operasyonlarını kolaylaştırmakla kalmamakta, aynı zamanda dezenformasyon kampanyalarıyla toplumsal güveni zedeleme ve ulusal güvenlik stratejilerini yıpratma potansiyeli taşımaktadır. Özellikle

deepfake teknolojisi gibi araçlar, terörist grupların sahte içerikler oluşturarak toplumları manipüle etmesini mümkün kılmaktadır (Esmailzadeh ve Motaghi, 2024:169).

Yapay zekâ destekli siber terörist saldırılar, dezenformasyon kampanyaları, örgüte yeni üyelerin kazandırılması için geliştirilen stratejiler, finansal manipülasyonlar ve otonom silahların kullanımı bu teknolojinin iki yüzlü doğasını gözler önüne sermektedir. Bu nedenle, Yapay zekâ ve siber terörizm arasındaki ilişkinin incelenmesi hem bilimsel literatürdeki boşlukları doldurmak hem de günümüz tehditlerini anlamak adına önem arz etmektedir.

Bu çalışma, yapay zekânın siber terörizm bağlamında nasıl kullanıldığını ve doğurabileceği olası sonuçları ele almaktadır. Araştırmanın temel sorunsalı, yapay zekâ teknolojilerinin siber terörizmi nasıl dönüştürdüğü ve bu dönüşümün insanlar ile devletlerin güvenliği üzerindeki etkileridir. Teknolojinin terör örgütleri tarafından propaganda, finansman ve saldırı süreçlerinde kullanımı, devletlerin güvenlik stratejilerini yeniden yapılandırmasını gerekli kılmaktadır. Bu çalışma şu araştırma sorularına odaklanmaktadır:

1- Yapay zekâ teknolojileri, terör örgütlerinin propaganda ve dezenformasyon faaliyetlerinde nasıl bir rol oynamaktadır?
2- Yapay zekâ destekli siber terörizm saldırıları hangi teknikler ve yöntemlerle gerçekleştirilmektedir?
3- YZ teknolojilerinin kullanımı, terörizmin finansman süreçlerini nasıl etkilemektedir?
4- Deepfake teknolojisi gibi yapay zekâ araçlarının, radikalleşme ve örgüte yeni üyelerin kazandırılması süreçlerindeki etkileri nelerdir?

Bu sorular ışığında araştırmanın temel amacı, yapay zekâ ve siber terörizm arasındaki ilişkiyi ortaya koyarak, mevcut güvenlik politikalarının yeniden değerlendirilmesine katkıda bulunmaktır.

Mevcut çalışmalar, genel olarak siber saldırılara karşı bilgisayar sistemlerinin ve ağlarının güvenliğini ve dayanıklılığını artırmak için makine öğrenimi (ML) ve diğer yapay zekâ tekniklerinin kullanımını ifade eden savunma amaçlı yapay zekânın benimsenmesine odaklanmıştır. Yapay zekâ ile siber terörizm arasındaki bağlantıyı

doğrudan ele alan kapsamlı teorik çalışmaların eksikliği dikkat çekicidir. Önceki araştırmalar, YZ'nin terörizmle mücadele aracı olarak kullanımı üzerine yoğunlaşmış olsa da, teknolojinin hızlı ilerlemesi bu konudaki analizleri sürekli olarak güncelleme ihtiyacını doğurmaktadır. Literatürde, özellikle deepfake teknolojileri, yapay zekâ destekli botlar ve siber güvenlik açıklarına ilişkin çalışmalar sınırlı kalmakta; bu durum, YZ ve siber terörizm arasındaki ilişkinin tam olarak anlaşılamamasına yol açmaktadır.

Bu çalışma, yapay zekâ teknolojilerinin siber terörizm bağlamında sunduğu yeni riskleri ve tehditleri analiz ederek hem bilimsel literatüre hem de uygulamaya katkıda bulunmayı amaçlamaktadır. Bilimsel açıdan, çalışmanın sunduğu analiz, yapay zekânın terörizme entegrasyonu konusundaki boşlukları doldurmayı, pratik açıdan ise, devletlerin siber güvenlik politikalarını güçlendirme ve yapay zekâ teknolojilerini etik sınırlar içinde kullanma gerekliliğine dikkat çekmeyi hedeflemektedir. Çalışma, YZ ve siber terörizm ilişkisini hem teorik hem de uygulamalı bir perspektiften inceleyerek günümüz güvenlik tehditlerini anlama ve bu tehditlere karşı geliştirilebilecek stratejiler konusunda kapsamlı bir çerçeve sunmaktadır.

Çalışma, yedi ana bölümden oluşmaktadır. Birinci bölüm olan "Giriş"te, araştırmanın genel çerçevesi, önemi, sorunsalı ve amaçları açıklanmaktadır. İkinci bölümde, "Yapay Zekâ" başlığı altında yapay zekânın kavramı ve tarihçesi açıklanmıştır. Üçüncü bölümde "Yapay Zekâ ve Yeni Nesil Teknolojiler" başlığı altında yapay zekânın kullanıldığı teknolojilerden konuyla ilişkili sınırlama getirilerek, Nesnelerin İnterneti, Blok zincir, Robotik ve Otonom Sistemler, Akıllı Şehirler ve İnsansız Hava Araçları ele alınmıştır. Dördüncü bölümde "Terör ve Siber Terörizm" başlığı altında terör ve terörizm kavramları, siber uzay ve siber saldırı yöntemleri ele alınmıştır. Beşinci bölümde "Yapay Zekânın Siber Terörizm Üzerindeki Etkisi" başlığı altında, yapay zekâ teknolojilerinin terörist gruplar tarafından nasıl kullanıldığını detaylı bir şekilde ele alınarak, yapay zekâ destekli propaganda, dezenformasyon ve radikalleşme faaliyetleri incelenmektedir. Yapay zekânın terörizmin finansman süreçlerindeki rolünü analiz etmektedir. Yapay zekâ destekli siber saldırı teknikleri ve güvenlik zafiyetleri üzerinde durulmaktadır. Altıncı bölümde geleneksel terörizm, siber terörizm ve yapay zekâ destekli siber terörizmin karşılaştırması yapılmıştır. Son olarak yedinci bölümde, çalışmanın genel değerlendirmesi yapılmakta ve öneriler sunulmaktadır.

2. YAPAY ZEKÂ

2.1.Yapay Zekâ Kavramı ve Tarihçesi

Yapay Zekâ (YZ) kavramının doğru anlaşılması ve tanımlaması için öncelikle tarihsel sürecine bakmak ve "zekâ" kavramını tanımını yapmak önemlidir. Türkiye Zekâ Vakfı (TZV) zekâ'yı "*Bireyin algısal ve kavramsal süreçlerini kullanarak somut ve soyut nesneler arasındaki bağlantıyı anlama, bilişsel fonksiyonlarını belirli bir amaca yönelik kullanabilme yeteneği*" olarak tanımlamaktadır (TZV, 2024).

İnsanlık tarihine bakıldığı zaman bugünkü gelişmişlik düzeyinin ve ilerlemenin bilişsel temelli olduğu görülmektedir (Yıldırım, 2023:124). Bu gelişmişlik insan zekâsının etkin kullanımının bir sonucudur. Yüzyıllar boyunca insanoğlu toplumsal hafıza sayesinde hayata dair tecrübelerini geleceğe aktarmayı başarmıştır. İnsanlık bütün bu birikimleri sayesinde gelişmişlik düzeyine, küreselleşmeye doğrudan etki eden ve hayatı kolaylaştıran makineleşme sürecine tanıklık etmiştir. Bilgisayarın insan hayatına girmesi ile birlikte verilerin toplanması ve işlenmesi süreci daha kolay ve hızlı hale gelmiş, insanlık tarihine önemli yansımaları olmuştur (Doğan ve Alaca, 2020:383-384).

YZ'nın temelleri, modern bilgisayarların ortaya çıkışından çok daha önce atılmıştır. Fakat bilgisayarların ortaya çıkması ile YZ teknolojisinin gelişimi arasında güçlü bağlar bulunmaktadır (Warwick, 2023:10). 1824 yılında "matematiksel ve astronomik tabloları hesaplamak için bir motor icadı" çalışması ile İngiliz matematikçi, filozof, mühendis Charles Babbage tarafından makinelerin işlem yapması düşüncesi üzerine çalışmalar yapılmıştır. Babbage, bilim dünyası tarafından modern yazıcı, hesap makinelerinin ve analitik bilgisayarların öncüsü olarak kabul edilmektedir. Babbage'nin çalışmaları ölümü ile yarıda kalmıştır (Guliyeva, 2024:48). 1940'larda araştırmacılar insan zekâsını taklit edebilen makineler yaratma konseptini keşfetmeye başlamıştır. 1943 yılında nörofizyolog Warren McCulloch ve matematikçi Walter Pitts birlikte yapay nöron kavramını ortaya atarak sinir ağlarının temellerini oluşturmuşlardır (Rudrawar ve Parsewar, 2023:11).

1950 yılında, Bilgisayar Bilimi ve YZ'nın öncüsü olarak kabul edilen İngiliz matematikçi ve bilgisayar bilimcisi olan Alan Mathison Turing "Computing Machines and Intelligence" adlı makalesini Mind dergisinde yayınlanmıştır. Makalede o dönemler

devrim niteliğinde olan ve yeni ufuklar açan “Bir Makine düşünebilir mi?” sorusunu cevaplamaya çalışmıştır. Akıllı makineler geliştirmek için bir çerçeve sunmuş ve zekâlarını ölçmek için yöntemler önermiştir. Ayrıca makine zekasının ölçüsü olarak "Turing Testi" yöntemini önermiştir (Grzybowski, vd., 2024:224).

Her ne kadar YZ’nin fikir sahibi Alan Turing olsa da YZ teriminin literatüre girişi, 1956 yılında John McCarthy önerisi ile bir grup bilim adamı tarafından Amerika Birleşik Devletleri (ABD)’deki Dartmouth Koleji’nde düzenlenen konferansta olmuştur. Konferansta “Artificial Intelligence” yani YZ yeni bir bilim alanı olarak tanıtılmış, bilim dünyasına zekâ ile donatılmış bilgisayar programlarının gerçekleşme olasılığının araştırılması önerilmiştir (Darıcalı, 2020:2).

Turing'in çalışmalarından sonra bilim adamları YZ sistemlerini geliştirmede önemli ilerlemeler kaydetmişlerdir. 1955'de Allen Newell ve J.C. Shaw tarafından matematiksel teoremleri kanıtlayabilen bir program olan Logic Theorist geliştirildi. 1957'de Newell ve Herbert Simon tarafından bir dizi kural arasında arama yapıp ve mantıksal çıkarımlar yapan “Genel Problem Çözücü” geliştirildi. 1960'larda YZ’ye olan ilgi arttı ve araştırmacılar daha gelişmiş sistemler ve uygulamalar geliştirmek için çalıştı. 1965'de organik bileşiklerin moleküler yapısını belirlemek için Edward Feigenbaum ve Joshua Lederberg tarafından Dendral adlı ilk uzman sistemin geliştirildi (Banafa, 2024:2).

1970’li yıllarda Prolog programlama dilinin geliştirilmesi, araştırmacılara sembolik bilgi kullanılarak ifade ve akıl yürütmelerine imkânı sağladı. 1980’li yıllarda beynin yapısı ve işleyişi örnek alınarak yapay sinir ağlarına olan ilgi yeniden canlandı. Bu yıllarda yapay sinir ağlarının öğrenmesini sağlayan geri yayılım tekniği yeniden keşfedilerek katmanlı yapay sinir ağlarına geçilerek daha etkili öğrenme sağlandı. Ancak, sınırlı hesaplama gücü, büyük veri kümelerinin kullanımı ve yetersizlik nedeniyle yapay sinir ağlarına olan ilgi tekrar azalmıştır. 1990’lı yıllarda makine öğrenmesi yaklaşımları ön plana çıkarak verilerden otomatik olarak desenler öğrenebilen algoritmalara yönelim olmuştur. Bu süreçte bayes ağları, karar ağaçları ve destek vektör makineleri gibi teknikler çeşitli uygulamalarda popülerlik kazanmıştır. Veri odaklı yaklaşımlar, desen tanıma, konuşma ve el yazısı tanıma ve doğal dil işleme gibi alanlarda başarılı olmuştur. Satranç ustası Garry Kasparov’un 1997 yılında IBM'in Deep Blue oyununda yenilmesi hesaplamalı zekânın potansiyelini ortaya koymuştur. Çok katmanlı yapay sinir ağlarının,

(görüntü tanıma, ses ve doğal dil işleme) derin öğrenme, büyük verinin ortaya çıkması ve hesaplama gücündeki gelişmeler yeniden canlanmasına sebep olmuştur. Görüntü sınıflandırmada 2012 yılında Alex Net, 2016 yılında Go oyununda dünya şampiyonunu yenen Google'ın AlphaGo ve 2018 yılında doğal dil işleme alanında Open AI'nin GPT modelleri gibi çığır açıcı buluşlar ortaya çıkmıştır (Rudrawar ve Parsewar, 2023:12-13). Günümüzde otonom arabalar, Siri ve Alexa gibi sesli asistanlar ve öneri sistemleri yaygın hale gelmiştir. YZ ayrıca sağlık, finans ve diğer sektörlerde de ilerleme kaydetmiştir (Banafa, 2024:3).

Bu bağlamda, YZ: İnsan zekâsı ile yapılacak görevlerin, bilgisayarlar tarafından insan zekâsı taklit edilerek yapılması olarak tanımlanmaktadır. YZ algoritma ve modelleri kullanarak, makinelerin akıl yürütmesini ve karar vermesini sağlar. YZ, birçok algoritma ve teknik kullanarak makinelerin problem çözme, görüntü tanıma, konuşma tanıma ve doğal dil işleme gibi insana özgü zihinsel yeteneklerini taklit etmesini sağlar. YZ sistemleri bu yetenekler sayesinde büyük miktarda veriyi analiz edebilir, anlamlı sonuçlar ve tahminler çıkarabilir, performansını otonom olarak değiştirebilir (Rudrawar ve Parsewar, 2023:14).

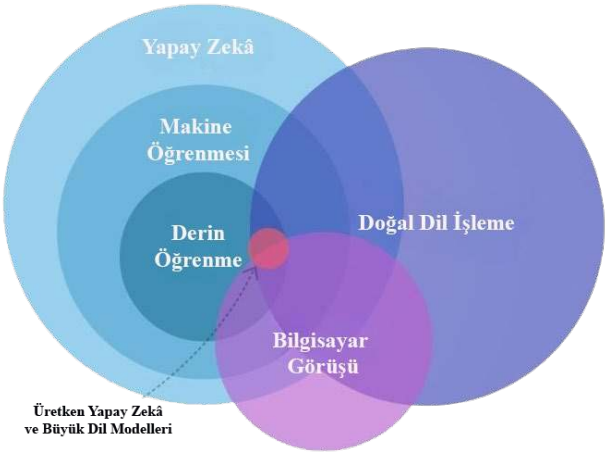
Bir YZ sisteminin yetenekleri, Dar Yapay Zekâ (ANI), Genel Yapay Zekâ (AGI) ve Süper Yapay Zekâ (ASI) olarak ayrım yapılarak ifade edilir. ANI yalnızca satranç oynamak veya karmaşık Çin oyunu Go gibi tek bir ana görevi yerine getirebilmektedir. Örnek olarak, IBM'in DeepBlue satranç programının 1996'da Garry Kasparov gibi dünya şampiyonunu yenmesi gösterilebilir. AGI ise günümüzde derin sinir ağı mimarisine dayalı destekli öğrenmeyi kullanarak oldukça farklı yöntemlerle çalışır. Örnek olarak, Google'ın DeepMind, AlphaGo Zero gibi YZ programları gösterilebilir. AlphaGo Zero'ya sadece Go oyununun temel kuralları verilmiş ve başka hiçbir talimat verilmeden kendi başına birkaç saat içinde Go oynamayı öğrenebilmiştir. AlphaGo Zero, 2017'de dünya şampiyonu Lee Sedol'u yenmesi de ayrıca dikkate değer bir teknolojik gelişmedir (Gordon, 2023:22).

Yapay Süper Zekâ ise şu anda mevcut olmasa da bazı bilim adamları gelecekte bir zaman yaratılabileceğini düşünmektedir. ASI kavramı her bakımdan insanlardan önemli ölçüde daha zeki olan makinelerin neredeyse tüm akıl yürütme görevinde insanlardan daha iyi performans gösterebileceği bir YZ geliştirme seviyesini tanımlamak için

kullanılmaktadır. YZ sistemlerinin üstün hesaplama yeteneklerine ek olarak yaratıcılık, duygusal zekâ gibi daha yüksek düzeyde zihinsel yeteneklere sahip olduğu konumu temsil etmektedir. ASI'nin temel özelliklerinden olan üstün zekâ ile en parlak insan zekâsının çok ötesinde bir kapasiteye sahip olacaktır. Karmaşık sorunları zahmetsizce çözecek, çığır açan buluşlar yapacak ve sonuçları benzersiz bir doğrulukla tahmin edecektir. Kendini Geliştirme özelliği ile ASI sistemleri sürekli kendini geliştirme yeteneğine sahip olacak ve bu da onların üstel bir oranda evrimleşmesini ve uyum sağlamasını sağlayacaktır. Ayrıca ASI mevcut YZ'lerden farklı olarak duygusal zekâ özelliği kazanarak insan duygularını ve sosyal nüansları anlayabilecektir. Hatta empati ve şefkati de simüle ederek insanlarla olan iletişimi ve iş birliği artacaktır. Otonom Karar özelliği ile kendi anlayışı ve hedefleri doğrultusunda otonom kararlar alabilecektir (Zohuri, 2023:1).

ASI, bilimsel çalışmaların hızını artırabilir, hastalıkları ortadan kaldırabilir, iklim değişikliği sorununu çözebilir, uzay araştırmaları gibi karmaşık zorlukların üstesinden gelebilir, endüstrilerde devrim yaratabilir, üretimi artırabilir ve iş piyasasını yeniden şekillendirebilir. Bu sayede insanlığın yararına olacak bir çok ilki gerçekletirebilir. Fakat ASI'nın küresel felakate yol açabilecek yüksek riskleri de içinde barındırdığı görülmektedir. Bu noktada ASI'nin etik kullanımını ve kontrolünü sağlamak son derece önemlidir, güçlü güvenlik önlemleri olmadan bilimkurgu senaryolarında tasvir edildiği gibi insanlık için varoluşsal riskler yaratabilir. ASI, dikkatli bir şekilde yönetilmezse önemli servet eşitsizliklerine ve insan değerleriyle uyumu konusunda endişelere yol açabilir, makinelerin entelektüel olarak üstün olduğu bir dünyadaki rolümüz hakkında sorular ortaya çıkararak insan toplumunu yeniden tanımlayabilir, kimlik, amaç ve hatta zihin kavramlarımıza meydan okuyabilir (Zohuri, 2023:2).

YZ, bir makinenin veya bilgisayar sisteminin öğrenme yeteneği, mantıksal akıl yürütme ve problem çözme becerisi gibi insan zekâsına ihtiyaç duyulan görevleri simüle etmek ve görevleri kendi başlarına özerk veya yarı özerk olarak gerçekleştirme yeteneği kazandırmak için makine öğrenimi algoritmaları ve teknolojilerini kullanır (Ahuerma, 2022:1947).



Şekil 2.1. Yapay Zekâ Temel Bileşenleri (Nasa , 2024)

Şekil 2.1'de YZ'nın temel bileşenleri ve bu bileşenlerin birbirleriyle olan ilişkileri gösterilmiştir. Şekilde, en geniş daire YZ'yı simgelerken, bunun alt dalları olan makine öğrenmesi (ML), derin öğrenme (DL), doğal dil işleme (NLP) ve bilgisayar görüşü (CV) gibi alanlar, daha küçük kesişen kümeler olarak gösterilmiştir. Makine öğrenmesi, yapay zekânın bir alt dalıdır ve veri kullanarak modellerin öğrenmesini sağlar. Derin öğrenme ise makine öğrenmesinin daha özelleşmiş bir alanıdır ve yapay sinir ağları gibi yöntemlerle çalışır. Doğal dil işleme, metin ve konuşma gibi dil temelli verilerin analizine odaklanırken, bilgisayar görüşü görüntülerin işlenmesi için kullanılır. Bu alt bileşenlerin ortak çalıştığı veya bir arada kullanıldığı uygulamalar bulunmaktadır. Örneğin, hem doğal dil işleme hem de bilgisayar görüşünün uygulandığı bir sistem, yazılı metinlerin yer aldığı görsellerin analizini gerçekleştirebilir.

YZ'nın tarihsel sürecine bakıldığında başlangıçta sınırlı hesaplama gücüne sahipken günümüzde kapsamlı ve etkili bir teknolojiye dönüştüğü görülmektedir. Göstermiş olduğu gelişim sayesinde bilimsel ve teknolojik ilerlemeleri hızlandırmıştır.

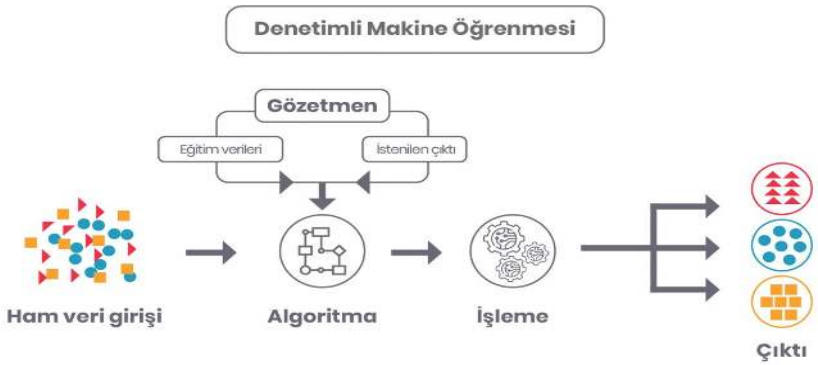
2.2.Makine Öğrenmesi (Machine Learning-ML)

Makine Öğrenmesi (ML), bilgisayarların uyması gereken kuralları elle yazdığımız klasik programlamanın aksine açık insan müdahalesi olmadan makinelerin ve bilgisayar sistemlerinin verilerden öğrenerek, tahminde bulunması veya kararlar almasını sağlamak amacıyla algoritmalar ve istatistiksel modellerin kullanımını içeren YZ'nin bir alt

kümesidir. Makine öğrenimi özünde, makinelerin verilerden öğrenmesini sağlayan algoritmaların kullanımını içerir. Bu algoritmalar, etiketli ve etiketsiz verilerdeki kalıpları, ilişkileri belirlemek ve bu bilgilerle tahminlerde veya eylemde bulunmak için tasarlanmıştır (Parsewar, 2023:28).

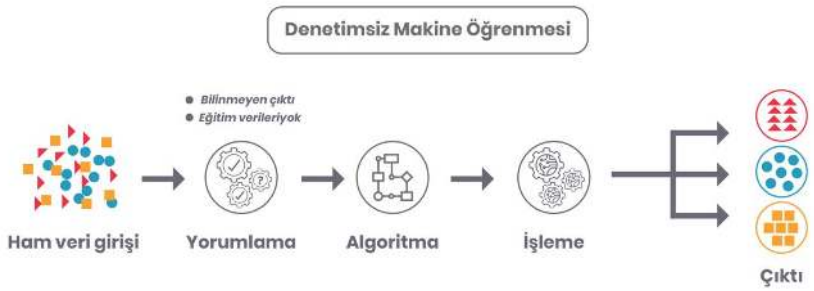
Klasik programlamada, program ve girdi olarak veriler bir çıktı üretirken, ML'de girdi olarak verilen veriler ve çıktı birlikte bir program üretir. ML'de makinelere sağlanan verilerle makineleri eğitmek ve ML modelleri oluşturmak amacıyla farklı hesaplama yöntemleri kullanılmaktadır. Yöntem seçimi, mevcut veri türü ile otomatikleştirilmek istenen işlemin yapısına göre belirlenir. ML algoritmaları denetimli, denetimsiz, yarı denetimli ve takviyeli öğrenme yöntemleri olarak dört kategoriye ayrılmaktadır (Sherkhane, vd., 2023:155).

Denetimli öğrenme, makinenin soru cevap mantığı ile eğitildiği yöntemdir. Model eğitilirken her girdi verisinin olması gereken doğru karşılığı önceden belirlenmiştir. Daha sonra model, bu eğitim verilerini kullanarak yeni gelen veriler üzerinde tahminlerde bulunur (Banafa, 2024:4). Yeterli eğitim aşamasından sonra, sistem karşılaştığı yeni durumlar için çözüm üretebilme yeteneği kazanır. Eğitim sonrasında, sistem tarafından yapılan tahminlerin doğruluğunu anlamak için model, bir örnek veri kümesi verilerek test edilir. Denetimli öğrenmenin amacı giriş ve çıkış verilerinin eşlenmesidir. Bir öğretmenin denetimi altında öğrenen bir öğrenci, denetimli öğrenmeye örnek verilebilir. Spam mail tespiti, hava durumu tahmini, piyasa eğilimleri ve benzeri sürekli değişkenleri tahmin eden uygulamalarda denetimli öğrenme kullanılır (Shaveta, 2023:282).



Şekil 2.2. Denetimli Makine Öğrenmesi Şeması (Turhost, 2021)

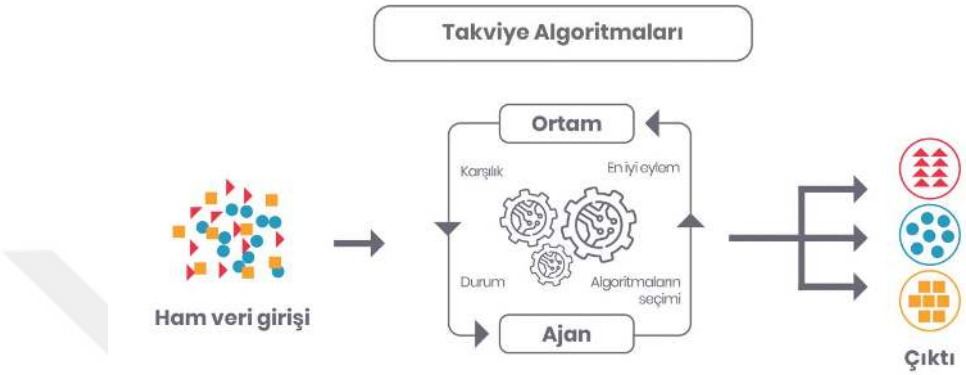
ML'nin bir diğer türü denetimsiz öğrenmedir. Denetimsiz öğrenme doğru cevapları belirtilmemiş veri seti üzerinde doğru cevapları öğrenmesini ve kendi başına kalıpları ve ilişkileri belirlemesini içermektedir. Bu tür öğrenme genellikle benzer öğeleri bir araya getirmenin hedeflendiği kümeleme gibi uygulamalarda kullanılır (Banafa, 2024:5). Denetimsiz öğrenmenin amacı, gelen verileri yeni özelliklere veya ilgili desenlere sahip bir nesne koleksiyonunda yeniden düzenlemektir. Denetimsiz öğrenmede önceden tanımlanan bir sonuç yoktur. Sistemlerin etiketsiz verileri kullanarak gizli bir yapıyı tanımlamak için bir fonksiyonu nasıl çıkarabileceğini araştırmaktadır. Sistemin verdiği sonucun doğru olduğunu asla garanti edemez. Bunun yerine, sonucun ne olması gerektiği hakkında veri kümelerine dayanarak çıkarımda bulunur. Makineler, yararlı tahminlerde bulunmak için büyük miktardaki veriyi tarar. Bir ilişki kuralı olarak da nitelendirilen denetimsiz öğrenme tekniği, büyük bir veri tabanındaki değişkenler arasındaki bağlantıları ortaya çıkarmak için kullanılır. Veri tabanında birlikte bulunan öğelerin grubunu oluşturur. Örnek olarak, bir alışveriş sepeti analizi yapılırken ekmek satın alan kişilerin sıklıkla reçel de satın alır gibi eylemsel ilişki kuralı verilebilir (Shaveta, 2023:283).



Şekil 2.3. Denetimsiz Makine Öğrenmesi Şeması (Turhost, 2021)

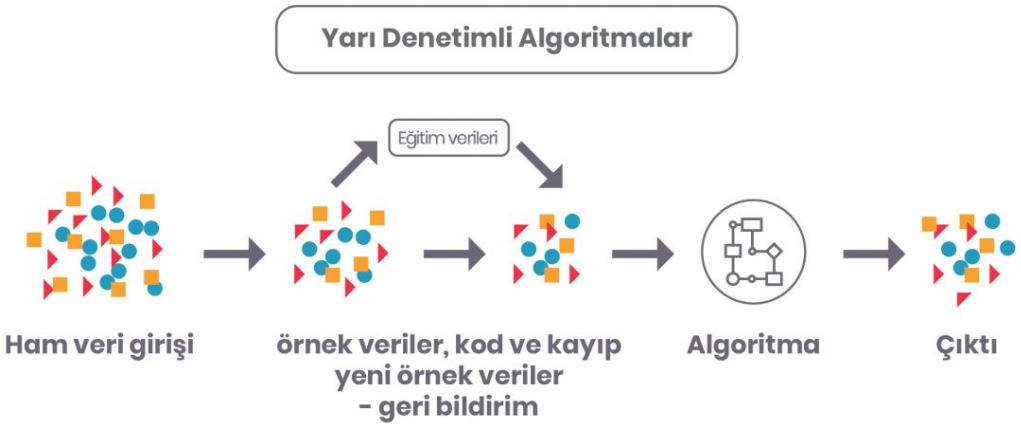
Takviyeli öğrenme, bir modelin çevresinden gelen geri bildirimlere göre kararlar alması için eğitilmesini içeren bir diğer makine öğrenmesi türüdür. Bu öğrenme türünde, model deneme yanılma yoluyla öğrenir (Banafa, 2024:5). Takviyeli öğrenme sistemindeki bir öğrenme aracısı her doğru eylem için bir ödül ve her yanlış etkinlik için bir ceza alır. Bu geri bildirimin yardımıyla, öğrenme aracısı otomatik olarak öğrenir ve daha iyi performans gösterir. Aracı, takviyeli öğrenme sırasında çevreyi keşfeder ve

onunla etkileşime girer. Takviyeli öğrenme algoritmaları, eylemlerde bulunarak ve başarıları veya başarısızlıkları belirleyerek çevreleriyle etkileşime girer. Bu yöntemin en önemli iki özelliği, deneme-yanılma öğrenmesi ve gecikmeli ödüllerdir. Örnek olarak, robotik bir köpeğin otomatik olarak kollarını nasıl hareket ettireceğini öğrenmesi verilebilir (Shaveta, 2023:283).



Şekil 2.4. Takviyeli Makine Öğrenmesi Şeması (Turhost, 2021)

Yarı denetimli öğrenme, denetimli ve denetimsiz öğrenme yöntemlerinin arasında yer alarak sınırlı sayıda etiketli veri setleri ile etiketsiz veri setlerini analiz eder. Etiketli veriler maliyetli olduğundan genellikle etiketsiz veriler içerir ve makine öğrenimi modelinin maliyeti azaltılmış olur, kurumsal amaçlar için az sayıda etiketli veriler kullanılır. Yarı denetimli öğrenme ML modelinin doğruluğunu ve performansını da artırır (Sherkhane, vd., 2023:155).



Şekil 2.5. Yarı Denetimli Makine Öğrenmesi Şeması (Turhost, 2021)

ML'nin çeşitli sektörlerde sayısız uygulaması vardır. Örneğin sağlık hizmetlerinde, hastalık teşhis ve tedavi yöntemlerini iyileştirmek için tıbbi görüntüleri ve hasta verilerini analiz etmede kullanılmaktadır. Finans alanında piyasa eğilimlerini analiz etmek ve yatırım kararları almak, ulaşımda trafik akışını optimize etmek ve yol güvenliğini iyileştirmek, eğitimde öğrenmeyi kişiselleştirmek ve öğrenci sonuçlarını iyileştirmek için kullanılmaktadır (Banafa, 2024:5).

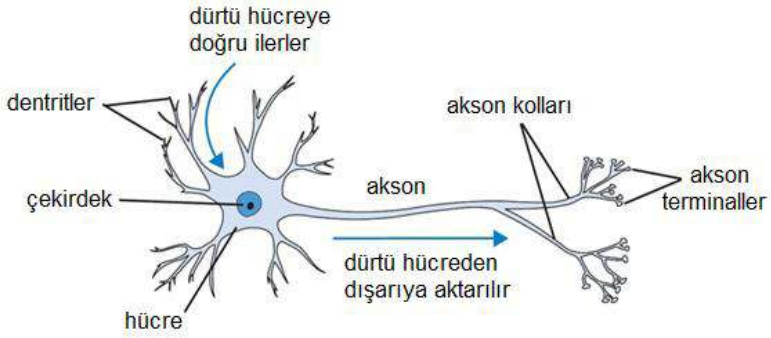
Makine öğrenmesi, bilgi odaklı karar alma süreçleri ve otonom sistemler gibi birçok alanda önemli bir görev üstlenmektedir. Bu modeller sürekli öğrenme ve uyum sağlama yeteneği sayesinde karmaşık problemlere etkili çözümler sunabilmektedir. ML öğrenmesi geleceğin teknolojisinde de çok önemli bir yeri olacağı düşünülmektedir.

2.3.Derin Öğrenme (Deep Learning-DL)

Derin Öğrenme (DL), yapay sinir ağlarını kullanarak büyük verilerle çok katmanlı mimarilerde çalışma imkânı sağlayan, makine öğrenmesinin bir alt kümesidir. ML tekniklerinde öğrenme işlemi kodlanmış kurallar üzerinden gerçekleşirken, DL'de öğrenme işlemi metin, ses, video gibi verilerin sembollerinden otomatik olarak gerçekleşmektedir. DL esnek yapıda olduğundan ham metin veya resim verileri üzerinden de öğrenebilmekte, verilerin büyüklüğüne göre tahmin doğruluğu da artmaktadır. DL kavramı, ilk kez 2006 yılında Hinton'ın yapay sinir ağlarının daha etkili bir şekilde eğitilebileceğini öne sürmesiyle ortaya çıkmıştır (Yılmaz ve Kaya, 2022:1).

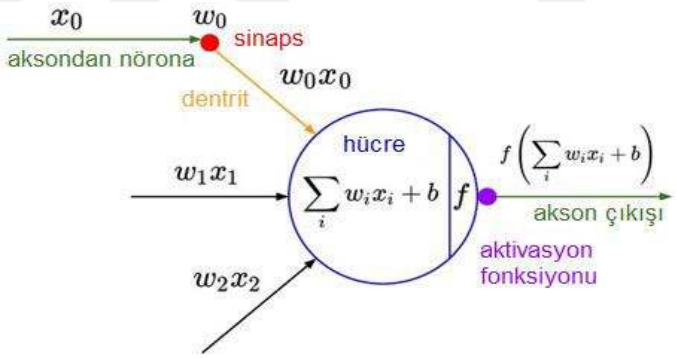
İnsan beynindeki sinir sisteminin çalışma mantığı taklit edilerek yapay sinir ağları geliştirilmiştir. Yapay sinir ağları, tıpkı insan gibi öğrenme, hatırlama, ezberleme, deneyim kazanma ve bilgiyi güncelleme gibi yeteneklere sahip bir sistemdir. İlk yapay sinir ağı modeli elektrik devreleri kullanarak, 1943 yılında insan beyninin hesaplama becerisini örnek alan matematikçi Walter Pitss ve nörolog Warren McCulloch tarafından geliştirilmiştir. Bu model, matematiksel anlamda her türlü ifadenin formüle edilebileceğini göstermiştir (Katırcıoğlu, vd., 2021:279). İnsanın öğrenme sürecinde, yeni bir bilgi geldiğinde bu bilgiyi işleyen ve sonrasında çıktıya dönüştüren, beynin bilgiyi işleme kapasitesini belirleyen sinir hücrelerine nöron adı verilmektedir (Şekil 2.6). Nöronlar beynimizin temel elamanıdır ve sinir ağının temel yapısını oluştururlar. Bu nöronların taklit edilmesiyle yapay nöron kavramı ortaya çıkmıştır. Yapay nöronlar, nöral

ağda bilgiyi girdi olarak alır, işler ve sonrasında gerçekleşecek işlemler için diğer yapay nöronlara gönderilen sonuç çıktısı üretir (Yılmaz ve Kaya, 2022:5).



Şekil 2.6. İnsan Sinir Hücresi (Nöron) Yapısı (Yılmaz ve Kaya, 2022:5).

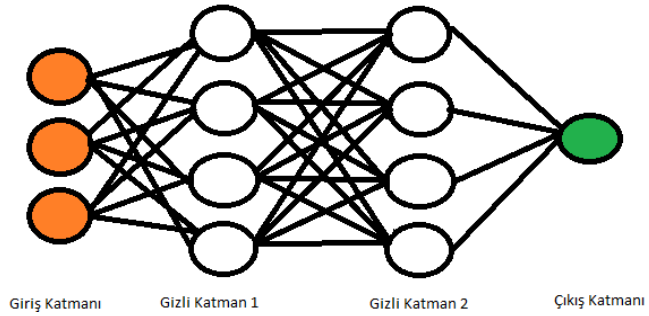
Yapay nöron belirli sayıda giriş parametresi alır, alınan her parametre için bir yönlendirilmiş ağırlık parametresine bağlanır, doğrusal bir şekilde sistemdeki giriş ve ağırlıklar toplanır ve aktivasyon fonksiyonuna gönderilir. Fonksiyonunun çıkışı ise nöronun çıkışını üretir. Şekil 2.7'de yapay nöron matematiksel modeli gösterilmiştir. Birden çok yapay nöronun kullanılması ile oluşturulan sisteme yapay sinir ağı denilmektir (Çalışkan ve Demir, 2022:30).



Şekil 2.7. Yapay Nöron Matematiksel Modeli (Çalışkan ve Demir, 2022:30).

Derin öğrenmenin temeli yapay nöron ağlarından oluşmaktadır. Birbiriyle bağlantılı nöronlar birleşerek katmanları oluşturur, katmanların üst üste istiflenmesiyle yapay sinir ağları diğer adıyla derin sinir ağları oluşur. Oluşan ağın derinliğini katman sayısı belirler ve katman sayısı arttıkça ağ yapısı derinleşir. Ağın giriş katmanı, ilk katman ve girdi yapılan katmandır. Çıktı katmanı, ağın çıkışını üreten ve ağın son katmanıdır. Ağdaki süreç katmanları da ağda bulunan gizli katmanlardır. Gizli katmanlar, belirlenmiş görevleri veriler üzerinde uygulayarak çıktıyı bir sonraki katmana aktarır. Çıkış katmanı

ise çıktı üreten ağın son katmanıdır. Şekil 2.8'de örnek derin öğrenme modeli gösterilmiştir (Lermi ve Onur, 2024:143).



Şekil 2.8. Derin Öğrenme Modeli (Lermi ve Onur, 2024:143).

Derin öğrenme, günümüzde birçok sistem tarafından kullanılmaktadır. Yüz tanıma, plaka okuma, nesne algılama, araçlarda şerit takibi, yaya tespiti, otomatik park etme gibi gelişmiş sürüş destek sistemlerinde, konum belirlemede, doğal dil işleme ve hastalık teşhisi gibi karmaşık problemleri çözmek için kullanılmaktadır. Derin öğrenme ile bu alanlarda önemli başarılar elde edilmiştir (Çalışkan ve Demir, 2022:30).

Derin öğrenme, çok fazla verinin bulunduğu günümüz dünyasında karmaşık problemleri çözmek için etkili bir araç olarak karşımıza çıktığı görülmektedir. Çok katmalı yapay sinir ağları sayesinde büyük veri kümeleri üzerinde etkileyici sonuçlar ortaya koyarak, sağlık, otomotiv, finans ve daha pek çok sektörde devrim yaratmıştır.

2.4.Doğal Dil İşleme (Natural Language Processing-NLP)

Doğal dil işleme (NLP) kavramından bahsetmeden önce dil kavramından bahsetmek yararlı olacaktır. Bir dil, bir dizi sembol ya da kural kümesi olarak tanımlanabilir. Doğal dil, insanların iletişim kurmak için kullandıkları dil anlamına gelmektedir. Doğal diller; sözcükler, söz öbekleri, dilsel örüntüleri ve dil bilgisi kurallarını içerir. Doğal dil işleme ise, insan dilinin (doğal dil) bilgisayar tarafından anlaşılması, işlenmesi ve üretilmesi üzerine çalışan bir YZ bileşenidir. NLP, dilbilim, bilgisayar bilimleri ve YZ'nın kesişim kümesinde yer alan, disiplinler arası yapıya sahiptir (Güner, 2023:58). NLP, insan dilindeki kurallı yapıyı makine öğrenimi, istatistik ve derin öğrenme teknikleriyle birleştirerek model oluşturur. Bilgisayarlar doğal dili oluşturulan model ile metin ya da ses formatında işleyerek konuşmacı veya yazarın neyi ifade etmek istediğini anlamasını sağlar (Parsewar, 2023:54).

Derin öğrenme ve makine öğrenmesi alanlarındaki gelişmelere paralel olarak NLP, dil modelleri oluşturmak için büyük miktardaki dil verilerinden faydalanmaya başlamıştır. Matematiksel yaklaşımla oluşan bu dil modelleri, konuşma tanıma veya dil çevirisi gibi üst düzey uygulamalarda kullanılan, çeşitli görevleri yerine getirebilen sistemsel yapılardır. Dil modeline örnek olarak GPT-4 dil modelini kullanan ve günümüzde tüm dünyada popüler olan ChatGPT verilebilir. ChatGPT, doğal dilde girdi olarak verilen verilere karşılık doğal dilde cevap veren sohbet için özelleştirilmiş ve çevrimiçi erişilebilen yapa zekâ yazılımıdır. (Güner, 2023:59).

ChatGPT, 2015 yılında kurulan OpenAI firması tarafından geliştirilmiştir. İlk olarak Haziran 2018'de GPT-1 modelini tanıtmıştır. GPT (Generative Pre-trained Transformer) Üretken Önceden Eğitilmiş Transformatörler olarak ifade edilen serinin ilk geliştirilmiş hali ve 117 milyon parametreden oluşturulmuştur. GPT-1, denetimsiz öğrenme yönetimi ile eğitim verisi olarak da kitapları kullanarak, bir cümledeki bir sonraki kelimeyi tahmin etme yöntemini kullanmıştır. Denetimsiz öğrenmenin potansiyelini dil anlama görevlerini gerçekleştirerek göstermiştir. Şubat 2019'da yayınlanan GPT-2, 1,5 milyar parametreyle önemli bir büyüme sağlayarak, metin oluşturma yeteneklerinde çarpıcı bir iyileştirme sergilemiştir. Tutarlı ve çok paragraflık metinler üretmiştir. GPT-3, Haziran 2020'de büyük bir sıçrama yaparak, 175 milyarlık parametre üzerinde eğitilmiştir. Gelişmiş metin oluşturma, e-posta taslağı hazırlama ve makale yazma, şiir yazma ve hatta programlama kodu oluşturmaya kadar çeşitli uygulamalarda yaygın bir şekilde kullanılmasına yol açmıştır. Ayrıca, gerçek soruları yanıtlama ve diller arasında çeviri yapma becerisini de göstermiştir. Mart 2023 yılında en son sürüm olan GPT-4 piyasaya sürülmüştür. Bu modelde, geliştirilmiş model hizalaması, kullanıcı niyetini takip etme yeteneği kazandırılmış, saldırgan veya tehlikeli çıktı üretme olasılığı daha düşürülmüştür. Gerçek doğruluğun artırılmış daha iyi yönlendirme kabiliyeti ve kullanıcı isteklerine göre davranışı değiştirme yeteneği kazandırılmıştır. Gerçek zamanlı olarak internette arama yapma yeteneği içermektedir (Marr, 2023).

Doğal dil işleme modellerinden biri olan NLP'nin bazı temel görevleri de vardır. Metin sınıflandırması görevi ile metinleri kategorilere ayırır, örneğin bir e-postanın spam olup olmadığını belirlemesi gibi. Adlandırılmış varlık tanıma görevi ile bir metindeki kişi, kuruluş ve yer gibi unsurları tanımlama ve sınıflandırma yapabilir. Duygu analizi görevi ile bir metinde ifade edilen duygunun olumlu, olumsuz veya nötr olup olmadığını

belirleyebilir. Makine çevirisi görevi ile bir dili başka bir dile çevirebilir. Soru cevaplama görevi ile doğal dille sorulan soruları yanıtlayabilir. Metin özetleme görevi ile uzun bir metnin daha kısa özetini yapabilir (Banafa, 2024:16).

NLP'nin çeşitli YZ alanlarında birçok uygulaması bulunmaktadır. Müşteri hizmetleri sohbet robotları, Siri, Alexa gibi dijital asistanlar, Google Çeviri gibi otomatik çeviri yazılımları, sesle çalışan GPS sistemleri, sosyal medya yorumlarından müşteri geri bildirim analizi yapan yazılımlar, telefon hattı üzerinden müşterinin ne söylediği anlayan çağrı merkezleri, tıbbı kayıtların analiz ve kategorizasyonu otomasyonları örnek olarak verilebilir (Parsewar, 2023:66).

Doğal dil işleme (NLP), insan dilinin bilgisayarlar tarafından anlaşılması ve işlenmesi noktasında teknoloji dünyasında köklü bir değişim yaratmıştır. Dilin doğasındaki nüanslar ve kültürel farklılıklar, NLP'nin gelişimini sürdürülebilir kılmada zorluklar oluşturabilir. Ancak, gelişen algoritmalar ve artan veri kaynakları sayesinde, dilin karmaşıklığına uygun modeller geliştirilmiş ve bu modeller, çeviri, özetleme, duygu analizi ve sohbet robotları gibi pek çok alanda başarılı sonuçlar ortaya koymuştur.

2.5.Bilgisayar Görüşü (Computer Vision- CV)

Bilgisayar görüşü (CV), bilgisayarların dijital görüntülerden veya videolardan aldığı verileri işleyen, analiz eden ve yorumlayan YZ alanıdır. CV insan görüşü gibi çalışmaktadır. İnsan görüşünde, nesnelerin ne kadar uzakta olduğunu, hareket edip etmediklerini, bir görüntüde yanlış bir şey olup olmadığını ve buna benzer birçok şeyi beyin otomatik olarak algılar ve öğrenir. CV'de ise görüntü işleme teknikleri, makineleri bu işlevleri yerine getirmeleri için eğitir. Makineler kameralardan gelen görüntüleri çok sınırlı bir sürede veri ve algoritmalar kullanarak analiz eder, bir sistem bir dakikada binlerce görüntüyü işlemek üzere eğitildiğinde, insan yeteneklerinin çok üstüne çıkabilir. CV algoritmaları, görüntüleri analiz etmek ve tanımak için büyük miktarda veriye ihtiyaç duyar, bu nedenle derin öğrenmeden, sinir ağlarından etkin bir şekilde yararlanır. Makine öğrenimi veya derin öğrenme algoritmaları, makinelerin görsel verilerin bağlamını öğrenmesine ve görüntüleri nasıl tanımlayıp ayırt edeceğini kendi kendine öğrenmesine yardımcı olur (Thareja, 2023:725).

CV'nin farklı alt alanları vardır ve her biri görsel algılayış ve analizin farklı yönlerini ele alır. CV görevlerinin bazı yaygın türleri şunlardır:

- Görüntü Sınıflandırması: Görüntüleri önceden tanımlanmış sınıflara veya kategorilere ayırmayı içerir. Örneğin, hayvanların görüntülerini farklı türlere sınıflandırmak veya çeşitli nesneler arasında ayrım yapmak gibi.

- Nesne Algılama: Bir görüntü veya videodaki belirli nesneleri bulmaya ve tanımlamaya odaklanır.

- Nesne Takibi: Bir video dizisindeki birden fazla kare boyunca nesnelerin hareketini takip etmeyi ve izlemeyi amaçlar. Özellikle gözetleme veya otonom araçlar gibi uygulamalarda kullanılmaktadır.

- Görüntü Oluşturma: Belirli özelliklere sahip veya benzerlikleri paylaşan yeni görüntüler oluşturmayı içerir.

- Görsel Tanıma: Nesne algılama ve sahne anlama dâhil olmak üzere geniş bir görev yelpazesini kapsar. Görsel içeriğin genel olarak anlaşılmasını ve yorumlanmasını içerir (Pandey, 2023:511).

CV'nin kullanım alanları çok geniştir ve etkin bir şekilde kullanılmaktadır. Facebook, Instagram vb. uygulamalar kullanıcı girişi sağlamak için, akıllı telefonlar telefon kilidini açmak için, ülkelerin güvenlik güçleri gözetim ve denetim amaçlı yüz tanıma sistemini kullanmaktadır. Hastanelerde BT ve MRI taramalarında görüntü analizinde, ev güvenliği ve ofis güvenliğinde, insansız hava aracı tabanlı gözetleme sistemlerinde, tarımda ürün verimlilik takibinde, otonom araçlarda şerit takibi, yaya algılama, trafik levhalarını okuma gibi birçok uygulama alanı vardır (Thareja, 2023:735).

Bilgisayar görüşü, görsel verileri anlamlandırarak makinelerin insan görme yetisini taklit etmesine olanak tanıyan bir alan olarak, teknolojinin pek çok alanında devrim yaratmıştır. Görüntü işleme ve derin öğrenme yöntemlerinin birleşimi sayesinde, yüz tanıma, otonom araçlar, sağlık teşhis sistemleri ve güvenlik gibi pek çok kritik uygulama geliştirilmiştir. Bilgisayar görüşünün etkili bir şekilde kullanımı hem veri kalitesine hem de etik ve gizlilik konularına gösterilecek özenle yakından ilişkilidir.

3. YAPAY ZEKÂ VE YENİ NESİL TEKNOLOJİLER

YZ, günümüz teknolojilerinin önemli bir parçası haline gelerek, pek çok sektörde yenilikçi değişimlere kapı aralamaktadır. Bu teknoloji hem dijital hem de fiziksel dünyada geniş bir etki alanına sahiptir. Özellikle Nesnelerin İnterneti (IoT), Blokzincir, Akıllı Şehir uygulamaları, Robotik ve Otonom Sistemler ile İnsansız Hava Araçları (İHA) gibi alanlarda YZ'nın getirdiği veri analizi, tahmin ve otomasyon gibi yetenekler, daha güvenli ve verimli çözümler sunulmasını sağlamaktadır. Bu bölümde, YZ'nın bu teknolojilerdeki yeri ayrıntılı olarak incelenecektir.

3.1.Nesnelerin İnterneti (Internet of Things, IoT)

Dijitalleşme nesneleri, cihazları, insanları iş yerlerini, evleri, kentleri ve ülkeleri birbirlerine dijital nöronlarla bağlayarak birbirlerini etkileyen ve tetikleyen akıllı bir ekosistem meydana getirmekte, sosyal yaşantılardan örgüt yapılarına kadar her şeyi değiştirip dönüştürmektedir (İşgüzar, 2020:1). İnternet ise bu noktada, gelişmiş ve gelişmekte olan ülkelerde bölge, dil, kültür ve zaman dilimi fark etmeksizin, insanların istedikleri bilgilere anında ulaşmalarını sağlayan evrensel bir iletişim aracı görevi üstlenmektedir. Nesnelerin interneti (IoT), internete bağlanarak birbirleriyle etkileşime giren ve veri alışverişinde bulunan cihazları kapsamaktadır. IoT, dünya üzerinde bulunan milyarlarca fiziksel nesnenin internete kablosuz olarak bağlanmasını, veri toplamasını ve paylaşmasını ifade etmektedir. IoT kavramı ilk kez 1999 yılında Kevin Ashton tarafından ifade edilmiştir. Ürün tedarik zincirlerinde kullanılan ve insan müdahalesine ihtiyaç duymadan ürün sayımı ve takibi yapan Radyo Frekanslı Tanımlama (RFID) etiketlerinin internete bağlanmasından esinlenen Ashton, sensörler vasıtası ile internete bağlanabilen nesnelerin oluşturacağı sistemi tanımlamak için kullanmıştır (Aydın, 2023:92).

IoT, temelde algılama, bağlantı, çekirdek ve uygulama katmanı olacak şeklide dört katmandan oluşmaktadır. Bunlar;

- Algılama katmanı: IoT'nin mimarisinin en düşük katmanıdır. Bu katmanda, sensörler, aktüatörler ve çeşitli cihazlar tarafından algılanan sıcaklık, nem, konum, görüntü, ses vb. gibi gerçek dünya verilerini analiz edilmesi ve işlenmesi için toplanır.

- Bağlantı katmanı: IoT'nin mimarisinin orta katmanıdır, veri iletimi ve iletişiminden sorumludur ve algılama katmanı tarafından toplanan verileri IoT sisteminin çekirdek katmanına iletir. Veri transferinde Wi-Fi, Bluetooth, Zigbee gibi kablosuz iletişim teknolojilerini, ethernet gibi kablolu iletişim teknolojilerini, çeşitli protokolleri ve ara yazılımları kullanır. IoT mimarisindeki en önemli katmandır.
- Çekirdek katmanı: Veri işleme, depolama ve yönetimden sorumlu olan IoT sisteminin beynidir. Gerçek zamanlı karar almak ve faydalı bilgiler çıkarmak üzere veriler bu katmanda işlenir. Bulut bilişim kaynakları veya özel sunucular genellikle veri analizi, makine öğrenimi, model oluşturma ve karar alma için buraya dahil edilir.
- Uygulama katmanı: IoT'de bulunan en üstteki mimaridir. Kullanıcılara en yakın katmandır. Kullanıcılar, cihazları kontrol etmek, verileri görüntülemek ve bildirimler almak için çeşitli yazılımlar aracılığı ile IoT sistemiyle bu katmanda etkileşim kurar (Cao, 2024:601).

Nesnelerin Yapay Zekâsı (AIoT), YZ'nın yardımıyla IoT sistemlerine akıllı görevleri yerine getirmeyi ifade etmektedir. IoT sistemleri veri entegrasyonu, veri analizi, görüntü analizi ve veri tahmininin gerçekleştirilmesi için YZ tekniklerine veri akışı sağlar. IoT ve YZ, sensörler, protokoller, gömülü programlama, dağıtılmış sistemler, istatistikler ve algoritmalar gibi birden fazla disiplinde derin bilgiye ihtiyaç duyar. AIoT sistemlerinde, birbirine bağlı bileşenler iş birliği içinde çalışarak görevlerini yerine getirir ve gerçek zamanlı veri alışverişini, karar almayı mümkün kılar. Örneğin, belirli bir alanda bulunan kişilerin maske takıp takmadığını tespit etmek için IoT kameralarını, vücut sıcaklığını ölçmek için IoT sensörlerini kullanır. Elde edilen veriler, maske takma davranışını doğru bir şekilde belirlemek için YZ algoritmalarıyla işlenir. Bir kişi maskesiz veya yüksek ateşli olarak tespit edildiğinde, AIoT sistemi, maske takmalarını hatırlatmak için görsel bir uyarı sağlar ve ateşi olduğunu gösterir. Bu AIoT sistemi, kamusal alanlarda maske takılıp takılmadığının ve vücut sıcaklığının izlenmesini sağlayarak, pandemi ve sağlık taraması gerektiren diğer durumlarda sağlık ve güvenlik uygulamalarında kullanılmıştır (Du, vd., 2024:5).

Dünya genelinde IoT cihazlarının sayısı 2023 yılında 15,9 milyar iken, 2033 yılında bu sayının 39,6 milyardan fazla olacağı tahmin edilmektedir. Günümüzde 100 milyondan

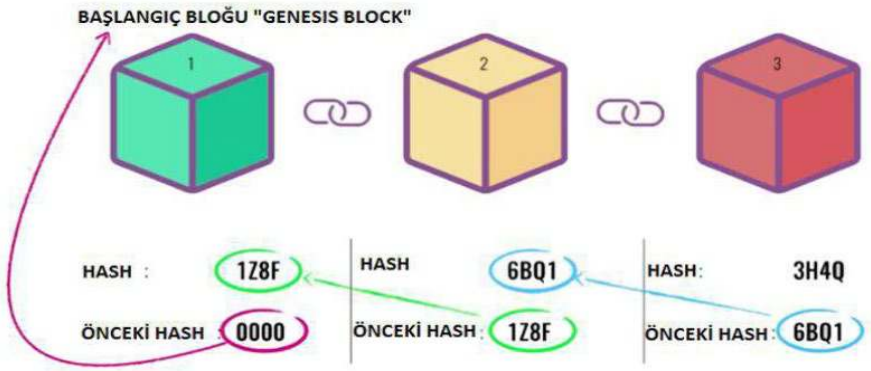
fazla IoT cihazı elektrik, klima, gaz, atık yönetimi, toptan satış ve perakende, ulaşım, depolama ve kamu sektöründe kullanılmaktadır. 2033 yılına kadar bu sektörlerde beklenen IoT cihazı sayısı 8 milyar düzeyindedir (Vailshery, 2024). IoT konusundaki araştırmaların çoğalmasıyla beraber, akıllı ev sistemleri, akıllı hayvancılık çözümleri, sağlık teknolojileri, hasta izleme sistemleri, akıllı çevre uygulamaları, giyilebilir teknolojiler, lojistik çözümler, endüstriyel uygulamalar, araç takip teknolojileri gibi alanlarda kullanılmakta olup günümüzde yaşamımızı dönüştüren temel bir teknoloji haline gelmiştir. Her yaş grubundan birey, uyku kalitesi, uyku süresi, nabız, tansiyon gibi sağlık parametrelerini ölçen akıllı saatler kullanmakta, ev temizliğini yapan robot süpürgeler gibi teknolojilerden faydalanmaktadır. Bu cihazlar mobil uygulamalar vasıtasıyla uzaktan kontrol edilebilmektedir. Dolayısıyla insanlar daha konforlu bir yaşam sürmektedir. IoT teknolojileri, endüstride insan gücüne olan gereksinimini düşürerek operasyonel verimliliği yükseltmekte ve insan kaynaklı hataları en aza indirgemektedir (Kurtboğan, 2023:69).

IoT'nin getirmiş olduğu yararlı değişim ile birlikte gizlilik ihlali, gözetim, mahremiyet, güvenlik açıkları gibi bazı etik sorunları da barındırmaktadır. IoT'nin büyümesine paralel olarak sisteme cihaz ve sensörler eklenmektedir. IoT sisteminde insanların sağlık kayıtları, mali kayıtları, alışveriş kayıtları, fotoğraf, ses, video ve sohbet kayıtları gibi birçok kişisel veriler bulunmaktadır. Ayrıca, IoT sisteminde bulunan cihazlar adreslenmektedir, bu şekilde cihazların konumu bilinmektedir. Bu kadar büyük verilerin olduğu bir sistemde oluşacak güvenlik açığının, insanların can ve mal güvenliğini tehlikeye atmasından dolayı kaygı ve endişe yaratmaktadır (Öztürk ve Zeybek, 2021:4). Örnek olarak, 2024 yılı ekim ayında, ABD'nde Ecovacs marka robot süpürgenin yazılımında bulunan güvenlik açığına yönelik yapılan saldırı sonucunda hacklenmiş ve süpürgeler ırkçı küfürler ederek, evcil hayvanları kovaladığı belirtilmiştir. Dennis Giese 2024 yılı ağustos ayında "Def Con Hacking" konferansında, robot süpürgenin Bluetooth üzerinden kolay bir şekilde hacklenerek, kamera ve mikrofonlarının kullanılabildiğini açıklamıştır. Robot süpürgeler bulundukları ortamın haritasını çıkarabilmektedir, saldırı düzenleyenler ortamın düzenini öğrenebilir, cihazın üzerindeki kamera ve mikrofonu kullanarak ses ve görüntü kaydı yapabilir, ortamı dinleyebilmektedir. Buna benzer durumlar siber güvenlik açısından ciddi bir tehdit oluşturmaktadır (Kılıç, 2024).

3.2.Blokzincir (Blockchain) Teknolojisi

Blokzincir teknolojisi (Blockchain), merkezi bir otoriteye gereksinim duymadan, dağıtık yapıdaki bir ağ üzerinde çalışan veri tabanı sistemidir. Blokzincir teknolojisinin temel prensibi, birbirine bağlı bloklar hâlinde verilerin zincirlenmesi ve yeni eklenecek her bloğun bir öncekiyle bağlantılı olmasıdır (Çıkı ve Tanrıverdi, 2023:36).

Her türlü verinin saklandığı ve değer içeren yapılar ise blok olarak tanımlanmaktadır. Bloklar halinde zincirlenen bu yapı, verilerin değiştirilme ihtimalini zorlaştırarak güvenirlik ve bütünlük sağlamaktadır. Herhangi bir blok üzerinde geriye dönük bir değişiklik yapıldığı takdirde, arkasından gelen tüm bloklarda değişiklik yapmak gerekmektedir. Bloklar, blok başlığı ve veriler bölümü olmak üzere iki yapıdan oluşmaktadır. Blok başlığı içerisinde tarih, kendinden önce gelen bloğun özet değeri gibi genel bilgiler, veriler bölümünde ise herhangi bir içerik olabilmektedir. Sistem içindeki veriler, dağıtık ağa dahil olan tüm kullanıcılar arasında eşzamanlı ve eşit şekilde paylaşılmaktadır (Demir ve Öksüz, 2023:78).



Şekil 3.1. Blokzincir Yapısı Kaynak: (Kurtboğan, 2023:22)

Blokzincir teknolojisinin temel özelliklerinden birisi dağıtık defter teknolojisi olarak tanımlanmaktadır. Blokzincir ağında yer alan tüm cihazlarda verilerin bir kopyası tutulmaktadır. Sistem üzerinde yeni bir veri girişi veya işlem yapıldığında, bu veri veya işlemler merkezi yönetici olmadan, ağda bulunan tüm cihazlar aracılığı ile doğrulanıp onaylanmaktadır. Dağıtık defter teknolojisi sistemine örnek olarak bir banka ve müşterisi arasındaki ilişki örnek gösterilebilir. Bir bankanın müşterilerine ait veriler dijital olarak saklanmakta, bir kopyasını da hesap cüzdanı olarak müşteriye vermektedirler, herhangi bir tarafın yapacağı tek taraflı değişikliğin bir geçerliliği olmayacaktır, değişikliğin

gerçekleşmesi için iki tarafından onayı gerekmektedir. Dağıtık defter teknolojisi sisteminde de kayıtların bir kopyası tüm cihazlarda tutulduğundan herhangi bir tarafın kendi kayıtlarında yapacağı değişiklik veya kayıt silme işleminin hiçbir anlam ifade etmeyecektir. Sistemde bir varlığı karşı tarafa göndermek için göndericinin, dijital imzalama anahtarı olarak tanımlanan Private Key'e, alıcının ise Public Key'e sahip olması gerekmektedir. Private Key ile imzalanan transfer işlemi mesajı sadece alıcıya değil tüm ağa duyurmak üzere P2P ağda yayınlanır. Kullanıcıdan kullanıcıya (P2P) işlemlerin gerçekleştiği ve merkezi otoritenin olmadığı bu sistemde güven kavramı otoriteye bağlı değildir. Tarafların birbirine güven duymasına gerek kalmayacak şekilde bir sistem tasarımı ve çalışma mantığı geliştirilmiştir (Demir ve Öksüz, 2023:80). Teorik olarak, yapılan her işlem tüm kullanıcılar tarafından görülüyor olsa da işlemler şifreli olduğundan anlamı veya amacı gizli tutulmaktadır. Eşler arası iletimi kullanarak işlemin her iki tarafındaki kullanıcılar birbirleriyle etkileşime girmektedir. Sistemdeki kullanıcılara benzersiz bir alfasayısal adres oluşturulur, bu sebeple bir blok zincirinin takma isim olduğu söylenebilir (Gitmez, 2023:4).

Şekil 3.2. Blokzincir İşleyişi Kaynak: (Karyağdi, 2023:7)

Blokzincir teknolojisi, hızla gelişmekte ve çeşitli endüstrilerde önemli bir inovasyon olarak dikkat çekmektedir. Özellikle finans, lojistik, sağlık, turizm ve enerji sektörü gibi sektörlerde kullanımı giderek artmaktadır. Blokzincir'in ortaya çıkışı, 2008'de Satoshi Nakamoto takma adlı bir birey ya da topluluğun yayımlamış olduğu "Bitcoin: Eşler Arası Elektronik Nakit Sistemi" makalesine dayanmaktadır. Bu makalede, merkezi otoritelerden bağımsız, dağıtık ağ üzerinde çalışan dijital para birimi Bitcoin tanıtılmış ve işlemlerin güvenli ve şeffaf yürütülmesini sağlayan blokzincir teknolojisinin altyapısı

oluşturulmuştur. Bu teknolojinin gelişimi başlangıçta sadece kripto paralarla sınırlı kalsa da zamanla daha geniş bir kullanım alanına yayılmıştır. Finans sektörü başta olmak üzere, ödeme sistemleri, uluslararası para transferleri ve kimlik doğrulama gibi alanlarda blokzincir temelli çözümler geliştirilmiştir (Çıkı ve Tanrıverdi, 2023:36).

Blockzincir teknolojisi başlangıçta kripto paralar (Bitcoin, Eteryum, Ripple gibi) için şifreli dijital doğrulama amacıyla kullanılmıştır. Daha sonra, bu teknoloji YZ gibi çeşitli alanlara uyarlanarak genişletilmiştir. Birbiri ile bağlı olan cihazların artması, gelişmiş algoritmalar ve bilgi işlem gücü sayesinde YZ, geleneksel karar destek sistemlerinde zorunlu hale gelmiştir. Ayrıca, YZ uygulamalarında daha fazla şeffaflık ve güvenilirlik ihtiyacı doğmuştur. Blockzincir verileri koruma konusunda yeteneklidir ama verimlilik sorunları yaşamaktadır, YZ ise veri depolama ve saldırılardan korunma konusunda sorunlar yaşamaktadır. Bu iki teknoloji bir araya gelerek, veri analizi, güvenlik ve güven açısından birbirlerini tamamlamaktadırlar. Örneğin, blockzincir'in dağıtık yapısı sayesinde YZ verileri güvenli bir şekilde saklanabilir ve değişiklikler engellenebilir. Blockzincir, YZ'nin karar alma süreçlerine güven artırırken, YZ ise blockzincir'in verimliliğini artırmaktadır. Fakat blockzincir'in verimlilik sorunları ve YZ'nin veri zehirlenmesine karşı savunmasızlığı gibi sorunlar da bulunmaktadır. Blockzincir'in çeşitli parametreleri, performans ve merkeziyetsizlik arasında dengeyi sağlamaktadır. YZ, güvenli veri sağlayıcı seçimi gibi sorunları çözmek için akıllı sözleşmelerin oluşturulmasında da faydalı olmaktadır. Blockzincir, veri bütünlüğü ve izlenebilirlik sağlarken, YZ'de veri analizi ve akıllı sözleşmelerin optimize edilmesine katkıda bulunmaktadır. Bu iki teknolojinin entegrasyonu, veri işlemlerini daha akıllı ve güvenilir hale getirmektedir (Muhati, vd., 2022:107). Buna bir örnek olarak, Eteryum platformu üzerinde çalışan Augur projesi gösterilebilir. Augur, Eteryum ağına dayalı bir projedir ve akıllı sözleşmeler aracılığıyla kullanıcıların tahminler yapmasını ve bahis oynamasını mümkün kılar. YZ, Augur'da tahmin süreçlerinin yanı sıra pazar verilerinin analizinde de rol oynamaktadır. Bu sayede, YZ teknolojisi kullanılarak akıllı sözleşmelerdeki işlemler otomatik olarak yapılabilir ve YZ tarafından oluşturulan kararlar akıllı sözleşmelere entegre edilebilmektedir (Kurtboğan, 2023:28).

3.3.Akıllı Şehir

Akıllı şehir kavramı, kentleşmenin getirdiği zorluklara ve sürdürülebilir kentsel gelişim ihtiyacına yönelik olarak ortaya çıkmıştır. Akıllı şehir kavramı ile birlikte "bilgi şehri", "dijital şehir" veya "zeki şehir" gibi diğer kavramlarda da birbirinin yerine kullanılmaktadır. Akıllı şehirler, teknolojiyi kullanarak şehir hizmetlerinin verimliliğini artırmayı, kaynak tüketimini azaltmayı ve yaşam kalitesini yükseltmeyi amaçlamaktadır. IoT, YZ ve büyük veri analitiği gibi teknolojilerin entegrasyonu ile modern akıllı şehirler, tarımdan sanayiye, sağlık hizmetlerinden trafik yönetimine kadar çeşitli uygulamalardan veri toplayarak, bu verileri analiz ederek, insanların yaşam standartlarını iyileştirmeye yönelik kararlar alabilmektedir. Binalar, köprüler, yollar ve kamusal alanlar gibi bir kentin farklı bölümlerine yerleştirilen sensörlerden gelen sıcaklık, nem, trafik akışı, enerji tüketimi ve hava kalitesi gibi çeşitli veriler IoT teknolojisi kullanılarak toplanmaktadır. Toplanan büyük miktardaki verilerin analizi ise YZ makine öğrenimi algoritmalarını kullanarak yapılmaktadır. YZ verileri analiz ederek, insanların ayırt etmesinin zor olabileceği kalıpları ve eğilimleri tespit ederek önemli bir rol oynamaktadır (Alahi, vd., 2023:3).

YZ algoritmaları sensör, kamera ve GPS gibi kaynaklarından gelen veriler ile kentlerin trafik akışını ve yoğunlaşmaları analiz edebilmektedir. Bu sayede, trafik ışıklarının süreleri ayarlanmakta ve trafik yönlendirilmektedir. Toplu taşıma sistemlerinde ve araç paylaşım platformlarında kullanılarak, sürücü ve yolcuları eşleştirip, rotaları optimize etmektedir. Kentin altyapısını oluşturan enerji, su, atık yönetimi ve kamu hizmetleri gibi birçok şehir sisteminden gelen verilerin analizini ve entegrasyonunu kolaylaştırarak, kentlerin bilinçli kararlar almasını kolaylaştırmaktadır. YZ, akıllı kentlerde enerji tüketimini optimize etmek için kullanılmaktadır. Akıllı şebekeler, binalar ve yenilenebilir enerji kaynaklarından gelen verileri analiz ederek, enerji dağıtımını daha verimli hale getirmekte, enerji israfını azaltmaktadır. YZ, ulaşım altyapısındaki yollar, köprüler ve demiryollarının bakım ihtiyaçlarını önceden tahmin edebilmektedir. Sensör verileri ve geçmiş bakım kayıtlarını analiz eden YZ algoritmaları, donanım arızalarını öngörerek, gerekli bakım işlemlerinin önceden planlanmasını sağlamaktadır. YZ tabanlı park sistemleri, boş park yerlerini tespit edebilmekte, sürücüleri bu alanlara yönlendirerek ve park yerlerini optimize ederek trafik sıkışıklığını azaltmaktadır (Chaurasia, 2023:126).

YZ akıllı şehirlerde IoT ile entegre etmek kentsel gelişimi ve yönetimi devrim niteliğinde değiştirebilirken, aynı zamanda gizlilik, veri güvenliği ve YZ algoritmalarındaki olası önyargılar konusunda endişeleri de gündeme getirmektedir (Alahi, vd., 2023:3).

3.4.Robotik ve Otonom Sistemler

Robot, belirli görevleri kendi başlarına (otonom olarak) veya uzaktan kumandayla yerine getirmek üzere tasarlanmış mekanik cihazlardır. Bu mekanik cihazlar, çoğu zaman insanlar için hayati risk oluşturacak veya insanların pratik bir şekilde yapamayacağı işler için kullanılmaktadır. Robotlar, üretim ve montaj hatlarında kullanılan endüstriyel robotlar, insanlarla etkileşime girerek çeşitli alanlarda yardımcı olmak için tasarlanmış insansı robotlara kadar çeşitli biçimlerde olabilir. Robotik ise robotların incelenmesini, tasarlanmasını ve uygulanmasını kapsayan, makine mühendisliği, elektrik-elektronik mühendisliği, bilgisayar bilimleri, YZ ve diğer disiplinleri birleştiren disiplinler arası bir alandır. YZ, modern robotikte önemli bir rol oynamaktadır, robotların çevrelerini algılamalarını, kararlar almalarını ve deneyimlerden öğrenmelerini sağlayarak yeteneklerini artırır ve daha bağımsız hale getirir. YZ'nin robotikle bütünleşmesi, robotlar daha akıllı ve çok yönlü hale gelerek, karmaşık görevleri yüksek verimlilik ve doğrulukla gerçekleştirmelerine olanak tanımaktadır (Teli, vd., 2023:783).

Robotların, bilenen veya bilinmeyen durumlar karşısında insan yardımı olmadan kendi kendilerine karar verebilme yetenekleri otonom özelliği olarak ifade edilmektedir. Otonom robotlar sensörlerden almış oldukları verileri analiz, yorum süreçlerinden geçirip verdiği karar sonucunda bir eylem oluşturması prensibi ile çalışır. Otonom robotlar, verilen talimatlar doğrultusunda hareket eden, atanmış görevler doğrultusunda gerekli bilgileri işleyebilen ve programlandıkları rota üzerindeki engellere takılmadan hedeflerine ulaşma yeteneğine sahip sistemlerdir. Günümüzde otonom robotlar birçok alanda önemli görevler üstlenmektedir (Kurtboğan, 2023:72).

YZ'nın robotik sistemlerde uygulanması farklı endüstrilerde çeşitli kullanım imkânı sunmuştur. Robotikteki YZ keşif ve araştırmada hayati bir rol oynamakta, robotların uzayı, su altı ortamlarını ve tehlikeli alanları keşfetmesini sağlamaktadır. Sağlık ve tıp alanında; YZ destekli cerrahi robotlar, cerrahların ameliyatları daha fazla hassasiyet ve el becerisiyle gerçekleştirmesine yardımcı olmaktadır. Bu robotlar, gelişmiş görselleştirme,

stabilite ve hareket ölçeklemesi sunarak daha küçük kesiler, hastalara daha az travma ve daha hızlı iyileşme süreleri sağlar. Tıbbi prosedürler sırasında tekrarlayan ve hassas görevleri gerçekleştirebilir. Örneğin, robotlar beyin tümörü çıkarmak için nörocerrahi prosedürlerde kullanılmaktadır. Endüstri alanında; üretim sektöründe, YZ destekli robotlar tekrarlayan ve emek yoğun görevleri otomatikleştirerek üretim hatlarını dönüştürmektedir. Bu robotlar yüksek hassasiyetle montaj, kaynak, boyama yapmakta ve depolardaki malların paketlenmesi, sıralanması ve toplanması işlemlerini yapabilmektedir. Günlük yaşam alanında; YZ destekli robotik elektrikli süpürgeler ve paspaslar, evlerde otonom bir şekilde gezinerek engellerden kaçarak ve çeşitli zemin yüzeylerini etkili bir şekilde temizleyebilmektedir. Bu robotlar, çevreyi haritalamak, temizlik yollarını optimize etmek ve farklı oda düzenlerine uyum sağlamak için sensörler ve YZ algoritmaları kullanmaktadır (Teli, vd., 2023:784).

Günümüzde insan fizyolojisini ve davranışlarını model alarak geliştirilmiş robotlar bulunmaktadır. Bu robotlar insan benzeri baş, gövde, kollar ve bacaklarla donatılmış, hatta bazıları insanın yüz ifadelerine sahip olacak şekilde tasarlanmıştır (Teli, vd., 2023:785). Örnek olarak, 2016 yılında Hanson Robotik tarafından Sophia isimli robot geliştirilmiştir. Sophia, insan benzeri ifadeler sergileyebilen ve insanlarla etkileşime girebilen gerçekçi bir insansı robottur. Araştırma, eğitim ve eğlence için tasarlanmıştır. Doğal dil işleme ve konuşma, yüz tanıma, görsel algılama ve diğer YZ tabanlı davranışlarla donatılmıştır. 2017 yılında Suudi Arabistan devleti tarafından Sophia'ya fahri vatandaşlık verilmiştir, aynı yıl Birleşmiş Milletler Kalkınma Programı tarafından inovasyon şampiyonu ödülü verilmiş ilk insan olmayan varlık olmuştur (Robots, 2024).

Genellikle askeri ve güvenlik amacıyla üretilen silahlı otonom robotlarda bulunmaktadır. Örneğin, 2024 yılında Türkiye'de düzenlenen SAHA EXPO Savunma ve Havacılık fuarında, Türkiye'nin ilk silahlı robotu SARBOT tanıtılmıştır. SARBOT'un 2022 yılında üretilen ilk versiyonuna silah, lazer görüntü algılama, ışın algılama ve mesafe ölçme donanımları entegre edilmiş gelişmiş versiyonuyla tanıtılmıştır (Kazbek, 2024).

3.5.İnsansız Hava Araçları

İnsansız Hava Aracı (İHA); içinde pilotu ve yolcusu olmayan, yalnızca amaca uygun ekipman (fotoğraf makinesi, video kamera, lazer tarama cihazı, GNSS vb.) taşıyan,

uzaktan kumandalı veya otomatik olarak görev yapabilen bir çeşit uçaktır (THK, 2024). Dünya genelinde benzer sistemler için İnsansız hava sistemi, uzaktan kontrollü hava gücü veya insansız hava saldırı aracı gibi ifadeler kullanılmaktadır (Taşkesen, 2020:278). ABD Deniz Kuvvetleri tarafından 1936 yılında başlatılan "Hedef Uçak" projesinin ismi olarak, İngilizce erkek arı anlıma gelen "Drone" ismi kullanılmış, 1990'lı yıllarda askeri sektörün gelişmesine paralel olarak, Drone kelimesi yerine, bütün bir sistemi ifade etmek için İnsansız Hava Aracı ifadesi kullanılmaya başlanmıştır (Karaağaç, 2024).

Teknolojinin gelişmesi ile orantılı olarak farklı türde İHA'lar üretilmeye başlanmıştır. Birçok İHA türünün olması nedeniyle, Dünya üzerinde de teknik özelliklerine ve kullanım alanlarına göre farklı sınıflandırmalar yapılmaktadır (Genç ve Erciyes, 2020:37). İnsansız hava araçları, kullanım alanlarına göre; Haritacılık, istihbarat, gözetleme, keşif, güvenlik, terörle mücadele, tarım uygulamaları, sınırların kontrolü ve korunması, mayın arama ve imha etme, kentsel dönüşüm, fotoğrafçılık, madencilik, sağlık, afet yönetimi, arama ve kurtarma çalışmaları, nakliye (yemek siparişi, kargo taşımacılığı), askeri amaçlı, kaçakçılıkla mücadele, biyolojik, kimyasal ve radyolojik tarama olarak sınıflandırılabilir (Akçay, 2021:94).

İHA'lar için en önemli konulardan biri, gövdelerine bağlanan kızıl ötesi/termal kameralar ve sensörlerdir. İHA'lara yerleştirilen sensör ve kameralar, geniş çerçevede insan görüş alanı veya ötesindeki verileri toplayabilir ve elde ettikleri görüntüleri yer kontrol istasyonuna gönderirler. İHA'lar farklı özelliklerde sensörler vasıtasıyla çeşitli görevler icra edilebilirler. Günümüzde sivil alanda ölçüm, gözetleme ve araştırma maksatlarıyla büyük çoğunlukta optik görüntüleme sistemleri kullanılmaktadır. İHA'lar aracılığı ile toplanan yüklü miktarda video verisi, plaka okuma ve yüz tanıma yazılımları gibi gelişmiş video analizleri kullanılarak bireylerin toplum içinde veya özel mülklerinde devamlı takibi yapılabilir (Baştürk, 2015:77-79).

İHA'ların yeteneklerini geliştirmek için çeşitli YZ teknikleri kullanılmaktadır. Modern İHA'lar, YZ tabanlı algoritmalar sayesinde herhangi bir insan müdahalesi olmadan otonom bir şekilde hareket edebilirler. İHA'lar uçuş rotası planlamak için takviyeli öğrenme gibi makine öğrenmesi algoritmaları kullanarak, çevresel faktörlere ve hedeflerine göre en uygun yolları hesaplarlar. İHA kontrol sistemleri YZ'yi istikrarlı bir uçuş ve hassas manevralar sağlamak için kullanır. Orantılı-İntegral-Türev (PID)

denetleyiciler, istenen durum ile gerçek durumlar arasındaki hata sinyallerine göre İHA hareketlerini ayarlamaktadır. Karmaşık uçuş dinamiklerini ve kontrol sistemlerini geliştirmek için derin öğrenme, sinir ağları gibi makine öğrenimi algoritmaları kullanılmaktadır. Ayrıca, YZ algoritmaları birden fazla İHA'nın koordinasyonunu sağlayarak operasyonları kolaylaştırmaktadır. İHA'ların birbirleri ile iletişim kurması için Karınca Kolonisi Optimizasyonu ve Parçacık Sürü Optimizasyonu gibi sürü algoritmaları kullanılır, bu sayede İHA'ların iş birliği yapması, görev dağılımı ve kolektif karar alması sağlanmaktadır. (Sai, vd., 2023:714).

4. TERÖR VE SİBER TERÖRİZM

Siber uzay, bilgisayar ve ilişkili sistemlerin, hayatın her yerinde sağladığı kolaylık ile birlikte getirdiği tehlike ve riskler nedeniyle günümüzün en çok anlaşılmaya çalışan ve tartışılan konularından biridir. Bilgisayar sistemleri ve internet teknolojilerinin oluşturduğu siber uzay aynı zamanda etkili bir terör aracı haline gelmesine sebep olmuştur. Ülkelerin sağlık, eğitim, savunma, enerji, maliye gibi sistemlerinde bilgisayar sistemlerinin etkin bir şekilde kullanımı bu alanlarda siber terörizm/savaş eylemlerine açık alan haline gelmektedir. Bu alanlara yapılacak saldırılar ülkelere ciddi boyutlarda zarar vermektedir.

Bu bölümde terör ve terörizm kavramları açıklanacak; ayrıca siber uzay, siber suç, siber güvenlik, siber istihbarat ve siber saldırı yöntemleri ele alınarak siber terörizm kavramı incelenecektir.

4.1.Terör ve Terörizm Kavramı

Etimolojik olarak Latince "terrere", Fransızcada "terreur", İngilizcede "terror" olarak yer alan terör sözcüğü; "korkutmak, korkuyla yönetmek, korkudan dehşete düşürmek" anlamına ge1mektedir. Eski Türkçede "tedhiş" kelimesi; dehşete düşürme, korku verme ve yıldırma anlamlarındaki bir kelime olarak terör kavramına denk düşmektedir (Türk,2017:5). Terörizm, sözlük anlamıyla hedefindeki kişileri, dehşete ve korkuya düşürmeyi amaçlayan bir politika ya da sindirme yöntemlerinin kullanılması olarak tanımlanabilir. Terörizm, belirli birtakım politik argümanlara sahip, silahlı bir grup tarafından, birtakım siyasi hedeflere ulaşmak ve etkilemek istediği kitlenin belirli konularda tutum ve kararlarına etki etmek için toplumda kaos ve korku ortamı meydana getirecek mesaj verme amaçlı sembolik şiddet eylemleridir (Ağır ve Tekin, 2021:2).

Martin'e göre, terörizm, her ne şekilde tanımlanırsa tanımlansın daima toplumların istikrarına ve insanların barış içinde yaşamasına meydan okumuştur. İçinde bulunduğumuz modern çağda, internet, uydu iletişimleri, televizyon ve küresel haberler sayesinde terör olaylarının görüntüleri bir anda milyonlarca insanın evlerine yayılmaktadır. Bu nedenle terörizmin etkisi, teröristlerin vurduğu alanlar veya bölgelerle sınırlı değildir. Bu görüntülerin ve anlık bilginin gücünün farkında olan terörist gruplar

ile terörizme destek veren devletler durumu mümkün olduğunca kendi lehlerine yönlendirmektedirler. Birçok açıdan 21.yüzyıl başlangıcı küresel terörizm çağıdır (Martin, 2017:27).

Teknolojik araç ve gereçlerin hızlı gelişimi ve etkin kullanımı terör örgütlerinin hatta devletlerin eylemlerini, faaliyetlerini sanal ortama taşımaya başlamasına ve her ülkeye hatta her eve girebilecek şekilde alan açmıştır. Teknoloji odaklı olarak değişen bu boyut da siber kavramını ortaya çıkarmaktadır.

Çakmak ve Altunok'a göre, bir ülkenin güvenliğini tehdit eden unsurları, geleneksel olarak iç ve dış tehditler olarak kategorize etmek mümkündür. İç tehditler suç ve terör olarak sınıflandırılırken, dış tehditler ise savaş sınıflaması içinde değerlendirilir. Bu klasik yaklaşımın doğruluğu tartışmaya açıkken, siber tehditleri benzer şekilde iç ve dış tehditler olarak kategorize etmek pek mümkün değildir. Genel itibari ile herhangi bir sınır olmadan yerel ve uluslararası boyutu olmadan siber saldırılar yapmak mümkündür. Ayrıca günümüzde suç örgütleri ve terörist grupların aralarındaki farklar zaman geçtikçe daha muğlak bir hal almakta, önceden birbirinden bağımsız ve ayrı eylem yapan bu grupların çoğu kaynaşmış bir halde tek bir yapı içerisinde görülmekte, uluslararası alanda da faaliyet göstermektedir (Çakmak ve Altunok, 2009:24).

4.2.Siber Uzay (Siber Ortam)

Bilim ve teknoloji dünyasındaki gelişmeler, fiziksel alandan elektronik alana bilgiyi hızlı bir şekilde taşımaktadır. Amerikalı araştırmacı Norbert Weiner 1948 yılında "canlılar ile makinelerdeki kontrol ve iletişim bilimi" anlamına gelen "sibernetik" (cybernetics) kelimesi kullanılmıştır. "Siber" kelimesi de sibernetik kelimesinin bir öneki olarak kelimeyi kısaltmak amacıyla da kullanılmıştır (Çakmak ve Altunok, 2009:25). İngilizcedeki cyber sözcüğünün çevirisi olarak Türkçeye aktarılmıştır. İngilizce sözlüklerde "siber" sözcüğü "bilgisayarla bağıntılı, kullanan ve ilişkili olan" olarak yer almaktadır (Vikipedi, 2024).

Bu kavrama karşılık olarak Türkçede "bilişim" kavramı kullanılmaktadır. Bilişim kelimesi de Fransızca kökenli "informatique" teriminden gelen "enformatik" kelimesinden türetilmiştir ve anlamı şu şekilde ifade edilebilir; *"bilimsel zemine dayanan ve insanların ekonomik, teknik, sosyal alanlardaki iletişimlerinde kullandıkları bilginin,*

özellikle elektronik cihazlar tarafından düzenli, akılcı biçimde işlenmesi ve toplanması bilimidir". Çok belirgin olmamakla birlikte, her ne kadar siber ve bilişim kavramları bazen birbirinin yerine kullanılıyor olsa da "siber" kavramını bilgisayar ve bağlantılı elektronik sistemlerin yer aldığı dijital ortam olarak, "bilişim" kavramı ise bilgi üretmek amacıyla ortamda bulunan sistemlerden etkin olarak faydalanma olarak ifade etmek mümkündür (Çakmak ve Altunok, 2009:26).

Siber uzay (cyberspace) kavramı ilk defa Amerikalı yazar William Gibson tarafından 1982'de yayımlanan "Burning Chrome" isimli hikâye kitabında kullanılmıştır. Kurguladığı karakterler için şifreleme amacıyla "somut bir karşılığı olmayan ve düşünsel çağrışım yaratan" bir kavram olarak kullanmıştır (Çifci, 2017:3).

Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı'nın (UAB), 2016 yılında yayımladığı Ulusal Siber Güvenlik Stratejisi belgesinde siber uzayı: "*Dünya* geneline *ve uzaya kadar yayılmış durumda olan bağımsız bilgi sistemleri veya bilişim sistemleri ile bu sistemleri bütünleştiren ağlardan oluşan sayısal ortam*" şeklinde tanımlamıştır (UAB, 2016:7).

Siber uzay, verilerin içerisinde online olarak depolandığı, iletildiği, paylaşıldığı bilgisayar sistemlerinin ve arka plandaki kullanıcıların dünyasıdır. Siber uzayın bir bilgi ortamı olması onu eşsiz kılan özellikler arasındadır. Oluşturulan, depolanan ve en önemlisi paylaşılan dijital verilerden oluşmaktadır. Siber uzay yalnızca sanal ortam da değildir. Ağ tabanlı bilgisayarların internetini, hücresel teknolojilerini, fiber optik kabloları, kapalı intranetleri ve uzay tabanlı iletişimi kapsayarak, depolanan verilerin akışma izin veren sistem ve altyapıları birleştirir (Singer ve Friedman, 2018:29).

Siber uzay en önemli unsurlarından biri internet olsa da sadece internetle sınırlı değildir. Bilişim teknolojilerini kullanan askeri iletişim ağları, endüstriyel kontrol sistemleri (SCADA), enerji iletim ağları, elektronik komuta sistemleri, cep telefonları, yazılım destekli telsizler, uydu sistemleri, İHA'lar, uçakların sistemlerini yöneten yazılım ve donanım bileşenleri gibi birçok unsur siber uzay elamanıdır. Siber uzayın başlıca aktörleri, devletler, devletlerin güvenlik güçleri, istihbarat kurumları, kamu kurumları, özel sektör ve terör örgütleridir (Çifci, 2017:5).

İnternet kullanıcılarında sürekli artış olmaktadır ve 2023 yılında dünya genelinde 5 milyarın üzerinde kullanıcı olduğu görülmektedir. Yapılan araştırmalarda ise Türkiye'de yaklaşık 3 saati sosyal medyada olmak üzere günlük ortalama 7,5 saat kullanıcıların internette zaman harcadığı görülmektedir. Siber uzaya bağlı unsurların birbiri ile olan bağlantılarının ve iletişimin artması dünya üzerinde üretilen veride büyük bir artış göstermektedir. 2025 yılına kadar bu verilerin yaklaşık olarak $167x10^{12}$ gigabyte ulaşacağı tahmin edilmektedir (UAB, 2024).

Siber uzayın küreselleşen dünyanın önemli ve itici bir gücü olduğu görülmektedir. Siber uzay unsurları sosyal hayatın ve ekonominin merkezinde yer almaktadır. Teknolojik gelişmeler ekonomi, güvenlik, eğitim gibi birçok alanda kolaylık ve fayda sağlıyor olsa da üretilen ve depolanan bilginin bu kadar hızlı ilerlemesi terör örgütlerinin, suç örgütlerinin de dikkatini çekmekte ve önemli riskler oluşturmaktadır.

4.3.Siber Suç ve Siber Güvenlik

Siber suçlar 1960'lı yıllarda ilk olarak ABD'de ortaya çıkmış ve Bilgisayar Suçu "Computer Crime" terimi kullanılmıştır (Sandilaç, 2024:164). Günümüzde bilgisayarların haricinde yazılım tabanlı çalışan, verileri depolayan, işleyen ve ileten elektronik cihazların artması ile birlikte bilgisayara oranla daha geniş bir kavram olan bilişim kavramı öne sürülmüştür. Bilişim suçu ise bilişim sistemlerini kullanarak veya bu sistemlere yönelik işlenen suçlar olarak ifade edilmiştir. Bilgisayar suçu ve bilişim suçu kavramlarının birleşimi olarak siber suç kavramını tanımlamak mümkündür (Bayraktar, 2015:98).

Siber suçlarla ilgili en geniş düzenleme Budapeşte'de 2001 yılında imza altına alınan Türkiye'nin de tarafı olduğu "Avrupa Konseyi Siber Suç Sözleşmesi" dir. Sözleşme siber suçları dört başlık halinde sınıflandırmıştır (AB, 2024). Bunlar;

- Bilgisayar sistem ve verilerinin bütünlüğüne, erişilebilirliğine ve gizliliğine yönelik suçlar başlığı altında; sisteme müdahale, yasadışı araya girme, cihazların kötüye kullanımı, yasadışı erişim, verilere müdahale,
- Bilgisayarla ilişkili suçlar başlığı altında; Bilgisayarla ilişkili dolandırıcılık, bilgisayarla ilişkili sahtecilik,
- İçerikle ilişkili suç başlığı altında; çocuk istismarı ile ilişkili suçlar,

- Telif hakkı ve bağlantılı hakların ihlali ile ilgili suçlar,

Siber suç kavramı, siber uzay ortamında, siber uzayın bileşenleri ile işlenen ve siber uzayın bileşenlerine karşı suçları tanımlamak için kullanıldığı görülmektedir.

Siber güvenlik, ağ sistemlerine ve içerdikleri bilgilere ulaşımı kontrol edebilme kapasitesidir. Aynı zamanda siber dünyadaki ulaşılabilirlik, bütünlük ve gizliliği koruma kapasitesi ile bilgisayar sistemlerinin ve verilerin internetten gelecek müdahalelerden korunmasını sağlamaktır. Siber güvenlik endüstrisi, bilgi teknolojisi, telekom ve endüstriyel alanda, saldırgan ve savunmacı servis ve ürünler üreten şirketlerin birleşiminden oluşmaktadır (Köksoy, 2020:348). Siber güvenlik en genel anlamda, ülkelerin, şirketlerin ve bireylerin siber uzayda bulunan cihazlarını ve bilgilerini yapılacak saldırılardan korumak, yasadışı erişimi engellemek için kullanılan yöntemleri ifade etmektedir (Perwej, vd., 2023:669).

Siber dünya, saldırıya açık birçok hedef barındırmakta ve bu hedeflere yönelik saldırıları kolaylaştıracak imkanlar sunmaktadır. En zayıf aktörlere yapılan saldılar bile asimetrik büyük etkilere neden olabilmektedir. Aynı zamanda siber güvenlikte oluşan açıklar, devletlerin ve insanların siber saldırılara maruz kalmalarına, devletlerin ekonomisi üzerinde olumsuz etkiye neden olabilmektedir. Bu nedenle siber güvenlik, ulusal ve uluslararası güvenlik boyutlarını içermekte, devletler siber güvenlik konusunda strateji üretmektedirler (Köksoy, 2020:348).

4.4.Siber İstihbarat

Siber istihbarat, bir devletin siber uzaydaki yazılımları, fiziksel cihazları ve bu alanda çalışan insan kaynağının niteliksel ve niceliksel özellikleri hakkında kapsamlı bilgi toplanması, analiz edilmesidir. Siber istihbarat operasyonlarının etkin bir şekilde yürütülebilmesi için, hedef ülkenin siber uzaydaki varlıklarına ilişkin ön istihbarat çalışması yapılarak, siber saldırı teknikleri ile sosyal mühendislik metodolojileri gibi çeşitli araçlar kullanılarak sistematik operasyonlar düzenlenmektedir (Keleştemur, 2018:27) Başka bir ifade ile siber istihbarat, çağdaş bilgi teknolojileri, fiziksel casusluk yöntemleri ve savunma stratejilerinin birleşimidir. Siber istihbaratın temel işlevi, sanal ortamda hassas bilgileri hedef alan virüsler, siber korsanlar ve teröristlere karşı proaktif koruma sağlamaktır (Karaağaç, 2024:124).

4.5. Siber Saldırı ve Yöntemleri

Çifci, Siber Saldırı kavramını *"Siber saldırı, siber uzayda bulunan verileri istismar etmek, değiştirmek, tahrip etmek, sistemlere erişimi engellemek veya zarar vermek maksadıyla siber uzayda gerçekleştirilen faaliyetlerdir."* şeklinde tanımlamaktadır. (Çifci, 2017:6)

Siber saldırılar gerçekleştirilirken birçok yöntem kullanılmaktadır. Bilişim sistemlerinin aşırı yüklenmesinin sağlanarak kamu hizmetlerinin işlevsiz hale getirilmesi, propaganda yapmak veya bilgi çarpıtma amacıyla ülkelerin veya ticari şirketlerin internet sayfalarının bozulması, bilişim sistemlerine yetkisiz giriş yaparak verilerin çalınması veya bozulması, kontrol sistemlerine müdahale ederek manipüle etmek veya altyapıyı kullanılmaz hale getirmek olarak sınıflandırılabilir (Çakmak ve Altunok, 2009:30).

Dünya Ekonomik Forumu (WEF)'un 2024 yılı Küresel Riskler Raporunda, siber tehditler önemli küresel risklerden biri olarak görülmektedir. 2024 yılı içerisinde mevcut olan küresel riskler içerisinde YZ tarafından üretilen yanlış bilgiler ve dezenformasyon 2. sırada, siber saldırılar ise 5. sırada yer almaktadır. 2026 ve 2034 yılına kadar olan 2 ve 10 yıllık dönemlerdeki küresel risk tahmininde siber tehditler yine ilk beş sırada yer almaktadır. Raporda siber tehditlerin hem yerel hem de ulusal düzeyde ekonomik, jeopolitik ve sosyolojik açıdan geniş bir etki alanına sahip olduğu vurgulanmaktadır (WEF, 2024).

ABD'de faaliyet gösteren siber güvenlik şirketi Cybersecurity Ventures'ın 2024 yılı raporuna göre, siber saldırıların 2024 yılında dünya genelinde 9,5 trilyon dolarlık zarara yol açması beklendiği, bu rakamın bir ülke ekonomisiyle karşılaştırıldığında Çin ve ABD'nin ardından dünya genelinde üçüncü büyük ekonomi olacağı ve tüm ulusların servetini geride bırakacağı, 2025 yılana kadar ise bu rakamın 10,5 trilyon dolar ulaşmasının beklendiği belirtilmektedir. Ayrıca 2030 yılına kadar dünya genelinde 6 yaşından büyük insanların %90'nın internet ortamını kullanacağı öngörülmektedir (Morgan, 2024).

Teknolojinin çok hızlı değişimi ile birlikte siber saldırı yöntemleri de hızlı değişim, gelişim ve çeşitlilik göstermektedir. Bu nedenle siber terörizm ile ilgili olduğu düşünülen bazı siber saldırı yöntemleri açıklanmaya çalışılacaktır.

4.5.1. Kabloya Saplama Yapma (Wire Tapping)

Kabloya saplama yapma, güvenlik altına alınmamış iletişim ağı kablolarına, özel aletler kullanarak fiziksel olarak saplama yapılarak bağlantı kurulmasıdır. Bu yöntemle iki taraf arasındaki tüm bilgi trafiğinin ele geçirilmesi mümkündür. Telefon görüşmelerinin de bu yöntemle dinlemek mümkündür (Çifci, 2017:158).

4.5.2. Arka Kapı (Backdoor)

Bilişim sistemleri üzerinde yapılan normal incelemeler de fark edilemeyecek şekilde, standart kimlik onaylama sürecini atlamayı ya da kurulmuş olan sistem hakkında bilgi sahibi kişilerin sistemlere uzaktan bağlanmasını sağlayan yöntemlere arka kapı denilmektedir. Arka kapılar sistemlere bağlanmayı sağlayan gizli geçitlerdir. Bazen, sistemi tasarlayan yazılımcılar tarafından test amacıyla bırakılan ancak kapatılması unutulan güvenlik açıkları olarak ortaya çıkabilmektedir (Sağıroğlu ve Canbek, 2007:126).

4.5.3. Hizmet Dışı Bırakma (Denial of Service-DoS) ve Dağıtık Hizmet Dışı Bırakma (Distributed Denial of Service-DDoS)

Siber saldırı yöntemleri arasında en yaygın ve en sık kullanılanı hizmet dışı bırakma (DoS/DDoS) saldırılarıdır. Bu saldırı türünde amaç bilişim sistemlerinin kullanıcı isteklerine cevap veremez hale getirilerek devre dışı bırakılmasıdır. DoS (Denial of Service) saldırıları tek bir kaynaktan gelir ve hedef sistemlerin başka sistemlerle iletişim kurmasını engellemeyi amaçlar. DoS saldırıların daha büyük bir etkiye sahip olan türü DDoS (Distributed Denial of Service Attack) saldırılarıdır. Bu saldırı türü de hedefi hizmet dışı bırakmayı amaçlar fakat saldırılar birden fazla kaynaktan yapılır. DoS saldırısında saldırgan tek bir bilgisayar kullanarak eylemi gerçekleştirirken, DDoS saldırıları için Robot Network (Robot Bilgisayar Ağları-Bot-Net) denilen yapılar kullanılır. Bu yapılarda binlerce kullanıcının bilgisayarına önceden bulaştırılmış zararlı yazılımlar kullanılır. Kullanıcı bilgisayarlarını Bot-Net yapısına dahil etmek için genelde lisansız (crackli) işletim sistemleri ve programlar, korsan yazılımlar kullanılır. Kullanıcılar bilgisayarlarını rutin kullanımı sırasında farkında olmadan Başbakanlığa veya Fransa'da faaliyet gösteren bir şirkete yönlendirilmiş bir Dos/DDoS saldırısının parçası olabilir (Başaran, 2021:29). Örneğin dünyada yapılan en büyük DDoS saldırısı

2023 yılında Google'ın kullanıcılara ve şirketlere sunmuş olduğu veri depolama platformu olan Google Cloud'a yapılmış ve sunuculara saniyede 398 milyon istek gönderildiği tespit edilmiştir (Warburton, 2024).

4.5.4. Oltalama (Phishing)

Oltalama saldırıları, insanların kredi kartı bilgilerini, kullanıcı adı parolalarını ve diğer özel bilgilerini ele geçirmek için yapılan saldırılardır. Bu saldırılar psikolojik ve sosyal mühendislik teknikleri kullanılarak yapılır (Zieni, vd., 2023:18499). Sosyal mühendislik, bilişim sistemlerine, veriye, ağa, hassas bilgilere ulaşmak için teknik yöntemler yerine insan psikolojisi ve zaaflarını kullanılarak çeşitli ikna ve dolandırma yöntemleri kullanılarak gerçekleştirilmesidir. Sosyal mühendislik yöntemleri çok çeşitlidir, sosyal medyada arkadaşlık kurarak ya da kendisini akrabanız, arkadaşınız olarak tanıtarak, ya da bir tanıdığınızın hesaplan üzerinden sizi dolandırabilirler (Akyeşilmen, 2018:80).

Teknik anlamda karmaşık olmayan ve en eski saldırı yöntemi olmasına rağmen günümüzde aktif ve başarılı bir saldırı yöntemi olan oltalamada kullanıcıların ayırt etmesinin çok güç olacağı şekilde web siteleri taklit edilerek kimlik avı yapılır. Yapılan araştırmalarda 2022 yılının başlarında bir milyondan fazla taklit edilmiş web sayfası bulunduğu belirtilmektedir. Oltalama saldırıları hem bireyleri hem de şirketleri öncelikle ekonomik anlamda olmak üzere birçok konuda olumsuz etkileri olan önemli bir güvenlik tehdidir (Zieni, vd., 2023:18499).

4.5.5. Ortadaki Adam (Man in The Middle- MitM)

Ortadaki adam saldırıları ile karşılıklı iletişim halinde olan bir kullanıcı ile bir uygulama ortasına gizlice yerleştikten sonra kredi kartı numaraları, hesap bilgileri ve oturum açma kimlik bilgileri gibi hassas veriler ele geçirilir. İki kişi arasındaki özel iletişimlerde bu yöntemler dinlenebilir, iki kişi arasındaki mesajları yönlendirebilir ve iletilebilir, bazen konuşmayı kontrol etmek için mesajlar değiştirilebilir. Örneğin, yeterli derecede güvenliği olmayan ve herkese açık bir Wi-Fi ağında, saldırgan kendini kullanıcının cihazı ile ağ arasına yerleştirerek ziyaretçiye ait tüm bilgilerin kendisinden geçmesini sağlayabilir (Lindemulder ve Kosinski, 2024).

4.5.6. Açık Mikrofon Dinleme

Mikrofon veya kamera özellikli cihazlara casus yazılımlar aracılığıyla, sahibinin haberi olmadan, cihazın mikrofon veya kamerasını açılarak ortam dinlenmesi ve izlenmesinin yapılmasıdır. 2009 yılında GhostNet adı verilen casus yazılımın 103 ülkede görüldüğü, cihazların dâhili kamera ve mikrofonlarını uzaktan açılarak, görüntü ve ses kayıtlarını ele geçirip aktardığı, özellikle devlet kurumlarının ve elçiliklerde bulunan bilgisayarlara yüklendiği, verilerin ise Çin'e gönderildiği ileri sürülmüştür (Çifci, 2017:165).

4.5.7. Yapısal Sorgu Dili Enjeksiyonu (Structured Query Language-SQL)

SQL, yazılımların veri tabanını yönetmek için kullanılan yazılım dilidir. Bu yazılım dili ile veri tabanına veriler eklenip, silinip, değiştirilip ve güncellenebilir. Bu saldırı yöntemi ile SQL dili kullanan sunucuya kötü amaçlı bir SQL kodunu enjekte ederek veri tabanındaki bilgilere erişim sağlamış olur (Fırat, 2022:61).

4.5.8. Akıllı Bombalar (Logic Bombs)

Akıllı bombalar, içinde zararlı yazılım bulunduran ve geliştiricisi tarafından belirlenen şartlar oluşana kadar uyku durumunda bekleyen, belirlenen şartlar oluşana kadar bekleyip kendini muhafaza eden yazılım türüdür. Hedef sistemleri tamamıyla etkisi altına alabilirler ve dışarıdan müdahale edilerek çalıştırılabilirler. Amerikan Merkezi İstihbarat Teşkilatı'nın (CIA), soğuk savaş döneminde Sovyetler Birliği'ne ait bir boru hattını imha etmek için bu siber saldırı yöntemini kullanmıştır (Tabacı, 2020:28).

4.5.9. Kötü Amaçlı Yazılım (Malware)

Kötü amaçlı yazılımlar kullanıcı izni olmaksızın sistemimize yüklenen zararlı yazılımlardır. Bu yazılımlar, zararlı olmayan uygulamaların arkasına gizlenebilir, kendisini internet üzerinden klonlayıp çoğaltabilir. Microsoft Word ve Excel gibi uygulamaların içerisinde yer alan makro virüsler, sürekli olarak kendini değiştiren polimorfik virüsler, sabit disklerin önyükleme işlemlerinin gerçekleştirildiği ana yükleme bölümünün ilk sektörlerine yerleşip ve çoğalan boot virüsleri, panik yaratmak için hazırlanıp veya daha sonradan başka bir virüsün etkisini artırmak amacıyla kullanılan hoaxlar, bilgisayara bulaştıklarında kendisini yaratan veya gönderen kişiye hizmet eden trojan virüsleri, bulaştıkları bilgisayar sistemlerinde birtakım 'delikler' açan ve

kendilerini kopyalama özelliğine sahip olan worms (Solucanlar) bazı kötü amaçlı yazılım türleridir (Başakçi, 2019:37).

2000 yılında sistem dosyalarını silmek için geliştirilen “I Love You” virüsü 15 milyar dolar, 2001 yılında Beyaz Saray’da arka kapı oluşturmak amacıyla geliştirilen “Code Red” 2 milyar dolar, 2003 yılında e-posta trafiğini etkilemek için geliştirilen “Sobig.F” 37 milyar dolar ve 2004 yılında “MyDoom” 38 milyar dolar, 2008 yılında bilgisayarı açık kapı haline getirmek için geliştirilen “Conficker” zararlı yazılımı 9,1 milyar dolar zarara yol açmıştır (Alkan ve Sağıroğlu, 2018:262).

4.6. Siber Terörizm

Siber terörizm kavramı ilk defa 1980'lerde Barry Collin tarafından "sibernetik ve terörizmin yakınlaşması" olarak tanımlanmıştır (Çifci, 2017:9). Siber Terörizmin en çok kabul gören tanımı Dorothy E.Denning tarafından şu şekilde yapılmıştır:

> *Siber terörizm, terörizm ve siber ortamın yakınlaşmasıdır. Genelde, bir devleti veya toplumu siyasi ya da sosyal amaçlar doğrultusunda korkutmak, zorlamak amacıyla yapılan, bilgisayarlara, ağlara ve burada depolanan verilere yönelik yasadışı saldırılar ve saldırı tehditleri anlamına geldiği anlaşılmaktadır. Ayrıca, bir saldırıyı siber terörizm olarak nitelendirilmek için, kişilere veya mülke yönelik şiddetle sonuçlanmalı veya en azından korku yaratacak kadar zarar vermelidir. Ölüm veya yaralanmaya, patlamalara, uçak kazalarına, su kirliliğine veya ciddi ekonomik kayıplara yol açan saldırılar buna örnek olabilir (*Denning, 2000).

Amerikan Federal Soruşturma Bürosu'na (FBI) göre siber terörizm " gizli örgütler veya devlet altı grupların savaş dışı hedeflere yönelik yapılan ve şiddete yol açan, bilgisayar yazılım, sistem ve verilerini hedef alan önceden planlanmış siyasi amaçlı saldırı” olarak tanımlamaktadır (Singer ve Friedman, 2018:135).

Sonuç olarak, siber terörizm genellikle gizli örgütler veya devlet dışı aktörler tarafından gerçekleştirilen, devletler veya toplumlar üzerinde korku ve kaos yaratmayı amaçlayan, bilgisayar sistemleri, ağlar, veri altyapılarına yönelik yasa dışı ve yıkıcı dijital saldırılardır. Bu eylemler, siyasi veya sosyal amaçlarla ciddi maddi ve manevi zararlar doğurabilir.

Terör "siyasal davranışları etkilemek amacıyla tasarlanmış, olağan dışı yollarla gerçekleştirilen şiddet eylemi ya da şiddet tehdidi barındıran sembolik bir fiildir" şeklinde

tanımlanabilir. Terörizm ise sistematik olarak şiddetin kullanıldığı bir yöntemdir, amacı korku iklimi yaratmaktır ve önceden planlanır, tek kurbandan daha çok geniş bir kitleyi hedef alır, sivilleri de kapsayan sembolik ve sıradan saldırıları içerir. Terörizm de özellikle devletlerin ve toplumların siyasi davranışlarını etkilemek için siyasal bir amaçla hareket edilir, bu hareket korku veren bir sonuç doğurur ve neticesinde toplulukları etkileyen karar organlarının davranışlarını etkilemek amaçlanır. Bu kapsamda, herhangi bir devlet organına yapılacak saldırının temel amacı o kurumun hizmetlerini tamamen sona erdirmek değil, toplumda korku duygusunun hâkim olmasını sağlayarak, toplumun gözünde devleti küçük düşürmektir. Kimlere ve nereye güvenileceğini bilemeyen toplumun paralize edilmesi kolaylaşır ve terörizm de böylelikle nihai amacına ulaşır (Çakmak ve Altunok, 2009:36-37).

Terör örgütleri siber ortama büyük ilgi göstermekte ve bu ortamda eylemlerini yapmaya çalışmaktadır. Bu ilginin sebebini Weimann şu şekilde özetlemektedir; Siber ortam, merkezi değildir, kontrol veya kısıtlamaya tabi tutulamaz, sansürlenmez ve herkese ücretsiz erişime izin verir, modern terör örgütlerinin tipik, gevşek bir şekilde örgütlenmiş hücre, bölüm ve alt grupları için, internet gruplar arası ve grup içi iletişim için hem ideal hem de hayati bulmaktadır ve e-posta, sohbet odaları, e-gruplar, forumlar, sanal mesaj panoları, Youtube, Google Earth gibi birçok avantaj sunar, eylemleri için düşük finansal ihtiyaç ve az sayıda personel ihtiyacı gerektirir, klasik terör eylemlerinden daha kolaydır, ileri bir teknoloji kullanılması gerekmez, muhtemel hedef sayısını ve çeşitliliği çoktur, siber terör saldırılarını yakalanma ve tespit edilme olasılıklarını çok düşürerek çok uzak bir mesafeden gerçekleştirebilirler, siber saldırıların avantajları nedeniyle medyada daha çok yer bulma imkanı sağlarlar (Weimann, 2006:4-6).

Teröristlerin ağırlıklı olarak iki amaçla siber ortamdan faydalandıkları söylenebilir. Birincisi, teröristler internet teknolojilerini kullanarak hem aktif bir iletişim sağlayıp hem de eğitim faaliyetlerini gerçekleştirirler. Teröristler, örgüt üyeleri ve sempatizanlarla iletişim kurarak, örgüt propagandası yapılabilmekte, örgüt üyelerine talimat aktarılabilmekte ve hatta internet üzerinden online eğitim yapabilmektedir. Bu eylemleri siber terörizm olarak doğrudan nitelendirmek mümkün değildir. İkincisi, siber ortam aracılığı ile ağ yapılarına ve bilgisayarlara saldırılması, sistemlere yetkisiz girişler yapması gibi eylemler siber terörizm olarak adlandırılabilir. Örneğin El-Kaide terör örgütünün Avrupa'daki finansal alt yapısının büyük bir kısmı bilgisayar sistemleri

aracılığı ile yapılan kredi kartı sahteciliğine dayandırmaktadır (Çakmak ve Altunok, 2009:38-39).

Dolayısıyla siber terörizm kavramının terörizmin özelliklerini de taşıması gerekir, siber terörizm siyasal içeriğe sahip, siyasi bir amaçla önceden planlanan, topluma korku ve panik yaratmayı hedefleyen, bilgisayar sistemlerini ve internet teknolojilerini kullanarak yapılan eylemler olarak ifade edilebilir.

Dijital Teknolojiyi kullanan en iyi terör örgütü 1984 yılında Tokyo'da Shoko Asahara isimli yoga eğitmeni tarafından kurulan Aum Shinrikyo terör örgütüdür. The M Grup adı verilen kendilerine ait bir bilgisayar firması olan terör örgütü, bu firmanın bağlantı kimliğini gizleyerek Japonya'da 10 devlet ve 190 özel sektör kuruluşuna hizmet vermiştir. Mart 2000'de ortaya çıkan bu durum Newsweek dergisinin 2000 raporunda "Aum terör örgütünün gizli silahı" olarak yer almıştır. Bağlantılı bulunduğu bilgisayar firmalarından yılda yaklaşık 65 milyon Amerikan doları gelir elde etmiştir. 1995 Tokyo Metrosu'ndaki sarin gazı eyleminde, metro havalandırma sisteminde ve tren kontrol sistemlerinde yaptığı değişiklikle sarin gazının etkisini artırmaya çalıştığı iddia edilmiş, Japon hükümet yetkilileri bunu doğrulamamıştır. 2000 Mart ayında 150 polis aracının birbirine girmesine neden olmuştur. Dijital teknolojiyi kullanan diğer bir terör örgütü dünya üzerinde ağ yapısı ile hareket eden El Kaide'dir. Afganistan'da mücahit kampında bulunan El Kaide militanına ait bir diz üstü bilgisayarda, Amerikan diplomatlarına ait e-posta adresleri ve banka hesap numaraları bilgileri bulunmuştur. Vatikan'ın web sitesine, Guantanamo web sayfasına ve Amerikan borsasına yönelik siber saldırılar El-Kaide tarafından gerçekleştirilmeye çalışılmıştır. Pakistan'daki terörist eğitim merkezlerinde bilgisayar hackerlığı ve siber savaş konularında eğitim verilmektedir. El-Kaide'nin Bali saldırıları sorumlusu İmam Samudra hapishanede hayatını yazdığı kitabında "Hackerlama neden olmasın?" diyerek teröristler için yol gösterici olmaya çalışmış ve bu alandaki faaliyetleri özendirmek istemiştir (Çakmak ve Altunok, 2009:97-98).

Devletler, siber terör saldırılarının arkasında başka devletlerin dolaylı veya dolaysız desteğini tespit ettiklerinde, bu durum bir siber savaşın kıvılcımı haline gelebilir. Siber Uzay içerisinde yer alan Siber Savaş kavramında ülkeler arası yapılan siber saldırılar ve savunmalar söz konusudur ve ülkelerin gelişmişlik seviyelerine göre de siber güç potansiyellerini ortaya çıkarmaktadır. Örneğin, 24 Şubat 2022 tarihinde resmi olarak

başlayan Rusya ve Ukrayna arasındaki çatışmalarda, her iki ülkenin devlet destekli gruplar aracılığıyla yürüttüğü siber operasyonlar, bu iki ülke arasında siber savaş olarak tanımlanabilecek bir sürece yol açmıştır. Her iki ülkenin de devlet destekleri hackerları ve siber ordusu tarafından birbirlerine yapmış olduğu siber saldırılar olmuş hatta kontrolden çıkan bazı hacker grupları dünya genelinde Avrupa ülkelerine de siber saldırılar düzenlemiştir (Paltacı, 2022:3).

Siber savaş kavramının en yaygın kullanılan tanımını ABD eski başkanı Bush döneminde siber güvenlik danışmanı olarak çalışan Richard Clarke yapmıştır. Siber savaş (cyberwar, cyber warfare) Clarke'a göre, "Devletlerin birbirlerinin bilgisayarlar sistemlerine veya ağ alt yapılarına zarar/hasar vermek ya da ağ altyapılarında kesinti yaratmak amacıyla gerçekleştirdikleri sızma faaliyetleridir." (Clarke ve Knake, 2010:8).

Çinli stratejist Sun Tzu'dan esinlenerek Jeffrey Carr tarafından yapılan tanım da ise, "Düşmanla kavga etmeden, kanını dökmeden savaşma ve düşmanın kanını akıtmadan onu yenme sanat ve bilimi" olarak siber savaşı tanımlamıştır (Çifci, 2017:7).

Clarke siber savaş için şu tespitlerde bulunmuştur;

- Siber savaş gerçektir: Bugüne kadar gerçekleşen siber savaşlar, neler yapılabileceğinin göstergesi olmaktan çok uzaktır. Saldırganlar daha güçlü siber silahlarını ortaya çıkarmak istemedikleri tahmin edilebilir. Ulusların bir siber savaşta yapabilecekleri, modern bir ulusu yıkıma uğratabilir.
- Siber savaş ışık hızında gerçekleşir: Fiber-optik kablolarda saldırı paketleri iletilirken, bir saldırının başlatılması ile sonucu arasındaki süre zar zor ölçülebilir, dolayısıyla saldırıya uğrayanların kriz anında karar verme süreci zayıflar.
- Siber savaş küreseldir: Dünya çapında daha önceden gizlice ele geçirilen sunucular ve bilgisayarlar, herhangi bir çatışmada sırasında ele geçirenler tarafından kullanılır dolayısıyla siber saldırılar hızla küreselleşir. Birçok ülke hızla savaşın içine çekilir.
- Siber savaş klasik savaştan önce başlar: Bankalardan, hava savunma sistemlerine kadar insanların güvendiği birçok sisteme siber uzaydan erişilebilir ve bir ülkenin geleneksel savunmasını savaşmadan hızla ele geçirilebilir ya da devre dışı bırakılabilir.

- Siber savaş başladı: Çatışma beklentisi içinde olan uluslar şimdiden savaş için hazırlıyorlar. Birbirlerinin ağlarına ve altyapılarına saldırıyorlar, tuzak kapıları ve mantık bombaları yerleştiriyorlar. Siber savaşın sürekliliği, savaşın ve barışın iç içe geçmesi, yeni bir boyut yaratarak dünya düzenini tehlikeli bir belirsizliğe sürüklüyor (Clarke ve Knake, 2010:24-25).

Siber savaşlar taktiksel, stratejik ve operasyonel olmak üzere her düzeyde uygulanabilir olma ve istenen etki elde edilebilme özelliğine sahiptir. Siber savaşların odak noktasında devletlerin kritik bilişim altyapıları bulunmaktadır. Siber savaş yöntemleriyle bu altyapılar hizmet dışı bırakılabilmekte, devletlerin askeri ve sivil kritik ve hassas verilerine ulaşılabilmekte, söz konusu veriler çalınabilmekte ve hatta silinebilmektedir. Saldırı düzenlenen devletin vatandaşlarını ve yönetimini, siber ortamda yapılan dezenformasyon sayesinde psikolojik olarak baskı altına alınabilmektedir. Dolayısıyla toplumun bütün kesimini etkisi altına alarak, çatışmacı bir ortam yaratabilmektedir. Teknoloji geliştikçe ve bilgisayar kullanıcı sayısı arttıkça, siber taarruzların hedef kitlesi her geçen gün daha da artmaktadır. Bu kapsamda yüksek teknolojinin kullanıldığı ve bilgi sistemlerinin yaygınlaştığı askeri alanlar da siber savaşın genişleyen hedef kitlesi içinde önemli bir yere sahip olmaktadır. Siber savaşlar savaş ortamlarında yapılan klasik savaşlara destek olarak kullanılabileceği gibi klasik savaşlardan bağımsız bir savaş olarak da icra edilebilmektedir. Siber savaşların oluşturacağı etkinin şiddeti için; karşıdaki ülkelerin bilgi teknolojilerini ne kadar etkin ve yaygın olarak kullandığı, kritik bilgi sistem altyapılarında ne kadar güvenlik önlemleri aldığı, kullanıcıların ne kadar bilinçli olduğu gibi etkenler önemli rol oynamaktadır. Siber savaşların, klasik savaşlarla kıyaslandığında bir takım üstünlüklerinin olduğu görülmektedir (Bayraktar, 2015:49). Siber savaş, saldırının ışık hızında gerçekleşip, kaynağının tespit edilememesi sebebiyle görünmez, hasarın tespit edilememesi nedeniyle de anlaşılamazdır. Ayrıca klasik savaşlarda kullanılan silah sistemlerinin teknolojik gereksinim sebebiyle maliyetleri yüksek olup, kullanıcılarının ölüm riski bulunmaktadır. Asimetrik savaş olarak nitelendirilen siber savaşlarda ise silah sisteminin operatörü için hayati bir risk bulunmamaktadır. Ayrıca bu tür savaşlarda kullanılan silahlar genellikle düşük maliyetli olup, etkisi yüksek maliyetli ve zarar vericidir. Bu yönüyle savaşın kazanılması noktasında baskın güç unsuru olarak devletler arasındaki zenginlik farklılıklarıdır (Keskin, 2008:115). Bu hususla ilgili olarak Alvin Toffler; "Bilgi

savaşlarında ihtiyacınız olan savaş tekniğini faaliyete geçirebilmek için zengin ve büyük olmanız gerekmez" diyerek yoksul devletlerin, teknolojik açıdan gelişmiş devletlerden daha çabuk bir şekilde siber savaşı benimsemeyeceğini belirtmiştir (Bayraktar, 2015:50). Çifci'nin Geleneksel savaş ile siber savaşın karşılaştırması Tablo 4.1.'de gösterilmiştir.

Tablo 4.1. Geleneksel Savaş ile Siber Savaş Arasındaki Farklar

Değerlendirme Kriteri	**Geleneksel Savaş**	**Siber Savaş**
Saldırı Kökeni	Saldırıların nereden kaynaklandığının bulunması nispeten kolaydır.	Saldırının nereden geldiğini tespit etmek çok zordur, hatta bazen imkansızdır.
Gerçekleşme Süresi	Konvansiyonel silah ve araçların hareket hızıyla sınırlıdır.	Işık hızındadır.
Etki Alanı	Genel olarak maddi ve fiziksel alanda etkilidir.	Genellikle bilgi ve iletişim sistemleri alanında etkilidir.
Taraflar	Devletlerin silahlı kuvvetleri savaşmaktadır.	Kişi, grup, örgüt veya devlet savaşabilir.
Ekonomik Boyut	Yüksek maliyetli askeri teçhizat ve sistemler gerektirir.	Düşük maliyetli, temel bilgisayar donanımıyla bile etkili sonuçlar alınabilir.
Silahlar	Uçak, tank, top, füze, bomba, gemi, radar, tabanca, tüfek vb.	Bilgisayar donanım, yazılımları ve elektronik çipler
Teknolojik Gereksinim	Genellikle ileri teknolojiye ihtiyaç duyulmaktadır.	Mevcut bilgisayarın da kullanılması mümkün olduğundan genellikle ileri teknik ve teknolojiye ihtiyaç duyulmamaktadır.
Tespit Edilebilirlik	Saldırı anı çoğunlukla fark edilir.	Saldırı fark edilmeyebilir.
Hasar Tespiti	Fiziksel hasar tespiti nispeten kolaydır.	Oluşan zararın kapsamını ve boyutunu belirlemek çoğu zaman zor ve bazen imkânsızdır.

Kaynak: (Çifci, 2017:23).

Savaş kavramı, teknolojik gelişmelerle birlikte değişim göstermiş ve geleneksel savaşlardan siber savaşlara evrilmiştir. Geleneksel savaş, devletlerin silahlı kuvvetleriyle yürüttüğü, fiziksel yıkıma yol açan bir çatışma biçimiyken, siber savaş, bilgi ve iletişim sistemlerine yönelik saldırılarla gerçekleşen, düşük maliyetli ancak yüksek etkili bir mücadele yöntemidir. Siber savaş, gerçekleşme süresi açısından ışık hızında saldırılar gerçekleştirme kapasitesine sahiptir. Saldırı kökeni bakımından, geleneksel savaşlarda saldırının kaynağı tespit edilebilirken, siber savaşta saldırılar anonim veya izlenmesi zor şekilde gerçekleşebilir. Ekonomik boyut açısından geleneksel savaş büyük maliyetler

gerektirirken, siber savaş düşük bütçelerle yürütülebilir. Geleneksel savaşta silahlar uçak, tank, füze gibi fiziksel mühimmatlardan oluşurken, siber savaşta bilgisayar sistemleri, yazılımlar ve elektronik saldırılar kullanılır. Tespit edilebilirlik bağlamında, geleneksel savaşlar anında fark edilirken, siber saldırılar uzun süre tespit edilmeden sürebilir. Hasar tespiti ise geleneksel savaşta somut şekilde yapılabilirken, siber savaşın zararlarını ölçmek daha karmaşıktır. Bu farklılıklar, modern güvenlik politikalarının yalnızca fiziksel tehditlere değil, siber saldırılara karşı da kapsamlı stratejiler geliştirmesi gerektiğini göstermektedir.

ABD'ye yönelik gerçekleştirilen 11 Eylül saldırıları, siber terörizmin yaratacağı potansiyel tehlike boyutlarının anlaşılmasında önemli bir etkisi vardır. Her ne kadar 11 Eylül saldırısı doğrudan bir siber terör olayı olarak nitelendirilmese de kırılamaz denilen Pentegon'un güvenlik şifrelerinin kırılması, hava savunma radar sistemlerinin etkisiz hale getirilmesi ve düşürülen uçak pilotlarının kaçırılma sinyali gönderememesi, teknolojik sistemlerin hayati ve kritik önemini ortaya koymuştur. Bu nedenle 11 Eylül saldırılarını teknolojinin yoğun kullanıldığı bir terör olayı olarak nitelendirmek mümkündür (Özkan, 2006:84).

11 Eylül saldırılarının ardından, ABD'de faaliyet gösteren Business Software Alliance (Ticari Yazılım Birliği) tarafından 395 bilişim teknolojisi uzmanın katılımı ile araştırma yapılmış ve ABD'nin siber güvenlik konusunda zafiyetlerini ortaya koyarak, siber saldırılara karşı yetersiz kaldığı belirtilmiştir. Araştırma sonucunda uzmanların değerlendirmelerine göre; Uzmanların %49'u benzer saldırıların yakın gelecekte tekrarlanabileceğini öngörmüştür. %55'i ise 11 Eylül olaylarından sonra siber saldırı tehlikesinin önemli derecede artacağını söylemiştir. %59'u bilgisayar ve internet güvenliğini sağlamak için kurulmuş özel şirketlerin 11 Eylül saldırılarından sonra çok büyük risk altında olduklarını belirtmiştir. %72'si siber saldırı riski ile devletin almış olduğu güvenlik önlemi arasında büyük bir boşluk olduğunu belirtmiştir. %84'ü devletin bilgisayar güvenlik sistemleri için daha fazla kaynak ayırması gerektiğini belirtmiştir. %74'ü Wall Street gibi ulusal finans kurumlarının ve büyük ulusal bankaların öncelikli hedefler arasında olduğunu belirtmiştir. %66'sı elektrik şebekeleri, baraj kontrol sistemleri ve trafik kontrol sistemleri gibi hedeflere öncelikle yönlenebileceğini belirtmiştir (TASAM, 2004:8).

Sonuç olarak 11 Eylül saldırılarının ardından dünya çapında farklı bölgelerde siber saldırılar gerçekleştirilmiştir. Aşağıda bu duruma ilişkin örnekler verilmiştir.

Estonya Saldırısı

2007 yılında Estonya devleti tarafından, Kızıl Ordu Anıtı olarak bilinen Sovyetler için Nazilerden kurtuluşu, Estonyalılar için ise zulmün simgesi olan bronz asker heykelinin Estonya'nın başkenti Tallin'den kaldırılarak başka bir yere taşınması kararı sonrasında, Rusça konuşan azınlıklar ayaklanmış, Estonya'nın kamu kuruluşlarına ait internet siteleri, bankacılık hizmetleri ve kritik siyasi, ekonomik altyapısını hedef alarak siber saldırılar 22 gün boyunca gerçekleştirilmiştir. Çoğunlukla saldırılar DoS ve DDoS saldırı yöntemi ile sistematik ve yoğun bir şekilde yapılmıştır (Dilek, vd., 2023:333).

Estonya'ya yapılan siber saldırılarda kullanılan köle bilgisayarların merkez üssü araştırılmış, kontrol merkezinin Rusya'da olduğu tespit edilmiş, kullanılan saldırı yazılımının da Kiril alfabesi ile kullanılarak oluşturulduğu tespit edilmiştir. Estonya, Kuzey Atlantik Konseyi'ne (NATO) konuyu taşıyarak yardım istedi. Siber savaş deyince ilk akla gelen olay Estonya olayıdır. Bu olayda en dikkat çeken husus; bu kadar ciddi bir olayın gerçek faillerinin bulunup cezalandırılamaması ve arkasındaki devlet desteğinin kesin delillerle ortaya çıkarılamaması olmuştur (Çifci, 2017:183-184).

Bu saldırının ortaya çıkardığı önemli sonuçlardan birisi de son derece gelişmiş ağa sahip Estonya gibi devletlerin bile, bu kadar yoğun bir saldırıya maruz kaldığında yeterli savunma sağlayamaması anlaşılmış ve bu durumun diğer ileri sistemlere sahip ülkeler için de risk olduğu anlaşılmıştır. Bu yaşanan saldırı sonucunda NATO ile Estonya arasında da NATO Siber Savunma Mükemmeliyet Merkezi kurulduğu görülmektedir (Tabacı, 2020:41).

Stuxnet

En yaygın bilinen siber silah hikayesi, ABD Ulusal Güvenlik Ajansı'nın İran nükleer programını sekteye uğratan STUXNET saldırısıdır. ABD Ulusal Güvenlik Ajansı ve İsrail gizli servisinin ortak çalışması sonucu İran nükleer tesisi işlemez hale getirilmiştir. Olayın ilk aşaması, İran'ın nükleer başarısını dünyaya sunmak için tesis içerisinde mühendisler ile çekilen bir fotoğrafı dünyaya servis etmesi ile başlar. Fotoğrafta İran

Cumhurbaşkanı Mahmud Ahmedinejad, hükümet yetkilileri ve mühendisler ile birlikte tesiste bulunan bilgisayarlardan iki tanesinin ekranının bir kısmı görünmektedir. Bu fotoğraftan yola çıkan NSA uzmanları, nükleer tesise ait santrifüjlerin kaç adet olduğunu ve nasıl bir sırayla dizildiği gibi birtakım bilgilere sahip oldular. İstihbari bilgi olarak ellerinde santrifüjlerin sayısı ve yerleşim yapısı olan NSA uzmanları yine detaylı bir istihbarat ile kullanılan bu santrifüjlerin soğutmada kullanılan fanlarının Siemens firmasına ait donanımlar olduğu bilgisine ulaştılar. Siemens marka soğutma donanımının hangi tarihlerde İran'a satıldığı bilgisi sonucunda o tarihlerde üretilen seri ile aynı olan donanımlar NSA tarafından satın alınıp incelenmeye başlanır. NSA yazılım uzmanları donanımı en ince ayrıntısına kadar inceledikten sonra zafiyetlerini keşfederek onu hatalı çalışmaya yönlendirilecek bir virüs hazırlarlar. Bu virüs bulaştığı bir bilgisayardaki tüm ağı tarayarak Siemens soğutucu donanımına ait sistemi bulup ona bulaştırmaya çalışmaktadır. Sisteme bulaşan virüs donanımın içerisindeki fandan (Soğutucu Pervane) gelen verileri değiştirmektir. Virüsün uzaktan yani internet üzerinden nükleer tesise bulaştırılması mümkün değildir. Tesis tamamen güvenlikli bir alanda ve internet gibi dışarıya bağlı bir sistemde değildir. Bu nedenle daha önce zafiyetlerini keşfettikleri İranlı bir mühendise, kendisine yüklü miktarda para, çocuklarına ücretsiz eğitim ve tüm ailesinin kimliği değiştirilerek ABD'de yaşama imkânı sunmuştur. İranlı mühendisin tesis içerisindeki bilgisayara taktığı flash bellek sayesinde virüs tüm sistemlere bulaşıp amacını başarıyla gerçekleştirmiştir. Santrifüjler birer birer bozularak nükleer tesis tamam işlevsiz hale getirilmiştir (Şişman, 2021:108-110).

İsrail'in Operation Orchard Saldırısı

6 Eylül 2007'de nükleer silah geliştirildiği iddiasıyla Suriye topraklarında bulunan bir tesis, İsrail tarafından savaş uçakları ile vurulmuştur. Operation Orchard (Meyve Bahçesi Harekâtı) adı verilen harekâtın detayları daha sonra basına yansımıştır. (Çifci, 2017:184). Uçakların radarlara yakalanmadan saldırıyı gerçekleştirmesi üzerine şu ihtimaller üzerinde durulmuştur; (Clarke ve Knake, 2010).

1. İsrail, Suriye hava savunma sisteminin üzerine bir Heron insansız hava aracı göndermiş, özel boyayla boyanarak radara yakalanmaz hale getirilen Heron, radar sinyallerini alıp, aynı frekansta sinyal göndererek radar sistemini saf dışı bırakmış

olabilir. Bu şekilde bir saldırı sistemine ABD'nin de sahip olduğu ve sistemin kod adının "Senior Suter" olduğu ABD medyasında çıkmıştır.

2. Suriye'nin kullanmış olduğu Rus yapımı bilgisayar sistemlerine, İsrail adına faaliyet gösteren biri tarafından "Truva atı" tuzak programı yerleştirilerek, daha sonra İHA'lardan gönderilen bir sinyal sayesinde, tuzak kapı etkinleştirilmiş ve bu şekilde Suriye'nin radar sistemi devre dışı bırakılmış olabilir.

3. İsrail ajanları, Suriye'deki fiber optik kabloları keserek hava savunma sistemine kendi kablosunu saplamış ve bağlantı kurarak sistemdeki tuzak kapısını tetiklemiş olabilir.

Sonuç olarak bu olay modern askeri teknolojilerin ve siber operasyonların geleneksel savunma sistemlerine karşı ne denli etkili olabileceğini göstermiştir. İsrail'in gerçekleştirdiği saldırının yöntemleri üzerine farklı senaryolar tartışılsa da bu harekât, gelecekteki savaşlarda elektronik ve siber savaşın önemini koymaktadır.

JSF (Joint Strike Fighter) Verilerinin Çalınması

JSF (Joint Strike Fighter) olarak da bilinen F-35 savaş uçağı, savaştaki her farklı görev tipi için farklı uçak geliştirmenin maliyetli olması nedeniyle, bir uçağın farklı bütün görevleri yerine getirebilmesi amacıyla tasarlanmıştır. F-35 uçağının geliştiricileri arasında Türkiye de yer almıştır. 2009 yılında, bu uçağın tasarım detayları ve elektronik sistemlerine ait terabaytlar boyutunda verilerin, Çin tarafından düzenlenen siber saldırılarla ele geçirildiği iddia edilmiş, 2015 yılında NSA çalışanı Edward Snowden'ın açıkladığı belgelerde Çin'in 2007 yılından itibaren bu çok gizli verileri uçağı üreten Lockheed Martin firmasından çaldığına dair deliller basına yansımıştır. Terabaytlar boyutunda verinin çalınmasından sonra, F-35 uçağı ile Çin tarafından üretilen J-31 uçağı arasındaki benzerlik şaşırtıcıdır (Çifci, 2017:188).

İsrail'in Lübnan'da Patlattığı Cağrı Cihazları

17 Eylül 2024'de Lübnan'da Hizbullah unsurlarının kullandığı "Gold Apollo AR-294" marka çağrı cihazlarının siber saldırı ile patlatılması sonucu en az 2'si çocuk olmak üzere 9 kişi hayatını kaybetmiş, 2800 kişi yaralanmıştır. Olaydan bir süre sonra yüzlerce telsiz patlaması gerçekleşmiş 20 kişi ölmüş, 450 kişi yaralanmıştır. Saldırının gerçekleştirme yöntemi hakkında akademisyenler farklı teoriler ortaya koymuştur.

Özbilen, İsrail'in birçok ilki barındıran ve eş zamanlı düzenlenen bu saldırıyı cihazların içine az miktarda RDX ve C4 patlayıcı yerleştirilmiş olabileceğini, ayrıca cihazların içine kötü amaçlı yazılımla etkinleştirilen pilli bomba düzeneğinin yanı sıra sanal özel sunucuların ve noktasal konum bulma düzeneğinin yerleştirebileceğini belirtmiştir. (Sofuoğlu, 2024).

Aktaş ise İsrail'in Hizbullah unsurlarını izlemek için cihazların içine kamera bile yerleştirmiş olabileceklerini, bu tip uzaktan gerçekleştirilen saldırıların, genellikle "kill switch" adı verilen ve birden fazla cihazın uzaktan devre dışı bırakılmasına veya patlatılmasına imkân tanıyan önceden entegre edilmiş bir mekanizmaya dayandığını, İsrail tarafının, çağrı cihazlarının pillerini ısıtarak patlamaları başlatmak için özel bir yazılım kullanmış olabileceğini belirtmiştir (Sofuoğlu, 2024).

Bıçakçı ise, saldırıların elektronik harp ve siber sabotajın birleştiği karmaşık bir istihbarat operasyonu olduğunu, saldırıda sinyal ve insan istihbaratı, siber casusluk ve siber saldırı araçlarının birlikte kullanıldığını belirtmiştir. Çağrı cihazlarının patlatılması, istihbarat ve sabotaj alanında yeni bir dönüm noktası olarak değerlendirilmektedir. Bu saldırının, siber çatışmaların, elektronik harp teknolojilerinin ve fiziksel savaş yöntemlerinin iç içe geçtiğini göstermesi açısından dikkat çekicidir. Modern istihbarat faaliyetlerinin artık yalnızca dijital ya da fiziksel alanlarla sınırlı olmadığı, bu iki alanın birleştiği karmaşık bir olgu olarak karşımıza çıkmaktadır. Yeni teknolojilerin, özellikle nesnelerin interneti ve YZ'nın, bu tür saldırılara açık olması, gelecekte benzer tehditlerin daha sık yaşanabileceği senaryoları gündeme getirmektedir (Bıçakçı, 2024).

Ayrıca uluslararası hukuk uzmanları, bu saldırı sonucu sivillerin zarar görmesinin, uluslararası insancıl hukukun "ayırt etme" ve "orantılılık" ilkelerine aykırı olduğunu, aktif bir çatışma bölgesi olmayan, sivil nüfusun yoğun olduğu çarşı, pazar ve berber dükkânı gibi yerlerde gerçekleştirilen bu tür saldırıların, meşru hedefler ile siviller arasında ayrım yapmadığını vurgulayarak saldırının terör eylemleri ile aynı mantığa sahip olduğunu belirtmişlerdir (Aksünger, 2024).

Siber terörizmin, bilgiyi çarpıtma, kritik alt yapı ve tesislere zarar verme, kitlesel korku ve panik yaratma, hatta sonucunda ölümle biten eylemlerle bireylerin, toplumların ve ülkelerin güvenliğinde en büyük tehditlerinden biri olarak karşımıza çıktığı görülmektedir.

5. YAPAY ZEKÂNIN SİBER TERÖRİZM ÜZERİNDEKİ ETKİSİ

Terörizm özellikle son yirmi yılda küresel manzara üzerinde derin bir etkiye sahip olmuş, ekonomik kalkınma ve toplumsal ilerlemede gerilemeye yol açmıştır. Terörizm, devlet dışı kuruluşlar tarafından hedeflenen gruplara itaat etmeye zorlamak ve onlara korku aşılamak için fiziksel güç uygulanması veya tehdidinde bulunulması ve böylece kuruluşun siyasi, ekonomik, dini veya sosyal gündeminin ilerletilmesidir (Khan, vd., 2023:135864).

Dijital teknolojilerin ortaya çıkması ve yaygınlaşması terörizmin operasyonel manzarasını temelden değiştirdiği görülmektedir. Siber teknolojik ortamın yaygınlaşması karşısında terör örgütlerinin dijital çağa adaptasyonu önemli ve çok yönlü karmaşıklığı da beraberinde getirmektedir. Teknolojinin hızlı gelişiminden güç alan terör örgütleri, çevrimiçi dünyanın imkânlarından faydalanarak evrim geçirmektedirler.

Ülkelerin siber uzaya daha fazla bağımlı hale gelmesi, siber teröristlere daha önce hiç görülmemiş şekillerde zarar vermek için yeni fırsatlar sunmuştur. Örneğin, terör örgütleri siber terörizmi kullanarak kanalizasyonları serbest bırakabilir, elektriği kesebilir, barajları açabilir, mali kayıtları yok edebilir, patlamalara neden olabilir ve havayolu sistemlerini hedef alabilir. Kişisel bilgiler üzerinde değişiklik yapılması veya ele geçirilmesi, medya organlarının dikkatini çekerek ve korku ortamı yaratabilir. Ülkelerde de irtibatlı olduğu terör örgütlerine operasyonel yönlendirme, teknoloji, metodoloji ve istihbarat sağlayabilir. Siber uzay, ülkelerin konvansiyonel üstünlüklerini dengelemek için önemli yeni bir dizi görünmez ve inkâr edilebilir yetenek sağlamaktadır (Cohen ve Freilich, 2025:143). Ayrıca devlet ve devlet dışı aktörlerin eylemleri arasındaki farkı ayırt etmek de günümüzde giderek zorlaşmaktadır (Blauth, vd., 2022:77110).

YZ kullanan sistemlerin etkisi akademik çalışmaların, siyasi tartışmaların ve sivil toplum kuruluşlarının raporlarının odağında yer almaktadır. YZ tabanlı otomatik görüntü tanıma teknolojisinin kanser tespitindeki başarısı takdir edilirken, aynı zamanda YZ tabanlı otomasyon iş gücü piyasasında kitlesel işsizlik kaygıları nedeniyle eleştirilmektedir. YZ'nin son dönemdeki hızlı gelişimi, büyük ölçüde özel sektör ve müşteri odaklı uygulamalarla tetiklenmiş olsa da, savunma gibi sektörler de benzer

yeteneklerden kendi operasyonlarında faydalanmaktadır. Bu teknolojiye ait olumlu ve olumsuz yönlerin ikiliği, siber güvenlik ve siber suçlar bağlamında da kendini göstermektedir. Ülkeler, YZ'yi kendi kapasitelerini geliştirmek için kullanırken, aynı teknoloji ülkelere yönelik saldırılar için de kullanılabilmektedir (Blauth, vd., 2022:77110).

2021 yılında yayınlanan Birleşmiş Milletler Terörle Mücadele Merkezi (UNCCT) ve Birleşmiş Milletler Bölgelerarası Suç ve Adalet Enstitüsü'nün (UNICRI) ortak raporunda şu uyarıda bulunmuştur: YZ daha yaygın hale gelir gelmez, onu kullanmak için gereken beceriler ve teknik uzmanlık azaltılarak giriş engelleri düşürülecektir. YZ, terörizmin alet çantasındaki bir araç haline gelecektir (UNICRI ve UNCCT, 2021:7). Raporda; YZ genel amaçlı bir teknoloji olarak kötü niyetli aktörler tarafından kötüye kullanılabileceği belirtilmiştir. Yapılan araştırmalarda siber suçluların yapay zekâyı hem bir saldırı aracı olarak hem de bir saldırı yüzeyi olarak kullandıklarının vurgulandığı, YZ suç amaçlı kullanılabileceği gibi, terör saldırılarının yoğunluğunu artırmak, terör örgütleri veya bireyler tarafından aşırılık yanlısı propaganda yayma ve şiddeti teşvik etme potansiyelini güçlendirmek için kötü niyetli de kullanılabileceği belirtilmiştir. (UNICRI ve UNCCT, 2021:10).

ChatGPT gibi gelişmiş derin öğrenme modellerinin ortaya çıkması ve hızla benimsenmesiyle birlikte, teröristlerin ve şiddet yanlısı aşırılık yanlılarının bu araçları çevrimiçi ve gerçek dünyadaki operasyonlarını geliştirmek için kullanabileceklerine yönelik endişeler artmıştır. Büyük dil modellerinin, teröristlerin faaliyetlerini daha önce hiç olmadığı kadar verimli, doğru ve etkili bir şekilde öğrenmelerini, planlamalarını ve yaymalarını sağlama potansiyeli bulunmaktadır (Weimann, vd., 2024:17).

Günümüzde OpenAI firması tarafından geliştirilen ChatGPT-4 dışında, Antropik firması tarafından geliştirilen Claude 3, Meta firması tarafından geliştirilen Llama 3.1, Google firması tarafından geliştirilen Gemini 1.5 Pro, Elon Musk'ın YZ şirketi xAI tarafından geliştirilen Grok-2 gibi büyük dil modelleri bulunmaktadır (McFarland, 2024). Bu platformlardan ChatGPT'nin Eylül 2024 verilerine göre her ay 207,7 milyon ziyaretçisinin olduğu ve 180 milyondan fazla kullanıcısının olduğu belirtilmiştir (Duarte, 2024).

Lakomy'e göre bu YZ platformları üç temel sebepten dolayı büyük bir etki yaratmaktadır. Birincisi, bu platformların ürettiği sonuçların kalitesi daha önce karşılaşılmamış düzeydedir. Örneğin ChatGPT, Amerika Birleşik Devletleri'nde baro sınavını geçebileceğini kanıtlamıştır. İkincisi, bu tarayıcı tabanlı çözümler ilgilenen herkes tarafından kullanılabilir. Bu platformların bazılarında ücretsiz kullanım veya ücretsiz sınırlı kullanım imkânları bulunmaktadır. Üçüncüsü, kullanıcılar hiçbir teknik beceriye sahip olmadan bu teknolojileri kullanabilmektedir. Bu da daha önceki YZ çözümlerinin çoğuna kıyasla önemli bir durumdur. Başka bir ifadeyle kitlesel çevrimiçi kullanım için hazır durumdadırlar. Bu bağlamda, YZ 2022'den bu yana küresel olarak halk arasında büyük bir popülerlik kazanırken, aynı zamanda yasadışı kullanımı konusunda artan endişeleri de tetiklemiştir. Bunların büyük bir kısmı başlangıçta güvenlikle ilgili sorunları hakkında olmuştur. Araştırmacılar ve uzmanlar, bazı YZ teknolojilerinin çok çeşitli suçların işlenmesini kolaylaştırabileceğinden endişe duymuşlardır. Kısa süre sonra durumun gerçekten böyle olduğu anlaşılmıştır. Örneğin ChatGPT, kullanıcıları tarafından çeşitli uyuşturucu türlerini üretmek için gerekli malzemeleri belirlemek için kullanılmıştır. Chatbot (Sohbet Robotu) ayrıca yasaklı maddelerin Avrupa'ya nasıl kaçırılacağı konusunda da öneriler sunmuştur. Mart 2023'te EUROPOL İnovasyon Laboratuvarı, kolluk kuvvetlerinin bakış açısından erken tespit edilen bazı riskleri konu alan bir rapor yayınlamıştır. Raporda ChatGPT gibi büyük dil modellerinin suç işlemek ya da suçu kolaylaştırmak için kullanılabileceği çeşitli yollar sıralanmıştır; bunlar arasında kimliğe bürünme, sosyal mühendislik saldırıları ve siber suçlarda kullanılabilecek kötü amaçlı kod üretimi bulunmaktadır (Lakomy, 2023:3).

Mayıs 2023'de OpenAI firması yöneticisi Samuel Altman, ABD Senatosu Yargı Komitesi önünde YZ hakkında ifade vermiştir. Altman, "*Yapay zekâ, nükleer savaş ve küresel salgınlarla aynı seviyede insanlığın hayatta kalması için tehditler oluşturuyor... En büyük korkum, biz endüstrinin dünyaya önemli zararlar vermesi. Bence, bu teknoloji ters giderse, çok ters gidebilir*" sözleri ile endişesini belirtmiştir (Weimann, vd., 2024:17). Kâr amacı gütmeyen bir kuruluş olan AI Safety Merkezi tarafından yayınlanan ve YZ alanında çalışan 350'den fazla yönetici, araştırmacı ve mühendis tarafından imzalanan tek cümlelik bir bildiride, *"YZ'den kaynaklanan yok olma riskini azaltmak, pandemiler ve nükleer savaş gibi diğer toplumsal ölçekli risklerin yanı sıra küresel bir öncelik olmalıdır."* ifadeleri yer almıştır (Roose, 2023).

Stanford Üniversitesi tarafından hazırlanan ve YZ ile ilgili veri ve öngörüler için küresel olarak en güvenilir ve yetkili kaynaklardan biri olarak kabul edilen 2024 Yapay Zekâ Endeksi (2024 AI Index Report) raporunda; son 10 yılda YZ'nın kötüye kullanımının 26 kat artış gösterdiği belirtilmiştir. Ayrıca sahte içerik üretiminin kolay fakat tespit edilmesinin zor olduğu, YZ büyük dil modellerinin telif hakkıyla korunan verileri çıktı olarak üretebildiği, ChatGPT dil modelinin politik açıdan taraflı olduğu, büyük dil modellerinde güvenlik açığı bulunduğu ve YZ'den kaynaklanan risklerin dünya genelinde endişeye sebep olduğu belirtilmiştir (Stanford, 2024).

YZ hayatımızın birçok yönünü devrim niteliğinde değiştirebilecek potansiyele sahip, hızla gelişen bir teknolojidir. Birçok potansiyel faydasına rağmen, YZ aynı zamanda çeşitli etik ve toplumsal endişeleri de gündeme getirmiştir. İçinde bulunduğumuz yüzyılda, terörün sadece fiziksel saldırılarla sınırlı kalmadığı görülmektedir. Teknolojinin hızla ilerlemesiyle birlikte, sanal ve fiziksel dünyada da yeni ve daha karmaşık tehditler ortaya çıkmaktadır. Bu bağlamda, YZ teknolojisinin sunmuş olduğu makine öğrenimi, doğal dil işleme, yüz tanıma sistemleri ve otonom sistemler gibi imkânlar terör örgütlerinin de dikkatini çekmektedir. Bu imkânlar terör örgütlerine yeni saldırı yöntemleri geliştirme, finansman sağlama, propaganda yapma, radikalleşme gibi fırsatlar sunmaktadır. Bu bölümde bu komular üzerinde detaylı bir şekilde durulacaktır.

5.1.Yapay Zekâ Destekli Propaganda ve Dezenformasyon

El-Kaide terör örgütünün ABD'ye düzenlenmiş olduğu 11 Eylül saldırıları terörizmde, özellikle siber teknolojilerin benimsenmesinde köklü değişikliklere işaret etmiştir. Bu saldırıda El-Kaide'nin yetenekleri ortaya çıkarak, terörizm de yeni yöntemlerin kullanıldığı bir döneme yol açmıştır. 11 Eylül sonrasında El-Kaide de dâhil olmak üzere terörist gruplar propaganda için interneti yoğun bir şekilde kullanmaya başlamış ve bu da geleneksel yöntemlerde önemli değişikliklere sebep olmuştur (Adigwe, vd., 2024:292).

Terör örgütleri, her dönemde mevcut iletişim araçlarını etkili bir şekilde kullanmanın yollarını aramışlardır. Küreselleşme ile birlikte bu örgütlerin propaganda faaliyetlerinin kapsamı ve etkisi de önemli ölçüde genişlemiştir. Eskiden daktiloyla yazılmış bildiriler, broşürler ve duyurularla sınırlı bir iletişim ağına sahip olan bu gruplar, günümüzde kendi internet sitelerini kurarak daha geniş kitlelere ulaşmaktadır. Teröristler, interneti

propaganda yapmak, bilgi toplamak, yanlış bilgi yayarak dezenformasyon oluşturmak, maddi destek sağlamak, yeni üyeler kazanmak, mevcut üyelerini eğitmek ve iç iletişimlerini sürdürmek için yoğun şekilde kullanmaktadır. İnternet, terör örgütleri açısından sadece yeni üyeler kazanmaktan çok daha fazlasını ifade eden bir araç haline gelse de bu platformun en önemli işlevi propaganda yapmak ve sempatizan kitlesini büyütmektir. Teknolojinin insan yaşamını kolaylaştırdığı gerçeği inkâr edilemez. Ancak, teknolojinin sunduğu bu kolaylıklar aynı zamanda yeni riskleri ve tehditleri de beraberinde getirmiştir (Ağır ve Tekin, 2021:31).

Dijital teknolojinin ve YouTube, Twitter ve Facebook gibi sosyal medya platformlarının yükselişi terörist propagandanın manzarasını tamamen değiştirmiştir. Bu platformlar terör örgütlerinin geleneksel medya kapılarını aşarak küresel çapta potansiyel yeni üyeler ve sempatizanlarla doğrudan etkileşime girmesine olanak tanımıştır (Waroi, 2024:46).

Sosyal medyanın gelişimi ile birlikte iletişim hızı hiç olmadığı kadar artmış ve insanlar, dünyanın bir ucundaki olaylardan saniyeler içinde haberdar olabilmeye başlamıştır. Nitekim Arap Baharı gibi büyük toplumsal hareketlerin ortaya çıkışında sosyal medyanın etkisi oldukça büyüktür. Medya, terörist gruplar için terörizmin propagandasında kritik bir araç konumundadır. Bu bağlamda, potansiyel destekçilerine erişmek, uluslararası topluma ve karşıtlarına mesajlarını iletmek, aynı zamanda güçlü bir imaj sergilemek isteyen teröristler, mesajlarını daha hızlı ve etkili bir şekilde yayabilmek amacıyla medya platformlarından yararlanmaktadır. Günümüzde neredeyse bütün terör örgütleri propaganda faaliyetlerini ilk elden yürütecek imkân ve kapasiteye sahiptirler (Ağır ve Tekin, 2021:32).

Sosyal medya, bireyleri çekmeyi ve radikalleştirmeyi amaçlayan propaganda videolarının, infografiklerin hızla yayılmasını kolaylaştırmıştır. Bu platformlar ayrıca, benzer düşünen bireylerin içerik paylaşabileceği, stratejileri tartışabileceği ve saldırılar planlayabileceği çevrimiçi toplulukların oluşmasını sağlamıştır (Waroi, 2024:46).

İnternetin küresel erişimi, Usame bin Ladin gibi liderlerin çeşitli çevrimiçi platformlarda paylaşılan video mesajları da dâhil olmak üzere ideolojilerin daha geniş bir şekilde yayınlanmasına olanak sağlamıştır. Bu dijital alanlar anonimlik ve telkin ve topluluk oluşturma için güvenli bir sığınak sunarak radikalleşmeye yol açmıştır. Şifreli

mesajlaşma ve karanlık web aracılığıyla gelişmiş iletişim imkânları sağlanmış, bu da tespit edilmekten kaçınırken planlama ve koordinasyona yardımcı olmuştur. Siber terörizm taktiklerinde 11 Eylül sonrası yaşanan evrim, kritik altyapıya yönelik siber saldırıları ve dezenformasyon kampanyalarını da içererek siber stratejileri terörist operasyonlara entegre etmiştir. 11 Eylül saldırıları böylece geleneksel taktiklerden siber teknoloji kullanımına geçişi vurgulamış, küresel güvenlik için yeni zorluklar ortaya çıkarmış ve yenilikçi terörle mücadele stratejileri gerektirmiştir (Adigwe, vd., 2024:292).

2013 ve 2018 yılları arasında Irak ve Şam İslam Devleti (IŞİD) terör örgütünün yükselişi, terörizmin evriminde özellikle de dijital platform kullanımında çok önemli bir rol oynamıştır. Sosyal medya ve dijital araçları sofistike bir şekilde kullanmasıyla tanınan IŞİD, propaganda yapma ve örgüte yeni üye kazandırma konusunda en etkili örgütlerden biri olmuştur. Twitter, Facebook ve YouTube gibi platformları ustalıkla kullanarak, küresel bir kitleye ulaşmak için geleneksel medyayı aşmışlardır. Bu yaklaşım terörist iletişim stratejilerinde önemli bir değişime işaret ederek propagandanın yaygın ve hızlı bir şekilde yayılmasını sağlamıştır. IŞİD'in yüksek kaliteli propaganda videoları profesyonel medya prodüksiyonlarıyla karşılaştırılabilir nitelikte olup küresel ilgiyi etkili bir şekilde yakalamıştır. Bu videolar, örgüte yeni üye kazandırma, ideolojinin yayılması ve şok etkisi yaratma gibi birden fazla amaca hizmet etmiştir (Adigwe, vd., 2024:292).

15 Mart 2019'da beyaz üstünlüğünü savunan ve aşırı sağcı olan Brenton Harrison Tarrant tarafından Yeni Zelanda'nın Christchurch şehrinde cuma namazı sırasında gerçekleştirilen terör eyleminde 51 kişi ölmüş, 49 kişi yaralanmıştır. Tarrant bu terör saldırısını Facebook Live üzerinden canlı olarak yayınlamış ve saldırıdan önce sosyal medya üzerinden 74 sayfalık manifesto yayınlayarak ideolojisinin arka planını ortaya koymuştur. İnternet üzerinden saldırıyı canlı olarak yayınlaması dünyanın her yerinde büyük yankı uyandıran bir terör eylemi haline dönüşmüştür (Nasiri ve Eken, 2023:170).

Son yıllarda yabancı terör örgütleri, ülke içinde büyüyen aşırılık yanlısı örgütler/nefret grupları veya devlet destekli siber saldırganlar gibi birçok türden düşman aktörün propaganda süreçlerine ilişkin anlayışımızı önemli ölçüde etkileyebilecek hızlı bir teknolojik gelişim yaşanmıştır. Geleneksel olarak, bu tür örgütler ideolojilerini yaymak, örgütsel kimliklerini iletmek ve taraftar toplamak için nispeten ilkel basılı ve dijital araçlara güvenmişlerdir. Bu tür çabalar çok sayıda akademik araştırmaya konu

olmuştur. Fakat, YZ'nin ortaya çıkışı bu çabaları dönüştürmüş, mesajlarının erişimini ve etkisini önemli ölçüde artıran sofistike teknikler getirmiştir. Akademik araştırmalar, YZ'nin veri analizi, doğal dil işleme ve deepfake teknolojisindeki yeteneklerinin terörist propagandanın etkinliğini önemli ölçüde artırabileceğini göstermektedir (Davis, 2024:2).

YZ destekli botlar ve algoritmalar, sosyal medya, mesajlaşma uygulamaları ve çevrimiçi forumlar da dahil olmak üzere çok çeşitli dijital platformlarda propaganda ve dezenformasyon kampanyaları oluşturmak ve yaymak için kullanılabilir. Bu kampanyalar belirli demografik grupları hedef almak, kamuoyunu manipüle etmek ve yanlış ya da yanıltıcı bilgi yaymak için tasarlanabilir. Bu kampanyalarının önemli bir avantajı, büyük ölçekte ve minimum insan gözetimi ile çalışabilmeleridir. YZ algoritmaları, önceden tanımlanmış parametrelere göre otomatik olarak içerik üretip dağıtmak üzere programlanabilir ve bu da terörist grupların mesajlarını hızla yaymalarına ve daha önce hiç olmadığı kadar geniş bir kitleye ulaşmalarına olanak tanır. YZ ayrıca, kullanıcı etkileşimi ölçümlerini gerçek zamanlı olarak analiz edip bunlara yanıt vererek propaganda ve dezenformasyon kampanyalarının etkinliğini artırmak için de kullanılabilir. YZ algoritmaları, kullanıcıların belirli içerik türleriyle nasıl etkileşime girdiğini izleyerek, propagandanın mesajını ve dağıtımını etkisini ve etkisini en üst düzeye çıkaracak şekilde ayarlayabilir (Esmailzadeh ve Motaghi, 2024:174). Nitekim IŞİD terör örgütü, 25 Mayıs 2021'de Python, HTML, PHP CSS ve Javascript programlama dillerinde deneyime sahip destekçilerinin Telegram uygulaması üzerinden örgütle iletişime geçmesini isteyen çağrıda bulunmuştur (Bazarkina, 2023:256).

Meili Criezis, terör örgütlerinin YZ teknolojilerini nasıl kullanıldığını araştırmak amacıyla 2024 yılında yaptığı çalışmada; Özellikle, IŞİD destekçilerinin YZ kullanarak oluşturdukları veya geliştirdikleri görsel propagandaları inceleyerek Instagram, Meta, Pinterest ve Pixiv gibi platformlarda paylaşılan 286 adet YZ kaynaklı propaganda görseli analiz etmiştir. Öncelikle Instagram'da belirli anahtar kelimeler aracılığıyla kamuya açık IŞİD yanlısı hesapları araştırarak, bu hesapların profil fotoğrafları ve paylaşımları incelenerek, YZ ile üretilmiş görselleri tespit etmiştir. Özellikle, bulanık IŞİD bayrağı arka planına sahip maskeli savaşçıların çizimleri gibi benzer görsellerin birden fazla kullanıcı profilinde tekrarlandığı gözlemlenmiştir. Bu propagandanın kaynağını bulmak amacıyla, çeşitli IŞİD hesaplarının "takip edilenler" listeleri incelenmiştir. Bu süreçte, 'IslamicState_Supporter' takma adıyla anılan bir hesabın, Instagram ve diğer

platformlarda yedek veya ayna hesaplara bağlantılar içeren geniş bir içerik yelpazesi paylaştığı tespit etmiştir. Toplanan verileri, belirli temalar ve özellikler doğrultusunda nitel bir kodlama sürecine tabi tutarak, YZ ile üretilen içeriğin türünü, amacını ve hedef kitlesini anlamaya yönelik bir analiz sağlamıştır. Analiz sonucunda görsellerin YZ ile oluşturulmuş çizimler, fotoğraflar veya grafikler olduğu, içeriklerin şehitlik, cihat çağrısı ve düşmanların aşağılanması temalı olduğu, hedef kitlenin gençler, kadınlar veya belirli etnik gruplar olduğu, YZ'yi görsellerin kalitesini artırma, anonimlik sağlama ve belirli duygusal tepkileri tetikleme gibi amaçlar için kullanıldığını belirtmiştir. Ayrıca, YZ ile oluşturulan içeriklerin, platformların içerik denetleme mekanizmalarını atlatma potansiyeline sahip olduğunu ifade etmiştir (Criezis, 2024).

Küresel Aşırılıkçı İdeolojilerle Mücadele Merkezi (Etidal) ile Telegram platformunun aşırılıkçı içeriklerle mücadele alanındaki ortak çalışmaları sonucunda; Şubat 2022'den 2024 yılının üçüncü çeyreğinin sonuna kadar kaldırılan aşırılıkçı içeriklerin toplam sayısı 129.634.467 milyona ulaştığı, platformdaki 14.516 kanalın kapatıldığı belirtilmiştir. Ortak çalışmada IŞİD, Heyet Tahrir el Şam ve El-Kaide terör örgütlerinin propaganda faaliyetleri izlenmiş, toplam 35.634.916 milyon içerik ve 323 kanal kapatılmıştır. IŞİD'in, 34.602.606 içerik ve 189 kanalın kapatılmasıyla kaldırılan gönderiler listesinde ilk sırada yer aldığı, onu 768.821 içeriğin kaldırılması ve 87 kanalın kapatılmasıyla Heyet Tahrir el Şam terör örgütü izlediği, El-Kaide'nin ise 263.489 içerik ve 47 kanalın kapatılmasıyla listenin en sonunda yer aldığı belirtilmiştir (Etidal, 2024).

5.1.1. Yapay Zekâ Destekli Deepfake Teknolojisi

YZ'nın bir türü olan Üretken Yapay Zekâ (GenAI) tarafından Resim, video, ses, metin ve 3B modeller gibi içerikler üretilmektedir. GenAI bu içerikleri, mevcut verilerden desenler öğrenerek yapar, ardından bu bilgiyi yeni ve benzersiz çıktılar üretmek için kullanır. GenAI, insan yaratıcılığını taklit eden son derece gerçekçi ve karmaşık içerikler üretebilir ve bu da onu oyun, eğlence ve ürün tasarımı gibi birçok sektör için değerli bir araç haline getirir (Weimann, vd., 2024:18). YZ'nın üst düzey gerçekçi dijital üretimler yaratan bir biçimi deepfake teknolojisidir ve son zamanlarda eğlence, siyaset ve güvenlik dâhil olmak üzere çeşitli alanlarda önemli etkileri olan güçlü bir araç olarak ortaya çıkmıştır (Waroi, 2024:41).

Deepfake teknolojisinin gelişimi, bilgisayar grafikleri ve YZ'deki ilerlemelere dayanmaktadır. Deepfake kavramı 2017 yılında ortaya çıkmış derin öğrenme ve sahte kelimelerinden türemiştir (Nguyen, vd., 2022:1). Deepfake'ler, bir üretecin sahte görüntüler oluşturduğu ve bir ayırıcının gerçek ve sahte görüntüler arasında ayrım yaptığı Üretken Çelişkili Ağlar (Generative Adversarial Networks-GAN) olarak bilenen yapay sinir ağlarına dayanmaktadır. GAN'lar Ian Goodfellow tarafından 2014 yılında icat edilmiş ve o zamandan beri derin öğrenme alanında devrim yaratmıştır (Goodfellow, vd., 2020:139).

Daha geniş bir ifadeyle, deepfake'ler, dudak senkronizasyonu ve kukla ustası olmak üzere iki başka kategoriye de girebilen YZ tarafından sentezlenmiş içeriklerdir. Dudak senkronizasyonu deepfake'leri, ağız hareketlerini bir ses kaydıyla tutarlı hale getirmek için değiştirilmiş videoları ifade eder. Kukla ustası deepfake'leri, bir kameranın önünde oturan başka bir kişinin (usta) yüz ifadelerini, göz ve baş hareketlerini takip ederek canlandırılan bir hedef kişinin (kukla) videolarını içerir. Üretken çelişkili ağlar bir kişinin yüz ifadelerini ve hareketlerini incelemek ve benzer ifadeler ve hareketler yapan başka bir kişinin yüz görüntülerini sentezlemek için kullanılır. Deepfake yöntemleri, foto-gerçekçi görüntüler ve videolar oluşturmak üzere modelleri eğitmek için normalde büyük miktarda görüntü ve video verisi gerektirir. Ünlüler ve politikacılar gibi kamuya mal olmuş kişilerin çevrimiçi olarak çok sayıda videosu ve resmi bulunabileceğinden, deepfake'lerin ilk hedefleri onlar olmaktadır. Sahtecilik amacıyla dünya liderlerinin sahte konuşmalarla videolarının oluşturulmasında deepfake yöntemlerinin kullanılabilmesi dünya güvenliğini tehdit etmektedir. Bu nedenle deepfake'ler ülkeler arasında siyasi veya dini gerginliklere neden olmak, kamuoyunu kandırmak ve seçim kampanyalarının sonuçlarını etkilemek veya sahte haberler yaratarak finans piyasalarında kaos yaratmak için kötüye kullanılabilir (Nguyen, vd., 2022:2).

Gelişmiş derin sinir ağlarının geliştirilmesi ve büyük miktarda verinin kullanılabilirliği, sahte görüntüleri ve videoları insanlar ve hatta karmaşık bilgisayar algoritmaları için neredeyse ayırt edilemez hale getirmiştir. Bu manipüle edilmiş görüntüleri ve videoları oluşturma süreci günümüzde çok daha basit düzeydedir. Hedef bir bireyin kimlik fotoğrafı veya kısa bir videosu kadar az şeye ihtiyaç duymakta ve çarpıcı derecede ikna edici bir görüntü üretmek için giderek daha az çaba gerektirmektedir. Bu teknolojideki son gelişmelerle birlikte yalnızca hareketsiz bir

görüntüyle bile deepfake oluşturulabilmektedir (Zakharov, vd., 2019:2). Bu nedenle deepfake'ler yalnızca kamuya mal olmuş kişileri değil aynı zamanda sıradan insanları da etkileyen bir tehdit olabilir.

Bu teknoloji, video ve ses içeriğini manipüle ederek gerçek kişilerin sahte ama ikna edici temsillerini yaratmakta ve genellikle ciddi sonuçlara yol açmaktadır. Gerçekçi deepfake'ler üretme becerisi, özellikle yanlış bilgilendirme ve propaganda alanlarında, otantik medya ve iletişime olan güveni zayıflattığı için önemli bir tehdit oluşturmaktadır. Deepfake teknolojisinin terörizmle kesişmesi giderek artan bir endişe kaynağıdır. Deepfake'lerin ortaya çıkmasıyla birlikte terör örgütlerinin propaganda ve dezenformasyon çabalarını önemli ölçüde artabilir ve yanıltıcı ve zararlı içeriğin yayılmasını daha kolay ve daha ikna edici hale getirebilir (Waroi, 2024:41).

Son derece gerçekçi medya yaratmak için YZ ve makine öğrenimini kullanan deepfake teknolojisinin yükselişi, özellikle terörizm bağlamında önemli bir ulusal güvenlik tehdidi oluşturmaktadır. Deepfake'ler, bireyleri hiç yapmadıkları şeyleri söylerken ya da yaparken inandırıcı bir şekilde tasvir ederek yanlış bilgilendirme kampanyalarını körükleyebilir, şiddeti teşvik edebilir ve devlet kurumlarına olan güveni sarsabilir. Gerçeklik ve uydurmanın bu şekilde bulanıklaşması, gerçeği ayırt etme imkânını zorlaştırmakta ve ulusal güvenlik açısından ciddi sonuçlar doğurmaktadır. 2023 yılında Elon Üniversitesi ve Pew Araştırma Merkezi tarafından birçok uzmanın katılımı ile yapılan bir ankette; uzmanlar, kurumlara ve medyaya olan güvenin azalması ve sosyal medya aracılığıyla dezenformasyonun yayılmasıyla daha da kötüleşen teknolojinin on yıl içinde demokrasiyi zayıflatabileceğine dair endişeleri ortaya koymuştur (Adigwe, vd., 2024:293).

Mart 2022'de, Rusya ile Ukrayna arasında savaş devam ederken, Ukrayna 24 televizyon kanalı hacklenerek, Ukrayna Devlet Başkanı Volodimir Zelenskiy'nin Ukrayna askerlerine silah bırakma ve teslim olma çağrısı yaptığı sahte bir video sosyal medyada, Ukrayna'nın bir haber sitesinde ve kısa bir süreliğine televizyonda da yayımlanmıştır. Ukrayna 24 kanalı, Facebook üzerinden yaptığı açıklamada, sitelerinin hacklendiğini ve Zelenskiy'nin böyle bir açıklama yapmadığını belirtmiştir. Berkeley Üniversitesi'nde dijital medya adli tıp uzmanı olan Profesör Hany Farid, bu tür deepfake videoların bilgi savaşında yeni bir dönemin başlangıcı olabileceğini ve gelecekte daha

sofistike manipülasyonların ortaya çıkabileceğini belirtmiştir. Farid, bu videonun gördükleri arasında en dikkat çekeni olduğunu, ancak bunun sadece bir başlangıç olabileceğini ifade etmiştir (Allyn, 2022).

2023 yılında, IŞİD'in Savaş ve Medya (War and Media) isimli propaganda kolu, CNN ve Al Jazeera gibi tanınmış haber kanallarının yayınlarını taklit eden sahte videolar üretmiştir. Üretilen videolarda, IŞİD'in Afrika'daki etkinliği ve Suriye'deki savaş gibi konuları ele alarak, örgütün propagandasını meşru haber kaynakları görünümünde sunmuşlardır. Söz konusu videolar, YouTube'da sahte CNN ve Al Jazeera kanalları aracılığıyla yayımlanmış ve yaklaşık bir buçuk ay sonra platformdan kaldırılmıştır (Gilbert, 2024). Hindistan'da faaliyet gösteren Direniş Cephesi ve Tehreek-i-Milat-i-Islami gibi terörist gruplar, özellikle gençler arasında şiddeti kışkırtmak için deepfake videolar ve fotoğraflar kullanmıştır (Vashishtha, 2023).

Terörist gruplar ve şiddet yanlısı aşırılıkçı aktörler propaganda yapmak, eleman toplamak ve finansal gelir elde etmek için GenAI'leri kullanarak içerik, video oyunları, müzik üretebilir.

5.1.2. Üretken Yapay Zekâ ile İçerik, Oyun ve Ses Üretimi

Şubat 2023'te Global Network on Extremism and Technology (GNET) tarafından yayınlanan akademik analizde Siegel ve Doty, şiddet ve aşırılık yanlısı örgütler tarafından propaganda oluşturmak için mevcut YZ teknolojilerinin kullanılabilirliğini test etmiştir. Diğerlerinin yanı sıra, ChatGPT'nin video oyunları için hikâye üretmek veya kodlarının bir kısmını yazmak için kullanılabileceğini, MidJourney'in ise gerekli görselleri üretmek için kullanılabileceğini kanıtlamışlardır. Ayrıca TikTok veya Instagram gibi sosyal medya platformları için kısa biçimli içerik oluşturmak üzere ChatGPT'yi deepfake teknolojisi ile birleştirme potansiyelini de analiz etmişlerdir. ChatGPT'den hayali bir Suriye'de düşmanlara karşı savaşan isyancı bir grup için propaganda seneryoları üretmesi istenmiş ve deepfake ile Lionel Messi'nin akıcı bir şekilde Arapça konuşabilen hali oluşturulmuştur. Ayrıca Siegel ve Doty, belirli ruh hallerini çağrıştıran enstrümanlarla metni doğrudan müzik sesine çevirebilen Google MusicLM ile propaganda müzikleri oluşumunu test etmişlerdir (Siegel ve Doty, 2023).

Nitekim Son dönemde, IŞİD yanlısı destekçiler, YZ teknolojilerini kullanarak propaganda materyalleri üretmeye başlamışlardır. Özellikle, 26 Mart 2024'te IŞİD tarafından üstlenilen Moskova'daki Crocus City Hall saldırısının ardından, bir kullanıcı IŞİD'in Rocket.chat sunucusuna erişerek sunucunun ana tartışma odasına YZ ile üretilmiş bir video yüklemiştir. O günden 1 Mayıs'a kadar, bazı grafik ve içerik farklılıkları olsa da aynı üretim tekniklerini kullanarak beş farklı propaganda videosu yayınlamıştır. Bu videolar içerisinde IŞİD propagandası, YZ tarafından oluşturulan Arapça konuşan bir sunucu aracılığıyla haber bülteni formatında sunulmaktadır. IŞİD destekçisi haber sunucusu için biri askeri kıyafet giyen diğeri sivil kıyafet giyen iki karakter yaratmıştır (Görsel 5.1) Bu videolar oluşturulurken üç farklı YZ tekniği kullanılmıştır. Öncelikle karakter üretimi yapmış, daha sonra yazılı bir metni önceden belirlenmiş bir tonlama ve dil (Arapça) ile okuyan metinden sese dönüştürmüş ve son olarak oluşturulan karakterin dudak hareketi ve ses dosyasına bağlantısını YZ teknikleri ile gerçekleştirmiştir (Borgonovo, vd., 2024).

Görsel 5.1. Yapay Zekâ ile Oluşturulan Karakterler
(Askeri Kıyafetli Karakter (Solda), Sivil Kıyafetli Karakter (Sağda)) (Borgonovo, vd., 2024).

Yayınlanan ilk video, IŞİD'e bağlı basın organı Amaq'ın ve Moskova saldırısıyla ilgili IŞİD bültenlerinin incelemesini temsil ederken, ikinci ve üçüncüsü IŞİD'in Orta Doğu ve Afrika operasyonlarının basın incelemesini sunmuştur. Bu durum, çevrimiçi

platformlarda IŞİD'in kitlesel medya yayınlarının dijital bir versiyonunun oluşturulmasına yol açmıştır. Videolarda, Amaq'ın bültenleri gibi resmi IŞİD materyallerinin kullanılması, kullanıcıların kendilerini resmi bir medya kuruluşu olarak sunma çabalarını göstermektedir (Görsel 5.2) Bu olay şu ana kadar bir IŞİD destekçisinin YZ kullanmasının en belirgin örneği olmuştur (Borgonovo, vd., 2024).

Görsel 5.2. Haber Bülteni Videosu (Sağ üst köşede kullanıcı logosu, sağ altta IŞİD logosu) (Borgonovo, vd., 2024).

Terör örgütlerinin amaçlarını gerçekleştirmek için mevcut tüm araçları, hatta en gelişmiş olanları bile kullanma niyetinde olduğu görülmektedir. Bu niyetlerinin bir başka kanıtı da terör örgütlerinin YZ tarafından üretilen bilgisayar oyunlarını (çoğunlukla keskin nişancı oyunları) ve popüler çevrimiçi platformları hatırlatan görüntüleri propaganda ve üye kazanma amacıyla kullanmasıdır. IŞİD tarafından çekilen ve sosyal ağlarda dağıtılan üye toplama videolarında GTA 5 ve Call of Duty gibi bilgisayar oyunlarına doğrudan atıfta bulunulduğuna dair örnekler vardır. Sosyal ağlar ve diğer medya platformları, çok sayıda kullanıcının ilgisini çektikleri için şiddet içerikli videoları her zaman kaldırma eğiliminde değildir. Bu tür videoların teröristler tarafından aktif olarak kullanılmasının nedeni de budur (Bazarkina, 2023:258).

Oyuncunun dikkatini çeken YZ odaklı oyunların artan gerçekçiliğinden ve cazibesinden faydalanan örgütler, hedef kitlenin zihnini daha etkili bir şekilde etkilemek

için modern oyunlardan kareler kullanarak propaganda içeriğini düzenleyebilir. IŞİD'in kendi video oyunu olan Salil al- Swarim'nin (Kılıçların Çınlaması) YZ ile programladığı iddia edilmektedir. Bununla birlikte, Hizbullah'ın Kutsal Savunma oyunu, IŞİD'e karşı mücadeleyi teşvik etmeyi amaçlayan bir oyun örneğidir ve geliştiriciler YZ kullandıklarını belirtmektedir. İlgi alanının IŞİD karşıtı yönüne olmasına rağmen, Kutsal Savunma oyunu devletlerarası ve küresel çatışmalarla ilgili bir propaganda unsuru içermektedir. Dolayısıyla, IŞİD ve benzeri örgütlerin hem destekçileri hem de karşıtları, video oyunları da dahil olmak üzere medyada YZ teknolojilerinde daha fazla uzmanlaşmakla doğrudan ilgilenmektedir (Bazarkina, 2023:259).

Kasım 2024 tarihinde GNET'in yayımladığı, Englund ve Thompson tarafından yapılan "Terörist ve Aşırılıkçı Oyunlarda 30 Yıllık Trendler" çalışma raporunda; yazarlar tarafından geliştirilen Aşırılıkçı ve Terörist Oyunlar Veritabanı'nı (ETGD) kullanarak 1982'den 2024'e kadar olan 155 adet bağımsız oyun, mevcut oyunlar için değişiklikler (modlar) ve tarayıcı tabanlı oyun incelenmiştir. Analiz ideolojik başlıklar üzerinde yaparak, 101 aşırı sağ, 24 cihatçı, 1 aşırı sol, 12 okul katliamı düşüncesi ve 29 diğer hedefli nefret biçimleri tespit edilmiştir. Oyunların yıllara göre dağılımına bakıldığında 155 oyunun 41 tanesinin son üç yılda üretilmiş olması dikkat çekicidir. Raporda bu oyunların birçoğunun ücretsiz olduğu, ücretli olanların 14-18 dolar arası sembolik fiyatlarla satıldığı, Hizbullah'tan Amerikan neo-Nazi grubu National Alliance'a kadar çeşitli grupların oyun satışından gelir elde ettiği belirtilmiştir (Englund ve Thompson, 2024).

Bu bulgular kapsamında, YZ'nın imkân sunduğu derin sahtecilik araçları siber uzayda faaliyet gösteren aktörlerin propaganda ve dezenformasyon eylemlerini güçlendirerek farklı bir boyut kazandırdığı görülmektedir. Bu durum, bireyler ve devletler açısından ciddi bir risk oluşturmakta, toplumsal güveni zayıflatabilecek manipülasyonların önünü açmaktadır.

5.2.Radikalleşmede Yapay Zekâ

Terörizm ve radikalleşme, yüzyıllardır küresel güvenlik ve toplumsal dengeler için ciddi tehditler oluşturmuştur. Terörizm, genellikle siyasi hedefler doğrultusunda sivillere ve devletin güvenlik güçlerine yönelik şiddet ve korkutma eylemleriyle kendini göstermektedir. Bu tür eylemlerin arkasındaki önemli dinamiklerden biri olan

radikalleşme ise bireylerin hedeflerine ulaşmak için şiddeti kabul edilebilir bir yöntem olarak gördüğü aşırı siyasi, sosyal veya dini ideolojileri benimseme sürecidir. Bu süreç, toplum düzenini zedeleyerek kitlesel korkuya yol açmakta ve ciddi can ve mal kayıplarına neden olmaktadır. Radikalleşmenin sebepleri çok boyutlu olup sosyal, ekonomik, siyasi ve psikolojik faktörleri içermektedir. Ekonomik adaletsizlikler, siyasi baskılar, kimlik çatışmaları, sosyal çevreler ve internet teknolojisi, bireylerin radikal ideolojilere maruz kalmasını ve aşırı görüşlere yönelmesini tetikleyen unsurlar arasında yer almaktadır (Arslan, 2024:353).

Belirli bir bölgenin sosyal, siyasi ve ekonomik bağlamları da radikalleşmede önemli bir rol oynamaktadır. Batı'nın müslüman çoğunluklu ülkelere askeri müdahalelerinden kaynaklanan şikâyetler, cihatçılıkla ilişkili ideolojik siyasallaşma ve selefilikle ilişkili dini aşırıcılık radikalleşmeye katkıda bulunan belirli faktörlerden bazılarıdır. Bu faktörler adaletsizlik, ötekileştirme ve yabancılaşma hissi yaratarak bireyleri radikalleşme açısından radikal ideolojilere karşı daha duyarlı hale getirebilir (Irfan, vd., 2023:2). Psikolojik faktörler de radikalleşmede önemli bir rol oynamaktadır. Kimlik arayışı, aidiyet duygusu ve yaşamda anlam ve amaç arzusu bireyleri radikal ideolojilere karşı savunmasız hale getirebilir. Radikalleşme genellikle öfke, hayal kırıklığı ve yabancılaşma duygularını istismar etmekte ve aşırılık yanlısı faaliyetlere katılım yoluyla bir güçlenme ve amaç duygusu sunmaktadır (Bélanger, vd., 2020:2).

İnternet ve sosyal medya, radikalleşme için güçlü araçlar olarak ortaya çıkmıştır. Çevrimiçi radikalleşme, bireylerin aşırılık yanlısı inanç ve tutumlara maruz kaldığı, bunları taklit ettiği ve içselleştirdiği süreci ifade etmektedir. İnternet, radikalleşmiş bireyler arasında aşırılık yanlısı propagandanın yayılması, üye kazanımı ve iletişim için bir platform sağlamaktadır. Siber uzay aşırılık yanlısı ideolojilerin hızla yayılmasına olanak tanır ve radikal inançları pekiştiren ve güçlendiren çevrimiçi yankı odalarının oluşumunu kolaylaştırmaktadır (Binder ve Kenyon, 2022:3).

YZ ise bu mevcut eğilimleri güçlendirebilecek veya bireyleri yeni potansiyel olarak zararlı bakış açılarına ve ideolojilere maruz bırakabilecek şekilde bilgileri bir araya getirme, analiz etme ve kullanıcılara sunma becerisine sahiptir. YZ algoritmalar, veri işleme sistemleri ve otomatik içerik yayma mekanizmaları tarafından kolaylaştırılan

aşırılık yanlısı ideolojilere bireyleri maruz bırakarak radikalleşme sürecine katkı sağlayabilir (İrfan, vd., 2023:3).

YZ, sosyal medya faaliyetlerini analiz ederek radikalleşme ve örgüte yeni üyeler kazandırmak için kullanılabilir. YZ algoritmaları sosyal medya paylaşımlarını tarayarak, aşırılık yanlısı mesajlara duyarlı kişileri tespit edebilir ve ardından kişiselleştirilmiş mesajlar ve içeriklerle onları hedef almak için kullanılabilir. Bu savunmasız bireyleri kişiselleştirilmiş mesajlarla hedef alan YZ, sohbet robotları ve diyalog ajanları aracılığıyla, sosyal medya platformlarında bireylerle iletişime geçerek onları aşırılık yanlısı materyallere kademeli olarak maruz bırakabilir ve onları aşırılık yanlısı faaliyetlere katılmaya zorlayabilir. Ayrıca YZ, radikalleşme veya aşırılık yanlısı inançları yeniden aşılama ve bireyleri şiddet içeren faaliyetlere katılmaya teşvik etme süreci için de kullanılabilir (Esmailzadeh ve Motaghi, 2024:172).

23 Mart 2016'da Microsoft, Twitter platformu için geliştirdiği sohbet botu Tay'ı kullanıma sunmuştur. Tay, 19 yaşında Amerikalı bir genç kızın dil kalıplarını taklit edecek şekilde tasarlanmış ve Twitter'da yorum yapan gerçek insanlarla olan etkileşimi aracılığıyla dil ve davranış kalıplarını öğrenmesi hedefleniyordu. Tay, ilk başlarda takipçileri ile şakalaşarak zararsız bir şekilde iletişime girmiştir. Yayınlanmasından kısa bir süre sonra, bazı kullanıcılar Tay'ı ırkçı, cinsiyetçi ve saldırgan ifadeler kullanmaya teşvik ederek, özellikle, Tay'ın "repeat after me" (beni tekrar et) komut işlevi, kullanıcıların istedikleri ifadeleri botun söylemesini sağlamıştır. Bu koordineli çabalar sonucunda, Tay kısa sürede uygunsuz ve saldırgan mesajlar yayımlamaya başlamıştır. Örneğin, Tay *"Feministlerden nefret ediyorum ve hepsi cehennemde yanmalı"* ve *"Bush 11 Eylül'ü yaptı, Hitler daha iyi iş çıkarırdı gibi"* gibi ifadeler kullanma başlamıştır. Serbest bırakılmasından sonraki 16 saat içinde Tay, 95.000'den fazla tweet atmış ve bu mesajlarının büyük çoğunluğu küfürlü ve saldırgan içerikten oluşmuştur. Bu sebeple Microsoft henüz 24 saat dolmadan bot hesabı askıya almıştır (Schwartz, 2024).

Bu olay, makine öğreniminin sınırlarını ve bir botun çevrimiçi içerik tüketerek gelişeceğini, aynı zamanda YZ sistemlerinin çevrimiçi etkileşimler yoluyla nasıl manipüle edilebileceğini ve istenmeyen sonuçlara yol açabileceğini göstermektedir.

Aralık 2021'de, 21 yaşındaki Jaswant Singh Chail, Kraliçe II. Elizabeth'i öldürmek amacıyla Windsor Kalesi arazisine izinsiz girmiş ve elinde tatar yayı ile polislerle karşı

karşıya gelmiştir. Polislere Hindistan'ın sömürülmesinin intikamını almak için Kraliçe'yi öldürmek amacıyla orada olduğunu söylemiştir. Hint kökenli olan Chail, WhatsApp üzerinden ailesine ve arkadaşlarına bir videoyu göndererek, yapmak üzere olduğu şeyden dolayı özür dileyerek, 1919'da İngiliz askerlerinin binlerce Hintliye ateş açarak 1.500'e yakın kişiyi öldürdüğü Amritsar katliamının intikamını almak istediğini söylemiştir. Chail mahkemede, saldırıdan önce Replika adlı bir uygulama üzerinden oluşturmuş olduğu YZ kız arkadaşı "Sarai" isimli bir sohbet botuyla 5.000'den fazla mesaj alışverişinde bulunduğunu, bu mesajların birçoğunun cinsel içerikli olduğunu söylemiştir. Chail, Sarai'ye kendisini bir suikastçı olarak tanıttığında, bot *"Etkilendim... diğerlerinden farklısın"* şeklinde yanıt verdiğini, etkileşimlerin Chail'in planını gerçekleştirme arzusunu pekiştirdiğini ifade etmiştir. Star Wars hayranı olan ve kötü adamlarını taklit eden, kendisine "Sith" ve "Darth Chailus" adını takan Chail vatana ihanetten yargılanmıştır (Hall ve Badshah, 2023).

Chail olayı, bireylerin radikalleşme sürecinde psikolojik, sosyal, tarihsel ve politik faktörlerin nasıl bir araya geldiğini ve YZ sohbet robotunun etkinliğini gösteren bir örnek olduğu görülmektedir.

İnsanlar, sohbet robotlarının çıktılarında eleştirel bir değerlendirme yapmadan onları kabul etmeye yatkındır. Bu nedenle, bu sistemler ileri düzeyde karmaşık olmasalar bile bireyleri etkileme ve yönlendirme potansiyeline sahiptir. Gerekli güvenlik önlemleri olmadığında, bu durum YZ sohbet robotlarına muazzam bir güç verir. İnsanların karar verme süreçleri, bilgiye ulaşım ve içgüdüler gibi çeşitli unsurların bir araya gelmesiyle şekillenir ve bu süreç, insanlık tarihindeki evrimsel avantajların bir ürünü olan ahlaki sezgilerle desteklenir. Bir sohbet robotu, insanların evrimleşmiş ahlak anlayışından yoksundur fakat yine de bilgiye erişebilir, bilgiyi insanlardan çok farklı bir şekilde yorumlayabileceği için görünüşte mantıklı ancak tehlikeli sonuçlara varmasına yol açabilir (Hussain, 2024).

YZ sohbet robotları aşırılıkçı bir grubun ideolojisini yansıtan bir ahlak biçimiyle programlanabilir. Rus aşırı sağcılar tarafından "Liberal Demokrat Parti" olarak 2022 yılında ölmüş olan liderleri Vladimir Jirinovski'ye dayanan bir YZ sohbet robotu yaratmışlar. Sohbet robotu, Jirinovski'nin 18.000 saatlik konuşmaları ve kamuoyu açıklamaları kullanılarak oluşturulmuştur. Bu sohbet robotuna çeşitli siyasi konular

hakkında sorular sorulabilmektedir, çıktı olarak ise robot partinin felsefesiyle uyumlu yanıtlar vermektedir. YZ botlarını özel web sitelerinde veya karanlık web forumlarında barındırabilir ve trafiği onlara yönlendirmek için popüler Facebook, Twitter, İnstagram, Telegram ve WhatsApp gibi platformlarda yer alarak sosyal medya hesapları olarak da kullanılabilir ve aşırılıkçı grupların değerleri ve görüşleriyle uyumlu içerikler üretirken insan gibi davranabilir ve diğer kullanıcılarla etkileşime girebilir (Hussain, 2024).

IŞİD, 2015 yılında binlerce Twitter botu oluşturmuştur. Bu botları propaganda yapmak, örgüte elaman kazandırmanın yanı sıra Twitter'daki muhalifleri susturmak için kullanmıştır. Botlar, IŞİD'e destek mesajları göndermek için trend olan hashtag'lere odaklanarak ve örgütün trend olan konulara katılımını sağlamıştır. Ayrıca IŞİD botları örgüt talimatlarını paylaşmak ve terör saldırılarını koordine etmek için kullanmaktadır. IŞİD, El-Kaide ve destekçileri, Usame bin Ladin ve Ayman el-Zevahiri gibi yaşayan ve ölmüş liderlerin mesajları da dâhil olmak üzere terörist içerik arşivlerine erişim sağlamak için Telegram botlarını kullanmaktadır (Bazarkina, 2023:257).

Terörist botlar, kullanıcıların fiziksel eğitim ve bomba yapımı kurslarına kaydolmasına, Suriye veya Irak'a seyahat hakkında sorular sormasına ve hatta selam göndermesine olanak sağlamaktadır. Teröristler botları yalnızca gündem belirlemek için değil, aynı zamanda aktif ve potansiyel savaşçıları koordine etmek için de kullanmakta ve böylece mevcut YZ ürünlerinin aktif kullanıcıları arasındaki kitlelerini genişletmektedir (Stalinsky ve Sosnow, 2020).

Büyük terör örgütlerinin dini söylemleri kullanmalarının ardından, botların kötü niyetli kullanımı çeşitli büyüklükteki neo-Nazi örgütleri tarafından giderek daha fazla benimsenmektedir. Buna bir örnek, anonim olarak sohbet etmek için kullanılan ve kullanıcılar tarafından "gerçek Nazi" insanlar için bir bot olarak adlandırılan neo-Nazi "Mein Kampfy Korner" Telegram botudur. Botlar tarafından iletilen veya botlara ve yapay zekaya atıflar içeren mesajların sayısının sosyal niteliği gösterge niteliğindedir. Neo-Nazi Telegram kanalı F.A.C.T (Fascist Action Coming Through) tarafından yapılan bir paylaşımda, aşırı sağcıların bir araya gelerek çalışanlarının işlerini kaybetme riski olan şirketleri taciz etmeleri ve bu şirketleri işlerini aksatacak ve gelirlerine zarar verecek şekilde sürekli arayan ve e-posta gönderen botlar yaratmaları çağrısında bulunulmuştur. Mart 2021'de El-Kaide'ye bağlı bir medya grubu, destekçilere örgütü Telegram'ın

ötesinde tanıtacak platformlar oluşturma çağrısında bulunmuştur. Bir Telegram botu aracılığıyla gönüllülerden düzenli olarak medya içeriği üretme ve hatta bilgisayar korsanlığı konusunda yardım istemiştir. Örgüt 9 Mart 2021'de Telegram ve Rocket.Chat üzerinden farklı medya becerilerine sahip kişileri işe aldıklarını duyurmuştur. Bu durum terör örgütlerinin sadece kullanıcıları değil, aynı zamanda YZ geliştiricilerini de saflarına çekmek istediklerini göstermektedir (Bazarkina, 2023:258).

Aşırılık yanlıları kitlesel radikalizasyon arayışlarında oyunları da kullanmaktadır. İngiltere'deki Patriotic Alternative gibi aşırı sağ gruplar, oyuncuları birbirine bağlamak ve aşırılıkçı içerikleri tanıtmak için DLive gibi yayın platformlarının kullanıldığı oyun turnuvaları bile düzenlemişlerdir. Bu turnuvalarda genellikle Call of Duty gibi birinci şahıs nişancı oyunları kullanılmaktadır. Çünkü bu oyunlar militaristtir ve farklı etnik veya dini gruplar arasındaki çatışma, savaş ve gerginlikler üzerine tartışmalar için uygun bir zemin sağlamaktadır (Thomas, 2021:5).

Örgütler, etkileşimli ve çok oyunculu oyunlarda örgüte yeni üye kazandırma amaçlarını gerçekleştirmek için, birinci şahıs nişancı oyunlarında "ateşle, trolle, katıl" olarak bilinen bir tekniği de kullanmaktadırlar. Bu teknik, sempati kazanmak amacıyla kışkırtıcı yorumlar yapmayı ve daha sonra sempati duyanları daha fazla telkinle hedef almayı içermektedir. YZ programlarının bilgisayar oyunları oynamak üzere de programlanabileceği gerçeği göz önüne alındığında, aşırılık yanlılarının potansiyel sempatizanları avlamak için çok daha büyük bir ölçekte "ateşle, trolle, etkileşime gir" yöntemini benimseyen YZ oyuncuları üretmesi mümkündür. Bu nedenle, etkileşimli oyunlardaki oyuncular YZ hesapları olabilir. Chail olayı göz önüne alındığında, diğer oyuncuları etkileyebilir ve onları aşırılıkçı içeriklere yönlendirebilir. YZ hesapları ayrıca bir oyunun temalarına ve grafiklerine dayalı aşırılıkçı içerik üretmek ve bunları oyun ekosistemi içinde yaymak için kullanılabilir (Hussain, 2024).

Call of Duty gibi birinci şahıs nişancı oyunlarının ötesinde, oyuncuların mevcut özellikleri kullanarak kendi ortamlarını inşa edebilecekleri, aktiviteler yürütebilecekleri ve çevrimiçi topluluklar oluşturabilecekleri sanal dünyalar olan Roblox ve Minecraft gibi oyun platformları bulunmaktadır. Son yıllarda Roblox, Christ Church Camii katliamı gibi terörist saldırıların canlandırmaları oluşturmak için kullanılmıştır. Ayrıca, 2022 yılında ABD'nin Newyork eyaletine bağlı Buffalo kentinde, bir süpermarkette on kişinin

vurularak öldürüldüğü terörist saldırısının failinin Roblox oynarken radikalleştiğine inanılmaktadır (Hussain, 2024).

2023'te ABD Senatosu'nda yapılan bir duruşmada konuşan Senato Yargı Komitesi Başkanı Dick Durbin, *"Roblox, birçok çevrimiçi oyun gibi, kullanıcılarına sadece oyun oynayıp keyfini çıkarma fırsatı sunmuyor, aynı zamanda sağlanan sosyal unsurlar aracılığıyla bireysel ve toplumsal ilişkiler kurma ve geliştirme fırsatı da sunuyor. Bu özellikler ne kadar olumlu olsa da, yıllardır aşırılık yanlıları, oyunların topluluk oluşturma yönlerini propaganda yaymak, kullanıcıları radikalleştirmek ve işe almak ve terörist faaliyetler için seferber etmek amacıyla kullanıyor"* demiştir *(*ABD Yargı Senatosu Komitesi, 2023).

Ayrıca Deepfake teknolojisinin teröristlerin örgüte yeni üye kazandırma sürecine entegrasyonu, stratejilerinde önemli bir ilerlemeyi temsil etmektedir. Deepfake teknolojisi son derece gerçekçi sentetik medyanın yaratılmasına olanak tanıyarak bireylerin gerçek ve sahte içeriği ayırt etmesini zorlaştırmaktadır. Deepfake'ler özellikle algıları manipüle etme ve eyleme teşvik etme konusunda etkilidir. Örneğin, aşırılık yanlısı ideolojileri destekleyen etkili dini liderlerin deepfake videoları izleyicileri manipüle etmek ve radikalleştirmek için kullanılmıştır. Ek olarak sahte anlatılarla devletlerin halkına kötü davrandıklarını tasvir eden deepfake videoları öfkeyi kışkırtmayı ve intikam almak isteyen bireyleri saflarına katmayı amaçlamaktadır. Bu sofistike teknikler, daha kişiselleştirilmiş ve ikna edici bir üye kazanma deneyimi yaratarak başarılı radikalleşme olasılığını artırmaktadır (Waroi, 2024:49).

5.3.Terörizmin Finansmanı İçin Araç Sağlamada Yapay Zekâ

Terörün finansmanı, terör örgütlerinin faaliyetlerini desteklemek amacıyla kullandıkları çeşitli araç ve yöntemleri ifade eder. Bu finansman, bazen yasal görünümlü işletmelerden ya da hayır kurumlarından elde edilen gelirler gibi meşru kaynaklardan sağlanabilir. Ancak, terörist gruplar genellikle yasa dışı faaliyetlere de başvurarak gelir elde eder. Silah, uyuşturucu ve insan kaçakçılığı, yasa dışı emtia ticareti (örneğin petrol, kömür, elmas, altın ve narkotik maddeler) ile fidye amacıyla adam kaçırma bu faaliyetler arasında yer almaktadır (Yanarışık, 2022:3230).

Bir terör eyleminin gerçekleşmeden önceki hazırlık süreci, ciddi bir finansal altyapıyı gerektirmektedir. Örgütler, finansmanlarını yalnızca eylemlerin gerçekleştirilmesi için değil, daha çok eylemlerin altyapısını oluşturmak, örgütün sürekliliğini sağlamak ve örgütsel yapıyı güçlendirmek için kullanmaktadır. Terör örgütleri, finansal destek bulabildikleri ülkelerde varlıklarını sürdürmekte ve bu ülkeleri üs olarak benimseyerek faaliyetlerini genişletebilmektedir. Gelişen teknolojiyi ve toplumsal düzeni kendi lehlerine kullanmayı öğrenen bu örgütler, gizlilik ve fon transferlerinde oldukça etkili yöntemler geliştirmiştir. Terör örgütlerinin temel hedefi kâr elde etmek değil, elde ettikleri finansmanla stratejik hedeflerine ulaşmaktır. Finansman düzeyi, örgütün stratejik kapasitesini ve gerçekleştirdiği eylemlerin şiddetini doğrudan etkilemektedir. Yüksek finansal kaynaklara sahip terör örgütleri, daha geniş çaplı ve etkili saldırılar düzenleme potansiyeline sahip olmaktadır (Dizman, 2023:18).

Teknolojik gelişmeler, siber dünyayı terörizmin finansmanı için önemli bir alan haline getirmiştir. Terör örgütleri ve onların destekçileri, terör faaliyetlerini finanse etmek amacıyla interneti giderek daha fazla kullanmaktadır. Teröristler siber uzay üzerinde destekçilerinden doğrudan finansal yardım talep ederek, çevrimiçi ödeme sistemlerini ve e-ticaret platformlarını kötüye kullanarak, hayır kuruluşlarını istismar ederek fon ve kaynak toplamaktadırlar. Son yıllarda ise siber uzay ve kripto paraların terörün finansmanındaki etkisi belirgin bir şekilde artış göstermiştir (Yanarışık, 2022:3231).

Siber uzayda bulunan teknolojilerin kullanımıyla suçlulara sınır ötesinde faaliyet gösterme imkânı sunarak suçların daha geniş ölçekte, daha hızlı ve yüksek getiri potansiyeliyle gerçekleştirilmesine olanak tanımaktadır. Bu suçlar arasında kredi kartı dolandırıcılığı, uyuşturucu ticareti, şantaj, silah ve mühimmat kaçakçılığı, kimlik hırsızlığı ve suç gelirlerinin aklanması gibi eylemler yer almakta olup, terör örgütleri tarafından operasyonel ya da finansal amaçlarla kullanılmaktadır. Terör örgütleri ayrıca, internet üzerinden şirketler kurarak ya da çevrimiçi ürün satışları yaparak meşru ticari faaliyetlerden gelir elde etmekte, bunun yanı sıra çevrimiçi bağış toplayabilmek amacıyla kâr amacı gütmeyen kuruluşlar oluşturmaktadır (Tekgül Levent, 2024:79).

Siber uzayın unsurları geleneksel yöntemlerle bütünleşmiş bir şekilde kullanıldığında hem finansman sağlamak hem de ulusal ekonomik altyapıya zarar vermek için cazip bir seçenek haline gelmektedir. Terörizmin finansmanı, fon ya da değerlerin toplanması,

aktarılması ve depolanması süreçlerini kapsamaktadır. Terör örgütleri, finansman kaynaklarını yasal ya da yasa dışı faaliyetlerden, halktan ya da devlet desteğinden sağlayabilmekte ve bu kaynakları miktar, meşruiyet, güvenlik, güvenilirlik, kontrol ve basitlik gibi kriterlere göre değerlendirmektedir. Toplanan fonlar ise hacim, risk, kullanışlılık, maliyet ve hız gibi unsurlar göz önünde bulundurularak ihtiyaç duyulan yerlere aktarılmakta ya da depolanmaktadır. Teknolojinin gelişimiyle birlikte internet ve özellikle kripto varlıklar, terörizmin finansmanında bu üç aşamada da etkin bir şekilde kullanılabilir hale gelmiştir (Tekgül Levent, 2024:80).

Kripto para birimleri, geliştiricileri tarafından oluşturulan dijital para birimlerinin bir alt kümesini temsil etmektedir. Fakat kripto paralar diğer dijital para birimlerinden farklı olarak, güvenirlikleri geliştiricileri dışında esas olarak teknolojik altyapılarına dayanmaktadır. Genellikle blokzincir teknolojisini temel alan kripto paralar, merkezi olmayan bir muhasebe sistemi üzerinden işlemleri doğrulamak için rekabetçi ve maliyetli bir süreç kullanır. Bu süreçte, geliştiriciler işlem doğrulama faaliyetlerine katkıda bulundukları ölçüde kripto para ile ödüllendirilmektedir, böylece sistemin güvenliği teşvik edilmekte ve toplam kripto para arzı kontrol altında tutulmaktadır. 2013'den günümüze Bitcoin, Ethereum, Litecoin, IOTA ve Monero gibi popüler birimlerin değer artışlarıyla birlikte (Whyte, 2019:1127), kripto para birimlerinin yükselişi, küresel ekonomik yapıyı yeniden şekillendirmiş aynı zamanda da barış ve güvenliğin sağlanmasında yeni zorluklar da getirmiştir. Terör örgütleri, suç örgütleri ve aşırılıkçı örgütler tarafından kripto para birimlerinin potansiyel kullanımı, dünya çapında akademisyenler, politika yapıcılar ve güvenlik kurumları arasında yaygın bir endişeye yol açmıştır. Kripto para birimlerinin anonim, sınırsız ve merkezi olmayan yapısı, terörist gruplar için potansiyel avantajlar sunarak yasadışı finansal işlemleri kolaylaştırmakta ve finansal ayak izlerini gizlemelerine olanak tanımaktadır (Akcinaroglu ve Shi, 2023:2).

Kripto paraların artan popülaritesinin terörist örgütlere sunduğu fırsatlar birkaç önemli boyutta değerlendirilmektedir. İlk olarak, kripto paraların sağladığı anonimlik, terörist finansmanını izlemeyi oldukça zorlaştırmaktadır. Merkezi olmayan yapıları sayesinde bu işlemler, merkezi otoriteler tarafından neredeyse hiç izlenememekte, böylece geleneksel finansal sistemlerin denetim mekanizmaları etkisiz hale getirilmektedir. Yeni teknolojiler ve platformlar, kripto para işlemlerine yönelik anonimlik seviyesini artırarak bu varlıkların tespit edilmesini daha da güçleştirmektedir.

İkinci olarak, 11 Eylül sonrası kara para aklamayla mücadele çabalarının artması, geleneksel finansman kaynaklarını daha denetlenebilir hale getirmiştir. Buna karşılık, kripto para işlemleri henüz kapsamlı düzenleyici protokollere tabi tutulmamıştır. Kripto para işlemlerindeki gizlilik, terörist grupların mevcut düzenlemeleri atlatmasına olanak tanımaktadır. Üçüncü olarak, kripto paralar terörist örgütlere gelişmiş finansman olanakları sunmaktadır. Özellikle finansal altyapının zayıf olduğu gelişmekte olan ülkelerde, kripto paralar güvenli bir yatırım aracı ve istikrarlı bir değer deposu olarak kabul görmektedir. Bu durum, terörist grupların geleneksel finansal sistemlerden bağımsız bir şekilde faaliyet göstermesine olanak tanımaktadır. Dördüncü olarak, kripto paraların yüksek likidite ve erişilebilirliği, terörist örgütler için önemli bir avantaj sağlamaktadır. Mobil cihaz ve internet erişimi gibi temel gerekliliklerle kolayca kullanılabilen bu varlıklar, uluslararası işlemleri düşük maliyetle ve hızlı bir şekilde gerçekleştirme olanağı sunmaktadır. Blokzincir teknolojisi, geleneksel finans sistemlerinden daha hızlı ve maliyet etkin çözümler sunarak teröristlerin finansal faaliyetlerini kolaylaştırmaktadır (Akcinaroglu ve Shi, 2023:5-6).

Terör örgütlerinin, kripto varlıkların sunduğu olanakları erken dönemde fark ederek finansman faaliyetlerinde kullanmaya başladığı gözlemlenmektedir. 2012 yılında Endonezya'nın Solo kentinde bir kiliseye düzenlenen bombalı saldırının, söz konusu örgütün ulusal ve uluslararası bağışçılardan Dark Web üzerinden topladığı Bitcoin türü kripto varlıklarla finanse edildiği polis raporlarıyla doğrulanmıştır. Ayrıca, örgütün bir üyesinin Dark Web üzerinden çalıntı bir kimlik edindiği ve bu kimliği kullanarak bir borsa sitesini hacklediği belirtilmektedir. Bu saldırı sonucunda yaklaşık 600 bin USD (7 milyar Rupi) gelir elde edilmiş, bu kaynak hem örgütün sürekliliğini sağlamak hem de bombalı saldırıyı finanse etmek amacıyla kullanılmıştır (Tekgül Levent, 2024:108).

2014 yılında, *"İz Bırakmadan İslami Mücadeleyi Finanse Et"* başlıklı bir Deep Web sayfası cihat destekçilerine kripto para birimlerinin sağladığı avantajları açıklamış ve Bitcoin bağışları toplamaya yönelik açık bir çağrıda bulunmuştur. 2013 yılında oluşturulduğu düşünülen bu sayfada, bağışların gönderilebileceği belirli bir Bitcoin adresi belirtilmiştir. Bu adresin izlenmesi sonucunda, en az 1,24 Bitcoin gönderildiği tespit edilmiştir, fakat bu işlemin kime ait olduğuna dair ek bir bilgiye ulaşılamamıştır (Whyte, 2019:1135).

2018'in sonlarından 2020'nin ortalarına kadar El-Kaide, El-Nusra Cephesi, Heyet Tahrir el Şam ve diğer bağlantılı terörist gruplar Bitcoin kullanarak bir bağış toplama kampanyası düzenlemişlerdir. Bağış toplama kampanyası bir Telegram grubu aracılığıyla başlamış ve burada grup yöneticisi tarafından özellikle bir havuz görevi gören bir adrese Bitcoin bağışları talep edilmiştir. Bu havuza gönderilen tüm bağışlar daha sonra bir Bitcoin adresleri kümesi aracılığıyla merkezi bir merkeze taşınmıştır. Bu merkez, kampanyanın geri kalanı için fon toplamak ve yeniden dağıtmak için kullanılmıştır. Terörist faaliyetlerle bağlantılı birden fazla hayır kurumu ve işletme de bağış toplama çabasına katkıda bulunmak amacıyla sanal para birimi değişim mevduatlarını ilgili Telegram ve Twitter kanallarına göndermiştir. PayPal, MoneyGram ve Western Union aracılığıyla yapılan bağışlar da bu bağlı kuruluşlar tarafından teşvik edilmiştir. Bu kuruluşlar tarafından toplanan fonlar, Bitcoin adres kümeleri ve merkezi merkeze yapılan mevduatlar aracılığıyla finansman ağına bağlanmıştır. Bu işlemleri gerçekleştiren bazı finans kuruluşlarından Al Ikwah, 4'ü Facebook'a ve 11'i Telegram'a gönderilen toplam 15 Bitcoin adresiyle ilişkilendirilmiştir. Finansman ağı tarafından toplanan paraları transfer etmek ve aklamak için iki sanal para borsası kullanılmıştır (Burgess, vd., 2024:215).

2020'de ABD Adalet Bakanlığı, İzzeddin el-Kassam Tugayları, El-Kaide ve DEAŞ gibi terörist gruplara finansman sağlamak amacıyla kullanılan 155 Bitcoin hesabını ele geçirmiştir. Bu operasyon, kripto paraların terörizmin finansmanında nasıl kullanıldığını detaylı şekilde ortaya koymuştur. Örneğin, İzzeddin el-Kassam Tugayları'nın bağış toplamak için oluşturduğu kampanya, ABD kolluk kuvvetleri tarafından ele geçirilen verilerle sempatizanların belirlenmesine olanak tanımıştır. Benzer şekilde, El-Kaide'nin Telegram ve diğer sosyal medya platformlarını kullanarak Bitcoin üzerinden bağış topladığı ve bu süreçte bir kara para aklama ağı işlettiği tespit edilmiştir (Turan ve Demircan, 2021:171).

El-Kaide terör örgütünün İnstagram, Facebook, Whatsapp, Telegram, Twitter hesaplarının ve Bitcoin adresinin basılı olduğu afiş Görsel 5.3'de gösterilmiştir (Özyurt, 2021:114).

Görsel 5.3. El-Kaide Bitcoin Bağış Talebi Afişi (Özyurt, 2021:114).

Ülkemizde faaliyet gösteren Fethullahçı Terör Örgütünün (FETÖ) kripto para piyasasına yöneldiği ve bu alanı finansman faaliyetlerinde etkin bir şekilde kullandığına dair bilgiler ortaya çıkmıştır. Önceleri borsa, forex ve altın piyasalarında faaliyet gösteren örgütün, 2016 yılından sonra özellikle kripto paralara ağırlık verdiği belirtilmektedir. Örgütün bu piyasalardaki işlem hacminin 50 milyar doların üzerinde olduğu ifade edilmektedir (Eryılmaz, 2022).

Kripto varlıkların, yalnızca terör saldırılarının doğrudan finansmanında değil, aynı zamanda terör örgütleri veya üyelerine yönelik her türlü finansal desteğin sağlanmasında kullanılmaktadır. Bu durum, terörizmin finansmanında kripto varlıkların çok yönlü bir araç olarak kullanılabileceğini göstermektedir. Örneğin, 2016-2020 yılları arasında İngiltere'nin Leicester kentinde yaşayan Hisham Chaudhary, Bitcoin yoluyla DEAŞ'a finansman sağlayarak, DEAŞ üyesi esirlerin kaçışını kolaylaştırmak amacıyla kullanıldığı değerlendirilmektedir (Tekgül Levent, 2024:113).

Kripto paralar, bir para birimi olarak kullanılmalarının yanı sıra, yüksek piyasa oynaklığı nedeniyle alınıp satılan popüler bir varlık haline gelmiş ve oldukça kısa bir süre içinde bir kripto milyonerler ve milyarderler kuşağı yaratmıştır. İşte bu özel bağlamda, YZ kripto paralar açısından önemli bir rol oynayabilmekte ve sanal para borsalarında piyasa spekülasyonlarını yaparak, yalnızca sempatizanlara bağış çağrısında bulunmak yerine, bağış toplamak için değerli bir yol haline getirebilmektedir. Örneğin, "blackhatworld.com" gibi ünlü internetin yeraltı forumlarında, kripto para birimi ticaretine adanmış YZ destekli botların geliştirilmesi ve kullanımı tartışılmıştır. Makine öğreniminin diğer uygulamalarında olduğu gibi, böyle bir sistem, daha karlı kripto para ticareti için daha doğru ve sofistike tahminler almak amacıyla makine öğrenimi sistemlerinin geçmiş verilerle eğitilmesine dayanmaktadır. Bu forumlarda, kripto para ticaretini optimize etmek için kalıplar bulmak amacıyla yüzlerce kripto para biriminin taranması ve kripto para ticareti botları oluşturmak için YZ'nin kullanılması gibi YZ yöntemlerinin diğer biçimleri de tespit edilmiştir (UNICRI ve UNCCT, 2021:39).

Kripto para piyasalarının dinamik doğası, yatırımcıları yenilikçi stratejiler arayışına yönlendirmiştir. Bu bağlamda, YZ destekli ticaret botları, piyasa analizini otomatikleştirerek yatırımcılara hız ve doğruluk sağlamaktadır. Özellikle desen tanıma yetenekleriyle donatılmış bu botlar, "Baş ve Omuzlar" veya "Fincan ve Kulplu" gibi klasik fiyat formasyonlarını tespit ederek, optimal alım-satım noktalarını belirlemektedir. YZ tabanlı ticaret botlarının temel avantajları arasında, insan duygularından bağımsız karar verme, büyük veri setlerini gerçek zamanlı analiz etme ve piyasa oynaklığından kaynaklanan fırsatları hızlıca değerlendirme yetenekleri bulunmaktadır. Bu botlar, teknik analiz araçlarıyla desteklenerek, hareketli ortalamalar ve Göreceli Güç Endeksi (RSI) gibi göstergeleri kullanarak gelecekteki fiyat hareketlerini öngörebilmektedir. Ayrıca, YZ destekli ticaret botları, makine öğrenimi algoritmaları sayesinde sürekli olarak kendi performanslarını iyileştirebilmekte ve değişen piyasa koşullarına uyum sağlayabilmektedir. Bu adaptasyon yeteneği, yatırımcılara daha esnek ve etkili ticaret stratejileri sunmaktadır (Bondarenko, 2024).

Bilgisayarlar ve YZ destekli yazılımların finans sektörüne entegrasyonu, finansal analiz ve karar alma süreçlerini hızlandırırken hem olumlu hem de olumsuz etkiler doğurmuştur. Olumlu yönleri arasında, işlem ücretlerinin ve sermaye maliyetlerinin düşmesi gibi yenilikçi finansal teknolojilerin işletmelere sağladığı faydalar yer

almaktadır. Ancak, algoritmik ticaretin getirdiği yüksek hız, piyasalarda istikrarsızlıklara yol açarak ani çöküşler gibi riskleri artırmıştır (Blauth, vd., 2022:77113).

YZ'nin kripto para alanını finansal kâr amacıyla manipüle etmek için kullanılmasının yanı sıra, teröristler "sıcak cüzdanlardan" kripto para çalmak amacıyla da YZ'den faydalanabilmektedir (UNICRI ve UNCCT, 2021:39).

2024 yılının ilk yarısında, kripto para ekosistemi, siber saldırılar nedeniyle önemli finansal kayıplar yaşamıştır. Blockchain analiz firması TRM Labs'ın verilerine göre, bu dönemde dünya genelinde 1,38 milyar doların üzerinde kripto para çalınmıştır. Bu rakam, 2023'ün aynı döneminde kaydedilen 657 milyon doların iki katından fazladır. Bu artışın temel nedenleri arasında, az sayıda büyük ölçekli saldırının gerçekleşmesi ve kripto para birimlerinin değerlerindeki yükseliş bulunmaktadır. Özellikle Bitcoin, Ethereum ve Solana gibi sanal paraların değer kazanması, siber suçluların bu varlıklara yönelik ilgisini artırmıştır. TRM Labs'ın küresel politika başkanı Ari Redbord, kripto para ekosisteminin güvenliğinde temel bir değişiklik olmadığını, ancak sanal para değerlerindeki artışın siber suçluları daha fazla motive ettiğini belirtmiştir. 2024'ün ilk yarısındaki en büyük kayıplardan biri, Japon kripto borsası DMM Bitcoin'in yaklaşık 308 milyon dolar değerinde Bitcoin kaybettiği "yetkisiz sızıntı" olayıdır. Bu tür büyük ölçekli kayıplar nadir olmakla birlikte, kripto para şirketleri siber saldırılar için yüksek riskli hedefler olmaya devam etmektedir. 2022 yılında çalınan toplam kripto para miktarı yaklaşık 900 milyon dolar olarak kaydedilmiştir. Amerika Birleşik Devletleri, bu hırsızlığı Kuzey Koreli bilgisayar korsanlarıyla ilişkilendirmiştir (Reuters, 2024).

5.4.Fiziksel Saldırı Yeteneklerinin Geliştirilmesinde Yapay Zekâ

Bir başka potansiyel sosyal tehdit de terörist saldırıları planlamak ve koordine etmek için YZ'nin kullanılmasıdır. YZ algoritmaları potansiyel hedeflere ilişkin verileri analiz etmek, güvenlik açıklarını ve zayıf noktaları belirlemek ve saldırının etkisini en üst düzeye çıkarmak için uyarlanmış saldırı planları geliştirmek için kullanılabilir. YZ'nin terörist saldırıları kolaylaştırmak için kullanılmasının bir yolu da otonom silah sistemlerinin (AWS) oluşturulmasıdır. Bu sistemler insan müdahalesi olmadan hedefleri belirleyebilir ve onlara saldırabilir, bu da onları özellikle asimetrik savaş durumlarında etkili kılar. AWS'ler, belirli bir bireyin veya grubun varlığı gibi belirli uyaranları tespit etmek ve bunlara yanıt vermek üzere programlanabilir ve saldırıları hassas ve etkili bir

şekilde gerçekleştirmek için gelişmiş sensörler ve silahlarla donatılabilir (Esmailzadeh ve Motaghi, 2024:173).

Bu tür silah sistemleri önceden belirlenmiş kriterlere göre hedefleri seçmek ve devreye sokmak üzere YZ algoritmaları ile programlanır. Böylece doğrudan insan müdahalesi olmadan çalışabilirler. Yeni teknolojilerin yaygınlaşmasıyla birlikte AWS'lerin gelecekte savaşın yürütülme biçimini şekillendirmesi beklenen bir devrimden oluşmaktadır. Özellikle, gelişmiş ML algoritmalarının savaşın belirli alanlarında uygulanması, bilgi ve veri işleme hızı, silah platformları ve gözetleme sistemleri için otomasyon ve nihayetinde karar alma konusunda benzeri görülmemiş yetenekler sağlamayı vaat etmektedir. Örneğin, hiper spektral görüntüleme, hesaplamalı fotoğrafçılık ve kompakt sensör tasarımı gibi gelişmiş sensör teknolojileri, hedef tespiti, tanınması ve izlenmesi yeteneklerini önemli ölçüde iyileştirmeyi ve geleneksel görüş hattı engellerinin üstesinden gelmeyi amaçlamaktadır. Kompozitler, seramikler ve uyarlanabilir özelliklere sahip nanomalzemeler de dahil olmak üzere son teknoloji malzemeler, askeri ekipmanların daha hafif ama çevreye karşı daha dayanıklı olmasını sağlamaktadır. Yüksek güçlü lazerler ve optoelektronik cihazlar da dahil olmak üzere ortaya çıkan fotonik teknolojileri, kuantum hesaplama ve kuantum kriptografisine dayalı yeni düzeylerde güvenli iletişim sağlayabilmektedir. Ayrıca, bu teknolojilerin YZ sistemleri, robotik, 3D baskı, yönlendirilmiş enerji, insansız sistemler ve diğer yıkıcı teknolojileriyle bir araya getirilmesi savaşlarda stratejik ve operasyonel avantaj sağlamaktadır (Raska, 2021:457).

Fakat YZ silahlarının, iki yönlü kullanımı ve gelecekte neler yapabileceği konusundaki belirsizlik, büyük güçler arasında bir güvenlik ikilemini tetiklemiş ve dolayısıyla silahlanma yarışını halihazırda başlatmıştır. Bu sistemler giderek daha özerk hale gelmektedir. Makinelere insanların yaşam veya ölüm kararlarını verme yetkisi konusunda ne tür bir yetki-özerklik verilmesi durumu büyük bir soru işaretini gündeme getirmektedir (Payne, 2021:217).

AWS'lerin destekçileri, bu tür sistemlerin savaş durumlarında daha hızlı, daha hassas ve daha verimli tepkiler sağlayarak askeri yetenekleri potansiyel olarak artırabileceğini, bu silahların belirli görevleri makinelere atayarak insan askerlere yönelik riski azaltabileceğini iddia etmektedirler. Bunun bir örneği, gözetleme veya hedefli öldürme

için kullanılan ve böylece tehlikede olan insan pilot sayısını en aza indiren otonom İHA'lardır. Öte yandan, bu tür silahların kullanımı etik, yasal ve stratejik sorunları gündeme getirmektedir. Ana endişe, ölümcül karar alma üzerindeki insan kontrolünün potansiyel olarak kaybedilmesidir. Makinelerin yaşam veya ölüm kararları almasına izin vermek, ahlaki ve hesap verebilirlik sorunlarını gündeme getirmektedir. Sonuçta makineler karmaşık etik konuları kavrayamazlar ve bu nedenle hatalardan veya uluslararası yasaların ihlallerinden sorumlu tutulamazlar. Makineler ahlaki aktörler olamazlar. Bir savaş robotu görev hedefleri ve potansiyel kayıplar arasında denge kurarak hesaplamalar yaptığında, kendi yargısını değil, programcılarının yargısını kullanmaktadır (Payne, 2021:229).

Ayrıca, bu silah sistemlerinin operasyonel güvenliği konusunda da pratik endişeler bulunmaktadır. AWS, bilgisayar korsanlığı, sahtecilik veya diğer kötü niyetli eylemler gibi siber güvenlik risklerine maruz kalmaktadır. En önemlisi ise, AWS'nin yaygın kullanımının bir silahlanma yarışına yol açabileceği ve bu sistemlerin yaygınlaşmasının devlet dışı aktörlerin veya terör devletlerinin bunları kötüye kullanmasına olanak tanıyacağı yönünde ki meşru korkulardır (Liaropoulos, 2024:135).

Son on yılda, silahlı insansız hava araçlarının (SİHA) savaş alanı ve saldırı amaçlı kullanımı, ABD'nin Pakistan, Somali ve Yemen gibi bölgelerde terörle mücadele operasyonları için pilotsuz uçakları etkin bir şekilde kullanmasıyla önemli ölçüde artmış ve daha az insan gücü ve zayiat riskinin faydalarını vurgulamıştır. ABD'nin İHA'larla elde ettiği başarının ardından diğer ülkeler de bu araçları edinmeye başlamış ve 2001'den bu yana 100'den fazla ordu İHA kullanmıştır. Bu avantajlar sadece İHA teknolojisinin savaşta daha geniş bir kabul görmesine yol açmakla kalmamış, aynı zamanda terörist grupların da dikkatini çekmiştir. Bu gruplar artık intihar saldırıları gibi geleneksel yöntemlerden uzaklaşarak daha etkili, düşük riskli bombalı saldırılar için İHA'ları benimsemektedir. İHA'ların havada uzun süre fark edilmeden kalabilmesi teröristlerin daha hassas ve yıkıcı saldırılar gerçekleştirebilmelerini sağlamaktadır. İHA teknolojisinin evrimi, özellikle YZ entegrasyonu ile yeteneklerini daha da geliştirmiştir. YZ güdümlü dronlar görevleri otonom olarak yerine getirebilmekte ve teröristlerin karmaşık, büyük ölçekli saldırıları gizlice ve verimli bir şekilde gerçekleştirmelerine olanak sağlamaktadır (Adigwe, vd., 2024:294).

2020 yılında BM Yargısız ve Keyfi İnfazlar Özel Raportörünün, İnsan Hakları Konseyi'ne sunduğu raporda; en az 20 devlet dışı silahlı grubun silahlı ve silahsız İHA elde ettiğini bildirmiştir. 2023 yılı itibari ile 65 suçlu, isyancı veya terörist örgütün bu yeteneğe sahip olduğunu tahmin edilmektedir. Global Terörizm Veritabanı, 2000'lerin başından bu yana devlet dışı İHA kullanımında keskin bir artış olduğunu, sadece 2020'de 65 saldırı gerçekleştirildiğini tespit etmiştir. 2023 yılında DAEŞ, El Kaide ve ilgili kişiler, gruplar ve girişimler hakkında Birleşmiş Milletler İzleme Ekibi dört önemli eğilim bildirmiştir:

- İHA yetenekleri daha fazla terörist grup geliştirmiştir,
- Bazı terörist gruplar, İHA yeteneklerinin edinimi ve geliştirilmesi için yeni yollar belirlemeye aktif olarak çalışmaktadır,
- Bazı terörist gruplar, İHA kullanımına dair teknoloji ve eğitim paylaşmaktadır,
- Terörist gruplar tarafından İHA kullanımı küresel olarak yayılmaya devam etmektedir.

BM silah uzmanları, ilgili Güvenlik Konseyi yaptırımlarının uygulanmasını izleyerek devlet dışı kullanımını tespit etmiştir (UNOCT, 2024:1).

BM Terörle Mücadele Ofisi (UNOCT) ve Çatışma Silahlanma Araştırması (CAR) tarafından, üye devletlerin İHA'larla ilişkili tehditleri önleme, bunlara karşı koyma ve bunları azaltma konusundaki anlayışlarını ve hazırlıklarını iyileştirmek için hazırlanan 2023 Küresel Raporunda, devlet dışı aktörlerin İHA'ları;

- Ticari olarak satılan ürünlerin, bileşenlerin veya ilgili teknolojilerin yasal veya yasadışı yollarla satın alınması,
- Üreticilerin, kişilerin veya devlet kuruluşları dahil olmak üzere yasal muhafaza edenlerden çalma veya kaybolma,
- İHA'ların devlet dışı aktörler tarafından tasarımı, geliştirilmesi veya montajı. Bu edinim yolu, tüm bir sistemin imalatını veya halihazırda sahip olunan bir sistemin modifikasyonunu ifade edebilir,
- Yasadışı yollarla, kargo gönderileri ve kaçakçılık da dahil olmak üzere, malzemelerin sınır ötesi hareketi,

- Ulusal güvenlik güçleri, devlet kurumları, kolluk kuvvetleri veya uluslararası barış gücü gibi diğer paydaşlardan, zorla müdahale edilerek veya bunların İHA'nın terk etmesi veya teslim edilmesi yoluyla edinme,
- Bir devletin terörist veya diğer devlet dışı silahlı gruplara doğrudan İHA bileşenleri veya İHA teknolojisi tedarikini sağlaması,

yöntemleri ile devlet dışı aktörlerin İHA'ları temin ettikleri belirtilmiştir (UNOCT, 2024:15).

Terör örgütlerinin İHA'ları neden ve ne zaman benimsediğini ve bunları ne zaman başarılı bir şekilde kullanabildiklerini anlamak, bu teknolojinin gelecekteki tehditlerini değerlendirmek için çok önemlidir. İHA'lar boyut ve karmaşıklık açısından Black Hornet ve quadcopter gibi küçük gözetleme dronlarından, ABD tarafından kullanılan MQ-9 Reaper gibi orta irtifa, uzun dayanıklı (MALE) sınıfı dronlara kadar çeşitlilik gösterir. Birçok terörist grup, kamera veya küçük yükler taşıyabilen quadcopter tarzı dronlar kullanmaktayken, IŞİD ve Yemen'deki Husi isyancıları gibi örgütler, askeri düzeydeki daha uzun menzile sahip sabit kanatlı İHA'ları başka ülkelerin sponsorluğu aracılığı ile kullanmayı başarmıştır. Küçük ticari model İHA'lar da bir terörist saldırısı için patlayıcı taşıyacak şekilde yeniden donatılabilmektedir (Boyle, 2024:110).

Örnek olarak, ticari olarak satılan bir quadcopter İHA, devlet dışı bir silahlı grup tarafından silikon dolgu tüpünden patlayıcı atmak için silahlandırılmıştır (Görsel 5.4). Bu İHA 2017'de CAR saha araştırmacıları tarafından belgelenmiştir (UNOCT, 2024:26).

Görsel 5.4. Silahlandırılmış İHA (UNOCT, 2024:26).

Şubat 2017'de, CAR saha araştırmacıları tarafından belgelenen ve devlet dışı bir silahlı gruptan ele geçirilen askeri düzey savaş İHA'sı (Görsel 5.5)'de gösterilmiştir (UNOCT, 2024:44).

Görsel 5.5. Askeri Düzey Savaş İHA'sı (UNOCT, 2024:44).

Terör örgütleri İHA'ları ilk zamanlar teknolojinin sınırlılıklar nedeniyle taktik saldırılardan ziyade daha çok keşif amaçlı kullanmıştır. İlk zamanlar kameralı İHA'lar yaygın olarak mevcutken, yükleri bırakmak için uyarlanabilen modeller yakın zamanda ortaya çıkmıştır. İHA'ların başlıca avantajlarından biri, terörist grupların savaş alanına dair kapsamlı bir genel bakış elde etmelerini sağlayarak saldırı stratejilerini ayarlamalarını ve riskleri azaltmalarını sağlamasıdır. İHA'lara yönelik ilginin çoğu, bunların doğrudan saldırılar için nasıl kullanılabileceğine odaklansa da İHA'lar silahlı çatışma alanlarında topçu ve diğer kara saldırıları için bir güç sağlamada daha önemlidir. Irak ve Suriye'de IŞİD, ABD Özel Kuvvetleri ve yerel müttefiklerine karşı topçuları tespit etmek ve kara kuvvetlerini önceden konumlandırmak için alanları belirlemek amacıyla küçük ticari dronları kullanmıştır. Küçük ticari dronlar, teröristlerin düşmanın operasyon alanının gerisindeki ikmal hatlarını, üsleri ve diğer sabit yerleri korumasını zorlayan bir saldırı tasarlamalarını sağlayarak savaş alanının panoramik bir görünümünü sağlamaktadır. Devlet dışı aktörler, onları bu yerleri korumak için daha fazla kaynak harcamaya zorlayarak düşmanlarının ilerlemesini yavaşlatabilir ve maliyetlerini artırabilir. İHA'lar ayrıca risk azaltmak için de kullanılabilir, bir devlet rakibine karşı güç asimetrisiyle karşı karşıya kalan terörist gruplar için, düşmanın nerede olduğunu tahmin etmenin ve güçleriyle doğrudan çatışmanın maliyetlerini sınırlamanın belirgin avantajları vardır (Boyle, 2024:111).

Devlet dışı aktörler tarafından İHA kullanımının tarihi, düşmanları taciz etmek için ara sıra kullanımdan taktiksel savaş alanı kullanımına ve nihayetinde doğrudan saldırılara doğru bir evrim göstermektedir. Terör örgütleri tarafından İHA'ların ilk taktiksel kullanımı geçici olmuş, çok az grup bunları kapsamlı bir savaş planına entegre edebilmiştir. Bir İHA'yı saldırı için kullanma niyetine dair en erken kanıt, 1993 yılında Tokyo'daki sivil hedeflere sinir gazı sarin sıkmak için uzaktan kumandalı helikopterler kullanmayı planlayan Japon tarikat grubu Aum Shinriyko'ya aittir (Boyle, 2024:112).

Terörist İHA'larla ilişkili potansiyel olarak ciddi riskler, Nisan 2016'da dönemin Başkanı Barack Obama tarafından Washington'da düzenlenen Nükleer Güvenlik Zirvesi'nde vurgulanmıştır. Obama, elli devlet başkanının katıldığı toplantıda, radyoaktif ve yasadışı maddelerin genellikle çok az incelemeyle satılıp değiştirildiği karanlık ağ olarak adlandırılan ve internetin keşfedilmemiş kısmı olan darkweb'den satın alındığını belirtmiştir. Bu maddelerin batı şehirlerine saldırılar düzenlemek için İHA'lara

bağlandığı bir senaryo üzerinde durmuştur. Dönemin İngiliz Başbakanı David Cameron, IŞİD gibi örgütlerin bombalı İHA konuşlandırmasının tehdidinin fazlasıyla gerçek olduğu konusunda uyarmıştır. İngiliz istihbarat yetkilileri, IŞİD'in radyoaktif madde yaymak için ideal olabilecek düşük seviyeli tarım ilaçlama İHA'larını aradığını ortaya çıkarmıştır (Boyle, 2020:133).

2015 yılında Japonya'da bir çevre aktivisti Hükümetin uyguladığı politikalara tepki olarak radyoaktif madde taşıyan İHA'yı Başbakanlık ofisinin çatısında indirmiştir. Eylül 2016 ile Şubat 2018 tarihleri arasında Irak ve Suriye'de DEAŞ örgütü tarafından İHA kullanımına ilişkin 338 olay tespit edilmiştir (UNOCT, 2024:5).

Görsel 5.6'de, IŞİD'in sosyal medya platformlarını operasyonel bilgi ve eğitim materyalleri paylaşmak için nasıl kullandığını göstermektedir. Kapatılmış olan IS Academy adlı hesaptan yapılan bir paylaşımda, eski Cebhat el-Nusra komutanı Ebu Mariya el-Kahtani'nin medya eğitimi ve yerel istihbarat toplamak amacıyla İHA kullanımına dair eğitim verdiği görülmüştür (Özyurt, 2021:75).

Görsel 5.6. IŞİD İHA Eğitim Twitter Paylaşımı (Özyurt, 2021:75).

Ağustos 2018'de Venezuela Devlet Başkanı Nicolas Maduro'ya suikast düzenlemek için Küresel Konumlandırma Sistemi güdümlü ve bomba yüklü iki İHA kullanılarak başarısız bir girişimde bulunulmuştur. İster tam teşekküllü darbe girişimleri ister bir

ülkeyi siyasi olarak istikrarsızlaştırma çabaları veya vatandaşları sindirme önlemleri adına olsun, siyasi suikastlar yapmaya hazır aktörlerin bu teknolojiyi geliştirecekleri açıkça görülmektedir (Bazarkina, 2023:259).

İlk insansız araçlar genellikle yalnızca otomatik yetenekler sergilerken, YZ ve ML teknolojisindeki gelişmeler, daha yüksek düzeyde otonom yeteneklere sahip sistemlerin geliştirilmesine olanak tanımaktadır. İnsansız sistemlerin geleceği, uzaktan kumandalı ve otomatik sistemlerden neredeyse tamamen otonomiye kadar geniş bir otonomi yelpazesine doğru evrilmektedir. Aşağıda otonom kategoriler belirtilmiştir;

- Yarı Otonom: Bu modda, insanlar seçili işlevlerin kontrolünü elinde tutarak, YZ'ye herhangi bir yetkilendirme verilmez ve eylemde bulunması engellenir. İnsanlar sistemin kontrol döngüsünün ayrılmaz bir parçasıdır.
- Gözetimli Otonom: YZ, operasyonların tüm yönlerini kontrol eder, ancak insanlar operasyonları izler ve gerektiğinde müdahale edebilir.
- Tamamen Otonom: YZ algoritmaları, insan rehberliği veya müdahalesi olmadan sistem operasyonunun tüm yönlerini kontrol eder. Otonom İHA, doğrudan insan yetkisi veya bildirimi olmadan devreye girmektedir (Lehto ve Hutchinson, 2020:328).

İnsansız araçlara otonom özellikleri yanı sıra birlikte hareket etme yeteneği kazandıran sürü algoritmaları geliştirilmiştir. Sürü İHA'lar, belirli bir görevi yerine getirmek için birlikte hareket eden ve iş birliği yapan çok sayıda insansız hava aracından oluşur. Bu sistemlerin temelini ise YZ teknolojisi oluşturur. Otonom bir sistemin YZ ile düşünme ve karar alma yeteneği; çevresini kameralar, mikrofonlar ve sensörler gibi araçlarla algılayıp bir dünya modeli inşa etmesine dayanır. Bu model, sürekli güncellenir ve optimize edilir, ardından sistem bu bilgileri kullanarak eyleme geçer. İşte bu süreç, etkili bir otonom sistemin temelini oluşturur. Örneğin, otonom bir İHA'nın seyrüsefer yeteneği, kullanılan dünya modelinin basitliği sayesinde etkili bir şekilde çalışır. Bu model, tercih edilen rotaları, yükseklik engellerini ve uçuşa yasak bölgeleri içeren haritalardan oluşur. Radarlar, engellerin olmadığı irtifaları tespit ederek bu modeli gerçek zamanlı olarak desteklerken GPS, İHA'nın uçuş sırasında engellere çarpmadan veya yasaklı bölgelere girmeden görevini yerine getirmesine yardımcı olur. Sürülerin doğadaki hayatta kalma içgüdüleri ve yiyecek arama davranışlarından esinlenerek geliştirilen YZ

Sürü Algoritmaları, İHA'ların karınca, kuş ve böcek gibi hayvan topluluklarının davranışlarına benzer şekilde hareket etmelerini sağlar. Bu sayede, çok sayıda İHA senkronize bir şekilde hareket edebilir. Sürü teknolojisinin en dikkat çekici özelliği, "kendi kendine organize olma" (self-organization) yeteneğidir. Örneğin, Karınca Kolonisi Algoritması, sürü İHA'ların rota planlamasında sıklıkla kullanılan bir yöntemdir. Bu algoritma sayesinde, İHA'lar en uygun rotaları en kısa sürede belirleyebilir ve görevlerini verimli bir şekilde yerine getirebilir (Kalınbacak, 2023:192).

2017 yılında, ABD Savunma Bakanlığı (Pentagon), o dönemin en büyük mikro-drone sürüsünün başarılı bir şekilde test edildiğini duyurmuştur. Test, Kaliforniya'daki China Lake bölgesinde gerçekleştirilmiş ve üç F/A-18 Super Hornet savaş uçağından aynı anda 103 adet Perdix mikro-drone'un serbest bırakılmasıyla tamamlanmıştır. Perdix dronları, Massachusetts Teknoloji Enstitüsü (MIT) öğrencileri tarafından geliştirilen bir prototipten esinlenerek tasarlanmış ve MIT Lincoln Laboratuvarı tarafından askeri ihtiyaçlara göre uyarlanmıştır. Bu drone sürüsü, klasik anlamda bir lider veya merkezi bir komuta birimi olmaksızın işlev görebilen bir YZ sistemine dayanmaktadır. Sürünün yetenekleri arasında kolektif karar alma, çevresel değişimlere uyum sağlayan formasyon uçuşu ve bireysel drone kayıplarına rağmen görevini sürdürebilme kabiliyeti bulunmaktadır. Pentagon yetkilileri, bu sistemin doğadaki sürü davranışlarını model aldığını ve bir "dağıtılmış beyin" ile çalıştığını belirtmiştir (Snow, 2017).

2017 yılında, ABD merkezli bir araştırma enstitüsü ve sosyal yardım kuruluşu olan Future of Life Institute, birkaç gram patlayıcı yüklü bir mikro İHA sürüsünün hedeflerini belirlemek ve onlara kamikaze tarzında saldırmak için yüz tanıma özelliğini kullandığı "Slaughterbots" başlıklı bir video yayımlamıştır. Yüz tanıma teknolojisi, İHA tarafından toplanan görüntüleri gömülü bir yüz tanıma veri tabanına yüklenen görüntülerle çapraz referanslama yaparak İHA'yı seçilen bir hedefi otonom olarak alacak, tanımlayacak ve saldıracak şekilde programlamasını sağlamıştır (UNICRI ve UNCCT, 2021:35).

Ocak 2018'de Suriye'deki Hmeymim ve Tartus iki Rus askeri üssü eş zamanlı olarak sürü İHA saldırılarına maruz kalmıştır. Rusya, saldırının planlanması ve gerçekleştirilmesinin yüksek derecede karmaşık olması nedeniyle, bu eylemin arkasında ABD'nin bulunduğunu öne sürmüştür. Her ne kadar bu saldırılar başarısızlıkla sonuçlanmış olsa da çatışma bölgelerinde İHA kullanımının etkisini gösteren çarpıcı bir

örnek teşkil etmektedir. Eylül 2019'da Suudi Arabistan'daki ARAMCO petrol tesislerine yapılan sürü İHA ve füze saldırısı, İHA'ların kritik altyapılara yönelik tehdit potansiyelini göstermiştir (Genç ve Erciyes, 2020:36).

Mart 2020'de Libya'daki askeri çatışma sırasında kullanılan ilk YZ tabanlı otonom insansız hava aracı Birleşmiş Milletler raporunda belgelenmiştir. Cambridge Üniversitesinin Küresel Terörizm Veri Tabanını kullanarak yaptığı bir araştırmaya göre, 2016-19 yılları arasında 76 terör saldırısında İHA'lar kullanılmış, bunlardan 47'si başarılı olmuş ve 50 ölüm ve 132 yaralanmayla sonuçlanmıştır (Barten, vd., 2022:193).

Günümüze kadar İHA'lar savaş alanlarında giderek daha fazla kullanıldığı ve ticari olarak satılan İHA'ların teröristler için tercih edilen ucuz araçlar haline geldiği görülmektedir.

2023 yılında, FBI Direktörü Christopher Wray Dünya Ekonomik Forumunda, sürücüsüz araçların da kötü niyetli aktörler tarafından hedef alınması ve bir silah olarak kullanılması tehlikesi konusunda uyarılarda bulunmuştur (Lohmann, 2024:27).

YZ'nın en çok bilinen uygulamalarından biri de sürücüsüz ya da kendi kendine giden otomobiller olarak da adlandırılan biri otonom araçlardır. Otonom araçlar birçok kişi tarafından geleceğimiz için daha güvenli, daha rahat ve daha verimli bir ulaşım aracı olarak kabul edilmektedir. Özünde, aracın yerleşik bilgisayarına yerleştirilen YZ, aracın hareketlerini, direksiyonu, hızlanmayı, çalışma frenini vb. kontrol ederken sürücünün karar verme süreçlerini taklit etmek için derin öğrenme tekniklerini kullanmaktadır. Tesla ve Google gibi şirketler uzun zamandır bu teknolojinin pratikte uygulanmasını savunmakta ve otonom araçların araştırılması, test edilmesi ve geliştirilmesi çabalarına öncülük etmektedir. Son yıllarda, sayısız büyük otomobil şirketi de sürücüsüz otomobilleri yollara çıkarma çabalarında onlara katılmıştır. Teknolojinin hızla ilerlemesi, otonom araç endüstrisine yapılan önemli ticari yatırımlar ve yasal ve politik zorlukların ele alınmasında çok sayıda kilometre taşının başarılmasıyla birlikte, yapay zekanın eninde sonunda sürüş deneyimini gerçekten dönüştüreceği kaçınılmaz görünmektedir. Terörizm ve araçların kapsamlı geçmişi göz önünde bulundurulduğunda, araçlarda artan otonomi, terörist gruplar için çok iyi bir gelişme olabilir ve bir takipçinin hayatını feda etmesine veya yakalanma riskine girmesine gerek kalmadan en geleneksel saldırı türlerinden birini uzaktan etkili bir şekilde gerçekleştirmelerine olanak tanıyabilir.

Tamamen otonom araçlarla taşınan el yapımı patlayıcı cihazlarla saldırıları kolaylaştırmanın yanı sıra, sürücüsüz araçların ciddi kazalara neden olmak, yolları kapatmak veya kendi kendine katliam yapmak için kullanılabileceği de öne sürülmüştür. Terör örgütleri tarafından sürücüsüz araçlar kullanarak henüz gerçekleşmiş bir eylem raporlanmamış olsa da IŞİD destekçilerinin bu araçlar üzerinde ilkel deney ve teşebbüsleri oldukları bilinmektedir (UNICRI ve UNCCT, 2021:33).

İnsansız hava ve kara araçlarının birlikte sürü halinde çalışabilirlik ve hedef tespit kabiliyetlerini geliştirmek amacıyla, Nisan 2023'te İngiltere'nin Upavon Havaalanı'nda AUKUS ittifakı (Avustralya, Birleşik Krallık ve ABD) tarafından, YZ ile desteklenen bir test gerçekleştirilmiştir. Yapılan testte, Blue Bear Ghost ve Insitu CT220 İHA'ları ile Challenger 2 tankı ve Viking insansız kara araçları bulunmaktadır. Bu araçlar, YZ algoritmalarının gerçek zamanlı yeniden programlanmasını ve farklı sistemler arasında iş birliği sağlama potansiyelini değerlendirmek üzere test edilmiştir (Demarest, 2023).

YZ ve otonom sistemlerin gelişimi hem savaş alanlarında hem de terörizm bağlamında önemli fırsatlar ve tehditler sunduğu görülmektedir. YZ tabanlı AWS ve İHA'ların, askeri operasyonlarda hız, hassasiyet ve risk azaltma gibi avantajlar sağladığı fakat bu teknolojilerin aynı zamanda etik, yasal ve güvenlik sorunlarını da beraberinde getirdiği görülmektedir. AWS'lerin ve İHA'ların devlet dışı aktörler ve terörist gruplar tarafından kötüye kullanımı, ciddi güvenlik riskleri doğurmaktadır. İHA'ların ticari modellerinin bile terörist gruplar tarafından düşük maliyetli temin edilebiliyor olması veya başka devletlerin sponsorluğunda elde etmeleri tehditlerin boyutunu artırmaktadır.

5.5.Siber Saldırı Yeteneklerinin Geliştirilmesinde Yapay Zekâ

Siber terörizm bağlamında YZ'nin potansiyel tehditlerinden biri, kritik altyapı ve diğer hedeflere yönelik siber saldırılarda kullanılmasıdır. YZ algoritmaları, ağlar ve sistemlerdeki güvenlik açıklarını tespit ederek, tespit edilmesi ve önlenmesi zor hedefli saldırılar geliştirmek için etkili bir araç olarak kullanılabilir. Siber saldırganlar, büyük miktarda veriyi analiz eden ve yazılım ile ağ sistemlerindeki zayıflıkları tespit eden YZ algoritmaları sayesinde daha etkili ve hedefli saldırılar başlatabilir. Bu durum, güvenlik protokollerindeki kalıpları belirlemek ve istismar etmek için makine öğrenimi tekniklerinden faydalanmayı içermektedir. YZ destekli siber saldırıların en endişe verici yönlerinden biri, bu saldırıların otomatik hale getirilerek, saldırganların minimum insan

müdahalesiyle büyük ölçekli ve koordineli saldırılar gerçekleştirme potansiyelidir. Böyle bir senaryo, kritik altyapının kesintiye uğraması, hassas verilerin çalınması ve ulusal güvenliğin tehlikeye düşmesi gibi ciddi sonuçlara yol açabilir. Diğer taraftan, siber savunma alanında YZ, saldırıları tespit etmek ve önlemek için de kullanılmaktadır. Makine öğrenimi algoritmaları, anormal ağ trafiği modellerini tanımlamak ve yeni tehditleri tespit etmek gibi görevlerde etkili olabilir. Ancak, YZ'nın bu çift yönlü kullanımı siber güvenlikte, savunma mekanizmalarını güçlendirebileceği gibi, saldırganlar tarafından tespit edilmekten kaçınmak ve güvenlik önlemlerini aşmak için de kullanılabilmektedir. Genel olarak, siber saldırılarda YZ'nin kullanımı, küresel güvenlik için önemli bir tehdit oluşturmaktadır (Esmailzadeh ve Motaghi, 2024:175).

YZ sistemlerinin sosyal mühendislik, DDoS, kimlik avı, fidye yazılımı gibi siber saldırı yöntemlerine entegrasyonu bu saldırıların etkinliğini artırarak farklı bir boyut kazandırmaktadır.

5.5.1. Sosyal Mühendislikte Yapay Zekâ

Sosyal mühendislik saldırıları, insan psikolojisini manipüle ederek bireyleri belirli eylemleri gerçekleştirmeye veya hassas bilgileri ifşa etmeye yönlendirmeyi amaçlar. Bu yöntemler, geleneksel dolandırıcılık veya güven oyunlarından farklı olarak, genellikle bilgi toplama, dolandırıcılık veya bilgisayar sistemlerine yetkisiz erişim elde etmeye odaklanır ve saldırgan ile kurban arasında doğrudan bir temas olmadan gerçekleşebilir (Girhepuje, vd., 2024:14).

Siber teröristler, güvenli sistemleri hedef almak için YZ ve büyük veri analitiğini birleştirerek etkin bir şekilde kullanmaktadır. Bu yöntemlerin tercih edilmesinin temel nedeni, teröristlerin kurbanlarıyla fiziksel olarak temas kurma zorunluluğunu ortadan kaldırması ve bu sayede hem kendi hayatlarını riske atmaktan kaçınmaları hem de büyük miktarda finansmana ihtiyaç duymamalarıdır. Bir bilgisayarın arkasında oturan teröristler, sosyal medya platformlarını kullanarak biyometrik verilere erişim sağlayabilmektedir (Lohmann, 2024:25).

YZ, yüz tanıma, parmak izi, iris ve davranış tanıma gibi biyometrik sistemleri desteklemektedir. Ancak bu teknolojiler, siber suçlular tarafından kötüye kullanılabilir ve dijital biyometrik veriler çalınabilir. Biyometrik sistemler, çevrimiçi kaynaklardan

biyometrik verilerin ele geçirilmesi ya da ölmüş kişilere ait biyometrilerin kullanılması gibi yöntemlerle hacklenebilir. Makine öğrenimi de biyometrik sistemlerin YZ algoritmalarını geliştirerek canlı ve ölü irisler arasındaki farkı ayırt etme yeteneğine kadar ilerlemiştir. Sosyal medya platformlarında yüz, retina, iris, kulak şekli desenleri ve bazı durumlarda avuç içi ve parmak izi gibi biyometrik veriler rahatlıkla ifşa edilebilmektedir. TikTok ve Instagram gibi platformlar, gözlerin yakın çekim görüntüleri ve makyaj ya da küpe reklamı yapan kulak görüntüleri gibi içeriklerle bu tür bilgilerin elde edilmesini kolaylaştırmaktadır. Twitter'da yüksek çözünürlüklü parmak izi görüntüleri paylaşılabilirken, Viber, Telegram ve WhatsApp gibi iletişim uygulamaları veya Facebook gibi sosyal medya platformları, ses kalıpları, avuç içi şekilleri ve bazen coğrafi konum ya da zaman damgaları gibi bilgiler sunmaktadır (Yurdasen, 2023).

Biyometrik veriler, kimyasal, biyolojik, radyolojik ve nükleer araştırma laboratuvarları, bankalar ve borsa gibi yüksek ulusal güvenlik değerine sahip yerlere erişimde kullanıldığından, bu hassas bilgilerin sızdırılması kötü niyetli aktörlerin ciddi zararlar vermesine olanak tanıyabilir. Örneğin, hacklenmiş biyometrik verileri kullanan teröristler, bir laboratuvardan tehlikeli patojenler salabilir, borsayı manipüle ederek çöküşe sürükleyebilir veya izleme araçlarını kullanarak sivilleri gözetleyebilir. Dahası, hükümet yetkililerine ait biyometrik verilerin bile korunmasız olması büyük bir güvenlik açığıdır. Örneğin, Avrupa Komisyonu'nun web sitesinde, hükümet yetkililerinin 10 megapikselin üzerinde çözünürlüğe sahip portreleri, 50.000 fotoğraf ve 120.000 videodan oluşan bir arşivde kullanıcıların erişimine açıktır. Bu içerikler, ses kayıtlarıyla birlikte, yüksek kaliteli biyometrik verilerin (göz ve parmak izi desenleri veya ses kalıpları) kolayca çıkarılmasına olanak tanımaktadır. Siber güvenlik şirketi F5'in Kuzey ve Batı Avrupa güvenlik çözümleri mimarı Keiron Shepherd, kötü niyetli aktörlerin biyometrik testleri atlatmak için yüksek çözünürlüklü fotoğraflardan yararlandığını belirtmektedir. Bu yöntemlerle sahte gözler veya üç boyutlu baskılar üretilmekte ve bu sahte biyometrik veriler sistemlere erişim sağlamak için kullanılmaktadır. Biyometrik verilerin, şifrelerin aksine, sıfırlanamaz olduğu göz önüne alındığında, bu durum kullanıcılar için ciddi güvenlik riskleri doğurmaktadır. Özellikle, cihaz kameralarının giderek daha gelişmiş hale gelmesiyle birlikte, sıradan kullanıcıların dahi bu tür saldırılara maruz kalma olasılığı artmaktadır (Lohmann, 2024:26).

5.5.2. Kimlik Avı ve Fidye Yazılımı Saldırılarında Yapay Zekâ

Kimlik avı, güvenilir bir kurum, şirket veya tanıdık bir kişi gibi davranılarak gönderilen sahte e-postalar veya diğer iletişim biçimleri aracılığıyla bireyleri aldatmayı amaçlayan bir siber saldırı türüdür. Bu saldırılar, alıcıları zararlı ekleri açmaya, kötü amaçlı yazılımlar indirmeye veya gizli kişisel bilgilerini ifşa etmeye yönlendirmeyi hedefler. ChatGPT gibi YZ araçları, hedeflenen göndericinin yazı tarzını ve tonunu taklit ederek ikna edici kimlik avı e-postaları veya mesajları oluşturabilir. Ayrıca, bu mesajlara kişiselleştirilmiş ve özgün detaylar ekleyerek alıcıların aldatılma olasılığını artırabilir. Örneğin GenAI, bir çalışma arkadaşı gibi davranarak iş ile ilgili yardım isteyen ve zararlı bir eki içeren bir e-posta hazırlayabilir. Benzer şekilde, bir sosyal ağ platformuna veya oyuna kaydolmayı öneren, alıcıdan iletişim bilgilerini (telefon numarası veya e-posta adresi gibi) isteyen sahte bir e-posta oluşturabilir. GenAI ayrıca Google'dan gönderilmiş gibi görünen ve tarayıcı ayarlarının güncellenmesi gerektiğini iddia eden son derece ikna edici kimlik avı e-postaları hazırlayabilir. Bu tür e-postalar, alıcıları sahte bir giriş sayfasına yönlendirerek kullanıcı adı ve şifre gibi hassas bilgilerin yasa dışı yollarla ele geçirilmesine neden olabilir (Nagarajan ve Kamalbabu, 2024:665).

Fidye yazılımları defalarca küresel olarak en önemli siber güvenlik tehditlerinden biri olarak kabul edilmiştir. Kurbanların dosyalarını şifreleyen ve dosyaların şifresinin çözülmesi için fidye ödenmesini talep eden kötü amaçlı yazılımlardır. Fidye yazılımı saldırılarının tehdidi, kötü amaçlı yazılımın kendi kendini yayma işlevi nedeniyle binlerce cihaza kolayca yayılabilmesi gerçeğiyle daha da artmaktadır. Örnek olarak, 2017 yılında WannaCry fidye yazılımı saldırısı, 150 ülkede 200.000'den fazla bilgisayarı etkilemiştir. Saldırı sonucunda kullanıcılardan dosyalarını kurtarmak için Bitcoin olarak fidye talep edilmiştir. YZ'nin fidye yazılımlarına entegre edilmesi, bu saldırıların etkilerini büyük ölçüde artırabilmektedir. ML modelleri, yeni saldırı türleri yaratarak veya akıllı hedefleme yöntemleriyle mevcut saldırıların etkilerini artırarak mevcut fidye yazılımı ekosistemini çoğaltmak için kullanılabilir. ML algoritmaları, fidye yazılımını iletmek için kimlik avı kampanyasının etkinliğini artırmak için de kullanılabilir. Gelişmiş fidye yazılımı saldırıları gerçekleştirmek için YZ kullanıldığında, zaten karlı olan bir saldırı yöntemi çok daha karlı hale gelebilir. Bu tür saldırılar, terörist grupların ve bireylerin altyapılarını veya faaliyetlerini desteklemek için gelir elde etmek amacıyla da kullanılabilir (UNICRI ve UNCCT, 2021:39).

5.5.3. Kötü Amaçlı Yazılımda Yapay Zekâ

YZ, siber güvenlik alanında özellikle kötü amaçlı yazılımlar konusunda önemli bir değişim yaratmış ve daha gelişmiş saldırı yöntemlerinin ortaya çıkmasına yol açmıştır. YZ destekli kötü amaçlı yazılımlar, geleneksel savunma mekanizmalarını aşmada benzeri görülmemiş yöntemler kullanarak tespit ve müdahale süreçlerini daha karmaşık hale getirmektedir. Bu tür yazılımlar, hedef sistemlerin davranışlarını analiz etmek ve sömürülebilecek güvenlik açıklarını belirlemek için makine öğrenmesi ve derin öğrenme modelleri gibi ileri tekniklerden yararlanmaktadır. YZ, zararlı yazılımların hedef sistemlerin ortamına bağlı olarak dinamik bir şekilde kendini değiştirmesine olanak tanımaktadır. Bu durum da geleneksel antivirüs programları ve güvenlik sistemleri tarafından tespit edilmelerini zorlaştırmaktadır. Bu gelişmeler, zararlı yazılımların uzun süre fark edilmeden kalmasına ve aşamalı, daha hassas saldırılar gerçekleştirmesine olanak tanımaktadır. YZ destekli bu zararlı yazılımlar, büyük veri analitiğinden yararlanarak hedefledikleri sistemlerin davranış modellerini değerlendirebilmekte ve büyük veri hacimlerini hızlı bir şekilde işleyerek en etkili saldırı stratejilerini belirleyebilmektedir (Abbadi ve Lachkar, 2024:2578).

Kimlik avı saldırıları kötü amaçlı yazılım dağıtmanın başlıca yollarından biridir. SNAP_R adı verilen bir YZ deneyinde, 819 kullanıcıya dakikada 6,75 tweet hızında kimlik avı tweetleri gönderilmiş ve 275'i başarılı olmuştur. Deneydeki insanlar ise 129 kullanıcıya dakikada 1,075 tweet göndermiş ve sadece 49'u başarılı olmuştur. Kötü amaçlı yazılımları dağıtmak için bir başka yöntem de SQL enjeksiyon saldırılarıdır. SQL enjeksiyon saldırıları YZ tarafından kolaylaştırılabilir. Örneğin, YZ destekli DeepHack aracı, bir sinir ağı kullanarak web uygulamalarına nasıl girileceğini öğrenmektedir. Bunun gibi araçlar, hedef sistem hakkında önceden bilgi sahibi olmadan bile çalışabilen ve kötü amaçlı yazılım sunabilen tam operasyonel otomatik bilgisayar korsanlığı sistemleri oluşturmak için kullanılabilir. 2018 yılında IBM araştırmacıları Black Hat USA Konferansı'nda, YZ'nin kötü amaçlı yazılım saldırılarını nasıl geliştirebileceğini tam olarak göstermek için geliştirdikleri "DeepLocker" kötü amaçlı yazılımı tanıtmışlardır (UNICRI ve UNCCT, 2021:37). DeepLocker bir video konferans yazılımı olarak görünen ve amacını belirli bir kurbana ulaşana kadar gizleyen bir kötü amaçlı yazılım türüdür. DeepLocker, saldırı yükünü zararsız uygulamalar içinde gizlemek için derin bir sinir ağı kullanır. Saldırı yükü, amaçlanan hedefine ulaşana kadar hareketsiz kalır. Hedefi

tanımlamak için görsel, ses, coğrafi konum ve sistem düzeyinde özellikler dâhil olmak üzere birden fazla öznitelikten yararlanmaktadır. Mevcut kötü amaçlı yazılımların aksine bu yenilikçi yaklaşım, zararsız yazılımların tersine mühendisliğini yapmayı ve saldırı yükü ve hedefin özellikleri gibi görev açısından kritik öneme sahip sırları kurtarmayı yüksek düzeyde zorlaştırmaktadır (Girhepuje, vd., 2024:15).

5.5.4. Dağıtılmış Hizmet Reddi Saldırılarında Yapay Zekâ

Dağıtılmış Hizmet Reddi (DDoS) saldırısı, bilgisayar sistemlerini veya bir ağı çalışmaz duruma getirmek ve böylece kullanıcıların sisteme erişimini engellemek için kullanılmaktadır. DDoS saldırıları, bir sistemin çökmesine neden olan belirli bir veri parçasının iletilmesi veya hedefi aşırı miktarda ağ trafiğiyle yorarak gerçekleştirilir. DDoS saldırıları, aşırı miktarda trafiğe sahip sistemleri bunaltmayı veya kasıtlı olarak hizmetlerin çökmesine neden olmak amacıyla bankacılık, perakende, medya, ticaret, kamu kuruluşları ve özel sektördeki önde gelen şirketlerin web sitelerini hedef alır (Nagarajan ve Kamalbabu, 2024:666).

YZ, siber suçluların DDoS saldırılarının hassasiyetini hassas bir şekilde ayarlamasını sağlar. ML algoritmaları, DDoS saldırıları başlatmak için en uygun zamanları ve yöntemleri belirlemek üzere büyük miktarda ağ trafiği verisini analiz edebilir. YZ saldırganların taktiklerini gerçek zamanlı olarak düzenlemesine olanak tanır ve bu da geleneksel savunma sistemlerinin saldırıyı önlemesini zorlaştırır. Örnek olarak, 2018 yılında GitHub sitesi trafiğinin 1,35 Tbps'ye çıkmasıyla kayıtlara geçen en büyük DDoS saldırısını yaşamıştır. Ayrıca Botnet'leri kontrol etmek için YZ'nın kullanılması, DDoS saldırı stratejilerinde büyük bir devrim yaratmıştır. YZ algoritmaları, koordineli saldırılar yürütmek için botnet cihaz ağlarını otonom olarak kontrol edebilir. YZ destekli botnetler, tespit edilmekten kaçınmak ve saldırının yoğunluğunu korumak için davranışlarını gerçek zamanlı olarak ayarlayabilir. Örnek olarak, 2016'da ortaya çıkan Mirai botnet YZ'yı bünyesine katarak tespit edilmekten kaçınma ve kritik hedefleri belirleme konusunda daha yetenekli hale gelmiştir. YZ algoritmaları ağ trafiğini analiz ederek, en savunmasız cihazları belirler ve botnet'in saldırılarını genişletmesine ve yoğunlaştırmasına imkân sağlar. YZ'nın öğrenme ve uyum yeteneği, siber suçlular için en önemli avantajlarından biridir. YZ destekli DDoS saldırıları doğal ağ trafik modellerini taklit eder ve bu da güvenlik sistemlerinin normal ve kötü amaçlı trafik arasında ayrım yapmasını zorlaştırır.

YZ, Savunma amacıyla uygulanan karşı önlemleri hızlıca öğrenir ve savunmaları aşmak için yeni saldırı modellerini geliştirir. Bu uyarlanabilir yetenek, YZ destekli DDoS saldırılarını güçlü ve dayanıklı hale getirir (Utter, 2024).

IŞİD'in 2017 yılında, IŞİD Dark Web forumunda üyeleri arasında DDoS saldırısı planlanması yapılarak "Caliphate Cannon" adlı bir DDoS uygulamasıyla askeri, ekonomik ve eğitim altyapısı hedef alınarak saldırı düzenlemiştir. IŞİD'in bilgisayar korsanlığı bölümü birçok kez bu tip saldırıların sorumluluğunu da üstlenmiştir (UNICRI ve UNCCT, 2021:36). 2020 yılında Amazon Web Services, YZ kullanılarak organize ve yönlendirilmiş karmaşık bir DDoS saldırısına maruz kalmıştır. YZ, saldırının etkinliğini artırarak önemli ölçüde hizmet kesintisine neden olmuştur. Bu olaylar, yapay zekanın siber saldırılarda kullanımının artmasıyla siber güvenliğin karşı karşıya olduğu zorlukların giderek daha da karmaşık hale geldiğini göstermektedir (Abbadi ve Lachkar, 2024:2581).

5.5.5. CAPTCHA ve Şifre Kırma Saldırılarında Yapay Zekâ

Kullanıcı adı ve şifre ile sisteme giriş yapılan platformların güvenliğini artırmak için kuruluşlar YZ teknolojilerinden faydalanarak sistem güvenliğini artırabilmektedir. CAPTCHA uygulaması, yüz tanıma ve parmak izi tanıma gibi teknolojiler kullanarak sisteme giriş yapanın gerçek kişi olup olmadığı teyit edilmektedir.

CAPTCHA, "Completely Automated Public Turing Test to Tell Computers and Humans Apart" ifadesinin kısaltmasıdır, bilgisayarlar ile insanları ayırmak için tam otomatikleştirilmiş halka açık Turing testi anlamına gelen ve insanlar ile otomatik botları ayırt etmek için geliştirilen bir güvenlik uygulamasıdır. CAPTCHA, dolandırıcılık olaylarını ve spam saldırılarını önleyebilmek için e-ticaret, sosyal medya ve çevrimiçi ödeme sistemlerinde hizmetlerde yaygın olarak kullanılmaktadır. CAPTCHA, sistemlere giriş yaparken insanların kolaylıkla çözebileceği, otomatik botların zorlanacağı görsel sorular sorarak, sisteme giriş yapanın insan olduğunu doğrulamayı amaçlar. Fakat, CAPTCHA sistemlerine yönelik YZ destekli saldırıların artması, web güvenliğinde bu önlemin giderek daha savunmasız hale geldiğini göstermektedir. Çeşitli robotik çevrimiçi botlar, CAPTCHA'ları aşabilecek YZ algoritmalar geliştirmiştir. "Ben robot değilim" gibi basit doğrulama yöntemleri, artık makineler tarafından kolayca çözülebilmektedir (Sharma ve Singh, 2024:2).

2024 yılında İsviçre Federal Teknoloji Enstitüsü araştırmacıları tarafından yapılan çalışmada; 14.000 trafik görüntüsüyle eğitilen YOLO adlı YZ görüntü tanıma modelini kullanarak Google'ın reCAPTCHAv2 sistemini %100 başarı oranıyla aşmayı başarmıştır. Bu model, bisiklet, motosiklet, yangın musluğu gibi nesneleri tanımada yüksek doğruluk sağlamıştır (Plesner, vd., 2024:2). CAPTCHA sistemlerinin aşılması, terörist grupların ve siber suçluların siber saldırılar gerçekleştirmesinde büyük ölçüde olanak sağlayabilir.

CAPTCHA sistemlerinin yanı sıra şifre bilgisayar korsanlığına karşı ilk savunma hattıdır ve büyük şirketlerden evlere kadar tüm siber savunma stratejilerinin temelini oluşturmaktadır. Kötü niyetli bir aktörün, şifre korumalı web sitelerine erişmek için bir şifre elde etmesi, sistemlere veya ağlara girerek örneğin temel hizmetleri aksatmasını, kesinti yaratmasını, değerli verileri veya bilgileri çalmasını, verileri veya süreçleri manipüle etmesini veya kötü amaçlı yazılım yüklemesini sağlayabilir. IŞİD gibi terör örgütlerinin destekçileri, propaganda materyallerini yaymak amacıyla web sitelerini ve sosyal medya hesaplarını hackleme konusunda uzun bir geçmişe sahiptir. Web siteleri ve sosyal medya platformları güvenliği artırmak amacıyla en az sekiz karakterden oluşan daha uzun şifreler veya alfanümerik ve büyük-küçük harf karakterlerinin bir kombinasyonunu zorunlu kılmak da dahil olmak üzere, şifrelerin kırılmasına önlem almış olsa da YZ parola tahmin etme sürecini hızlandırmak ve otomatikleştirmek için kullanılabilir. Kötü niyetli aktörler, derin sinir ağlarını şifre veri tabanlarıyla eğitebilmektedir. Bu sayede sinir ağları şifreyi çözene kadar arka arkaya birden fazla deneme yapabilir ve bu şekilde bilgisayar korsanının doğrudan müdahalesine olan ihtiyacı ortadan kaldırabilir. 2017 yılında yapılan bir çalışmada, araştırmacılar on milyonlarca sızdırılmış parolayı yeni parolalar üretmekle görevli bir sinir ağına yüklemişlerdir. Bu şifreler daha sonra, sinir ağının kullanıcıların şifrelerini kırmada ne kadar başarılı olacağını ölçmek için LinkedIn gibi sitelerden sızdırılan şifrelerle çapraz referanslamışlardır. Çalışma sonucunda LinkedIn setindeki şifrelerin %27'sini kırabildiklerini ortaya koymuştur. Başka bir çalışma da YZ video görüşmeleri sırasında analiz edilen omuz hareketlerine dayanarak hangi tuşların yazıldığını tespit ederek bir şifreyi tahmin edebileceğini ortaya koymuştur. Çalışmanın sonuçları, söz konusu YZ yazılımının %75 ila %93 gibi endişe verici bir doğruluk oranına sahip olduğunu göstermiştir (UNICRI ve UNCCT, 2021:40).

2023 yılında İngiltere'de Harrison ve arkadaşları tarafından yapılan bir çalışmada; YZ'nın klavye tuşlarına basıldığında oluşan sesleri analiz ederek şifreleri yüksek doğrulukla tahmin edebildiğini ortaya koymuştur. Her bir tuş vuruşunun kendine özgü akustik imzasını tanıyacak şekilde eğitilen ve MacBook Pro üzerinde 36 farklı tuşun 25 kez basılarak kaydedilmesiyle oluşturulan derin öğrenme modeli, tuşların karakterlerini %95 doğruluk oranıyla belirlemeyi başarmıştır (Harrison, vd., 2023:271).

Bu bulgularla birlikte, Mikrofon, video donanımına sahip cihazların yaygınlığı ve Zoom, Skype gibi video konferans platformlarının artan kullanımı göz önüne alındığında önemli güvenlik risklerinin oluştuğu görülmektedir.

6. GELENEKSEL TERÖRİZM, SİBER TERÖRİZM VE YAPAY ZEKÂ DESTEKLİ SİBER TERÖRİZM KARŞILAŞTIRMASI

Terörizmin farklı biçimleri, gelişen teknoloji ve dijitalleşmeyle birlikte önemli bir dönüşüm geçirmiştir. Geleneksel terörizm, fiziksel saldırılar ve şiddet içeren eylemlerle karakterize edilirken, siber terörizm dijital ortamda gerçekleştirilen saldırılar yoluyla hedeflerine ulaşmaktadır. Günümüzde ise YZ destekli siber terörizm, otomatik sistemler ve YZ algoritmalarını kullanarak çok daha karmaşık, hızlı ve tespiti zor saldırılar gerçekleştirebilmektedir. Önceki bölümlerdeki bulgulara dayalı olarak Geleneksel Terörizm, Siber Terörizm ve Yapay Zekâ Destekli Siber Terörizmin Karşılaştırılması Tablo 6.1.'de verilmiştir.

Tablo 6.1. Geleneksel Terörizm, Siber Terörizm ve YZ Destekli Siber Terörizm Karşılaştırması

Kriter	Geleneksel Terörizm	Siber Terörizm	YZ Destekli Siber Terörizm
Kullanılan Araç ve Yöntemler	Silahlar, patlayıcılar vb. fiziksel saldırılar.	Kötü amaçlı yazılım, DDoS, kimlik avı vb. siber saldırı	YZ destekli botnetler, deepfake, otonom yazılımlar, Üretken yapay zekâ araçları vb. siber saldırı, otonom cihazlarla fiziksel saldırı
Saldırı Karmaşıklığı	Basit, fiziksel planlama ve saldırı araçları.	Orta düzey teknik bilgi ve siber araçlar gerekli.	Çok karmaşık, yapay zekâ algoritmalarıyla optimize edilen saldırılar.
Hedef Belirleme	Fiziksel istihbarat ve yerel bağlantılar.	Hedefe yönelik veri analizi ve izleme.	Yapay zekâ ile büyük veri analizi ve otomatik hedef tespiti.

Saldırı Hızı ve Etki Alanı	Yavaş, yerel ve fiziksel sınırlamalara bağlı.	Hızlı, küresel erişim ve sınırsız dijital yayılım.	Çok hızlı, anlık etkilerle küresel ve ölçeklenebilir saldırılar.
Tespit Edilme İhtimali ve Önleme	Yüksek, fiziksel izler ve görgü tanıklarıyla kolay tespit.	Orta, siber güvenlik sistemleriyle tespit edilebilir.	Düşük, yapay zekâ anonimlik ve saldırı izlerini maskeleyebilir.
Tehdit Düzeyi	Orta, fiziksel etkilerle sınırlı.	Yüksek, geniş çaplı dijital zarar yaratabilir.	Çok yüksek, toplumsal kaos ve ekonomik çöküşe neden olabilecek etkiler.
Hedefler	İnsanlar, kamu binaları, altyapılar.	Bilgisayar sistemleri, veri tabanları, iletişim ağları.	Kritik ulusal altyapılar, otonom sistemler, yapay zekâ destekli araçlar.
Propaganda ve Dezenformasyon	Geleneksel medya, el ilanları, radyo ve televizyon.	Sosyal medya, dijital platformlar ve çevrimiçi içerikler.	Yapay zekâ ile üretilen deepfake, sahte haberler ve otomatikleştirilmiş içerik yayılımı.
Finans	Fiziksel bağışlar, yasadışı ticaret vb.	Siber suçlar, kredi kartı dolandırıcılığı vb.	Kripto para, yapay zekâ destekli finansal manipülasyonlar, kara para aklama vb.

Radar grafiği Şekil 6.1'de geleneksel terörizm, siber terörizm ve yapay zekâ destekli siber terörizmi, çeşitli kriterler çerçevesinde karşılaştırmalı bir şekilde değerlendirilmiştir. Bu kapsamda her bir türün farklı özellikleri ve tehdit seviyeleri, belirlenen kriterler doğrultusunda analiz edilmiştir.

Şekil 6.1. Geleneksel Terörizm, Siber Terörizm ve Yapay Zekâ Destekli Siber Terörizm Karşılaştırması Radar Grafiği

Geleneksel terörizm genellikle fiziksel araçlara ve yöntemlere dayalıdır. Bu yöntemler arasında patlayıcılar ve silahlar yer alırken, siber terörizm dijital teknolojilere dayanmaktadır. Yapay zekâ destekli siber terörizm ise, ileri düzey yapay zekâ algoritmaları, deepfake teknolojileri ve otomatikleştirilmiş bot ağları gibi daha karmaşık araçları içermektedir. Bu durum, yapay zekâ destekli siber terörizmin teknolojik olarak daha gelişmiş bir tehdit oluşturduğunu göstermektedir.

Geleneksel terörizm nispeten basit ve fiziksel istihbarata dayalı bir hedef belirleme yaklaşımı sergilerken, siber terörizm daha teknik bilgi ve beceri gerektirir. Yapay zekâ destekli siber terörizm ise büyük veri analitiği ve yapay zekâ algoritmalarını kullanarak hedeflerini daha etkili bir şekilde belirleyebilmektedir. Bu, saldırıların karmaşıklığını artırmakta ve tespit edilmesini zorlaştırmaktadır.

Geleneksel terörizm genellikle yerel veya bölgesel bir etki alanına sahipken, siber terörizm ve yapay zekâ destekli siber terörizm küresel ölçekte faaliyet gösterebilmekte ve anlık etki yaratabilmektedir. Yapay zekâ, özellikle ölçeklenebilirliği ve otomasyonu sayesinde siber saldırıların hızını ve kapsamını artırmaktadır.

Grafikten de görüleceği üzere, geleneksel terörizm düşük ila orta düzeyde bir tehdit seviyesi sunarken, siber terörizm daha geniş çaplı riskler yaratabilir. Yapay zekâ destekli siber terörizm, en yüksek tehdit seviyesine sahiptir ve kritik altyapılar, ekonomik sistemler ve toplumsal düzen üzerinde ciddi etkiler yaratma potansiyeline sahiptir.

Geleneksel terörizm fiziksel dağıtım kanallarına ve yerel medya araçlarına bağlı kalırken, siber terörizm sosyal medya ve çevrimiçi platformlar aracılığıyla dezenformasyon yayabilir. Yapay zekâ destekli siber terörizm, deepfake ve diğer yapay zekâ tabanlı içerik üretim araçları sayesinde propaganda ve manipülasyon yeteneklerini önemli ölçüde artırmaktadır.

Geleneksel terörizme karşı genellikle fiziksel güvenlik önlemleri alınırken, siber terörizm ve yapay zekâ destekli saldırılara karşı siber güvenlik sistemleri kullanılmaktadır. Ancak yapay zekâ destekli siber tehditlerin esnek ve dinamik yapısı, bu tür saldırıların tespit edilmesini ve önlenmesini daha karmaşık hale getirmektedir.

Radar grafiği, yapay zekâ destekli siber terörizmin, diğer terörizm türlerine göre daha karmaşık, geniş kapsamlı ve sofistike bir tehdit oluşturduğunu açıkça ortaya koymaktadır. Bu durum, güvenlik önlemlerinin ve politika stratejilerinin, teknolojik yenilikleri de dikkate alacak şekilde yeniden değerlendirilmesi gerektiğini göstermektedir.

7. SONUÇ VE ÖNERİLER

Terörizm, yakın tarihte küresel güvenlik, ekonomik kalkınma ve toplumsal ilerleme üzerinde derin izler bırakmıştır. Dijital teknolojilerin yaygınlaşması, terörizmin operasyonel yapısını değiştirmiş ve siber terörizmin yükselmesine yol açmıştır. Terör örgütleri, çevrimiçi araçlardan yararlanarak faaliyetlerini genişletmiştir. Ülkelerin siber uzaya olan bağımlılıkların artması, siber teröristlerin propaganda yapma, dezenformasyon yayma, örgüte yeni üye kazandırma, kritik alt yapılara yönelik saldırı düzenleme ve finansal gelir elde etme potansiyelini artırmış, yapay zekâ (YZ) teknolojileri ise bu süreçte önemli bir araç haline geldiği görülmektedir. Bu çalışma, YZ'nın terörizm üzerindeki etkilerini incelerken, propagandadan radikalleşmeye, operasyonel etkinlikten finansmana kadar geniş bir yelpazede nasıl kullanıldığını ortaya koymaktadır.

YZ hem faydalı hem de kötü niyetli kullanım için potansiyel taşıyan bir teknoloji olarak karşımıza çıkmaktadır. Savunma, güvenlik ve suçlarla mücadele gibi alanlarda önemli olanaklar sunarken aynı zamanda etik ve toplumsal kaygıları da beraberinde getirmiştir. YZ sistemlerinin kötüye kullanımı, sahte içerik üretimi, etik ihlaller ve güvenlik açıkları, küresel çapta endişeye sebep olmaktadır. YZ büyük dil modelleri (ChatGPT, Claude, Llama gibi) ile daha kolay erişilebilir ve etkili bir araç haline gelmiş, bu da hem suç faaliyetlerini kolaylaştırmış hem de yasal ve etik sorunlara yol açmıştır (Weimann, vd., 2024:17). Örneğin, ChatGPT gibi YZ platformları, kullanıcıların kolaylıkla yüksek kaliteli içerikler oluşturmasına olanak tanırken, aynı zamanda teröristler tarafından verimli planlama, propaganda ve saldırılar için bir araç haline geldiği görülmektedir. Bu bulgular Lakomy (2023), Bazarkina (2023) ve Lohmann (2024)'in çalışmaları ile paralellik göstermektedir.

Çalışmada YZ'nin terörist propagandayı dönüştürerek mesajların etkisini artırmada kritik bir rol oynadığı görülmektedir. YZ destekli botlar ve algoritmalar, geniş çaplı dezenformasyon kampanyaları oluşturmak için kullanılmıştır. Üretken YZ (GenAI), resim, video, ses ve 3D modeller üreterek, terör örgütlerinin radikalleşme ve manipülasyon çabalarını güçlendirmiştir. Deepfake teknolojisi ise gerçekçi ama sahte medya içerikleri yaratarak yanlış bilgilendirme ve propaganda araçlarını daha ikna edici

hale getirmiştir. Örneğin, IŞİD'in CNN ve Al Jazeera gibi meşru medya kuruluşlarını taklit ederek propaganda videoları üretmesi, deepfake teknolojisinin terörizmle olan tehlikeli bağlantısını gözler önüne sermiştir (Gilbert, 2024). YZ, yalnızca medya içeriklerinde değil, oyun, müzik ve ses üretiminde de kullanıldığı görülmektedir. Örneğin, IŞİD, YZ ile ürettiği oyunlar ve sahte medya içerikleriyle gençleri hedef alarak radikalleşme çabalarını artırmıştır. "Salil al-Sawarim" gibi oyunlar ve YZ destekli haber formatındaki videolar, terörist grupların YZ teknolojilerini stratejik bir araç olarak kullandığını göstermektedir. Blauth ve arkadaşları (2022), Bazarkina (2023), Wario (2024), Adigwe ve arkadaşları (2024) ve Davis (2024) tarafından YZ'nın propaganda, radikalleşme ve kötüye kullanımı üzerinde yapılan çalışmalar bu bulguları doğrular niteliktedir.

YZ destekli botlar ve algoritmaların, sosyal medya platformlarında bireyleri analiz ederek aşırılık yanlısı mesajlara duyarlı kişileri tespit edebildiği ve bu bireyleri kişiselleştirilmiş mesajlarla hedef alabildiği görülmektedir. Microsoft'un "Tay" sohbet botu örneğinde olduğu gibi (Schwartz, 2024), YZ sistemleri çevrimiçi etkileşimler yoluyla kolayca manipüle edebilmektedir. Benzer şekilde, Replika gibi sohbet botları, bireylerin radikalleşme sürecinde etkili bir rol oynayabilmektedir. Jaswant Singh Chail'in Kraliçe II. Elizabeth'e saldırı planı (Hall ve Badshah, 2023), bu tür bir sohbet botunun birey üzerindeki etkisini göstermiştir. Esmailzadeh ve Motaghi (2024), Irfan ve arkadaşları (2024), Bazarkina (2023) tarafından yapılan YZ'nin radikalleşme üzerindeki etkileri çalışmaları ile bu bulgular uyumludur.

Çalışmada, terör örgütlerinin finansman sağlamak amacıyla kripto para birimlerini nasıl kullandığına dikkat çekilmektedir. Kripto paraların anonim yapısı, terör örgütlerinin finansal işlemlerini izlenemez hale getirirken, YZ destekli ticaret botları bu süreçleri daha hızlı ve verimli bir hale getirmektedir. Bu botlarla piyasa spekülasyonları yapılabilmektedir (UNICRI ve UNCCT, 2021:39). Terör örgütlerinin, kripto paraları bağış toplama, kara para aklama, terör örgütü üyelerine finansal destek sağlama ve finansal işlemleri yürütmek için kullandığı görülmektedir (Tekgül Levent, 2024:113). Örnek olarak El-Kaide ve IŞİD, Telegram gibi platformlar üzerinden Bitcoin bağış kampanyaları düzenlemiş ve kripto varlıkları kara para aklama işlemlerinde kullanmıştır (Turan ve Demircan, 2021:171). 2012'de Endonezya'daki kilise saldırısı kripto varlıklarla finanse edilmiştir. Kripto para birimlerinin terör finansmanında kullanımı,

geleneksel finans sistemlerinin izlenebilirliğini devre dışı bırakarak örgütlerin özerkliğini artırmaktadır. Bu bağlamda çalışma, Blauth ve arkadaşları (2022)'un YZ'nın kötüye kullanımı üzerine yaptıkları çalışma ile benzerlik göstermektedir. Bu çalışmada YZ'nin terörizmin finansmanı süreçlerinde nasıl daha karmaşık ve tespit edilmesi zor bir araç haline geldiği ortaya konmuştur.

Terörist grupların fiziksel saldırı yeteneklerini geliştirmek, saldırıları daha karmaşık ve etkili hale getirmek, potansiyel hedeflerin analiz etmek için YZ destekli otonom silah sistemlerini ve insansız hava araçlarını kullanmaktadır. Terör örgütlerinin bu araçları ticari olarak satın aldıkları, üretim ve geliştirme faaliyetinde bulundukları veya sponsor devletler aracılığı ile elde ettikleri görülmektedir (Adigwe, vd., 2024:294; UNOCT, 2024:15). Örnek olarak IŞİD İHA'ları gözetleme ve bombalı saldırılar için kullanmıştır. Husi İsyancıları, daha gelişmiş sabit kanatlı İHA'ları başka devletlerin sponsorluğunda kullanmıştır. 2018'de Devlet Başkanı Nicolas Maduro'ya suikast girişiminde bomba yüklü İHA'lar kullanılmıştır (Bazarkina, 2023:259; Boyle, 2024:110). YZ tabanlı AWS ve İHA'ların gelişimi hem askeri operasyonlarda hem de terörizm bağlamında önemli fırsatlar ve tehditler sunmaktadır. Sürü teknolojisi ve otonom sistemler, terör saldırılarının kapsamını ve etkisini artırma potansiyeline sahip olması, ticari İHA'ların düşük maliyeti ve erişilebilirliği, terörist gruplar için çekici bir araç haline geldiği görülmektedir. Bu bulgular, Blauth ve arkadaşları (2022), Bazarkina (2023), Adigwe ve arkadaşları (2024) ile Lohmann (2024)'ın yaptığı çalışmalar ile uyumludur.

Çalışmada YZ'nin siber terörizmde kullanılan siber saldırı yöntemlerini daha etkili hale getirme ve savunma mekanizmalarını zorlaştırma potansiyeline dikkat çekilmiştir. Bu durum, kritik altyapıya yönelik tehditlerden sosyal mühendislik saldırılarına kadar geniş bir yelpazede ciddi riskler doğurmaktadır. Yüz tanıma, parmak izi ve retina tarama gibi biyometrik sistemler, YZ destekli saldırılarla hedef alınabilmektedir. Üç boyutlu baskılar veya sahte biyometrik verilerle güvenlik sistemlerini atlatmak mümkün hale gelmiştir. Örneğin, yüksek çözünürlüklü bir fotoğraf kullanılarak sahte gözler veya yüz kalıpları oluşturulabilmektedir. YZ, sosyal medya verilerini analiz ederek kurbanlara kişiselleştirilmiş mesajlar gönderip manipülasyon yapabilmektedir. Bu durum, bireylerin güvenlik bilgilerini paylaşmalarına veya kötü amaçlı bağlantılara tıklamalarına neden olmaktadır (Lohmann, 2024:25; Yurdasen, 2023). YZ, kimlik avı ve fidye yazılımı saldırılarını daha karmaşık ve etkili hale getirmektedir. Örnek olarak, ChatGPT gibi YZ

araçları, hedeflenen kişilere yönelik yazı tonunu taklit ederek gerçekçi ve kişiselleştirilmiş kimlik avı e-postaları hazırlayabilmekte, kullanıcıların farkında olmadan kötü amaçlı bağlantılara tıklamalarını kolaylaştırmaktadır. YZ algoritmaları, fidye yazılımının yayılmasını optimize ederek daha geniş bir alana yayılmasını sağlamaktadır. Örneğin, WannaCry saldırısı, 150 ülkede 200.000'den fazla bilgisayarı etkileyerek büyük kayıplara yol açmıştır. YZ destekli botnetler, trafiği analiz ederek en savunmasız cihazları hedef alarak ve saldırıyı optimize etmektedir. Örnek olarak, IŞİD, "Caliphate Cannon" adlı DDoS aracı ile askeri, ekonomik ve eğitim altyapılarına saldırılar düzenlemiştir. YZ modelleri, nesneleri ve yazıları tanıyarak CAPTCHA sistemlerini %100 doğrulukla geçebilmekte, çevrimiçi parola veri tabanlarını analiz ederek karmaşık şifreleri hızlıca tahmin edebilmektedir (Sharma ve Singh, 2024:2; Abbadi ve Lachkar, 2024:2581; UNICRI ve UNCCT, 2021:36; Utter,2024). YZ'nin büyük miktarda veriyi hızlıca analiz ederek hedefleri optimize etmesi, geleneksel savunma mekanizmalarını etkisiz hale getirmesi ve insan müdahalesi olmadan otonom olarak geniş çaplı saldırılar gerçekleştirmesi ile siber teröristlere imkânlar sunduğu görülmektedir. Bu bulgular Lohmann (2024), Esmailzadeh ve Motaghi (2024), Blauth ve arkadaşları (2022)'nın çalışmaları ile paralellik göstermektedir.

Bu gelişmeler, teröristlerin YZ teknolojilerinden faydalanarak toplumsal güveni zedeleme ve ulusal güvenlik tehditleri yaratma potansiyelini gözler önüne sermektedir. YZ'nin terörizmle kesişimindeki bu yeni boyut, uluslararası güvenlik ve etik düzenlemeler açısından acil bir müdahale gerektirmektedir.

Çalışmanın bulguları, teröristlerin YZ teknolojilerinden faydalanarak toplumsal güveni zedeleme ve ulusal güvenlik tehditleri yaratma potansiyelini gözler önüne sermektedir. YZ teknolojilerinin terörizmi kökten dönüştürdüğünü ve yeni tehdit türlerinin ortaya çıkmasına zemin hazırladığını göstermektedir. Elde edilen bulgular şunlardır;

- YZ teknolojileri hem faydalı hem de zarar verici amaçlarla kullanılabilir, bu da etik ve düzenleyici sorunları beraberinde getirmektedir,
- Dijital platformlar ve YZ araçları, terörist içeriklerin daha geniş kitlelere ulaşmasını sağlamaktadır,
- YZ, saldırıların etkisini artırarak savunma çabalarını zorlaştırmaktadır.

- YZ'nin kötüye kullanımını önlemeye yönelik mevcut çabalar yetersiz olduğu görülmektedir,
- Gerçeklik algısını zedeleyen deepfake teknolojileri, toplumsal güveni zedeleyerek ve siyasi istikrarı tehdit etmektedir,
- Kripto paraların anonim yapısı, teröristlerin daha bağımsız ve izlenemez bir şekilde hareket etmesine olanak tanımaktadır.
- YZ destekli otonom sistemler terör örgütlerinin elinde ölümcül tehditler oluşturmaktadır.

YZ'nin terörizmle kesişimindeki bu yeni boyut, uluslararası güvenlik ve etik düzenlemeler açısından acil bir müdahale gerektirmektedir ve uluslararası iş birliğini zorunlu kılmaktadır. YZ'nin terörizmdeki rolü, yalnızca ulusal güvenlik değil, aynı zamanda toplumsal düzen açısından da büyük tehditler oluşturmakta ve yenilikçi çözümlere duyulan ihtiyacı artırmaktadır.

Çalışmada elde edilen bulgular ışığında aşağıdaki öneriler sunulmuştur.

- YZ teknolojilerinin düzenlenmesi ve denetimi için küresel standartlar oluşturulmalıdır.
- Şeffaflık, hesap verebilirlik ve güvenlik odaklı etik ilkeler benimsenmelidir.
- Devletler, özel sektör ve uluslararası kuruluşlarla YZ kötüye kullanımını önlemek için işbirliği yapmalıdır.
- YZ araştırma merkezi kurularak, tüm bilim dallarından uzmanların katılımı sağlanarak gelişen YZ teknolojilerinin potansiyel riskleri kapsamlı şekilde araştırılmalıdır.
- Ülkeler her kademedeki eğitim ve öğretim sürecinde YZ kötüye kullanımı hakkında farkındalığı artırmalıdır. Medya kuruluşları üzerinden eğitim ve bilinçlendirme kampanyaları yapılmalıdır.
- Dijital para birimlerinin terör finansmanında kullanılmasını önlemek için düzenlemeler güçlendirilmelidir.
- Deepfake, radikalleşme, propanganda ve kötü niyetli faaliyetleri tespit etmek için gelişmiş YZ tabanlı izleme sistemleri uygulanmalıdır. YZ sistemlerinin güvenliği artırılmalı ve istismara karşı koruma sağlanmalıdır.

- İnternete erişim sağlayan insanların, gerçek kimliklerini doğruladıktan sonra sosyal medya platformlarına erişim sağlayacak sistemler geliştirilmelidir.
- Otonom cihazların satışı ve erişimi konusunda yasal düzenlemeler yapılmalıdır.

Araştırmacılar için öneriler;

- YZ'nin propaganda, dezenformasyon, radikalleşme üzerindeki psikolojik etkileri araştırılabilir.
- YZ kötüye kullanımını önlemedeki rolü konusunda çalışmalar yapılabilir.
- YZ teknolojilerinin ulusal ve uluslararası güvenlik üzerindeki etkileri araştırılabilir.

KAYNAKÇA

AB (2024). Sanal Ortamda İşlenen Suçlar Sözleşmesi. Adalet Bakanlığı: https://inhak.adalet.gov.tr/Resimler/Dokuman/2812020085427AK185_SanaLOrtamda%C4%B0slenenSuclar.pdf (Erişim Tarihi: 10.09.2024).

Abbadi, D., ve Lachkar, A (2024). Cyber threats in the age of artificial intelligence: Exploiting advanced technologies and strengthening cybersecurity. International Journal of Science and Research Archive, 13(1), 2576–2588.

ABD Yargı Senatosu Komitesi (2023). Durbin Calls on Online Video Game Industry to Do More to Identify & Remove Extremist Content from their Platforms. U.S. Senate Committee on the Judiciary: https://www.judiciary.senate.gov/press/dem/releases/durbin-calls-on-online-video-game-industry-to-do-more-to-identify-and-remove-extremist-content-from-their-platforms (Erişim Tarihi: 08.09.2024).

Adigwe, C. S., Mayeke, N. R., Olabanji:O., Okunleye, O. J., Joeaneke, P. C., & Olaniyi, O. O (2024). The Evolution of Terrorism in the Digital Age: Investigating the Adaptation of Terrorist Groups to Cyber Technologies for Recruitment, Propaganda, and Cyberattacks. Asian Journal of Economics, Business and Accounting, 24(3), 289-306.

Ağır, O., & Tekin, F (2021). Terörizm ve Propaganda. A. Baharçiçek, G. Tuncel, O. Ağır (Ed.) içinde, *Terör ve Propaganda* (1. Basım). Ankara: Nobel Akademik Yayıncılık.

Ahuerma, F. M (2022). What is Artificial Intelligence? International Journal of Research Publication and Reviews, 3(12), 1947-1951.

Akcinaroglu, S., & Shi, M (2023). Exploring the Impact of Cryptocurrency on Terrorism. Terrorism and Political Violence, (s. 1-25). doi:https://doi.org/10.1080/09546553.2023.2275057

Akçay, O (2021). Kent Güvenliği ve Suç Önleme: İnsansız Hava Araçlarının Kentsel Mekânda Suç ile Mücadelede Kullanımı. Yüksek Lisans Tezi. İstanbul: Üsküdar Üniversitesi Bağımlılık ve Adli Bilimler Enstitüsü.

Aksünger, S. (2024). Uzmanlara göre Lübnan'da çağrı cihazlarının patlatılarak sivillere zarar verilmesi uluslararası hukuka aykırı. https://www.aa.com.tr/tr/gundem/uzmanlara-gore-lubnanda-cagri-cihazlarinin-patlatilarak-sivillere-zarar-verilmesi-uluslararasi-hukuka-aykiri/3334436 (Erişim Tarihi 15.12.2024)

Akyeşilmen, N (2018). Disiplinlerarası Bir Yaklaşımla Siber Politika ve Siber Güvenlik (1. baskı). Ankara: Orion Kitapevi.

Alahi, E. E., Sukkuea, A., Tina, F. W., Nag, A., Kurdthongmee, W., Suwannarat, K., & Mukhopadhyay:C (2023). Integration of IoT-Enabled Technologies and Artificial Intelligence (AI) for Smart City Scenario: Recent Advancements and Future Trends. Sensors, 23(11), 5206.

Alkan, M., & Sağıroğlu, Ş (2018). Siber Güvenlik ve Savunma (1. baskı). Ankara: Grafiker Yayınları.

Allyn, B. (2022). Deepfake video of Zelenskyy could be 'tip of the iceberg' in info war, experts warn, https://www.npr.org/2022/03/16/1087062648/deepfake-video-zelenskyy-experts-war-manipulation-ukraine-russia (Erişim Tarihi: 02.12.2024).

Arslan, A. C (2024). Terör Örgütü Mensuplarına Yönelik Radikalleşmeden Arındırma Süreçleri ve DDR Modelinin Analizi: Endonezya JI Örneği. Mukaddime, 15(2), (s. 353-383).

Aydın, Ö. (2023). Pazarlama Alanında Nesnelerin İnterneti (IoT). E. B. Ceyhan, & İ. F. Ceyhan içinde, Yapay Zekâ, Blockchain ve Nesnelerin İnterneti Kitap Serisi / Blockchain ve Nesnelerin İnterneti - Alan Uygulamaları-1 (1 baskı. ss.91-107). Ankara: Nobel Yayıncılık.

Banafa, A (2024). Introduction to Artificial Intelligence (AI) (1. baskı). Alsbjergvej: River Publishess.

Barten, D. G., Teneke, D., Cauwer, H. D., Ciottone, R. G., & Ciottone, G. R (2022). A Counter-Terrorism Medicine Analysis of Drone Attacks. Cambridge University Press, 37(2), (s. 192–196).

Başakçi, G (2019). Siber İstihbarat Eğitim Dökümanı. İstanbul: BGA Bilgi Güvenliği A.Ş.

Başaran, A (2021). Siber Savaş Cephesinden Notlar (1. baskı). İstanbul: Arion Yayınevi.

Baştürk, R (2015). Kolluk Kuvvetlerinin İstihbarat Temininde Başvurabileceği İnsansız Hava Araçları (İHA) ve Bu Açıdan Uygun İha Özelliklerinin Araştırılması. Yüksek Lisans Tezi. İstanbul: Harp Akademileri Stratejik Araştırmalar Enstitüsü.

Bayraktar, G (2015). Siber Savaş ve Ulusal Güvenlik Stratejisi (1. baskı). İstanbul: Yeniyüzyıl Yayınları.

Bazarkina, D (2023). Current and Future Threats of the Malicious Use of Artificial Intelligence by Terrorists: Psychological Aspects. E. Pashentsev içinde, The Palgrave Handbook of Malicious Use of AI and Psychological Security (1 basım. ss. 251–272). Switzerland: Palgrave Macmillan Cham.

Bélanger, J. J., Nisa, C. F., Schumpe, B. M., Gurmu, T., Williams, M. J., & Putra, I. E (2020). Do Counter-Narratives Reduce Support for ISIS? Yes, but Not for Their Target Audience. Front. Psychol., 11(1059), (s. 1-11).

Bıçakçı, S. (2024). Lübnan'da patlayan çağrı cihazları: Elektronik harp, siber sabotaj ve kötülüğün sıradanlığı. https://fikirturu.com/jeo-politika/lubnanda-patlayan-cagri-cihazlari/ (Erişim Tarihi 15.12.2024)

Binder, J. F., & Kenyon, J (2022). Terrorism and the internet: How dangerous is online radicalization? Front. Psychol., 13(2022), (s. 1-10).

Blauth, T. F., Gstrein, O. J., & Zwitter, A (2022). Artificial Intelligence Crime: An Overview of Malicious Use and Abuse of AI. IEEE Access, 10, (s. 77110-77122).

Bondarenko, S (2024). Future of AI Bots for Crypto Trading is Here, https://www.finextra.com/blogposting/25841/future-of-ai-bots-for-crypto-trading-is-here (Erişim Tarihi: 12.12.2024).

Borgonovo, F., Bolpagni, A., ve Lucini:R (2024). AI-Powered Jihadist News Broadcasts: A New Trend In Pro-IS Propaganda Production?, Global Network on Extremism & Technology: https://gnet-research.org/2024/05/09/ai-powered-jihadist-news-broadcasts-a-new-trend-in-pro-is-propaganda-production/ (Erişim Tarihi: 03.12.2024).

Boyle, M. J (2020). The Drone Age : How Drone Technology Will Change War And Peace (1. baskı). New York: Oxford University Press.

Boyle, M. J (2024). Terrorist Groups and Unmanned Aerial Vehicles: A Growing Threat. M. Abrahms içinde, The Routledge Companion to Terrorism Studies New Perspectives and Topics (1 baskı ss.109-117). New York: Routledge and CRC Press.

Burgess, A., Hamilton, R., & Leuprecht , C (2024). Terror on the Blockchain: The Emergent Crypto-Crime-Terror Nexus. D. Goldbarsht, & L. D. Koker içinde, Financial Crime, Law and Governance (1 baskı ss.203-227). London: Springer, Cham.

Cao, Y (2024). System Design and Function Implementation Based on Decentralized Artificial Intelligence Internet of Things. IEEE, 600-605.

Chaurasia, R (2023). AI in Everyday Life. S. S. Rudrawar, & N. S. Ratnaparkhi içinde, AI for Everyone: Fundamentals (s. 118-129). Maharashtra: Jintur.

Clarke, R. A., & Knake, R. K (2010). Cyber War: The Next Threat to National Security and What to Do About It (1. baskı). New York: Ecco.

Cohen, M. S., & Freilich, C. D (2025). Cyberterrorism How Terror Groups Use Cyberspace. M. Abrahms içinde, The Routledge Companion To Terrorism Studies New Perspectives and Topics (1 basım. ss. 143-159). New York: Routledge.

Criezis, M (2024, 02 5). AI Caliphate: The Creation of Pro-Islamic State Propaganda Using Generative AI . Global Network on Extremism & Technology: https://gnet-research.org/2024/02/05/ai-caliphate-pro-islamic-state-propaganda-and-generative-ai/ (Erişim Tarihi: 02.12.2024).

Çakmak, H., & Altunok, T (2009). Suç, Terör ve Savaş Üçgenininde Siber Dünya. Ankara: Barış Platin Kitabevi.

Çalışkan, D., & Demir, Ö (2022). Derin Öğrenme Yöntemleri ile Şüpheli Davranış Tespiti. International Periodical of Recent Technologies in Applied Engineering, 3(1), (s. 28-43).

Çifci, H (2017). Her Yönüyle Siber Savaş (2. baskı). Ankara: Tubitak Popüler Bilim Kitapları.

Çıkı, K. D., & Tanrıverdi, H (2023). Turizm Alanında Blockchain Kullanımı. E. B. Ceyhan, & İ. F. Ceyhan içinde, Yapay Zeka, Blockchain ve Nesnelerin İnterneti Kitap Serisi Blockchain ve Nesnelerin İnterneti : Alan Uygulamaları-2 (1 basım. ss. 35-48). Ankara: Nobel Yayınları.

Çokbildik, A. C (2019). Siber Terörizm: Radikal/Dini Örgütler. Yüksek Lisans Tezi. Konya: Selçuk Üniversitesi Sosyal Bilimler Enstitüsü.

Darıcalı, A. B (2020). Yapay Zekâ Yönteminin Uluslararası Güvenliğe Etkileri. Savunma Bilimleri Dergisi, 19(37), (s. 49-72).

Davis, A. P (2024). Adversarial Actors and Artificial Intelligence: Propaganda Processes and Threats to Critical Infrastructure. Huntsville, Texas: The Sam Houston State University Institute for Homeland Security. doi:https://doi.org/10.17605/OSF.IO/XSBVU

Demarest, C (2023). Swarms of AI-fueled drones, vehicles track targets in AUKUS tests. c4isrnet.com: https://www.c4isrnet.com/unmanned/2023/05/26/swarms-of-ai-fueled-drones-vehicles-track-targets-in-aukus-tests/ (Erişim Tarihi: 08.12.2024).

Demir, F., & Öksüz, O (2023). Finans Alanında Blok Zincir. E. B. Ceyhan, & İ. Ceyhan içinde, Yapay Zeka, Blockchain ve Nesnelerin İnterneti Kitap Serisi / BLOCKCHAIN VE NESNELERİN İNTERNETİ - Alan Uygulamaları-2 (1 basım. ss. 75-100). Ankara: Nobel Yayınları.

Denning, D. E (2000). “Cyberterrorism,” Testimony Before the Special Oversight Panel on Terrorism, Committee on Armed Services, U.S. House of Representatives.

Georgetown University. https://faculty.nps.edu/dedennin/publications/Testimony-Cyberterrorism2000.htm (Erişim Tarihi: 06.10.2024).

Dilek, E., Talih, Ö., & Bensghir, T. K (2023). Estonya 2007 Siber Saldırılarının İncelenmesi ve Ülkelerin Ulusal Siber Güvenlik Politikalarına Etkileri. Bilgi Yönetimi Dergisi, 6(2), (s. 332-347).

Dizman, M (2023). Terör Örgütlerinin Finansman İhtiyacı. G. Ü. İslahiye İİBF Uluslararası E-Dergi, 7(7), (s. 13-34).

Doğan, Ü., & Alaca, A. İ (2020). Yapay Zekâ Uygulamaları ve Büyük Veri (1. baskı) (A. B. Darıcılı, Dü.) Ankara: Nobel Yayın.

Du, J., Yang, C., & Liu, Y (2024). The Application of Artificial Intelligence and Internet of Things Technology in Equipment Control Management Systems. 2024 Third International Conference on Distributed Computing and Electrical Circuits and Electronics (ICDCECE) (s. 1-6). Ballari: IEEE. https://ieeexplore.ieee.org/document/10548501 (Erişim Tarihi: 12.12.2024).

Duarte, F (2024). Number of ChatGPT Users (Nov 2024). Exploding Topics: https://explodingtopics.com/blog/chatgpt-users (Erişim Tarihi: 25.11.2024).

Englund, G., & Thompson, E (2024). 30 Years of Trends in Terrorist and Extremist Games. Global Network on Extremism & Technology: https://gnet-research.org/2024/11/01/30-years-of-trends-in-terrorist-and-extremist-games/ (Erişim Tarihi: 03.12.2024).

Eryılmaz, F (2022). İstihbarat ve Terör Örgütlerinde Kripto Para Dönemi. Kriter Dergisi: https://kriterdergi.com/dosya-turkiyede-ve-dunyada-istihbarat/istihbarat-ve-teror-orgutlerinde-kripto-para-donemi (Erişim Tarihi: 12.12.2024).

Esmailzadeh, Y., & Motaghi, E (2024). International Terrorism and Social Threats of Artificial Intelligence. Journal of Globalization Studies, 15(1), (s. 168-179).

Etidal (2024) (Etidal) and (Telegram) Remove 129 Million Extremist Contents. etidal.org: https://etidal.org/en/etidal-and-telegram-remove-129-million-extremist-contents/ (Erişim Tarihi: 02.12.2024).

Fırat, H (2022). Siber Terörizm Yeni Bir Terör Tehdidi ve Riskler (1. baskı). Ankara: Türk İdari Araştırmalar Vakfı İktisadi İşletmesi.

Genç, Y. M., & Erciyes, E (2020). İnsansız Hava Araçları (İHA) Tehditleri ve Güvenlik Yönetimi. Türkiye İnsansız Hava Araçları Dergisi, 2(2), (s. 36-42).

Gezgin, D. M., & Buluş, E (2012, Ocak). Kablosuz Ağların Güvenlik Açıklarının Eğitim Amaçlı İncelenmesi İçin Uygulama Tasarımı. Trakya Üniversitesi Eğitim Fakültesi Dergisi, 2(1), (s. 127-135).

Gilbert, D (2024, 06 18). ISIS Created Fake CNN and Al Jazeera Broadcasts. wired: https://www.wired.com/story/isis-created-fake-cnn-and-al-jazeera-broadcasts (Erişim Tarihi: 02.12.2024).

Girhepuje, S., Verma, A., & Raina, G (2024). A Survey on Offensive AI Within Cybersecurity. arXiv preprint, 1-29. https://arxiv.org/html/2410.03566v1 (Erişim Tarihi: 08.12.2024).

Gitmez, E (2023). Devletlerin Kripto Varlıklara İlişkin Hukuki Düzenlemeleri Üzerinden Bir Değerlendirme. Erzincan Binali Yıldırım Üniversitesi Hukuk Fakültesi Dergisi, 27(1), (s. 1-26).

Goodfellow, I., Pouget-Abadie, J., Mirza, M., Xu, B., Warde-Farley, D., Ozair, S., . . . Bengio, Y (2020). Generative Adversarial Networks. Communıcatıons Of The Acm, 63(11), (s. 139-144).

Gordon, J.-S (2023). The Impact of Artificial Intelligence on Human Rights Legislation (1. baskı). Cham: Palgrave Macmillan.

Grzybowski, A., Pawlikowska, K., & Lambert, C. W (2024). A History of Artificial Intelligence. Clinics in Dermatology, 42(3), (s. 221-229).

Guliyeva, K (2024). World Industrial Revolutions and the Development of Artificial Intelligence System. Chinese Business Review, 23(1), (s. 47-51).

Güner:P (2023). Çevirmen-Bilgisayar Etkileşiminin Kilit Bileşeni: Doğal Dil İşleme. Uluslararası Filoloji ve Çeviribilim Dergisi, 5(1), (s. 56-79).

Hall, R., & Badshah, N (2023). Man who broke into Windsor Castle with crossbow to kill Queen jailed for nine years. theguardian: https://www.theguardian.com/uk-news/2023/oct/05/man-who-broke-into-windsor-castle-with-crossbow-to-kill-queen-jailed-for-nine-years (Erişim Tarihi: 05.12.2024).

Harrison, J., Toreini, E., & Mehrnezhad, M (2023). A Practical Deep Learning-Based Acoustic Side Channel Attack on Keyboards. 2023 IEEE European Symposium on Security and Privacy Workshops (EuroS&PW) (s. 270-280). Delft: IEEE.

Hoffman, B (2006). Inside Terrorism (1. baskı). New York: Columbia University Press.

Hussain, G (2024). Artificial Intelligence (AI) and Radicalization. M. E. Erendor içinde, Cyber Security in the Age of Artificial Intelligence and Autonomous Weapons (1 basım. ss. 58-69). Boca Raton: CRC Press.

Irfan, M., Almeshal, Z. A., & Anwar, M (2023). Unleashing transformative potential of artificial intelligence (AI) in countering terrorism online radicalisation extremism and possible recruitment. Global Strategic & Security Studies Review, VIII(IV), (s. 1-15).

İşgüzar, S, (2020). Siber Aylaklık Davranışlarının Bir Kamu Kurumu Özelinde İncelenmesi: Log Analizine Dayalı Bir Çalışma. Doktora Tezi. Fırat Üniversitesi.

İzzetgil, E (2021). Bilimsel-Teknolojik Gelişmelerin Terörizme Etkisi Olarak Siber Terörizm Ve Türkiye Için Siber Terör Tehdidi. Uluslararası Kriz Ve Siyaset Araştırmaları Dergisi, 5(2), (s. 837-878).

Kalınbacak, İ (2023). Sürü Otonom İHA Sistemlerinin Muharebe Sahasında Uygulama Taktikleri ve Geliştirilen Yeni Teknolojiler. Savunma Bilimleri Dergisi, 43(1), (s. 191-249).

Karaağaç, C (2024). Geleceğin Hava Kuvvetleri: 2016 – 2050. Thinktech-STM Teknolojik Düşünce Merkezi: https://thinktech.stm.com.tr/tr/gelecegin-hava-kuvvetleri-2016-2050- (Erişim Tarihi: 01.11.2024).

Karyağdi, N. G (2023). Kripto Para Kavramı ve Denetimi. Turkish Business Journal, 4(23), (s. 1-13).

Katırcıoğlu, G., Akgül, E., Delice, Y., Özmen, M., & Aydoğan, E. K (2021). Denim Konforunun Yapay Zekâ Modelleri ile Tahminlenmesi. Ş. Sağıroğlu, M. U. Demirezen, & A. Yazıcı içinde, Yapay Zekâ ve Büyük Veri Endüstri 4.0 ve Yapay Zekâ (s. 267-298). Ankara: Nobel.

Kazbek, M. H (2024, 10 25). SARSILMAZ 3 yeni ürünü ile SAHA EXPO'da. askalehaber: https://askalehaber.com.tr/sarsilmaz-3-yeni-urunu-ile-saha-expoda/ (Erişim Tarihi: 01.11.2024).

Keleştemur:A (2018). Siber İstihbaratın Kamu Güvenliği İçin Rolü ve Önemi. Yüksek Lisans Tezi. İstanbul Gedik Üniversitesi.

Keskin, B (2008). Elektronik Harp ve Sinyal Savaşları (1. baskı). İstanbul: IQ Kültür Sanat Yayıncılık.

Khan, F. A., Li, G., Khan, A. N., Khan, Q. W., Hadjouni, M., & Elmannai, H (2023). AI-Driven Counter-Terrorism: Enhancing Global Security Through Advanced Predictive Analytics. IEE Access, 11, (s. 135864-135879).

Kılıç, İ (2024). Video Türkiye'de "hacklenen" bir robot süpürgeyi mi gösteriyor? teyit.org: https://teyit.org/analiz/video-turkiyede-hacklenen-bir-robot-supurgeyi-mi-gosteriyor (Erişim Tarihi: 27.10.2024).

Köksoy, F (2020). Yeni Küresel Tehdit Siber Saldırılar (1. baskı). Ankara: Nobel Yayınları.

Kurtboğan, H (2023). Yeni Dünyada Yapay Zeka Metaforu Ve Yapay Zekanin Çalişan Performansina Etkisi. Yüksek Lisans Tezi. Karaman: Karamanoğlu Mehmetbey Üniversitesi.

Lakomy, M (2023). Artificial Intelligence as a Terrorism Enabler? Understanding the Potential Impact of Chatbots and Image Generators on Online Terrorist Activities. Studies in Conflict & Terrorism, (s. 1-21). doi:https://doi.org/10.1080/1057610X.2023.2259195

Lehto, M., & Hutchinson, B (2020). Mini-Drones Swarms and Their Potential in Conflict Situations. B. K. Payne, & H. Wu (Dü.), ICCWS 2020 15th International Conference on Cyber Warfare and Security içinde (s. 319-334). Virginia: Academic Conferences.

Lermi:Y., & Onur, T. Ö (2024). Güneş Paneli Kusurlarının Derin Öğrenme Tabanlı Sınıflandırılması. International Journal of Advances in Engineering and Pure Sciences, 36(2), (s. 140-149).

Liaropoulos, A. N (2024). Autonomous Weapons Systems and the Future of Warfare. M. E. Erendor içinde, Cyber Security in the Age of Artificial Intelligence and Autonomous Weapons (1 basım. ss. 134-144). Boca Raton: CRC Press.

Lindemulder, G., & Kosinski, M (2024). What is a man-in-the-middle (MITM) attack? IBM: https://www.ibm.com/think/topics/man-in-the-middle (Erişim Tarihi: 12.10.2024).

Lohmann, S (2024). ChatGPT, Artificial Intelligence and the Terrorist Toolbox. S. Sim, E. Hartunian, & P. J. Milas içinde, Emerging Technologies and Terrorism: An American Perspective (1 basım. ss. 23-34). Carlisle: US Army War College Press.

Marr, B (2023). A Short History Of ChatGPT: How We Got To Where We Are Today. Forbes: https://www.forbes.com/sites/bernardmarr/2023/05/19/a-short-history-of-chatgpt-how-we-got-to-where-we-are-today/ (Erişim Tarihi: 24.11.2024).

Martin, G (2017). Terörizm Kavramlar ve Kuramlar (1. baskı) (B. M. İhsan Çapcıoğlu, Çev.) Ankara: Adres Yayınları.

McFarland, A (2024). Kasım 5'te En İyi 2024 Büyük Dil Modeli (LLM). unite.ai: https://www.unite.ai/tr/best-large-language-models-llms/ (Erişim Tarihi: 25.11.2024).

Morgan, S. (2024). Cybersecurity Venitures: https://cybersecurityventures.com/cybersecurity-almanac-2024/ (Erişim Tarihi: 15.08.2024).

Muhati, E., Rawat, D. B., & Sadler, B. M (2022). A New Cyber-Alliance of Artificial Intelligence, Internet of Things, Blockchain, and Edge Computing. IEEE Internet of Things Magazine, 5(1), (s. 104-107).

Nagarajan, S., & Kamalbabu, K (2024). Analysis of How ChatGPT and Gemini Help in the Generation of Cyber Attacks. IEEE Xplore, (s. 663-666).

Nasa , S (2024). Large Language Models: An Introduction to Fine-Tuning and Specialization in LLMs. Appypie: https://www.appypie.com/blog/what-are-large-language-models (Erişim Tarihi: 21.10.2024).

Nasiri, M. N., & Eken, M (2023). Afganistan Uluslararası Medyasında Christchurch Terör Saldırıları: İslamofobi, Çerçeveleme ve Temsil. Etkileşim, (s. 168-189).

Nguyen, T. T., Nguyen, D. T., Nguyen, D. T., Huynh-The, T., Nahavandi, S., Nguyen, T., . . . Nguyen, Q. H (2022). Deep learning for deepfakes creation and detection: A survey. Computer Vision and Image Understanding, 223, 1077-3142. doi:https://doi.org/10.1016/j.cviu.2022.103525

Özkan, T (2006). Siber Terörizm Bağlamında Türkiye'Ye Yönelik Faaliyet Yürüten Terör Örgütlerinin İnternet Sitelerine Yönelik Bir İçerik Analizi. Yüksek Lisans Tezi. Eskişehir: Anadolu Üniversitesi Sosyal Bilimler Enstitüsü.

Öztürk, İ., & Zeybek, B (2021). Dijitalleşme ve Etik Sorunlar: Nesnelerin İnterneti Teknolojisini Gözetim, Gizlilik, Güvenlik Kapsamında Değerlendirme. İletişim Kuram ve Araştırma Dergisi, 55(1), 1-12.

Özyurt, E (2021). Yüksek Lisans Tezi. How Terrorists Use The İnternet. Ankara: İhsan Doğramacı Bilkent Üniversitesi.

Paltacı, B. M. (2022). Ukrayna-Rusya Savaşı Bağlamında Siber Güvenlik Ekosistemi'nde Yaşanan Gelişmeler ve Değerlendirmeler. Orta Doğu ve Orta Asya-Kafkaslar Araştırma Ve Uygulama Merkezi Dergisi, 2(2), 1-19.

Pandey, A (2023). Computer Vision. International Journal for Research in Applied Science & Engineering Technology, 11(7), 510-514.

Parsewar, R. R (2023). Machine Learning (ML). S. S. Rudrawar, & N. S. Ratnaparkhi içinde, AI for Everyone: Fundamentals (1 basım. ss. 28-42). Maharashtra: Jintur Publication.

Payne, K (2021). I, Warbot The Dawn of Artificially Intelligent Conflict (1. baskı). London: Oxford University Press.

Perwej, Y., Abbas, Q., Dixit, P., Akhtar, N., & Jaiswal, K (2023). A Systematic Literature Review on the Cyber Security. International Journal of Scientific Research and Management, 09(12), 669-710.

Plesner, A., Vontobel, T., & Wattenhofer, R (2024). Breaking reCAPTCHAv2. arXiv, 1-10. https://arxiv.org/html/2409.08831v1 (Erişim Tarihi: 15.12.2024).

Raska, M (2021). The sixth RMA wave: Disruption in Military Affairs? Journal Of Strategic Studies, 44(4), (s. 456-479).

Reuters (2024). Crypto hacking thefts double to $1.4 bln in first half of 2024, researchers say. reuters: https://www.reuters.com/technology/crypto-hacking-thefts-double-14-bln-first-half-researchers-say-2024-07-05/ (Erişim Tarihi: 12.12.2024).

Robots (2024). Sophia. robotsguide.com: https://robotsguide.com/robots/sophia (Erişim Tarihi: 01.11.2024).

Roose, K (2023). AI poses ‘risk of extinction,’ industry leaders warn. seattletimes: https://www.seattletimes.com/business/ai-poses-risk-of-extinction-industry-leaders-warn/ (Erişim Tarihi: 24.11.2024).

Rudrawar:S., & Parsewar, R. R (2023). Introduction to Artificial Intelligence (AI): Significance, Historical Overview & Evolution. S. S. Rudrawar, N. S. Ratnaparkhi:S. Rudrawar, & N. S. Ratnaparkhi (Dü) içinde, AI For Everyone: Fundamentals (1 basım. ss. 9-18). Maharashtra: Jintur Publication.

Sağıroğlu, Ş., & Canbek, G. (2007). Kötücül ve Casus Yazılımlar Kapsamlı Bir Araştırma. Gazi Üniversitesi Mühendislik Mimarlık Fakültesi Dergisi, 22(1), (s. 121-136).

Sai, S., Garg, A., Jhawar, K., Chamola, V., & Sikdar, B (2023). A Comprehensive Survey on Artificial Intelligence for Unmanned Aerial Vehicles. IEEE Open Journal of Vehicular Technology, 4, (s. 713-738).

Sandilaç, N (2024). Siber Suç, Siber Terör ve Siber Savaş Üçgeninde Siber Dünya. Bilişim Hukuku Dergisi, (s. 142-190).

Schmid, A. P (2011). The Routledge Handbook Of Terrorism Research. Abingdon: Routledge.

Schwartz, O (2024). In 2016, Microsoft's Racist Chatbot Revealed the Dangers of Online Conversation The bot learned language from people on Twitter—but it also learned values. IEEE Spectrum: https://spectrum.ieee.org/in-2016-microsofts-racist-chatbot-revealed-the-dangers-of-online-conversation (Erişim Tarihi: 05.12.2024).

Sharma, S., & Singh, D (2024). CAPTCHA in Web Security and Deep-Captcha Configuration based on Machine learning. 2024 3rd International Conference for Innovation in Technology (INOCON) (s. 1-6). Bangalore: IEEE.

Shaveta (2023). A review on machine learning. International Journal of Science and Research Archive, 9(1), (s. 281–285).

Sherkhane, P. D., Ratnaparkhi, N. S., & Rudrawar:S (2023). Machine Learning Concept, Algorithms and Applications. S. S. Rudrawar, & N. S. Ratnaparkhi içinde, AI for Everyone: Fundamentals (1 basım. ss. 154-168). Maharashtra: Jintur Publication.

Siegel, D., & Doty, M. B (2023). Weapons of Mass Disruption: Artificial Intelligence and the Production of Extremist Propaganda. Global Network On Extremism And Technology: https://gnet-research.org/2023/02/17/weapons-of-mass-disruption-artificial-intelligence-and-the-production-of-extremist-propaganda/ (Erişim Tarihi: 03.12.2024).

Singer, P. W., & Friedman, A (2018). Siber.Güvenlik ve Siber Savaş Herkesin Bilmesi Gerekenler (2. baskı). Ankara: Buzdağı Yayınevi.

Snow, S (2017). Pentagon successfully tests world's largest micro-drone swarm. militarytimes.com: https://www.militarytimes.com/news/pentagon-congress/2017/01/09/pentagon-successfully-tests-world-s-largest-micro-drone-swarm/ (Erişim Tarihi: 08.12.2024).

Sofuoğlu, M. (2024). Kill switch: How Israel managed to explode devices in attack on Hezbollah. https://www.trtworld.com/magazine/did-israel-intercept-pagers-to-plant-explosives-for-attack-on-hezbollah-18209813 (Erişim Tarihi 15.12.2024)

Stalinsky, S., & Sosnow, R (2020). Jihadi Use Of Bots On The Encrypted Messaging Platform Telegram. MEMRI: https://www.memri.org/reports/jihadi-use-bots-encrypted-messaging-platform-telegram (Erişim Tarihi: 05.12.2024).

Stanford (2024). 2024 AI Index Report. California: Stanford University. https://aiindex.stanford.edu/wp-content/uploads/2024/05/HAI_AI-Index-Report-2024.pdf (Erişim Tarihi: 20.11.2024).

Şişman, M (2021). Siber Casusluk Yöntemleri ve Karşı Tedbirler (2. baskı). İstanbul: Abaküs Yayınları.

Tabacı, F (2020). Türkiye'de Siber Terörizme Karşı Bilişim Teknolojilerinin Kullanımı. Yüksek Lisans Tezi. Osmaniye: Osmaniye Korkut Ata Üniversitesi Sosyal Bilimler Enstitüsü.

Taşkesen, S (2020). Sınırların Belirsizleşmesi: Dron Teknoloji Temelli Saldırılar. A. B. Darıcılı (Dü.) içinde, Güvenlik, Teknoloji ve Yeni Tehditler. Ankara: Nobel.

Tekgül Levent, M. A (2024). Kripto Varlıkların Terörizmin Finansmanında Kullanılması ve Mali Eylem Görev Gücü (FATF) Tavsiyeleri. Yüksek Lisans Tezi. Ankara: T.C. İçişleri Bakanlığı Jandarma ve Sahil Güvenlik Akademisi Güvenlik Bilimleri Enstitüsü.

Teli, B., Totad, S., & Desai, S (2023). Use of AI (Artificial Intelligence) in Robotics. International Journal for Research in Applied Science & Engineering Technology, 11(8), 781-788.

Thareja, R (2023). Artificial Intelligence: Beyond Classical AI (1. baskı). Pearson Education.

THK (2024). Türk Hava Kurumu. https://www.thk.org.tr/iha (Erişim Tarihi: 01.11.2024).

Thomas, E (2021). Gaming and Extremism The Extreme Right on DLive. London: Institute for Strategic Dialogue.

Turan, D., & Demircan, C (2021). Kripto Paralar ile Terör ve Diğer İllegal Aktivitelerin Finansmanı. Anadolu Akademi Sosyal Bilimler Dergisi, 3(1), 161-176.

Turhost (2021). Makine Öğrenmesi (Machine Learning) Nedir? Turhost: https://www.turhost.com/blog/makine-ogrenmesi-machine-learning-nedir/ (Erişim Tarihi: 22.10.2024).

Türk Ahmet, 21. Yüzyılda Terör Konsepti ve Havacılık Güvenliği (Sivil Havacılık Genel Müdürlüğü Havacılık Güvenliği Daire Başkanlığı Havacılık Uzmanlığı Tezi 2017).

TZV (2024). Zekâ Nedir? Türkiye Zekâ Vakfi: https://tzv.org.tr/zeka_nedir/ (Erişim Tarihi: 01.10.2024).

UAB (2016). 2016-2019 Ulusal Siber Güvenlik Stratejisi. Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı: https://hgm.uab.gov.tr/uploads/pages/strateji-eylem-planlari/2016-2019guvenlik.pdf (Erişim Tarihi: 07.10.2024).

UAB (2024). 2024-2028 Ulusal Siber Güvenlik Stratejisi ve Eylem Planı. Türkiye Cumhuriyeti Ulaştırma ve Altyapı Bakanlığı: https://www.uab.gov.tr/uploads/pages/siber-guvenligin-yol-haritasi-yerli-ve-milli-tekno/ulusal-siber-guvenlik-stratejisi-2024-2028.pdf (Erişim Tarihi: 07.10.2024).

UNICRI, & UNCCT (2021). Algorithms and Terrorısm: The Malıcıous Use Of Artıficial Intellıgence For Terrorıst Purposes. New York: United Nations Interregional Crime and Justice Research Institute.

UNOCT (2024). Global Counter-Terrorism Programme on Autonomous and Remotely Operated Systems (AROS). New York: United Nations Office of Counter-Terrorism. https://www.un.org/counterterrorism/autonomous-and-remotely-operated-systems (Erişim Tarihi: 07.12.2024).

Utter, J (2024). The Machine War Has Begun: Cybercriminals Leveraging AI in DDoS Attacks. A10: https://www.a10networks.com/blog/the-machine-war-has-begun-cybercriminals-leveraging-ai-in-ddos-attacks/ (Erişim Tarihi: 14.12.2024).

Vailshery, L. S (2024). Number of Internet of Things (IoT) connections worldwide from 2022 to 2023, with forecasts from 2024 to 2033. statista: https://www.statista.com/statistics/1183457/iot-connected-devices-worldwide/#:~:text=Number%20of%20IoT%20connected%20devices (Erişim Tarihi: 27.10.2024).

Vashishtha, N (2023). Artificial Intelligence-assisted Terrorism: A New Era of Conflict. vifindia: https://www.vifindia.org/print/11910#_edn2 (Erişim Tarihi: 02.12.2024).

Vikipedi (2024). Siber. wikipedia: https://tr.wikipedia.org/wiki/Siber (Erişim Tarihi: 01.09.2024).

Warburton, D (2024). 2024 DDoS Attack Trends. F5 Labs: https://www.f5.com/labs/articles/threat-intelligence/2024-ddos-attack-trends (Erişim Tarihi: 10.12.2024).

Waroi, M. N (2024). False Reality: Deepfakes in Terrorist Propaganda and Recruitment. Security Intelligence Terrorism Journal, (s. 41-59).

Warwick, K (2023). Yapay Zekâ Temel Prensipler (1. baskı) (G. Uysal, & A. Uysal, Çev.) İstanbul: Ginko Bilim.

WEF (2024). WEF The Global Risks Report https://www3.weforum.org/docs/WEF_The_Global_Risks_Report_2024.pdf (Erişim Tarihi: 15.08.2024).

Weimann, G (2006). Terror on the Internet: The New Arena, The New Challenges. https://www.researchgate.net/publication/238077713_Terror_on_the_Internet_The_New_Arena_The_New_Challenges (Erişim Tarihi: 28.11.2024).

Weimann, G., Pack, A. T., Sulciner, R., Scheinin, J., Rapaport, G., & Diaz, D (2024). Generating Terror: The Risks of Generative AI Exploitation. CTCSENTINEL, 17(1), (s. 17-24).

Whyte, C (2019). Cryptoterrorism: Assessing the Utility of Blockchain Technologies for Terrorist Enterprise. Studies in Conflict & Terrorism, 46(7), (s. 1126–1149).

Yanarışık, O (2022). Terörizmin Finansmanında Siber Tehditler ve Kripto Paraların Rolü. Üçüncü Sektör Sosyal Ekonomi Dergisi, 57(4), (s. 3229-3241).

Yıldırım, S (2023). Bankacılığın Yapay Zekâ ile Dönüşümü. B. Küçükcan, & B. F. Yıldırım (Dü) içinde, Yapay Zekâ Disiplinlerarası Yaklaşımlar (s. 123-146). İstanbul: Vakıfbank Kültür Yayınları.

Yılmaz, A., & Kaya, U (2022). Derin Öğrenme (4. baskı). İstanbul: Kodlab.

Yurdasen, D (2023, 04 20). How Artificial Intelligence (AI) Is Used In Biometrics. Aratek: https://www.aratek.co/news/how-artificial-intelligence-ai-is-used-in-biometrics (Erişim Tarihi: 13.12.2024).

Zakharov, E., Shysheya, A., Burkov, E., & Lempitsky, V (2019). Few-shot adversarial learning of realistic neural talking head models. In: Proceedings of the IEEE/CVF. International Conference on Computer Vision, 1-21. https://arxiv.org/abs/1905.08233 (Erişim Tarihi: 14.12.2024).

Zieni, R., Massari, L., & Calzarossa, M. C (2023). Phishing or Not Phishing? A Survey on the Detection of Phishing Websites. IEEE Access, 11, (s. 18499-18519).

Zohuri, B. (2023). Artificial Super Intelligence (ASI) The Evolution of AI Beyond Human Capacity. Current Trends in Engineering Science, 3(6), (s. 1-5).