TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI

YAPAY ZEKA ULUSLARARASI İLİŞKİLERDE ASKERİ ALANDA DEVRİM MİDİR? ABD VE ÇİN REKABETİ ÜZERİNDEN BİR DEĞERLENDİRME

YÜKSEK LİSANS TEZİ

SEMİH AYSAL

ANKARA, 2022

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI

YAPAY ZEKA ULUSLARARASI İLİŞKİLERDE ASKERİ ALANDA DEVRİM MİDİR? ABD VE ÇİN REKABETİ ÜZERİNDEN BİR DEĞERLENDİRME

YÜKSEK LİSANS TEZİ

SEMİH AYSAL

TEZ DANIŞMANI
DOÇ.DR. ÖZLEM KAYGUSUZ

ANKARA, 2022

TÜRKİYE CUMHURİYETİ
ANKARA ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
ULUSLARARASI İLİŞKİLER ANABİLİM DALI

YAPAY ZEKA ULUSLARARASI İLİŞKİLERDE ASKERİ ALANDA DEVRİM MİDİR? ABD VE ÇİN REKABETİ ÜZERİNDEN BİR DEĞERLENDİRME

YÜKSEK LİSANS TEZİ

TEZ DANIŞMANI
DOÇ.DR. ÖZLEM KAYGUSUZ

TEZ JÜRİSİ ÜYELERİ

Adı ve Soyadı	İmza
1)Doç. Dr. ÖZLEM KAYGUSUZ	…….
2)Doç.Dr. KLEVİS KOLASİ	…….
3)Dr. Öğr. Üyesi ÇAĞLAR KURÇ	…….

Tez Savunma Tarihi 25.04.2022

ANKARA ÜNİVERSİTESİ SOSYAL BİLİMLER ENSTİTÜSÜ MÜDÜRLÜĞÜNE

Bu belge ile, bu tezdeki bütün bilgilerin akademik kurallara ve etik davranış ilkelerine uygun olarak toplanıp sunulduğunu beyan ederim. Bu kural ve ilkelerin gereği olarak, çalışmada bana ait olmayan tüm veri, düşünce ve sonuçları andığımı ve kaynağını gösterdiğimi ayrıca beyan ederim. (25/04/2022)

SEMİH AYSAL

TEŞEKKÜR

Akademik gelişim sürecimde katkısı olan ve emeği geçen tüm hocalarıma teşekkür ederim.

Akademik hayatımın her evresinde sonsuz desteklerini hissettiğim ailemin tüm üyelerine teşekkür ederim.

Çalışmamı bitirdikten sonra tamamını okuyup yazım yanlışları konusunda geri bildirimlerde bulunan abim Servet Aysal ve dostum Muhammed Ahmet Ruşen'e katkıları için teşekkür ederim.

SEMİH AYSAL

İÇİNDEKİLER

GİRİŞ

Toplumsal hayatın akışı içinde yaşanan kırılmalar ve dönüşümlerin neredeyse tamamı bir teknolojinin etkisiyle ortaya çıkmıştır. Avcı – toplayıcı kavimlerden yerleşik tarım toplumuna, imparatorluk düzenlerinden ulus-devlet formuna geçişlerde teknolojinin rolü oldukça büyüktür. Buhar makinesinin icadı çılgınca bir sanayileşmenin gerçekleşmesine yol açmıştır. Bu sanayi devriminin ikincisi elektrik ile, üçüncüsü ise internetin icat edilmesiyle gerçekleşmiştir. 21. yüzyıl ise insanlara birçok alanda rakip olan zeki makinelerin yüzyılı olmaya başlamıştır.

Birinci Sanayi Devrimi üretim ilişkilerini değiştirmiş, gerektirdiği nitelikler bakımından çalışan nüfusun demografik yapısında değişikliklere sebep olmuştur. Fabrikalarda çalışacak insan ihtiyacı kırdan kente göçü tetiklemiş, beraberinde kentlerde hızlı bir şekilde artan nüfus nedeniyle toplumsal sorunlara neden olmuştur. İkinci Sanayi Devrimi elektriğin icadı ile hem üretim ilişkileri hem de toplum üzerinde etkilere neden olmuştur. 1980'li yıllara gelindiğinde internetin sivil yaşamın hizmetine sunulması, bilginin üretimini ve yayılımını artırmış ve bilgi toplumunu ortaya çıkarmıştır. 21. Yüzyıl, Endüstri 4.0 olarak adlandırılan akıllı makinelerin insan yaşamına girdiği ve giderek yaygınlaştığı bir yüzyıl olarak anılmaktadır.

C.P. Snow 1959 yılında verdiği Rede Konferansı'nda ve sonrasında buradaki konuşmalarının yer aldığı *"iki kültür"* isimli eserde doğa bilimleri ile edebi entelektüeller arasında kültür farkı olduğunu ifade ederek, doğa bilimcilerin üstünlüğünden yana taraf olmuştur. Diğer taraftan dönemin beşeri bilimcileri olan edebiyatçıları keskin bir şekilde eleştirmektedir (Snow, 2005). Eleştirinin temelinde beşeri bilimlerin Sanayi Devrimi ve bu devrimin toplum üzerindeki etkilerini öngörüp, bilimsel çalışmalara konu etmemiş olmaları yatmaktadır.

Yapay Zeka (YZ) ile Uluslararası İlişkiler arasında nasıl bir ilişki olabileceğine dair ilk sorular 2017 yılında Snow'un kitabı okunduktan sonra oluşmaya başlamıştır. Bu yıllarda artan hız ve miktarda, ütopik ve distopik senaryolardan, ekonomik yaşama ilişkin beklenti ve kaygılara; ulusal ve uluslararası düzeyde hukuki düzenlemelere olan ihtiyaçtan, uluslararası örgütlerin konuyla ilgili işbirliği yapma gerekliliklerine kadar oldukça çeşitli düşünce yazıları yayınlanmaya başlamıştır. Örneğin Chatham House hazırladığı raporda yapay zeka özelinde bir durum tespiti yaparak bir yandan hükümetler ile özel sektör arasında işbirliği önerirken diğer yandan hükümetlerin ve kuruluşların işbirliğiyle YZ'nin insani amaçlara kanalize edilmesinin

mümkün olduğunu vurgulamıştır (Cummings et al., 2018: 44 vd). Ray Kurzweil teknolojik gelişim ve insan hayatı arasında iyimser bir gelecek tahayyülüyle, biyolojik ve teknolojik evrimi ele aldığı eserinde, evrimin aşamalarını 6 çağa ayırmıştır. Bu altı çağdan sonuncusu teknoloji ile bütünleşmiş insan zekasının evrene yayılmasını anlatmaktadır (Kurzweil, 2005). İnsan Hakları İzleme Örgütü YZ altyapısıyla hazırlanan silahların onay sürecine dikkat çekmekte, tedirgin bir yaklaşımla, silah onay süreçlerinin hassasiyetle değerlendirilmesi ve insanlığın geleceği arasında ilişki kurmaktadır (HRW, 2012). Hem YZ'nin etki alanının çok geniş olması hem de uluslararası ilişkilerin çok yönlü olması birçok kesişim ve etkileşim noktasını mümkün kılıyordu.

Yoğun etkileşim noktalarından bir tanesi de uluslararası güvenlik konusu olarak tespit edildi. YZ'ye dair beklentilerin muğlaklığı ile uluslararası ilişkilerin karmaşık ve belirsiz yapısı içinde en somut görünen çalışma alanı uluslararası güvenlik olarak değerlendirildi (Gray, 2005; Hoffman, 2017; Kania, 2021; Krepinevich & Watts, 2015; Krepinevich, 1994; Martyanov, 2019; Murray, 1997; Murray & Knox, 2001; Raska, 2021). Çalışmanın kuramsal çerçevesi Askeri Alanda Devrim (RMA) literatürü üzerine kurgulanmıştır. Özellikle Askeri Devrim (MR) ve Askeri Alanda Devrim (RMA) ayrımına odaklanılarak YZ destekli güvenlik çalışmalarının nasıl konumlandırılacağı ele alınmıştır. Çalışmada ABD ve Çin devletlerinin YZ politikaları ele alınmış ve YZ teknolojilerini askeri alana uygulamak için nasıl politikalar geliştirdikleri incelenmiştir.

Çalışmada cevap aranan temel sorular şunlardır: i) YZ destekli güvenlik araçları üzerine yürütülen çalışmalar Askeri Devrim *(Military Revolution - MR)* kapsamında mı yoksa Askeri Alanda Devrim *(Revolution in Military Affairs - RMA)* Kapsamında mı konumlandırılmalıdır? ii) OSS ve Siber Güvenlik son RMA dalgasını tetikleyen teknolojiler olarak kabul edilebilir mi? iii) ABD ve Çin arasında YZ-RMA bağlamında stratejik rekabet var mıdır? Çalışmanın bulgularından hareketle YZ'nin, RMA bağlamında değerlendirilmesi gerektiği sonucuna ulaşılmıştır. Çünkü incelenen devletlerin stratejik ve doktrinel değişimlerini tetikleyen bir nitelik taşımaktadır. YZ geliştirilmesi ve askeri alana uyarlanabilmesi hem güçlü bir ekonomi hem de uzmanlık bilgisi gerektirmektedir. Bunların da ötesinde küresel etkiye sahip politik bir gücün varlığı da böylesi bir teknolojinin geliştirilmesinde önem kazanmaktadır. Bu gereklilikleri karşılayan dünyanın önde gelen iki büyük gücü olan ABD ve Çin örnek ülkeler olarak seçilmiş ve incelenmiştir.

Çalışma kapsamında Türkçe ve İngilizce dilinde yayınlanmış akademik kaynaklar, devletlerin strateji belgeleri, uluslararası kuruluşların raporları veri olarak kullanılmış ve

doküman analizi yöntemiyle toplanan veriler incelenmiştir. Türkçe literatürde YZ-RMA konusu çalışılmamış bir konudur. Bu yönüyle çalışmanın Türkçe literatüre katkı sunması beklenmektedir.

Çalışmanın en önemli kısıtı şudur: İncelenen devletlerin sahip oldukları tüm askeri teknolojiler gizlilik kısıtları nedeniyle incelenememiştir. Sadece akademik yayınlara, raporlara ve strateji belgelerine yansıyan teknolojiler çalışmada kullanılabilmiştir.

Birinci bölümde YZ teknik yönüyle ele alınıp incelenmiş ve Uluslararası İlişkiler ile ilişkisine değinilmiştir. II. Bölümde MR ve RMA kavramları açıklanarak aralarındaki farklara değinilmiştir. RMA dalgaları, OSS ve Siber Güvenlik konularına yer verilmiştir. III. Bölümde ABD ve Çin'in YZ politikaları, OSS, Siber Güvenlik ve RMA yaklaşımları incelenmiştir. IV. Bölümde çalışmada ele alınan sorular cevaplanmaya çalışılmıştır.

Çalışmanın temel argümanı şudur: "YZ destekli güvenlik araçları MR yerine RMA kapsamında konumlandırılmalıdır." RMA dalgalarının sonuncusunu oluşturan ve otonom silah sistemleri ile siber uzay gibi YZ temelli yeni mücadele alanlarının üzerinde şekillenen dalga aynı zamanda ABD-Çin rekabetinin de mücadele alanını oluşturmaktadır. Çünkü ABD ve Çin RMA kapsamındaki stratejilerini kurgularken belirli düzeyde birbirlerini rakip olarak konumlandırarak, dengeleme amacı gütmüşlerdir. Buradaki politika oluşturma ve dengeleme çabası askeri doktrinler ve stratejilerde yaşanan değişimlerle gözlemlenebilir boyuta ulaşmıştır. Bu nedenle anılan devletlerin stratejik rakip oldukları söylenebilir.

I. BÖLÜM: YAPAY ZEKANIN TARİHÇESİ, TANIMI VE ULUSLARARASI İLİŞKİLER İLE İLİŞKİSİ

A. Genel Olarak Yapay Zeka Kavramı ve Tarihçesi

Yapay zeka eğitimden sağlığa, tüketici davranışlarının öngörülmesinden finansal işlemlere, sosyal medya hesaplarında karşılaşılan reklamların kişiselleştirilmesinden ses ve görüntü işlenmesine kadar günlük hayatın birçok alanında kullanılmasına rağmen, tanımı yapılması oldukça zor ve karmaşık bir kavramdır. Bunun nedenlerinden belki de en önemlisi YZ' ye yüklenen anlamın tarihsel süreç içerisinde geçirdiği evrim ve yaklaşık olarak son 20 yılda muazzam bir hızla gelişip çok farklı alanlarda ve farklı amaçlarla kullanılmaya başlanmış olmasıdır.

İnsansı özellikler gösteren mekanik aletlerin tarihçesine ilişkin çalışmaları, mitolojik tanrılara ve ortaçağ sanatkarlarının ilk girişimlerine dayandıranlar (Mayor, 2020), Leonardo Da Vinci'nin çizimlerini ilk örneklerden biri kabul edenler (Nilsson, 2010: 21), Descartes'in bilgi kuramı, Bole tarafından geliştirilen 0-1 mantığı olarak bilinen mantık üzerine çalışmaları, Leibniz'in akıl yürütmeyi diferansiyel ve integral hesabıyla ele alan düşüncelerini ileri düzeydeki çalışmaların öncüsü kabul eden yayınlar (Ekmekci & Arda, 2020: 2) olduğu gibi ; somut çalışmaların başlangıcı olarak 1940'lı yıllar ve özellikle İngiliz matematikçi Alan Mathison Turing'in 1950 yılında *Mind* dergisinde yayınlanan *''Computing Machinery and Intelligence''* adlı makalesi kabul edilebilir. Turing bu zihin açıcı eserinde temel bir soruyu ortaya atmış ve kendi ismiyle anılan bir test geliştirmiştir (TURING, 1950). Turing'in temel sorusu şudur: ''Makineler düşünebilir mi?'' Bir makinenin insan gibi düşünüp düşünemediğini test edebilmek için geliştirdiği yöntem ise makalenin orijinalinde taklit oyunu *(imitation game)* adı verilen, sonraları ise Turing Testi olarak bilinen testtir. Buna göre bir odada mülakatı uygulayan kişi, diğer tarafta ise bir insan ve düşünüp düşünemediği test edilen makine konumlandırılır. Mülakatı uygulayan kişi sorular sorar ve bu sorulara hem makinenin hem de diğer insanın cevap vermesi istenir. Eğer mülakatı uygulayan kişi hangi cevabın bilgisayardan, hangisinin insandan geldiğini anlayamıyor ise makinenin düşünebildiği kabul edilir[1]. Anılan makalede Turing tek hamlede

[1] Turing Testi Canlandırması için bkz. ''The Machine'' Filmi dakika 6:34-7:40 ve 8:51-11:12. https://www.youtube.com/watch?v=QL0P_MyAJs0 (erişim tarihi 01.08.2021)

mat içeren bir satranç sorusu da sorar ancak makalede kullanılan İngiliz notasyonu, günümüzde kullanılan cebirsel notasyondan farklı olarak anlam belirsizliği de içermektedir[2].

Turing'in ortaya attığı soru, bilim dünyasında karşılık bulmuş ve insansı özellikler gösteren makineleri ve programları betimlemek için ilk defa Yapay Zeka kavramının kullanıldığı Dartmouth Konferansı, 1956 yılında düzenlenmiştir. YZ'nin isim babası kabul edilen John McCarthy'nin daveti üzerine Dartmouth'ta toplanan, Yapay Zeka Dartmouth Yaz Araştırma Projesi'ne YZ'nin önde gelen dört ismi başta olmak üzere alanla ilgili çalışan bilim insanları davet edilmiştir. 1955 yılında Rockefeller Vakfı'na maddi destek için yazılan ve destek talebi kabul gören araştırma önerisinden anlaşıldığı gibi, YZ'nin önde gelen dört ismi ve onları öne çıkaran nitelikleri şunlardır: i) John McCarthy Dartmouth College'da matemetikçi olup, düşünce sürecinin matematiksel doğası ile ilgili sorunlar, beyin modeli ve çevresi ile ilişkileri, Turing makinesinin teorisi, bilgisayarların hızı ve makineler tarafından kullanılan diller üzerine çalışmaktadır. ii) Marvin Lee Minsky Harvard Üniversitesi'nde matematik ve nöroloji alanlarında çalışmakta ve Princeton Üniversitesi'nde hazırladığı *''Neural Nets and the Brain Model Problems''* isimli doktora teziyle tanınmaktadır. Ayrıca Minsky, 1959 yılında Massachusetts Institute of Technology (MIT) yapay zeka laboratuvarını kurmuştur. iii) Nathaniel Rochester IBM'de bilgi araştırmaları müdürü olarak çalışmaktadır. İlk seri üretimi yapılan bilimsel bilgisayar olma niteliğine sahip IBM 701'in iki tasarımcısından birisidir. Aynı zamanda sembolik çeviri programının da yazarıdır. iv) Claude Elwood Shanon, Bell telefon laboratuvarında çalışmakta olup, matematikçi, elektrik mühendisi ve kriptografi uzmanıdır. Bilginin istatistiksel teorisini geliştirmiştir (McCarthy et al., 2006). Bu kısaca anılan dört isim dışında 1978 Nobel ekonomi ödülü sahibi olmasının yanı sıra Herbert A. Simon, matematik, psikoloji, sınırlı karar verme modeli kapsamında yönetim bilimi üzerine yaptığı çalışmalara yapay zekayı da eklemiştir. Özellikle Allen

[2] Turing'in makalesinde 1950'li yıllarda uygulanan İngiliz notasyonu kullanılmıştır. Soruda verilen pozisyon şudur: *''I have K at my K1, and no other pieces. You have only K at K6 and R at R1. It is your move. What do you play?''* Bu notasyonda K= King = Şah ve R=Rook= Kale taşlarını sembolize etmektedir. Verilen pozisyonda 'sen' ve 'ben' ifadelerine karşılık gelen renkler belirtilmediği için, 1950'li yıllarda uygulanan İngiliz notasyonunun günümüzde kullanılan cebirsel notasyona dönüştürülmüş hali için 4 farklı olasılık bulunmaktadır. Makalede yer verilen örnek sorunun önemi, sadece tek hamlede mat hamlesinin bulunması değil, bunun da ötesinde makineden farklı varyasyon olasılıklarını da hesaplamasının beklenmesidir. Zira makalede soruya verilen yanıt ''R-R8 mate.'' olmuştur. Bu yanıt 4 olasılığa göre de mat hamlesidir. Detaylı bilgi için bkz. A. Voronkov (ed.), Turing-100 EPiC Series, vol. 10, içinde; Jeroen Fokker, ''The Chess Example in Turing's Mind Paper is Really About Ambiguity,'' https://easychair.org/publications/open/fMWM#:~:text='I%20have%20K%20at%20my%20K1'%20then%20means%20that%20I,as%20'R%2DR8'. (erişim tarihi: 03.08.2021)

Newel ile birlikte YZ'nin geleceğine dair Simon'un öngörüleri, zaman tahminleri bakımından yanılmış olsalar da, büyük oranda gerçekleşmiştir (Simon & Newell, 1958).

Yapay zekanın interdisipliner niteliği gereği, bu alanda çalışmalar yürüten öncü bilim insanlarının da matematik, nöroloji, felsefe, elektrik mühendisliği gibi farklı alanlarda çalışmalar yürüttüğü görülmektedir. Araştırma önerisinde anılan dört öncü isim alanlarıyla ilgili çalışma projeleri belirterek, YZ çalışmalarına önemli katkılar sunmuşlardır. Bunlardan özellikle anılması gerekenleri şu şekilde özetlemek mümkündür: McCarthy'nin oyun oynayabilen ve diğer görevleri yerine getirebilen bir programı olanaklı kılacak yapay dil geliştirme önerisi, C. Shanon'un teoremlerin ispatı, satranç oynama, müzik yazma gibi en ileri insan etkinliklerinin makineler tarafından yapılabileceği öngörüsüne dayanarak beyin modeli ve çevresi arasındaki bilgi sürecinin makinelere kazandırılması önerisi, M. Minsky'nin duyusal ve motor soyutlama yeteneği kazandırılarak, çevresel değişimlere yeni duyusal durumlar üretebilen programlama projesi, N. Rochester ise problemlere özgün çözüm getirebilecek makinenin nasıl üretilebileceğini araştırmayı önermiştir (McCarthy et al., 1955).

Araştırma önerisinde yer verilen en önemli tespitlerden biri (McCarthy et al., 1955: 2)*''Günümüzdeki bilgisayarların hızları ve hafıza kapasiteleri insan beyninin daha yüksek işlevlerini taklit etmek için yetersiz olabilir, fakat en büyük güçlük makine kapasitesinin yetersizliği değil, sahip olduğumuz şeylerin tümünden yararlanabileceğimiz programları yazmaktaki yetersizliğimizdir.''* tespitidir. Bu tespit eldeki imkanları tümüyle kullanmayı sağlayacak programların yazılmasına yönelik çalışmalara zemin hazırlamıştır. Bir tarafta elektrik-elektronik mühendisliğinin teknik imkanları ve makine kapasiteleri gelişme gösterirken, diğer yandan her bir gelişmenin tam kapasite kullanılması için programlama çalışmaları hız kazanmıştır.

Yapay zeka tarihçesi üzerine en kapsamlı çalışma Türkçeye de kazandırılmış olan Nils J. Nilsson'un eseridir. Eserde YZ'nin tarihsel gelişimi 8 başlıkta ele alınmaktadır[3], bunlar: i) *Tomurcuklar* başlığı altında mitolojik eserlerden Aristoteles'in kölelik yaklaşımına kadar düşünsel boyutu ele almaktadır. ii) *İlk keşifler* başlığı altında 1950 ve 1960'lı yıllarda

[3] Eser hem hacimce büyük hem de oldukça detaylı bilgiler içermektedir. Ne var ki bu bölümün amacı yapay zeka tarihini derinlemesine anlatmak değil, gelişim evreleri ve temel fikirler hakkında genel bilgi vermek olduğundan sadece bölüm başlıkları ve belirtilen dönemde ortaya çıkan teknolojiler 6 madde halinde aktarılmakla yetinilecektir.

gerçekleşen gelişmelere yer verilmiş olup, uluslararası toplantılar, örüntü tanıma, geometri teoremlerinin ispatı, oyun oynayan programlar, doğal dil işleme, yapay çeviri ve programlama dilleri başta olmak üzere, düşünsel boyuttan gerçek kullanım evresine geçen ilk örneklere yer verilmektedir. iii) *Çiçeklenme* başlığı altında 1960'ların ortasından 1970'li yılların ortasına kadar uzanan dönem incelenmiş, bilgisayarla görme, bilgi gösterimi ve uslamlama, hareketli robotlar, doğal dil işlemede ilerleme, oyun oynama üzerine çalışmaların örnek uygulamalarına yer verilmiştir. iv) Eserin dördüncü beşinci ve altıncı bölümlerinde, 1970'lerden 1980'lerin ilk yarısına kadar gerçekleştirilen ilerlemelere yer verilmiştir. Bu dönemde konuşma ve tanıma anlama sistemleri, uzman sistemler, sorgu ve sinyalleri anlayan makineler, bilgisayarla görme teknolojisinde ilerleme gözlemlenmiş ve dönem yazar tarafından YZ'nin yükseliş dönemi olarak nitelendirilmiştir. Aynı dönemde hem yeni nesil projeler olarak adlandırılan bilgisayar sistemleri ortaya çıkmış, hem de YZ ilerlemelerinde tıkanmalar yaşanmıştır. Tıkanmaların nedenleri teknik kapasite yetersizlikleri ve paradigmalar üzerindeki anlaşmazlıklar olarak gösterilmektedir. v) Nilsson, 1980 – 2010 yılları arasındaki gelişmeleri incelediği *Büyüyen Cephanelik* başlığını verdiği bölümde nitel akıl yürütme, bayes ağları, yapay öğrenme, doğal dil işleme ve bilgisayarla görme teknolojilerindeki ilerlemeler ve zeki sistem mimarilerini ele almıştır. vi) Modern YZ: Bugünü ve Yarını başlığını taşıyan son bölümde ise oyunlar, robot sistemleri, navigasyon sistemleri, ileri sürücü yardım sistemleri, reklamların ve sosyal medya paylaşımlarının kullanıcılara göre kişiselleştirilmesi, evlerde kullanılan YZ aletleri, otomatik alışveriş, yüz tanıma sistemleri başta olmak üzere günlük kullanım ve teknik gelişmelere ilişkin örnekler vermektedir (Nilsson, 2010).

1940'lı yıllarda ilk çabaların, bir sonraki on yılda ise daha organize girişimlerin görüldüğü YZ alanında, örnek oluşturabilecek teknolojilerin hepsine yer vermek çalışmanın kapsamı dışındadır. Bu nedenle gelişim süreci satranç örneği üzerinden açıklanacaktır.

Makinelere insan gibi düşünebilme, karar verebilme yeteneği kazandırılmasına yönelik çalışmaların ilerlemesinde, zeka ve muhakeme gücü gerektiren oyun programları yazmak önemli bir aşama olmuştur. Özellikle satranç oynayan programlar yazabilme arzusu 1950'li yıllara dayanmaktadır. YZ ile satranç arasındaki bağlantıyı kurabilmek ve satrancın YZ çalışmalarına uygun bir zemin oluşturduğunu kavrayabilmek için, C. Shanon'un (Shannon, 1950: 257) tespit ettiği dört hususu şu şekilde özetlemek mümkündür: i) hem izin verilen hamleler hem de nihai hedef olan mat etmek keskin bir şekilde tanımlanmıştır. ii)

Satranç makinesi önemsiz sayılacak kadar basit olmadığı gibi, tatmin edici bir çözüm için zor da değildir. iii) Genellikle satrancın becerikli bir oyun için düşünme gerektirdiği kabul edilir. Bu sorunun çözümü bizi ya makineleştirilmiş düşünme olasılığını kabul etmeye ya da düşünme kavramımızı daha fazla sınırlandırmaya zorlar. iv) Satrancın belirli yapısı modern bilgisayarların dijital doğasına çok iyi uyuyor.

Shanon'un tespitlerinden anlaşıldığı gibi, YZ ve düşünme yeteneği kazandırılan makinelere satranç ile başlanmasının en önemli iki nedeni; satrancın kural ve amacının açık ve net olması ile olasılık hesapları sonucu karar verme gerekliliğinin bilgisayar diline çevrilmeye uygun olmasıdır. Satranç için *YZ'nin drosophila*sı[4] denilmektedir (Copeland, 2004: 562). Satranç üzerine ilk program 1951 yılında Dietrich Prinz tarafından yazılmıştır. Ancak bu program baştan sona bir satranç oynama kapasitesine sahip olmayıp, iki hamlede mat sorularına doğru cevaplar verebilmektedir (Copeland, 2004: 564). Tam anlamıyla satranç oynayan ilk program ise 1957'de Alex Bernstein'in, IBM 704 işletim sistemi üzerine yazdığı programdır (Heath et al., 1997: 64). Aynı yıl Newell ve Simon (1958: 7) yazdıkları makalede, eğer satranç yarışmasının kurallarında bir değişiklik olmazsa 10 yıl içinde dijital bilgisayarın satrançta dünya şampiyonu olacağı tahmininde bulunmuşlardır. Newell ve Simon'un tahmini yaklaşık 40 yıl sonra, 1997 yılında IBM tarafından yazılan Deep Blue isimli satranç motorunun Dünya şampiyonu Garry Kasparov'u yenmesi ile gerçekleşmiştir.

IBM tarafından geliştirilen satranç motoru Garry Kasparov ile 1996 ve 1997 yıllarında iki defa karşılaşmıştır. Karşılaşmaların ikisi de 6 oyun üzerinden oynanan bir maç şeklinde düzenlenmiştir. Maçların sonuçlarına bakıldığında; 1996 yılında 4-2 'lik üstünlükle G. Kasparov'un kazandığı görülürken, ertesi yıl yapılan rövanş maçında 3,5 – 2,5 Deep Blue kazanmıştır (*Kasparov vs Deep Blue*).

Makine satrancının gelişimi yapay zeka teknolojisindeki ilerlemelerle doğru orantılı olarak artış göstermiştir. 1997'de Kasparov'un makine satrancına yenilmesinin ardından, makine satrancı üzerine çalışmalar da hız kazanmıştır. 2016 yılında En iyi Satranç Motorları

[4] ***Drosophila Melanogaster :*** Sirke sineği ya da meyve sineği (fruit fly) olarak adlandırılan sinek türü, 20.yy'nin başlarından itibaren genetik bilimi çalışmalarının önemli bir kısmında kullanılmıştır. Meyve sineğinin genetik bilimi çalışmaları için uygun olmasının nedeni öğrenme ve hatırlama gibi sinir hücrelerine ilişkin görevleri yapmalarını sağlayan karmaşık bir sinir sistemine sahip olmalarıdır. Bu sinekler anatomik olarak insanlardan farklı olmasına rağmen, işlevsel olarak insana benzer bir sinir sistemine sahiptir ve sinir sistemleri yaklaşık 100.000 nörondan oluşur. Detaylı bilgi için bkz. Stephenson, R. & Metcalfe, N. H. (2013). Drosophila Melanogaster: a fly through its history and current use. *The Journal of the Royal College of Phisicians of Edinburgh*, Vol.43, Issue 1, pp. 70-75.

Şampiyonası'nda *(2016 Top Chess Engine Championship)* Stockfish isimli satranç motoru şampiyon olmuştur. Bundan bir yıl sonra ise Google tarafından geliştirilen Alpha Zero isimli motor sadece satrançta değil, Şhogi (Japon satrancı) ve Go oyunlarında da dünyanın en başarılı motoru olmuştur. Alpha Zero'yu diğerlerinden ayıran en önemli özelliği ise açılış kitabı, oyun sonu taktikleri, piyon düzeni, çift fil avantajı gibi satrancın taktik bilgilerinin veri olarak yüklenmemiş olması; bunun yerine taşların hareket şekli, rok atma ve oyunun amacı gibi çok temel düzey bilgilerin yüklenerek, motorun kendi kendine oynadığı oyunlar ile satrancı öğrenmesi olmuştur. Bir başka deyişle, Alpha Zero "tabula rasa" olarak kurgulanmış ve kendi deneyimleri ile satrancı öğrenmiştir. Sadece 4 saatlik bir çalışma sonucunda Stockfish ile karşılaştırılmıştır. Hamle başına bir dakika düşünme süresi verilen 100 oyunluk maçta Alpha Zero, beyaz taşlarla oynadığı 50 oyunun yarısını kazanıp, diğer yarısında berabere kalırken; siyah taşlarla oynadığı 50 oyunun 3'ünü kazanıp, 47'sinde berabere kalmıştır (Silver et al., 2017: 5)[5]. İki satranç motorunun oyun metodoloji ve pozisyon değerlendirme hızları karşılaştırıldığında, Alpha Zero saniyede 80.000 pozisyon değerlendirirken, Stockfish saniyede 70.000.000 pozisyon değerlendirmektedir (Silver et al., 2017: 19). Aradaki yaklaşık 1000 katlık değerlendirme farkında geride kalmasına rağmen Alpha Zero aradaki farkı, insanımsı bir şekilde, derin sinir ağlarını kullanarak daha gelecek vadeden hamlelere odaklanmasıyla telafi etmektedir (Silver et al., 2017: 5).

Satranç özünde olasılıklar içinden en kazançlı olanı seçebilme sanatıdır. Yani doğru karar verebilmek satrancın en temel kuralıdır. Makinelere de kazandırılmak istenen nitelik belirlenmiş ve tanımlanmış usullerle, belirlenmiş amaçlara ulaşmak için en doğru kararı verdirebilmektir. Bunu insanlar daha çok hislerine ve tecrübelerine dayanarak yaparlar. Örneğin satranç örneği üzerinden konuya bakıldığında; Shanon'un hesaplamalarına göre[6] bir satranç oyununda 10^{120} farklı varyant söz konusudur. Bir varyantı mikro saniyede hesaplayan bir makinenin tüm varyantları hesaplaması yaklaşık 10^{93} yıl sürecektir. Shanon ayrıca mümkün pozisyonların sayısını $64! / 32! (8!)^2 (2!)^6$ formülüyle yaklaşık 10^{43} olarak

[5] Satrançta beyaz taşlarla oynayan taraf ilk hamle avantajına sahip olduğu için kazanca daha yakındır. Birçok dünya şampiyonluğu maçında oyuncular beyaz taşlarla oynadıklarında kazanca, siyah taşlarla oynadıklarında ise beraberliği tutmaya çalışırlar. Ayrıca armagedon adı verilen eşitlik bozma usulünde de beyaz taşlarla oynayan taraf 5 dakika ile oynarken, siyah taşlarla oynayan taraf 4 dakika zamana sahip olmakta, armagedon maçında beraberlik olması halinde de siyah taşlarla oynayan taraf kazanmış sayılmaktadır.

[6] Shanon sayısı olarak da bilinen bu hesaplamanın çıkış noktası satrançtaki 50 hamle kuralına dayanmaktadır. 50 hamle kuralı ise kısaca şudur; bir satranç oyununda taraflardan biri 50 hamle boyunca bir piyon hamlesi yapmazsa ya da herhangi bir taş yenmezse oyun berabere biter. Bu kural satrancın zorunlu olarak sonlu bir hamle sayısında bitmesini gerektirmektedir. Shanon'un hesaplamasıı daha sonraları, iki şahın aynı anda tehdit altında olduğu ya da piyonların ilk sırada olduğu pozisyonları da içermesi bakımından eleştirilmiştir. Ancak yaklaşık olarak doğru bir sayı hesapladığı söylenebilir.

hesaplamıştır. Aynı zamanda bir satranç oyununda beyaz hamlesini yaptıktan sonra siyahın cevap olarak 20*20= 400 farklı hamlesi mevcuttur (Shannon, 1950: 260). Sayıların astronomik boyutlarda olduğu düşünüldüğünde, bir insanın satranç oynarken bu kadar olasılığı aynı anda hesaplamadığını kabul etmek gerekir. İşte tam da bu nokta da Alpha Zero'nun özelliği ortaya çıkmakta derin sinir ağları kullanılarak tıpkı insanların yaptığı gibi hamlelerin önemine göre bir öncelik sıralaması yapma ve bu öncelik sıralaması içinde kalan hamleler arasında karar verme özelliğinin önemi anlaşılmaktadır.

Diğer taraftan dama oyununun satranca göre daha az olasılıkla oynandığı ve günümüz teknolojileri ile tüm olasılıkların hesaplanarak ilk hamleden son hamleye kadar iki tarafın da hata yapmaması halinde oyunun berabere biteceği varyant çözümlenebilmiştir. Ancak aynı çözümün satranç için yapılabilmesi yakın zamanda mümkün görünmemektedir (Schaeffer et al., 2007: 1522). Bunun nedeni, satrançta olasılıkların damaya göre çok fazla olmasıdır.

Toparlamak gerekirse, Turing'in bir sorusuyla bilim dünyası gündemine yerleşen, üzerine akademik çalışmalar ve uluslararası konferanslar düzenlenen YZ çalışmaları, yaklaşık 70 yılda, inişli çıkışlı da olsa, sürekli bir gelişim göstermiştir. Bir YZ uygulama alanında denenip, kullanılan teknikler diğer alanlara da uygulanabilmiştir. Her ne kadar günümüz teknolojileri satranç örneğinde olduğu gibi belirli bir alanda insandan daha başarılı sonuçlara varabiliyor olsa da, YZ'nin mutlak üstünlüğünü iddia etmek şu an için kolay değildir. Çünkü YZ'nin de sınırlılıkları bulunmaktadır. 1956 Dartmouth Konferansı araştırma önerisinde yer alan en önemli tespitlerden biri olarak yukarıda anılan *"... mevcut tüm imkanlardan yararlanabileceğimiz programlara sahip değiliz..."* saptaması güncelliğini sürekli koruyacaktır. Bilgisayar bilimleri ve fizikte elde edilen gelişmeler yoğunlaştıkça, teknik imkanlar genişlemekte ve bu teknik imkanları kullanarak elde edilen programlanabilir alanlar da genişlemektedir. Başka bir deyişle, YZ ilerlemeleri zorunlu olarak bilgisayar bilimleri, fizik, elektrik-elektronik mühendisliği, psikoloji ve nöroloji çalışmalarına bağımlıdır. YZ'ye teknik imkanlar sağlayan çalışmalarda ilerleme olmadıkça, YZ'nin ilerlemesi mümkün değildir.

B. Yapay Zeka Tanımı, Bileşenleri ve Teknolojileri

Bu başlık altında öncelikle YZ için yapılmış tanımlara yer verilecek, ardından YZ'nin başlıca bileşenleri aktarılacak ve son olarak örnek YZ teknolojileri açıklanacaktır.

1. Yapay Zekanın Tanımı ve Türleri

Yapısı gereği birden fazla disiplin tarafından desteklenerek zenginleşen YZ üzerine yapılan tanımlar da değişiklik göstermektedir. Üzerinde net bir uzlaşılmış tanım olmasa da, tanımlar benzer kavram ve kelimeler üzerinden şekillenmektedir. Birkaç tanıma yer vermek gerekirse şunlar örnek olarak gösterilebilir:

- McCarthy (2007: 2) *" ...özellikle zeki bilgisayar programları olmak üzere, zeki makinalar yapma mühendisliği ve bilimidir..."*
- Nilsson (2010: 13) *"Yapay Zeka, makinelere zeka kazandırmaya adanmış etkinliktir; zekaysa, bir varlığın kendi ortamında doğru düzgün ve olan biteni öngörerek işlev görmesini sağlayan niteliktir."*
- Sebastian Thrun[7] : *" karmaşık bir şeyi algılama ve uygun karar verme"* (Ersoy, 2018: 29; Peter Warren Singer, 2009: 58).
- Rich ve Diğerleri (2009: 3): *"Yapay Zeka bilgisayarların, insanların şu anda daha iyi yaptığı şeyleri nasıl yapacağının çalışmasıdır."*
- Say (2021: 83): *"Doğal sistemlerin yapabildiği (zekice olsun veya olmasın) her bilişsel etkinliği (gerekirse bedenleri olan) yapay sistemlere, daha da yüksek başarım düzeylerinde nasıl yaptırabileceğimizi inceleyen bilim dalıdır."*

Tanımların yaklaşık olarak aynı hususlara odaklandığı görülmekle birlikte; YZ, makinelerin zeki davranışlar sergilemesi, karar verme, karmaşık yapıları algılama ve adaptasyon gibi nitelikler kazanması yolunda yapılan çalışmalara genel olarak verilen isimdir. Yukarıda yer verilen tanımların içerisinde, literatürde en kabul gören tanımın Nilsson'un yaptığı tanım olduğu söylenebilir (Grosz et al., 2016: 12). YZ'yi teknik bakımdan ele aldıkları eserlerinde Russell ve Norvig (Russell & Norvig, 2021: 1-4), YZ'ye bir tanım yapmak yerine daha önce yapılmış tanımları sınıflandırmayı tercih etmişlerdir. Buna göre; yapay zekayı insan fiillerine uygunluk bakımından ele alanlar ile soyut, resmi tanımlar getiren rasyoneller bir boyutu oluştururken; diğer boyut düşünce ile davranış ayrımına dayandırılmıştır. Yazarlar iki boyutun kendi içinde de ikişer karşıtlık barındırmasından hareketle; YZ'yi dört farklı kategoride değerlendirmiştir. Bu kategoriler şunlardır: i) insan

[7] Sebastian Thrun, Stanford Üniversitesi Yapay Zeka Laboratuvarı müdürüdür.

gibi eylemde bulunmak, ii) insan gibi düşünmek, iii) rasyonel düşünmek ve iv) rasyonel olarak eylemde bulunmak.

Yapay Zeka'nın türleri bakımından en önemli ayrıma John Searle'nin eserinde rastlanmaktadır (1980: 417). Searle *zayıf yapay zeka* ve *güçlü yapay zeka* ayrımı yaparak; zayıf yapay zekayı, zihin çalışmalarında bilgisayarın değerinin araç niteliğinde olduğunu belirterek açıklamaktadır. Güçlü YZ derken ise; gerçek bir zihne sahip olan, diğer bilişsel durumları da anlayabilen programlanmış bilgisayarları kastetmektedir. Searle'nin ayrımına benzer biçimde günümüzde de YZ türlerinden bahsedilmektedir. Şöyle ki; temel olarak d*ar yapay zeka* ve *genel yapay zeka* ayrımı yapılmakta, ilki Searle'nin zayıf yapay zeka sınıflandırmasına karşılık gelirken; ikincisi güçlü yapay zeka sınıflandırmasına karşılık gelmektedir. Günümüzde dar/genel yapay zeka sınıflandırmasına ek olarak bir de *süper yapay zekadan* bahsedilmektedir (Acar, 2020: 16; Corea, 2019: 17).

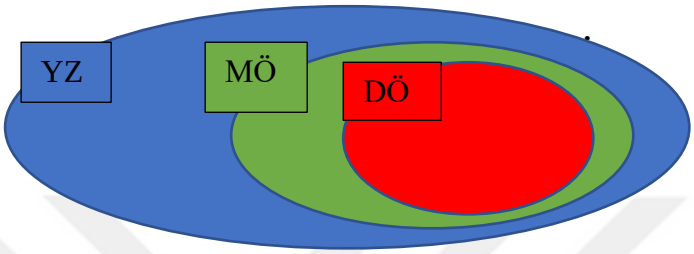
Dar YZ, tek bir amaca odaklanan ve bu amacı insanlardan daha iyi gerçekleştirebilen yapay zekaları ifade etmektedir. Örneğin; satranç motorları, doğal dil işleme yazılımları, görüntüleme ve izleme teknikleri gibi alanlarda dar yapay zeka türleri kullanılmaktadır. Genel yapay zeka ise ulaşılmak istenen amacı ifade etmektedir. Aynı anda birden fazla uzmanlık gerektiren işi tek başına yapabilen yapay zeka türüdür. Buradaki "birden fazla iş" ifadesini bir parça daha açmak gerekirse; kastedilen ayrı ayrı dar yapay zeka uygulamalarını tek bir uygulamada toplamak değildir; aksine tüm yetenekler arasındaki entegrasyonun makinelere kazandırılabilmesidir. Başka bir deyişle, genel yapay zeka spesifik bir amaç için programlanmamış, uygulamalardan öğrenebilen ve öğrendiklerini farklı çevrelere uygulayabilen yapay zeka türüdür. Yukarıda da değinildiği gibi genel yapay zeka günümüzde mevcut olanı değil, ulaşılması arzulanan türü ifade etmektedir. Günümüzde genel yapay zekaya en yakın uygulama olarak Google Deep Mind gösterilmekle birlikte, insanların yapabildiği zihinsel görevleri yapamadığı için de tam anlamıyla genel yapay zeka kabul edilemeyeceği belirtilmektedir (Corea, 2019: 16-17).

Süper yapay zeka ise daha çok bilim kurgu eserlerinde ele alınan, yapay zeka yazılımları yapmak dahil, bilişsel, zihinsel ve fiziksel olarak insanın yapabileceği her türlü eylemi insandan daha başarılı olarak yapabilen tek bir bilgisayar üretebilme arzusudur. Süper yapay zeka kapsamında değerlendirilecek program, yazılım ya da robotlardan beklenen özellikler özetle şu şekildedir: i) insan zekasından daha büyük bir zekaya sahip olmak, ii) bilimsel ve yaratıcı düşünebilmek, iii) sosyal beceriler ve belki de duygusal becerilere sahip olmak

(Corea, 2019: 17). Süper yapay zekanın mümkün olup olmadığına dair görüşler ileri sürülmüş olsa da, bu görüşler sübjektif kanaatlerden öteye gitmemektedir[8].

2. Yapay Zekanın Bileşenleri

Yapay Zeka mühendislik tekniği bakımından makine öğrenmesi ve derin öğrenme başta olmak üzere farklı bileşenlerin bir kapsayıcı kümesi olarak ortaya çıkmaktadır. Basitçe makine öğrenmesi, derin öğrenme ve YZ ilişkisi şöyle bir şema yardımıyla gösterilebilir:



Makine öğrenmesi açıkça programlanmamış bilgisayarlara öğrenme yeteneği veren bir çalışma alanıdır (El Naqa & Murphy, 2015: 6). Bilgisayara girdiler ve çıktılar kodlanarak eğitme işlemi yapılması mantığına dayanır. Eğitme işleminde girdi ile çıktı arasındaki istatistiksel doğruluk değeri üzerinden hesaplanan hata payı, başlangıçta belirlenen değerin altına düşene kadar eğitme işlemine devam edilir ve sonrasında değerler sabitlenir (Elmas, 2018: 98). Eğitilmiş makineler örüntü tanıma ve verilerin sınıflandırılması başta olmak üzere finansal tahminlerde, bilgisayarla görme, medikal ve biyomedikal uygulamalarda kullanılır (El Naqa & Murphy, 2015: 5; Elmas, 2018: 97). Makine öğrenmesi yöntemi kullanılarak askeri personellerin intihar eğilimleri (Lin et al., 2020) ya da zihinsel sağlık sorunları ile karşılaşma olasılıklarının değerlendirildiği çalışmalar (Nissen et al., 2021) da yürütülmüştür. Makine öğrenmesi kendi içerisinde gözetimli öğrenme, gözetimsiz öğrenme

[8] Bu tez çalışması büyük güç olarak kabul edilen devletler içinden örneklem olarak seçilenlerin, uluslararası güvenlik bağlamında geliştirdikleri ve geliştirme vizyonu ortaya koydukları güvenlik araçları ile bu araçların büyük güç siyaseti üzerindeki etkilerine odaklanmaktadır. Dolayısıyla geliştirilmesinin mümkün olup olmadığı tartışmalı olan ve senaryolar üzerinden görüş belirtilen teknolojilere detaylı olarak yer verilmeyecek, sadece var olan tartışmaya değinilmekle yetinilecektir. Ray Kurzweil'in 2005 yılında yayınladığı eserindeki öngörüsüne göre; 2045 yılında tüm insanlığın sahip olduğu toplam zekadan bir milyar kat daha güçlü yapay zeka yaratılacaktır. Bkz. Kurzweil, R. (2005). *The singularity is near: When humans transcend biology*. Penguin. S.122, 203 v.d. Nick Bostrom daha temkinli bir şekilde süper yapay zekanın, insan seviyesinde yapay zeka üretildikten bir süre sonra mümkün olacağını öngörmektedir. Bkz. Bostrom, N. (2014). *Superintelligence : paths, dangers, strategies* (First edition. ed.). Oxford University Press. S.20 v.d. McCharty insan seviyesinde YZ'nin muhtemelen Dartmouth Konferansının 100. yılı olan 2056 yılında üretilmiş olabileceğini ifade ederken, Selfridge'e göre insan seviyesinde YZ mümkün değildir. Moore ise makinelerin her zaman insanların hakimiyeti altında olacağını ummaktadır. Bkz. Moor, J. (2006). The Dartmouth College artificial intelligence conference: The next fifty years. *AI magazine, 27*(4).

ve yarışmacı öğrenme olarak farklı teknik uygulamalara ayrılmaktadır (Elmas, 2018: 98,v.d.).

İlk olarak Rina Dechter (Dechter, 1986: 180) tarafından kullanılan derin öğrenme, insan beyninin işlevlerini taklit eden yapay sinir ağlarına dayanan bir YZ üretme tekniği olup, çoğunlukla ses, video ve görüntü işleme, görüntü sınıflama, bir görüntü içinde yer alan nesnelerin birbiri ile ilişkisini anlamlandırma amaçlarıyla kullanılmaktadır (Elmas, 2018: 149,v.d.). Yukarıda yer verilen şemada da görüldüğü üzere; makine öğrenmesinin özel bir türü olan derin öğrenme, girdi katmanının üzerine bir gizli katman oluşturularak yapay sinir ağlarının eğitilmesi ile elde edilen bir tekniktir. Bu eğitme süreci, YZ'nin diğer uygulamalarında da olduğu gibi, zorunlu olarak donanımlardaki gelişmelere paralel olarak ilerleyebilmektedir. Özellikle bilgisayar donanımlarından Grafik İşleme Birimi ve Merkezi İşleme Birimi kapasitelerindeki gelişmeler derin öğrenme tekniğini güçlendirmiş, daha çok katmandan oluşan yapay sinir ağlarının makinelerin eğitimi için kullanılabilmesini mümkün kılmış, bunun sonucu olarak da devasa boyutlarda verilerin sınıflandırılması ve işlenmesine olanak tanımıştır.

Devasa boyutlardaki veriler literatürde büyük veri olarak adlandırılmaktadır. Sosyal medya hesaplarında üretilen içeriklerden, izleme sistemlerinin elde ettiği görüntülere, internet ortamında bireylerin hazırladığı bloglardan kurum ve kuruluşlar tarafından yapılan işlemlere kadar internetin kullanıldığı her saniyede büyük veriye veri akışı ve depolanması devam etmektedir (Doğan & Alaca, 2020: 393 v.d.). Aralarındaki ilişki saptanmadan büyük bir yığın halinde bulunan verilerin anlamlı hale getirilmesi, sınıflandırılması, ham veriden bilgi üretilmesi derin öğrenme tekniği ile mümkün hale gelmiştir (Russell & Norvig, 2021: 44 v.d., 837 v.d.).

Büyük veri ile özelde makine öğrenmesi ve derin öğrenme genel olarak ise YZ'nin ilişkisi çift yönlü bir ilişkidir. Bir yönüyle programların eğitilmesinde büyük veri kullanılmakta, diğer yönüyle eğitilmiş programlar büyük verilerin işlenmesinde kullanılmaktadır. Örneğin yapılan bir çalışmada (Hiippala, 2017), derin öğrenme yöntemiyle sosyal medya hesaplarındaki paylaşımlar kullanılarak askeri araçların algılanması için geliştirilen bir sistem gösterilmiştir.

3. Yapay Zeka Teknolojileri

Yapay Zeka kullanılarak geliştirilen teknolojiler genel hatlarıyla bölümün başında tarihçe başlığı altında anılmıştı. Bu alt başlıkta sınıflandırılmış biçimiyle YZ teknolojilerine yer verilecektir. Bilgisayar bilimciler konunun teknik kısmına odaklandıkları için, yaptıkları sınıflandırmalar da bu çalışmanın kapsam ve amacını aşacak derecede detaylı olmaktadır. Dolayısıyla çalışmanın amacına daha uygun düştüğü için, YZ teknolojileri Clarke (2019: 424 v.d.) tarafından yapılan dörtlü sınıflandırma kapsamında ele alınacaktır. Clarke'ın sınıflandırmasının, savunma ve YZ ilişkisini ele alan başka çalışmada da kullanıldığı görülmektedir (Türkkan & Özdaş, 2021: 302). Bu dört sınıf şunlardır: i) robotik, ii) sibernetik organizmalar, iii) kural tabanlı uzman sistemler ve iv) yapay sinir ağları.

a) ***Robotik***

Clarke'ın yaptığı tanıma göre robotiğin programlanabilirlik ve mekanik kapasite olmak üzere iki kurucu unsuru bulunmakta, yaygın tasarımlarda da robotun çevresindeki verileri elde etmek için sensörler gerekmektedir (Clarke, 2019: 425). Singer (2009: 54) ise robotları şu şekilde tanımlamaktadır : *"...çevreyi izleyen ve çevredeki değişiklikleri keşfeden **sensörler**, nasıl karşılık vereceğine karar veren **YZ ya da işlemciler** ve robotun çevresindeki dünyada bir tür değişim yaratacak ve alınan kararları yansıtacak biçimde çevre üzerinde eyleme geçen **efektörler** olmak üzere üç temel bileşenden oluşan insan yapımı cihazlardır."* Bir diğer robot tanımı ise şöyledir : *"... fiziksel ve zihinsel bağlamda özne nitelikleri gösteren ama biyolojik anlamda hayatta olmayan, inşa edilmiş sistemlerdir"* (Ersoy, 2018: 6). *Robotik*, robot üretme çalışmalarına verilen genel bir isimdir. Bunun yanı sıra *bot* ise robot ile benzer özellikler gösteren fakat fiziksel bir görüntüsü olmayan, sadece yazılım olarak hazırlanmış programlardır.

Robotlar fabrikalarda üretim faaliyetlerinde, temizlik gibi işler için evlerde, yaşlı bakım servislerinde ve askeri alan dahil olmak üzere geniş bir yelpazede kullanılmaktadır. Çoğunlukla bilim kurgu filmlerinde insan görünümlü robotlar kurgulandığı için, robot algısı da insan görünümlü olarak şekillenmektedir. Ancak yukarıdaki tanımlar dikkate alındığında; sürücüsüz araçlar, dronelar ya da fabrikada üretim süreçlerinde yer alan algılama, karar verme ve harekete geçme özelliklerinin üçünü birden taşıyan cihazlar da robot olarak kabul edilmektedir.

b) *Sibernetik Organizmalar (Cybernetic Organisms / cyborgisation)*

Sibernetik ve organizmalar kelimelerinin İngilizce karşılıklarından türetilmiş olan cyborg kavramı, köken itibariyle dünya dışı çevrelerde hayatta kalma bağlamında, teknolojik olarak güçlendirilmiş insan olarak tanımlanmaktadır. İnsanlardaki uzuv ya da uzuvlarındaki işlev kaybı protez, ortez ya da implant kullanılarak telafi edilmeye çalışılmaktadır. Salt işlev kaybını gidermeye yönelik teknolojik güçlendirmeler, çoğunlukla YZ teknolojileri kapsamında sibernetik organizmalar olarak değerlendirilmemektedir (Clarke, 2019: 425).

Sadece bacak/kol ampütasyonu sonrası bacağını/kolunu kaybeden bir kişinin protez kullanması ya da görme bozukluğu yaşayan insanın gözlük kullanması veya dişini çektiren bir kişinin diş implantı taktırması bu kişileri cyborg olarak nitelendirme nedeni olamaz. Ancak tasarlanan protez normal insan bacağının/kolunun işlevinin ötesinde bir işlev sağlıyorsa örneğin; bir insanın kaldırabileceği ağırlığın anlamlı derecede üstünde bir ağırlığı kaldırmaya imkan veriyor veya zıplayabileceği yükseklikten önemli ölçüde daha uzak bir mesafeye zıplamasını mümkün kılıyorsa; tasarlanan gözlük sadece görme bozukluğunu gidermeyi değil, aynı zamanda görüntüleri internet bağlantısı kullanarak işlenmesi için bir program ya da veri tabanına yönlendirmeyi amaçlıyorsa bu teknolojik güçlendirmelerin kazandırıldığı insanları cyborg olarak nitelemek yerinde olur.

Cyborg meselesi özellikle hukuki bakımdan eşitsizlikler yaratacağı düşüncesiyle kamuoyunda kaygılara neden olmaktadır (Türkkan & Özdaş, 2021: 303). Bir yönüyle insanların bir hastalık ya da kaza sonucu dezavantajlı konuma düşmelerini telafi etmek amaçlanırken, diğer taraftan teknolojik olarak güçlendirmenin sınırının belirlenmesi kolay değildir. Son dönemlerin konu bağlamındaki önemli çalışmalarından birinde, 16 yıl boyunca görme engelli olarak yaşamını sürdüren Bernardeta Gomez isimli kadının, beynine yerleştirilen bir implant ile görme yeteneğini yeniden kazandığı gösterilmiştir (Cassella, 2021; Fernández et al., 2021). Gomez'in cyborg olarak tanımlanıp tanımlanamayacağı sorunu, beynine yerleştirilen implantın başkaca bir özellik kazandırıp kazandırmadığı bilgisi üzerine yorumlanabilir. Operasyonun henüz çok yeni olması nedeniyle böylesi bir bilgi bulunmasa da, mevcut teknolojik imkanların vardığı boyutun bir insanı cyborga dönüştürebilmek için yeterli olduğu açıkça anlaşılmaktadır.

c) ***Kural Temelli Uzman Sistemler (KTUS)***

Clarke, KTUS'yi açıklarken gelişim sürecini üç dönem halinde ele almıştır: i) 1940-1960 arası dönemi, hesaplama uygulamalarında verilerden çıkarım yapmak için, donanımla bütünleşik çevirici dillerin kullanıldığı dönem, ii) 1960-1990 arası dönemi, çözülmesi beklenen bir problem ve o problemin çözüm usulüne dayanan algoritmik programların kullanıldığı dönem ve iii) 1980'lerden itibaren KTUS dönemi olarak ifade etmektedir. KTUS, insan tecrübelerinin veri olarak girilmesiyle ve sonrasında, kaydedilen tecrübeleri programın çözülmesi istenen problem alanına uygulaması ile oluşturulmaktadır (Clarke, 2019: 425).

KUTS uygulamalarının ilk örneği 1969 yılında geliştirilen DENDRAL isimli uygulamadır. DENDRAL projesi Stanford Üniversitesi'nden Feigenbaum ve Buchanan başta olmak üzere bir uzman ekip tarafından geliştirilen, kimya molekülleri üzerindeki insan uzmanlık bilgisini bilgisayar diline aktararak, insanların yaptığı işleri daha az maliyetle program aracılığıyla yapmayı amaçlayan bir projedir. Uygulamaya, moleküllerin başlangıç formülleri ve bir elektron ışını tarafından radyasyona tabi tutulduğunda üretilen, molekülün çeşitli parçalarının kütlelerini veren kütle spektrumu olmak üzere iki tür veri girişi yapılmaktadır. Uygulama ise formül ile uyumlu tüm olası yapıları üretebilmekte ve bunları gerçek kütle spektrumları ile karşılaştırarak hangi kütle spektrumlarının gözlemleneceğini tahmin etmiştir (Russell & Norvig, 2021: 40). 1970'li yılların başında DENDRAL projesinden esinlenilerek, Shortliffe, Buchanan ve Cohen tarafından geliştirilen MYCIN projesi ise, belirli semptomların varlığının veri olarak girilmesi halinde bulaşıcı hastalıkların tanı ve tedavisinde insanların yaptığı işlerin program tarafından yapılmasını sağlamıştır (Nilsson, 2010: 296). MYCIN projesi kapsamında, insan uzmanlık bilgilerinin bilgisayar diline aktarımı " EĞER – İSE" kalıpları aracılığıyla yapılmış olup, programın akıl yürütmesi şöyledir : *" EĞER a,b,c semptomları var İSE nedeni büyük olasılıkla X'tir"* (Nilsson, 2010: 297 v.d.).

KUTS, insanların mesleki kariyerlerinde sadece sınırlı bir alanda uzmanlık bilgisine sahip olmalarından yararlanarak yaptıkları işlerin bilgisayar programları tarafından yapılabileceğini gösteren ilk örnek olması bakımından önem kazanmaktadır. Farklı alanlarda da şirketlerin, maliyetlerini düşürmek amacıyla, insan uzmanlık bilgilerini bilgisayar diline aktaracak AR-GE birimleri kurdukları görülmektedir. Yazılım-donanım ilişkisi KUTS bakımından da gündeme gelmiş ve işlemci gücü yüksek bilgisayarlara ihtiyaç duyulmuştur. 1981 yılında Japonların Beşinci Nesil projesi bu ihtiyaca cevap vermek amacıyla tasarlanmaya başlamış, günümüz değeriyle 1.3 Milyar dolarlık bir bütçe ayrılmıştır. 1980'lerin başından sonuna doğru YZ

endüstrisi milyon dolarlar seviyesinden, milyar dolarlarla ifade edilecek bir ekonomik büyüklüğe ulaşmıştır (Russell & Norvig, 2021: 41-42).

KUTS'nin önemli özelliklerinden bir tanesi programın karar verirken uyguladığı akıl yürütme sürecinin insan uzmanlar tarafından gözlemlenebiliyor olmasıdır (Clarke, 2019: 425), diğer yandan ise bu uygulamaların zayıf yönü kendi tecrübelerinden öğrenemiyor olması ve dolayısıyla da analizlerinin girilen veri ile sınırlı kalmasıdır (Russell & Norvig, 2021: 42).

d) ***Yapay Sinir Ağları (YSA)***

Yapay Sinir Ağları, insan ve hayvan beyinlerinin psikolojik ve biyolojik yapısının modellenmesi ve bu modellerin bilgisayar programlarına kazandırılarak bilgilerin işlenmesi amacına yönelik olarak geliştirilmiştir (Elmas, 2018: 26 v.d.). KTUS'nin programın kendi deneyimlerinden öğrenme yeteneğinden yoksunluğu, YSA ile giderilmeye çalışılmıştır. YSA'nın, KTUS'den ayırt edici en önemli özelliği çıkarım yapmak için kullandığı akıl yürütmenin insan uzmanlar tarafından anlaşılamıyor olmasıdır (Clarke, 2019: 425). Çünkü sinir ağları yukarıda değinilen makine öğrenmesi ve derin öğrenme teknikleriyle bir eğitim sürecine tabi tutulur, ardından program bu eğitim sürecinde öğrendiklerini ve uygulama yaptıkça kendi tecrübelerinden öğrendiklerini problem alanı olarak gösterilen veri kümelerine uygular (Clarke, 2019: 425-426).

YSA katmanlardan oluşur. Geri yayılım algoritması adı verilen bir teknik ile katmanlar arasındaki geçişlerdeki hata payı düşürülür ve programın yaptığı çıkarımın en doğru çıkarım olması amaçlanır. YSA ile öğrenme yöntemleri, hava trafik denetimi, kredi kartı sahtekarlıklarının tespit edilmesi gibi alanlarda kullanılmaktadır (Nilsson, 2010: 518).

C. Uluslararası İlişkiler ile Yapay Zeka Nasıl İlişkilenmeye Başladı?

Uluslararası güvenliğin dönüşümünü konu edinen bir çalışmada, avcı-toplayıcı kabilelerden başlayıp günümüze kadar gelen dönüşüm süreci iki temel dinamik üzerinden incelenmektedir (Denk, 2019). Bunlardan ilki üretim araçları diğeri ise güvenlik araçlarıdır. Çalışmanın odak noktası üretim araçları ile güvenlik araçlarının zaman içerisinde birbirinden ayrılması ve güvenlik araçları özelinde de, güvenlik aracını kullanan özne ile hedef arasındaki mesafe uzadıkça güvenlik aracının tahrip gücünün arttığına yönelik saptamadır(Denk, 2019: 6).

Buradan hareketle uluslararası ilişkileri etkileyen bir unsur temelde iki farklı açıdan ele alınabilir. İlk olarak ekonomik düzen ve üretim ilişkileri üzerindeki etki, ikinci olarak ise güvenlik araçlarındaki değişim, dönüşüm ve mülkiyet bakımından etkileri incelenebilir. Bunlara ek olarak YZ'nin yapısı gereği ele alınması gereken bir üçüncü düzlem ise dış politika yapım ve uygulama süreçlerinde YZ'nin kullanım alanlarıdır. Acemoğlu ve Restrepo (2018: 203 v.d) çalışmalarında YZ bağlantılı teknolojilerin ekonomik üretkenliği artırdığını göstermişlerdir. YZ ile ekonomi ilişkisini inceleyen diğer çalışmalar YZ'nin ekonomi üzerindeki olumsuz etkisi olarak değerlendirilen eşitsizliği artırıcı bir faktör olduğu sonucuna ulaşmışlardır (Bissio & WATCH, 2018: 83 v.d.; Cockburn et al., 2019: 195). Üretkenliğin artmasının doğal sonucu arz fazlasının oluşması olacaktır. Bununla birlikte gelir eşitsizliğinin artmasına bağlı olarak talepteki kaymalar ekonomi modelini etkileme potansiyeline sahiptir. Başka bir deyişle arzın artmasına karşılık tüketim talebi gelir eşitsizliğinden dolayı mevcut toplumsal gruplar düzeyinde gerçekleşmeyecek, üst gelir gruplarıyla sınırlı kalacaktır.

YZ-uluslararası güvenlik üzerine yapılan çalışmalar 1970'li yıllara kadar uzanmakla birlikte, 1990'lı yıllarda hızlanmış olup RMA literatürü bağlamında gelişmiş ve zenginleşmiştir (Martyanov, 2019: 69). Krepinevich askeri devrim kavramı etrafında teknoloji- askeri örgütlenme biçimleri arasındaki ilişkiyi tarihsel olarak incelemekte ve sınıflandırmaktadır (Krepinevich, 1994). Murray ve Knox (2001) MR ve RMA arasındaki farka vurgu yapmakta ve RMA'nın teorik çerçevesini çizmektedirler. Hoffman (2017) savaşın doğası bağlamında, YZ etkisiyle savaşın geleceğini tartışmaktadır. Raska (2021) RMA tarihçesini sınıflandırdığı eserinde RMA dalgalarına yer vermiş ve YZ'yi son RMA dalgası olarak adlandırmıştır.

YZ'nin metodolojik bir yöntem olarak uluslararası ilişkiler çalışmalarında kullanılmasının başarılı örnekleri, teknolojinin yaygınlaşmaya başladığı 1990'lı yıllara dayanmaktadır. Schrodt 1991 yılında yaptığı çalışmasında nicel yöntemleri ve YZ modellemelerini kullanarak tarihteki savaş içeren ve savaş içermeyen krizleri kodlamış, geliştirdiği model ile örüntü izleme tekniği kullanarak dış politika analizi yapmıştır (Schrodt, 2019). Ancak hem uluslararası ilişkiler fenomenlerinin çok fazla değişken içermesi hem de YZ'nin öğrenme sürecine yetecek kadar dijital verinin bulunmaması bu alanda nicel yöntemlerin kullanımının sınırlı bir düzeyde kalmasına neden olmuştur (Hudson & Day, 2019: 193 v.d.). Özellikle uluslararası güvenlik alanında nicel metodoloji kullanılarak yapılan analizler çok sınırlıdır.

Çalışmanın bu bölümünde Uluslararası İlişkiler ile YZ nasıl ilişkilenmeye başladı? Sorusuna cevap ararken, öncelikle ekonomik açıdan gözlemlenen etkilere genel hatlarıyla yer

verilecek, akabinde akademik çalışmalarda ve dış politikada YZ'nin kullanım alanlarına değinilecektir. YZ – Uluslararası ilişkiler arasındaki ilişkinin güvenlik boyutu ise takip eden bölümde detaylı olarak ele alınacak ve incelenecektir.

1. Yapay Zeka Ekonomi İlişkisi

Ekonomik ilişkiler üzerindeki yapay zeka etkisi en temelde istihdam ve üretim ilişkileri olmak üzere iki açıdan ele alınabilir. İstihdam bakımından insanların yerine getirdiği görevlerin makineler tarafından yapılmaya başlanması, fordist üretim teknikleri olarak bilinen seri üretim bantlarının icat edilmesiyle başlamıştır. Bir alanda aşırı uzmanlaşmanın ve bir insanın tek bir işi sürekli olarak yapmasının bir sonucu olarak, bu yetenek makinelere de kazandırılabilmiştir. YZ destekli makinelerin üretimde kullanılmasını eklektik bir süreç olarak değerlendirmek yerinde olur. Şöyle ki; öncelikle tüm işler insanlar tarafından yapılmaya başlanmış, ardından seri üretim sürecinde bir işi oluşturan görevler bölünerek her bir insanın bir görevde uzmanlaşması sağlanmıştır. Sınırları ve yapılması gerekenler keskin bir şekilde belirlendikten sonra da bir görevin makinelere, insan düzeyinde hatta insandan daha başarılı bir şekilde yaptırılabilmesi mümkün olmuştur. Bunun sonucunda da geleneksel mavi yaka işleri başta olmak üzere, işlerin büyük çoğunluğu makineler tarafından yapılabildiği ve üretim maliyetlerini düşürdüğü için bu alanlardaki işler otomasyona aktarılabilme imkanı bulmuştur.

Otomasyon ile işsizlik arasındaki ilişkiyi öngörmeye yönelik çalışmalar başlıca iki grupta toplanabilir. Bunlardan ilki mesleklere odaklanan çalışmalar diğeri ise yapılacak işe ilişkin görevlere odaklanan çalışmalardır. Frey ve Osborne (2017: 265) ABD iş piyasası üzerine yaptıkları çalışmada 702 mesleği otomasyona aktarılabilme imkanı bakımından incelemiş ve önümüzdeki 10-20 yıllık süreçte, çalışmada incelenen mesleklerin %47'sinin otomasyona elverişli olduğunu öngörmüşlerdir. PwC analistlerinin mesleklere odaklanarak, 29 ülke üzerinde yaptıkları çalışmada; meslekleri üst düzey görevlilerden başlayıp makine operatörleri ve montajcılara kadar sekiz farklı kategoride değerlendirmişler ve üst düzey görevlilerin meslekleri %10 seviyesinde otomasyonlaştırılabilirken, bu oran makine operatörleri ve montajcılarda %64 seviyelerine kadar çıkmaktadır (Hawksworth et al., 2018: 23).

Görev temeline dayanan araştırmalarda, meslekleri iş faaliyeti/görev bakımından ayrımlara tabi tutarak bu görevlerin otomasyona aktarılabilme potansiyelleri incelenmiştir. Bu yöntemle araştırma yapan McKinsey'in bulgularında, tamamen otomasyona aktarılabilme potansiyeline sahip meslekler %5'ten daha az olarak saptanırken, var olan tüm mesleklerin

%62'sinin en az üçte birlik iş faaliyetleri otomasyona aktarılabilir olarak gösterilmiştir (Manyika et al., 2017: 27.vd).

İşsizliğin kitlesel olarak artış eğilimine girmesi, iş piyasasında arz fazlası oluşacağı için ücret ve çalışma koşullarında düşüş yaşanmasına, ulus-devletler içinde gelir dağılımı adaletsizliklerinin yükselmesine bağlı olarak istikrarsızlıkların yaşanmasına ve bu istikrarsızlıkların da göç eğilimini artırmak suretiyle uluslararası ilişkileri etkileyebilecek nitelikte olduğunu söylemek mümkündür. Bu nedenlerle olacak ki yukarıda yer verilen akademik çalışma ve danışmanlık şirketleri araştırmalarına ek olarak OECD (Ekonomik Kalkınma ve İşbirliği Örgütü) ve Dünya Ekonomi Forumu gibi uluslararası örgütler de konuyu gündemlerine almış ve raporlar hazırlamışlardır. OECD 2012-2019 yılları arasındaki otomasyona elverişli işler ile bu işlerdeki istihdam oranları arasındaki ilişkiyi incelediği raporunda istihdamın düşmediğini eskiye oranla daha düşük oranda bir artış gösterdiğini tespit etmiştir. Rapora göre otomasyon bakımından yüksek riskli işlerde istihdam oranlarındaki artış %6 olarak ifade edilirken, otomasyona elverişlilik bakımından düşük riskli işlerde istihdam artış oranı %18 olarak bulunmuştur. Raporda öne çıkan bir diğer husus ise düşük eğitimli işçilerin durumuna ilişkin saptamalardır. Şöyle ki; istihdam bakımından en riskli grup olarak düşük eğitimli işçiler gösterilmekte, bu grup işçilerin yaptığı işlerin otomasyona daha yatkın olduğu ifade edilmektedir, ancak analiz sonuçları düşük eğitimli kişilerin istihdam oranlarında anlamlı bir azalma olmadığını göstermiştir. Raporda bu durumun nedeni olarak öncelikle düşük eğitimli kişilerin emekli olup yerine daha yüksek eğitimli kişilerin geçmesi, buna ek olarak da işçilerin becerilerinin çalışma hayatı içinde yükseltilmesi gösterilmektedir (Georgieff & Milanez, 2021: 8-9).

Dünya Ekonomi Forumu Başkanı Klaus Schwab, Dördüncü Sanayi Devrimi ismini verdiği eserinde otomasyon-istihdam ilişkisini kısa vadede yıkıcı ama uzun vadede geliştirici olarak özetlemektedir. Başka bir deyişle bazı meslekler ya da görevler teknolojinin yıkıcı etkisiyle yok olsa da yerine yine teknolojinin etkisiyle yeni iş gücü ihtiyaçları doğacaktır. Yazara göre sorun mevcut işlerin yok olması ile ikame edilecek işlerin ortaya çıkması bakımından hangisinin daha hızlı olacağı ve insanların yeni işlerin gerektirdiği nitelikleri kazanmakta ne kadar zamana ihtiyaç duyduklarının henüz öngörülebilir olmaktan uzak olmasıdır (Schwab, 2017: 44 vd.).

Her ne kadar farklı örneklemler ve değişkenler tanımlamak suretiyle farklı sonuçlara ulaşan çalışmalar bulunsa da, çalışmaların tamamı iş gücü piyasasında ve istihdam konusunda köklü değişikliklerin yaşanacağını göstermektedir. Bu durumun bir nedeni teknolojideki

ilerlemeler ve YZ temeline dayanan otomasyon iken, bir diğer neden daha yapısal olarak 20. yüzyılın ilk yarısından itibaren çalışanların seri üretim sürecinde araçsallaştırılmış olmasıdır. Çalışmanın başında detaylı olarak yer verildiği üzere YZ üretebilmenin en önemli aşaması amaçları, eylemleri ve yöntemleri keskin bir şekilde tanımlayabilmek ve bunu bilgisayar diline aktarabilmektir. İş gücü piyasası ve istihdam bakımından bunu mümkün kılan fordist üretim mantığı olmuştur. Daha net ifade etmek gerekirse; iş gücü piyasasında insanlaşan robotlara giden yolun taşları robotlaşan insanlarla döşenmiştir.

2. Uluslararası İlişkiler Çalışmalarında, Dış Politika Yapım ve Uygulama Sürecinde Yapay Zeka Kullanım Alanları

Siyaset bilimi literatüründe 1960'larda başlayan davranışçı yaklaşım çerçevesinde uluslararası ilişkileri anlamak ve açıklamak için nitel yöntemlerin yanı sıra nicel yöntemler de kullanılmaya başlanmıştır. Yaygın olarak kullanılan yöntemler istatistiksel modeller, bireysel rasyonalite modelleri ve dinamik modellerdir (Schrodt, 1988: 72). Davranışçı metodolojiye dayanan çalışmalar genel olarak, karar verme mekanizmaları başta olmak üzere aktör davranışları arasında örüntüler saptamayı ve geleceğe dair öngörülerde bulunmayı amaçlamışlardır. Ölçülebilir veriler ve nicel metodolojiyi temel alan davranışçı yaklaşımı benimseyen araştırmacılar uluslararası ilişkiler ile dış politika analizi çalışmalarının entegrasyonunu amaçlamışlardır (Hudson & Day, 2019: 212). Walker ve öğrencileri ile Mintz ve öğrencileri nicel yöntemleri kullanarak dış politika analizi ve liderlerin karar verme davranışları üzerine çalışmalar yapmışlardır (Geva et al., 2000; Mintz, 1993, 2004; Mintz et al., 1997; Walker, 1981; Walker et al., 1998'den akt. Day & Hudson, 2019: 212). İnsan beyninin modellenmesi ve bulguların sosyal bilimler metodolojisine aktarılması 2010'lu yıllarda gerçekleşmiştir (Poole & Mackworth, 2010).

1970'li yıllarda kural temelli uzman sistemlerin geliştirilmesinden yaklaşık 10 yıllık bir süre sonra, psikolojideki ilerlemelerin de katkısıyla, uluslararası ilişkiler üzerine yapılan çalışmalarda bu yöntemlerin kullanılmaya başlandığı görülmektedir (Johnson, 1977'den aktaran Hudson & Vore, 1995 : 218). İnsan uzmanlarla aynı seviyede doğruluk değerine sahip sonuçlar gösterilebilmiştir. Bireysel davranış ve karar alma süreçlerinden ziyade kurumsal kararlarda kullanımı daha uygundur. Çünkü kurumlar belirli bir kural sistemi içinde karar alır ve bu kurallar uzman sistemlere daha kolay aktarılır (Schrodt, 1988: 78). Kural temelli sistemlerin sorunlu yanı kuralların elle giriliyor olması ya da insan uzmanlarla yapılan mülakatlar sonucu elde ediliyor olmasıdır. Tam da bu sorunu çözen yaklaşım makine öğrenmesi olmuştur. Makine öğrenmesi daha az veri ile çalıştırılabilmekte ve kuralları doğrudan verileri

kullanarak çıkarabilmektedir. Örneğin makine öğrenmesi tekniği kullanılarak geliştirilen bir algoritma aracılığıyla, uluslararası uyuşmazlıkların sonuçları tahmin edilmeye çalışılmıştır. Çalışmada 38 değişken makine öğrenmesi tekniği ile 5'e indirilmiş ve doğruluk değerinde sapma yaşanmamıştır. Çalışmanın sonucunda algoritma uyuşmazlık sonuçlarını %95 oranında doğru tahmin etmiştir (Schrodt, 1988: 78).

Dış politika yapım ve uygulama alanında YZ'nin kullanımı analitik roller, öngörüsel roller ve işlevsel roller olarak üç kategoride incelenebilir (Cummings et al., 2018: 2). Analitik roller, sensörlerin çıktılarını izlemek ve değerlendirmek gibi insanlar tarafından yapıldığında zaman alıcı ve yorucu rutin işlerin makinelere yaptırılmasında YZ'ye yüklenen rollerdir. Örnek olarak hava limanlarında ülkeye giriş çıkış yapan yabancıların, yüz tanıma sistemleri ile kayıtlarının alınıp bir suç kaydının bulunup bulunmadığı, daha önce deport edilip edilmediği gibi verilerin makine tarafından karşılaştırmalı olarak değerlendirilmesi ve tehlikeli gördüğü kişiler için uyarı vermesi amacıyla geliştirilen sistemler gösterilebilir. Ya da göç yönetimi ve politikaları konusunda yaygınlaşmaya başlayan eşleştirme programları örnek olarak gösterilebilir (Beduschi, 2020).

Yapay zekanın dış politika yapım ve uygulama aşamasında yer aldığı bir diğer kategori olan öngörüsel roller uluslararası ilişkilerin karmaşık ve belirsizliklerine rağmen, YZ'nin geleceğe yönelik planlama yapılmasında ve özellikle de müzakere süreçlerinde karşı tarafın davranış ve taktiklerini önceden kestirmeye yönelik amaçlarla kullanılmasıdır (Cummings et al., 2018: 4). Birleşik Krallık - Avrupa Birliği arasında yapılan brexit görüşmeleri ve sonuçları ile görüşmeler sırasında atılan tweetlerin arasındaki ilişkiyi ele alan bir çalışmada 13 milyondan fazla tweet Büyük Veri Analizi ve Duygu Analizi yöntemleriyle incelenmiştir. Çalışma görüşmeler bittikten yaklaşık 6 ay sonra yapılmıştır. Bulgulara göre müzakere sırasında karar vericiler tarafından Büyük Veri Analizi yöntemiyle vatandaş tercihleri ölçülebilir ve kamu politikaları ile vatandaş tercihleri arasındaki boşluğu giderme imkanı bulunabilirdi (Georgiadou et al., 2020). Bir devletin görüşme sırasında elini güçlendirecek ya da zayıflatacak olan kamu oyu desteği ve genel eğilim sadece sosyal medya hesaplarının analizi ile mümkün hale gelmiştir. YZ'ye dayalı öngörüler, uluslararası ilişkiler bakımından önemli görüşmelerde, görüşmenin tarafları için yeni bir araç olarak kullanılabilir.

Operasyonel roller ise YZ destekli botların ya da robotların, insan karar verici ya da uygulayıcıları destekleyici görevler üstlenmek yerine, doğrudan doğruya bir görev ifa etmek için kullanılmasıdır. Bu anlamda öne çıkan hususlar otonom araçların kara, deniz ya da havada kullanılması, robotların askeri alan dahil olmak üzere ekonomik ve güvenlik alanlarında görev

icra etmesi olarak sayılabilir. YZ- Ekonomi ilişkisi başlığı altında ele alındığı gibi robotların üretimde kullanılması işsizlik yaratıcı bir husus olarak görülebilir. Otonom araçların yaygınlaşması da lojistik sektörü başta olmak üzere birçok kişinin işsiz kalması ile sonuçlanabilecektir.

Operasyonel rollerin bu tez çalışması için daha önemli olan kullanım alanı ise otonom araçların güvenlik amacıyla kullanılmasıdır. Takip eden bölümde detaylı olarak ele alınacak olsa da burada operasyonel roller bağlamında otonom sistemlerin güvenlik alanında kullanımına kısa bir giriş yapılacaktır.

Otonom araçlar kendi içerisinde sürücüsüz araçlar ve Otonom Silah Sistemleri (OSS) olarak ikiye ayrılarak incelenebilir. Sürücüsüz araçlar kara, deniz ya da hava araçları olarak geliştirilebilmektedir. Sürücüsüz araçların karar verme mekanizmalarını işletebilmeleri ve doğru kararlar verip bu kararları uygulamaları, belirsizlik durumları ile ters orantılıdır. Dolayısıyla sürücüsüz araç geliştirmek için en elverişli alan hava sahası, en elverişsiz alan ise kara yollarıdır. Çünkü karayollarında sürücüsüz bir aracın hareket halinde bulunduğu yolda, diğer sürücüler, bisikletliler ya da yayalar tüm kurallara uyarak hareket etmediğinden, bu durum belirsizlikler yaratarak doğru karar vermeyi güçleştirmektedir. Günümüzde karayolları için üretilen sürücüsüz araçların sensörleri bisikletlileri algılamakta güçlükler yaşamaktadır. Karayollarında sürücüsüz araç geliştirmek daha çok ekonomik ve ticari amaçlara dayanıyor olsa da, askeri alanda drone olarak da adlandırılan İnsansız Hava Araçlarının (İHA) geliştirilmeye daha elverişli olduğu görülmektedir (Cummings et al., 2018: 7.vd.).

İHA'ların temel kullanım alanı keşif yapmak ve istihbarat toplamaktır. Bu araçlara füze ve bomba başta olmak üzere silahlar eklenebilmekte ve Silahlı İnsansız Hava Araçları (SİHA) üretilebilmektedir. Hemen belirtmek gerekir ki, SİHA ve OSS üst kategoride birer robot olarak kabul edilse de, temelde birbirinden farklıdır. Ayırt edici husus ise robotun karar verme ve eyleme geçme süreçlerinde insan müdahalesinden ne derecede bağımsız olduğudur. SİHA'larda robot ile fiziksel yakınlıkta bir insan bulunmamakta ancak eyleme geçme süreci insan müdahalesi ile gerçekleştirilmektedir. OSS üzerinde etik kaygılarla beslenen bir uluslararası direnç bulunmakta ve bu sistemlerin askeri sahada kullanımının uluslararası insancıl hukuk kurallarına aykırı olduğu yönünde görüşler ileri sürülmekte ve durdurulması için kampanyalar yürütülmektedir. Bu konu detaylı olarak II.B başlığında ele alınacaktır.

Güvenlik alanında operasyonel roller bağlamında YZ'nin bir diğer kullanım şekli ise siber saldırılardır. Siber saldırı fiziksel alanda gerçekleştirilen saldırıların, siber uzay adı verilen

ve tüm teknolojik cihazların etkileşim içinde olduğu kabul edilen soyut bir alanda veya teknolojik cihazların kullanılmasına imkan veren somut kritik altyapılara yöneltilmesidir. Bu konu ve uluslararası güvenlik ile ilişkisine II.C başlığında detaylı olarak yer verilecektir.

Yukarıda teknolojinin özel olarak da YZ'nin teknik özellikleri, uluslararası ilişkiler ile olan bağı ve potansiyel etkilerine yer verilmiştir. YZ'nin etkilerinin devletlerin güvenlik paradigması ve dış politikalarına olan etkisini incelemek için Askeri Alanda Devrim literatürünü incelemek yerinde olur. Söz konusu literatür bağlamında YZ – Uluslararası güvenlik ilişkisi kurulabilecek ve devletlerin politikalarını değerlendirmek için kuramsal çerçeve oluşturulabilecektir. Takip eden bölümde öncelikle askeri devrim ve Askeri Alanda Devrim kavramları açıklanacak ardından YZ etkisiyle ortaya çıkan güvenlik sistemleri ile Askeri Alanda Devrim kavramı ilişkilendirilmeye çalışılacaktır.

II. BÖLÜM : ASKERİ ALANDA DEVRİM VE YAPAY ZEKA

Bu bölüm üç başlıkta kurgulanmış olup ilk olarak Askeri Devrim (Military Revolutions - MR) – Askeri Alanda Devrim (Revolutions in Military Affairs - RMA) kavramlarına yer verilecek farkları ve ayırt edici özellikleriyle RMA kavramı açıklanacaktır. Ardından YZ desteğiyle geliştirilen ve Otonom Silah Sistemleri ve Siber Güvenlik kavramları ele alınıp incelenecektir. Bu bölümün amacı MR - RMA dalgaları çerçevesinde yeni bir dalga olarak kabul edilebilecek yeni teknolojileri incelemektir. Bu tez çalışmasının temel amacı YZ'nin Uluslararası İlişkilerde, özel olarak da uluslararası güvenlik alanındaki etkisini tanımlamak ve büyük güç siyasetindeki yansımalarını incelemektir. Bu nedenle tezin argümanının dayanacağı temel Askeri Alanda Devrim literatüründeki çalışmalar olacaktır.

A) Askeri Alanda Devrim Kavramı (*Revolution in Military Affairs -RMA*) ve Yapay Zeka

Teknolojik gelişmelerin güvenlik araçları ve askeri sistemler üzerindeki etkilerine odaklanan çalışmaların ilk örnekleri 20. Yüzyılın ikinci yarısında ortaya atılmış ve yüzyılın son 10 yılından itibaren bir literatür oluşmaya başlamıştır. Literatürde öne çıkan çalışmalar Askeri Devrimler *(Military Revolutions - MR)* ve Askeri Alanda Devrimler *(Revolutions in Military Affairs - RMA)* olmak üzere iki kavramsallaştırma üzerinden konuya yaklaşmaktadır.[9] Bu bölümün iki alt başlığında öncelikle MR – RMA ayrımına değinilecek, RMA kavramını farklı kılan hususlar hakkında literatürde ileri sürülen argümanlara yer verilecektir. Ardından RMA dalgaları olarak değerlendirilen gelişmeler aktarılarak kırılma noktaları tespit edilmeye çalışılacaktır.

1. RMA Kavramının Tarihsel Gelişimi ve MR Kavramıyla Arasındaki İlişki

RMA çalışmaları, bir tarihçi olan Michael Roberts'in Queens Üniversitesi'nde 1955 yılında verdiği bir ders ile başlamış ve 90'lı yıllara gelindiğinde 16. Ve 17. Yüzyıllarda ki Askeri Devrimlere *(MR)* odaklanılmıştır (Murray, 1997). Literatürde RMA kavramına yüklenen anlamın açıklanabilmesi için MR kavramının öncelikli olarak ele alınıp incelenmesi gerekir. Çünkü RMA, MR üzerine inşa edilmiş bir kavramdır.

a) Askeri Devrim (Military Revolution - MR)

Askeri Devrim (MR), yeni bir teknolojinin çatışmanın yürütülmesini ve kararkterini temel olarak değiştirecek bir biçimde, yenilikçi operasyonel konseptler ve örgütsel uyum ile

[9] Kavramların Türkçe karşılıkları anlam karmaşası yaratabileceğinden dolayı çalışmanın devamında büyük ölçüde MR ve RMA kısaltmaları kullanılacaktır.

birleştirilerek önemli sayıda askeri sistemlere uygulandığında ortaya çıkan şeydir (Krepinevich, 1994: 30). Yukarıdaki ifadeden de anlaşılabildiği gibi Krepinevich'e göre bir MR 4 unsurdan oluşur. Bu unsurlar şunlardır: teknolojik değişim, sistemlerin gelişimi, operasyonel yenilik ve örgütsel uyum (Krepinevich, 1994: 30). Krepinevich 14. yy'dan eserini yazdığı 1994 yılına kadar 10 tane MR gerçekleştiğini ifade etmekte ve bu devrimleri şu şekilde sıralamaktadır (Krepinevich, 1994):

- Piyade devrimi (100 yıl savaşları /1337-1453)
- Top devrimi (100 yıl savaşları /1337-1453)
- Kale/Hisar Devrimi (16.yy)
- Tüfek ve Barut Devrimi (16.yy ortaları)
- Napolyonik Devrim (hızlı hareket edebilen ordu, yıldırım harekatları)
- Fransız Devrimi (Ulus için savaşma ve işgale karşı kitlesel askere alma)
- Kara Savaşları Devrimi (demiryolları ve telgraf kullanımı/ABD içsavaşı, Kırım Savaşı)
- Deniz Devrimi (19.yy ortaları, buhar gücünün gemilerde kullanımı)
- İki Savaş Arası Devrimler (makineleşme, havacılık ve bilgi 1918-1941)
- Nükleer Devrim (Soğuk savaş dönemi)

14. yüzyıldan itibaren sürekli gelişen teknolojinin askeri devrimler üzerinde her zaman doğrusal bir etkisi olmayacağına ilişkin görüşlerini açıklarken Krepinevich yukarıda yer verilen devrimlerden çıkarılabilecek 7 ders olduğunu ifade etmektedir.

Krepinevich, ilk olarak yeni ortaya çıkan teknolojiler ile askeri devrimler arasındaki ilişkiyi ele almaktadır. Buna göre her ne kadar teknolojiler askeri devrimleri mümkün kılan gelişmeler olsa da teknolojinin tüm potansiyelini farketmek yeni süreçleri ve örgütsel yapıları gerektirmektedir. Bu argümanın dayanağı olarak, II. Dünya Savaşı sırasında büyüklükleri benzer olan Alman ve Müttefik kuvvetler orduları arasındaki mücadeleyi göstermektedir. Çünkü yeni operasyonel konseptleri başarıyla uygulayabilen Alman Ordusu 6 haftada Fransa'yı işgal edebilmiştir.

Krepinevich'in vurguladığı ikinci ders, MR'nin rekabetçi avantajları kısa süreli olup ilk başta avantaj sağlasa da uzun vadede göreceli bir avantaj seviyesine düşer (Krepinevich, 1994: 37). 19.yy Deniz Devrimi'nde Fransız inovasyonlarının Britanya tarafından edinilip daha üst seviyeye taşınarak denizel üstünlük sağlaması bu duruma örnek gösterilebilir. Üçüncüsü ise kaynaklar üzerindeki sınırlar, potansiyel düşmanların sayısı, ulusal hedefler ve stratejik kültürler arasındaki asimetriler uzman rakiplere fırsatlar verebilmektedir. Dördüncü olarak

savaş ile savaşta devrim arasında ayrım yapmaktadır. II. Dünya Savaşı'nda olduğu gibi savaş bazı spesifik teknolojilerin farkındalığını ortaya çıkartarak devrimi tetikleyebilir. Bir diğer ders rakip avantajları farketme hızı ile kesinlik arasındadır. Bu hususstaki örnek olay ise şudur: Amerikan İçsavaşı'nda taraflar savaşın başında demir yolları ve telgraf ile avantaj yakalamış olsalar da yıllar geçtikçe yivli silahlar ve tüfeklerin savaşta kullanımı, avantaj dengesini de rakibin avantajını farketme hızının etkisini de değiştirmiştir (Krepinevich, 1994: 38). Kripinevich'in bir diğer çıkarımı askeri devrimlerin (MR) altında yatan teknolojilerin çoğunlukla askeri sektör dışında geliştirildiğidir. Demir yolları ve telgrafın geliştirilmesinin kural olarak askeri sektör içinden çıktığı söylenemez. Keza kuruluş aşamasında ticari otomotiv ve uçak sanayisinin de askeri sektörden ziyade ticari sektörle yakın ilişkili olduğu söylenebilir. Askeri teknolojilerden yazarın çıkardığı son ders ise Askeri bir devrimin maliyeti ile sağladığı ekonomik fayda arasında uçurum olmadığı, harcanan paranın karşılığının alındığı yönündedir (Krepinevich, 1994: 40).

b) Askeri Alanda Devrim (Revolution in Military Affairs - RMA)

Murray ve Knox (2001) eserlerinde MR – RMA ayrımını belirginleştirecek argümanlar sunmuşlardır. MR'ın tanımlayıcı özelliği savaşın yapısında esaslı değişiklikler yapmasıdır. Yazarlara göre MR, kontrol edilemez, tahmin edilemez ve öngörülemezdir. Ayrıca bu tür teknolojiler toplumda ve siyasette sistemik değişikliklere neden olurlar. Avrupa özelinde MR kapsamında etkili olan 5 MR şu şekilde özetlenebilir (Murray & Knox, 2001: 6):

- Disipline edilmiş askeri güce bağlı olarak 17. yy'da modern ulus-devletin yaratılması.
- 18.yy sonlarında kitlesel politikalar ve savaşı birleştiren Fransız Devrimi.
- 18.yy sonlarında silah, yiyecek, kıyafet, ücret gibi faydaları mümkün kılan ve kitlelerin hızla savaş alanına kaymalarına yol açan Sanayi Devrimi.
- Fransız ve Sanayi Devrimleri'nin miraslarını birleştiren I. Dünya Savaşı.
- Soğuk savaş döneminin temel meselesi nükleer silahların ortaya çıkışı.

Fransız Devrimi ile Kral yerine Ulus'un geçmesi fikri ordunun gücünü artırmıştır. Fransa, *"levee en messe"*[10] politikası ile ordusunu bir yıldan az bir sürede 3 katına çıkarmıştır. Sanayi Devrimi'nin özellikle İngiltere'ye kazandırdığı finansal güç Napolyon'a karşı kurulan ittifakın destekçisi olmuştur. Sanayi Devrimi'nin bir diğer önemli etkisi Kırım Savaşı ve Amerikan

[10] İşgal karşısında kitlesel askere alma politikası.

İçsavaşında ilk kez kullanılan yivli tüfekler, buharlı gemiler, telegraf ve demir yolu gibi teknolojiler savaşın niteliği ve sürdürülmesi üzerinde etkili olmuştur (Murray & Knox, 2001: 9-10).

Askeri Devrimler (MR) kapsamında ele alınan konular ve gelişmeler gerek Krepinevich'in çalışması gerekse Murray ve Knox'un eserinde benzer hususları öne çıkarmaktadır. Özellikle Krepinevich'in MR unsurları olarak saydığı teknolojik gelişim, sistemlerin gelişimi, operasyonel yenilik ve örgütsel uyum; Murray ve Knox'un çalışmasından referansla yukarıda sıralanan 5 MR için de geçerlidir. Dolayısıyla ortaya çıkan bir teknolojinin Askeri Devrim bağlamında değerlendirilebilmesi için Krepinevich tarafından vurgulanan ve Murray & Knox tarafından da desteklenen dört unsur güvenilir inceleme kriterleridir.

Bütüncül değişikliklerden daha az dönüşümü vurgulamak için ortaya atılan kavram ise Askeri Alanda Devrim (RMA) kavramıdır. Esasen RMA kavramı Sovyetler Birliği teorisyenleri tarafından 1970'li yıllarda benzer durumları tanımlamak amacıyla kullanılan Military Technological Revolution (MTR) kavramına karşılık olarak üretilmiştir (Martyanov, 2019: 69. vd.).

Tatmin edici bir RMA tanımına Murray ve Knox 'un eserinde rastlamak mümkündür (Murray & Knox, 2001: 179): "*RMA, silahlı kuvvetlerin doktrin, taktikler, süreçler ve teknolojideki değişiklikleri ilgilendiren yeni kavramlar geliştirdikleri inovasyon periyotlarıdır."* RMA, savaşa ya da özelleştirilmiş bir savaş altdalına yeni bir kavramsal yaklaşım uygulamak amacıyla; teknolojik, doktrinel, taktik ve örgütsel yenilikleri birleştirmeyi gerektirir (Murray & Knox, 2001: 12). Bu ifadeden ve yukarıdaki tanımdan anlaşıldığı şekliyle RMA'yi MR'dan ayıran en temel farklar sürece dair sistemli ve iradi müdahalenin varlığı ile taktik ve stratejinin vurgulandığı doktrinel bir değişimi gerektirmesidir. Yukarıda yer verildiği gibi MR öngörülebilir ya da kontrol edilebilir teknolojilerden oluşmaz. Dolayısıyla da MR konusu olayın sistemli bir planın/stratejinin ya da doktrinin parçası olması beklenemez. Halbuki RMA doğası gereği doktrinel bir değişimin ve stratejinin varlığını gerektirir.

RMA, MR'dan bağımsız olmamakla birlikte bir Askeri Devrim (MR) içinde birden fazla Askeri Alanda Devrim (RMA) olduğu/olabileceği görülmektedir. Çünkü MR çerçevesinde ortaya çıkan bir durum üzerine farklı taktik ve stratejik değişiklikler planlamak, doktrinel kavramlar çerçevesinde duruma yaklaşmak mümkündür. Bu nedenle de bir MR devresinde birden çok RMA olabilmektedir. Örneğin; İngiltere'nin Sanayi Devrimi sonrası elde etmeye başladığı geliri, finansal ve ekonomik güç olarak kullanmak bir doktrin ve strateji

gerektirdiğinden dolayı RMA olarak değerlendirilebilir. Diğer yandan Sanayi Devrimi'nin bir diğer çıktısı olan taşımacılık da RMA içinde değerlendirilebilir. Yani bir askeri devrim olarak ele alınan durumun üzerine taktik ve stratejiler geliştirerek birden fazla RMA elde etmek mümkündür (Murray & Knox, 2001: 13).

RMA'lerin itici gücü teknolojiden ziyade politika ve strateji kavramlarıdır (Gray, 2005: 59; Murray & Knox, 2001: 179). Başka bir deyişle aynı teknoloji benzer nitelikteki farklı devletlerin elinde olsa da, ortaya konulacak politik davranışın aynı olması beklenemez. Çünkü RMA determinist bir biçimde aynı teknolojinin aynı yöntemlerle kullanılması ve aynı sonuçların alınması gibi bir eşitlik vaaz etmez. Aksine doktrinel görüşler ve stratejiler aynı zamanda ilgili devletin politik kültürü ve jeopolitik konumunun da etkisinde gelişeceğinden dolayı, farklı politika tercihleri mümkün olacaktır (Gray, 2005: 211; Krepinevich & Watts, 2015: 226).

Askeri Devrimler (MR)	**Askeri Alanda Devrimler (RMA)**
MR1: 17. yy Ulus Devletlerin ve modern askeri kurumların kurulması.	*Alman ve İsveç Taktik reformları, Fransız taktik ve örgütsel reformlar, Deniz Devrimi, İngiltere Finansal Devrimi *7 yıl savaşlarını takiben Fransız Askeri Reformları
MR2-3: Fransız ve Sanayi Devrimleri	*Ulusal siyasi ve ekonomik hareketlilik, Napolyonik Savaşkanlık, Sanayileşmeye dayalı finansal ve ekonomik güç. *Savaşta ve taşımacılıkta teknolojik devrim (demiryolu, telgraf, buharlı gemi, seri ateşli top…), deniz savaşlarında devrim: büyük silahlar, savaş gemileri ve donanma.
MR4: Birinci Dünya Savaşı	Birleştirilmiş silahlar, taktikler ve operasyonlar. Yıldırım Harekatı operasyonları, Stratejik bombalama, taşıyıcı, denizaltı ve amfibi savaşları, radar ve istihbarat sinyalleri.
MR5:Nükleer Silahlar ve Balistik Füze Gönderim Sistemleri	Hassas izleme ve saldırı, bilgisayarlaşma ve bilgisayar ağlarının komuta ve kontrolü, geleneksel mühimmatların öldürücülük seviyelerinde artış, gizlilik.

Tablo I. MR-RMA ilişkisi. (Murray & Knox s.13'ten esinlenilerek hazırlanmıştır.)

Takip eden bölümde RMA dalgalarına yer verilerek bir RMA dalgası tanımlaması yapabilmek için gerekli kriterler gözlenmeye çalışılacaktır. Ardından bu kriterler çerçevesinde OSS ve Siber Güvenlik değerlendirilecek olup, hem MR-RMA tartışmasındaki konumları hem de RMA dalgası olabilme potansiyeli bakımından tartışılacaktır. MR ile RMA arasındaki farkın belirginleştirilmesi bu tezin oluşturulması bakımından önemlidir. Çünkü YZ'nin nasıl ve ne yönde etki edeceğini saptayabilmek ve bu etkileri tanımlayabilmek için ayırt edici faktörler belirlemek gerekmektedir. Yukarıda yer verilen kavramsal açıklamalardan çıkarılabileceği üzere; bir teknolojinin etkilerinin MR kapsamında değerlendirilebilmesi için belirsizlik ve önlenemezlik faktörleri öne çıkarken; RMA kapsamında değerlendirebilmesi için öne çıkan faktörler, ilgili teknolojik gelişmeye bağlı olarak devletlerin politika, strateji ve doktrin düzeyinde değişiklikler ortaya koymalarıdır.

2. RMA Dalgaları: Yeni Teknolojiler ve Yeni Rakip Olarak Çin

Yeni ortaya çıkan bir teknolojinin üzerine inşa edilen RMA'lar, teknolojinin niteliğine bağlı olarak farklılıklar içermektedir. Dönemsel olarak yapılan sınıflandırmalardan yararlanarak söz konusu teknolojinin niteliği ile RMA dönemi arasında ilişki kurulabilir. Belirli bir dönemde teknoloji güvenlik ilişkisini domine eden periyotları tanımlamak için RMA dalgaları kavramı kullanılabilmektedir. Raska (2021) çalışmasında 5 tane bilgi teknolojilerinde RMA (IT-RMA) ve son olarak da YZ'de RMA dalgalarını ele almıştır. Bu dalgalar incelenerek genel olarak YZ'nin özel olarak da Otonom Silah Sistemleri ve Siber Güvenlik araçlarının RMA dalgaları içinde konumlandırılması mümkündür. Raska'nın dalga sıralaması şu şekildedir:

- 1. RMA Dalgası: Elektronik Savaşkanlık & MTR
- 2. RMA Dalgası: ABD Ordusunda kavramsal uyum
- 3. RMA Dalgası: Bilgi Savaşı IT-RMA Technophilia
- 4. RMA Dalgası: Savaşın Dijitalleşmesi & Savunmanın Dönüşümü
- 5. RMA Dalgası: Hibrit Savaş ve Modernizasyon
- 6. RMA Dalgası: Otomatize edilmiş savaş ve Stratejik rekabet.

Sırasıyla bu dalgaların öne çıkan yönleri incelenecektir.

1980'li yılların başında Sovyet stratejistleri MTR kavramını kulanarak ilk dalga RMA tartışmalarını yürütmüşlerdir (Martyanov, 2019: 69). Gorbaçov'un 1984 yılındaki savunma ve ulusal güvenlik ilişkilerinde "yeni düşünce" çağrısı üzerine askeri ve sivil teorisyenler MTR kapsamında görüşler ileri sürmeye başladılar. ABD'nin hassas güdümlü füze ve elektronik harp

süreçlerinde kendilerinden daha ileride olduğunu bilen Sovyet düşünürler "geleceğin savaşları" konseptine odaklandılar. Bu tartışmaların çıktısı olarak iki operasyonel kavram geliştirdiler: 1) RSC: Keşif-Saldırı Kompleksleri *(Reconnaissance-Strike Complexes)*. 2) OMG: Operasyonel Manevra Grupları (Raska, 2021: 462 v.d.). İkinci RMA dalgası ABD'nin askeri düzenine uyarlama yapma sürecini içermektedir. Bu konu III.A-4 başlığında detaylı olarak ele alınacaktır.

Üçüncü dalga ise 1990'lı yıllarda, ABD'nin daha düşük maliyetlerle yeni teknolojilerden faydalanarak askeri gücünün etkinliğini nasıl artıracağı sorusuna odaklanmıştır. Bu kapsamda Amiral Wiiliam Owens tarafından geliştirilen sistemler sistemi yaklaşımı RMA için operasyonel vizyonu şekillendirmiştir. Bu kavramla şemsiyesi altında geliştirilen diğer kavramlar ise C4I ve DBK olmuştur (Raska, 2021: 464). C4I[11], karşılıklı hizmet platform ve sistemlerinde komuta, kontrol, bilgisayarlar, iletişim ve bilgi sistemlerini; istihbarat, izleme ve keşif sistemleriyle eşleştirmek anlamında kullanılmaktadır. DBK ise Baskın Savaş Alanı Bilgisi *(Dominant Battlespace Knowledge)* anlamında kullanılmıştır (Raska, 2021: 464 v.d.). Bu dönemin genel özelliği bilgi istihbaratı ve bu bilgiler çerçevesinde ABD'nin RMA yaklaşımını teknolojik, örgütsel, yapısal ve doktrinel yönleriyle oluşturmaktır.

Dördüncü dalga 2000'li yılların başlarında savaşın dijitalleşmesi ve savunma dönüşümü başlığı altında ele alınmış olup, savunmada dönüşüme yönelinmesinin temel sebepleri 11 Eylül saldırılarının bu döneme denk geliyor olması ve devlet dışı aktörler ve asimetrik tehditlerin yükselmiş olmasından kaynaklanmıştır. Doktrin düzeyinde insansız hava araçlarının ordu tarafından kullanılmasının temelleri atılmış, siber uzay ve küresel izleme sistemleri çalışmaların gündemine girmiştir. Ortaya atılan kavramlar ise NCW ile EBO kavramlarıdır. NCW ağ merkezli savaş *(Network-Centric Warfare),* EBO *(Effect-Based Operations)* ise Etki Temelli Operasyonlar anlamında kullanılmaktadır (Raska, 2021: 466-467). Dördüncü dalganın önemi YZ'nin askeri alanda kullanılmaya başlanmasının ilk örneklerini oluşturmasından kaynaklanmaktadır.

Beşinci dalga, 2000'li yılların ortasından sonlarına doğru IT-RMA yaklaşımı fayda-maliyet ikilemine sıkışmış ve savunmada dönüşüm üzerine ileri sürülen görüşler başarılı bir şekilde uygulamaya geçirilememiştir. Temel motivasyon ağ temelli yetkinliklerin uygulanması iken, sadece ABD'de değil batı dünyası ve NATO başta olmak üzere bu dönemde aynı amaçla RMA

[11] C4I: Command, Control, Computers, Communications and Information Systems kelimelerinin baş harflerinden türetilmiştir.

faaliyetleri yürüten diğer devletlerde de örgütsel, teknolojik ve özellikle de bütçe güçlükleriyle karşılaşılmıştır (Raska, 2021: 468-469).

Altıncı dalga otomatikleştirilmiş savaş ve stratejik rekabet çerçevesinde ortaya çıkmıştır. 2010'lu yıllarda gelişen teknolojilerin askeri alana uyarlanması dönemin temel karakterini oluşturmaktadır. Raska'ya göre bu dönemin üç temel itici gücü bulunmaktadır. Bunlar şöyle özetlenebilir: i) Dünyanın büyük güçleri arasında siyasal, ekonomik ve askeri-teknolojik üstünlüğü için stratejik rekabet. Üçüncü dalga RMA rekabetinin büyük oranda ABD- Çin arasında geçiyor olması nedeniyle bu tez çalışmasında incelenen iki devlet ABD ve Çin olarak belirlenmiştir. Anılan iki devlet kadar aktif ve belirleyici olmamakla birlikte Rusya da rekabetin bir diğer aktörü olarak kabul edilebilir. ii) Askeri teknolojideki yeniliklerin beslendiği kaynaklarda değişimin meydana gelmiş olması. Şöyle ki; YZ, bilişsel manüpülasyonlar, insan-makine etkileşimi ve siber alanı da içine alan bilimsel gelişmeler hız kazanmıştır. Askeri sektör dışında gelişen bu bilimsel çalışmaları askeri alana uyarlamak yeni RMA dalgasının konusunu oluşturmuştur. iii) Ortaya çıkan teknolojilerin çifte kullanım özelliği bir yönünü bilimsel ve ticari çalışmalara dayandırmakta, diğer yönünü ise askeri alanda otonom ve YZ destekli gelişmelere dayandırmaktadır. Bu durum sadece büyük güçlere değil aynı zamanda küçük devletler ve orta büyüklükteki güçlere de avantaj sağlamaktadır. Raska ilk beş RMA dalgası ile son dalga arasındaki farkları üç maddeyle sunmaktadır. Bu farklılıklar özetle şöyledir (Raska, 2021: 458):

- ABD on yıllardır ilk kez Doğu Asya başta olmak üzere jeopolitik olarak ve kendi YZ-RMA modellerini geliştiren stratejik bir rakip olarak Çin ile karşı karşıya kalmıştır.
- Gelişmiş askeri-sanayi sektörleri artık yeni teknolojinin birincil itici gücü değildir. Bunun temel nedeni teknolojinin çifte kullanım özelliğine sahip olması ve ticari amaçlarla geliştirilmesinin daha öncelikli olmasıdır. Bu sayede küçük devletler ve orta büyüklükteki güçler hem ekonomik rekabette hem de askeri modernizasyon süreçlerinde avantajlı konuma gelebilmektedirler.
- Otonom silahların ve YZ destekli sistemlerinin yayılması gelecek savaşlardaki insanın konumu hakkında meydan okur niteliktedir.

RMA dalgaları birlikte değerlendirildiğinde; öncelikle ortaya çıkan teknolojinin askeri alana uyarlanması sürecinde önceliklerin nasıl belirleneceği hususunda, karar vericiler uluslararası politik ortam, tehdit tanımlamaları, rakiplerin kabiliyet ve kapasiteleri gibi sınırlılıklara sahiptirler. Bunun yanısıra teknolojinin imkan tanıdığı politikalar da belirleyici

olmaktadır. İlk iki dalgada ortaya çıkan politikalar üzerinde Sovyet RMA çalışmalarının büyük etkisi görülmektedir. Üçüncü dalgada ABD'nin politika oluşturma sürecinin merkezinde, rakiplerinin RMA çalışmaları hakkında topladığı istihbaratlar bulunmakta olup, dahası politikalar mevcut teknolojileri kullanarak daha fazla istihbarat toplamaya odaklanmaktadır. Dördüncü dalgada uluslararası ortamın RMA çalışmaları üzerindeki etkisi gözlenmektedir. Beşinci dalga bir yönüyle sınırlılıkları ortaya koyarken, diğer yönüyle Bilgi teknolojileri temelli RMA çalışmalarının beklenen faydaları sağlamadığını göstermiştir. Tam da bu nedenle altıncı dalga RMA ve bunun altında yatan teknoloji önem kazanmakta yeni dalganın nasıl şekilleneceği, politikaların başarıya ulaşıp ulaşamayacağı önem kazanmaktadır. Tez çalışmasının iddiası geleceğe yönelik bir projeksiyon geliştirmek ya da başarı olasılıklarını hesaplamak olmamakla birlikte, bu çalışmayla altıncı dalganın, ilk 5 dalgadan ayrılan yönlerini ve mevcut durumunu tespit etmek mümkündür.

Son RMA dalgası ise çift yönlü bir özellik taşımaktadır. Bunlardan ilki Otonom Silah Sistemleri ve Siber Uzay gibi YZ temelli yeni mücadele alanlarının üzerinde şekilleniyor olmasıdır. Diğer özelliği ise Çin'in ABD'ye stratejik rakip olabilecek potansiyele sahip olup olmadığı meselesidir. OSS ve Siber güvenlik konularının teknik özellikleri ve gelişim evrelerine takip eden başlıklarda yer verilerek son RMA dalgasının teknolojik alt yapısı açıklanacaktır. Çin'in RMA çalışmaları ve ABD'ye rakip olabilme potansiyeli ise III./B-4 başlığı altında değerlendirilecektir. ABD-Çin stratejik rekabetinin mücadele alanı olarak değerlendirilmesi mümkün olan YZ-RMA dalgasının önemi ve sınırları, iki devletin OSS ve Siber Güvenlik alanlarında birbirlerine karşı konumlanmalarının incelenmesiyle anlaşılabilir.

B) Otonom Silah Sistemleri (OSS)

Bu başlık iki alt başlıktan oluşmaktadır. İlk başlıkta OSS kavramı, tanım ve türleri açıklanacaktır. Ardından tam otonom silah sistemlerine yönelik etik ve hukuki kaygılarla şekillenen eleştirilere yer verilecektir. Bu bölümün amacı OSS teknolojilerinin niteliğini saptayarak, OSS'nin etkilerini tartışmak için teknik bilgileri edinebilmektir. Çünkü YZ-RMA dalgasının altında yatan teknolojilerden biri OSS'lerdir.

1. OSS kavram, tanım ve türleri

Otonom Silah Sistemleri üzerine yapılan tanımlar incelendiğinde ortak özelliklerine göre üç grup oluşturulabilir. İlk grup, insan-makine arasındaki kontrol ve yönetim ilişkisini temel alarak bir silah sisteminin otonom olup olmadığına karar vermektedir. ABD Savunma

Bakanlığı *(DoD - Deparment of Defence)* ve İnsan Hakları İzleme Örgütü (*HRW - Human Rights Watch organization)*, OSS'yi bu tanım kapsamında değerlendirmektedir (DoD, 2012b; HRW, 2012).

İkinci grup Birleşik Krallık tarafından benimsenen yetenek parametrelerini değerlendiren tanımdır. Buna göre OSS, *"daha yüksek niyet ve yön anlama yeteneğine sahip sistemlerdir" (Unmanned Aircraft Systems, 2017)* . Birleşik Krallık Savunma Bakanlığı tarafından hazırlanan raporda, sistemin tanımlanabilmesi bağlamında en önemli vurgu otomatik (automated) sistemler ile otonom (autonom) sistemler arasında ayrım yapılmasıdır. Otomatik sistemler önceden girilen verilerin belirli bir mantıksal yöntem izleyerek çıkarımda bulunmasıdır. Bu nedenle otomatik sistemlerin çıkarımda bulunacağı sonuçlar öngörülebilirdir. Ancak otonom sistemler çevreyi algılama ve yeni koşullara göre karar verme gibi önemli yeteneklere de sahip olduğu için varacağı sonuçlar genel olarak öngörülebilir olsa da, bazı durumlardaki tekil sonuçlar öngörülemez (*Unmanned Aircraft Systems*, 2017: 13).

Üçüncü grup tanım ise Uluslararası Kızılhaç Komitesi'nin geliştirdiği makinenin sahip olduğu hayati işlevlere odaklanan tanımdır. Hayati işlevler olarak görülen işlevler ise insan müdahalesi olmadan robotun seçim, saldırı ve hedefleme yapabilmesidir. Stockholm Uluslararası Barış Araştırmaları Enstitüsü *(SIPRI – Stocholm International Peace Research Institute)* ise bu üç grup tanımdan çıkartılabilecek karma bir tanımın üç unsurunu saptamaktadır. Buna göre OSS tanımı yaparken; makine üzerindeki denetimin süresi ve derecesi, robotların davranışlarının tahmin edilebilirliği ve robotların kullanıldıkları çevrenin karakteristik özellikleri göz önünde bulundurulmalıdır (Verbruggen & Boulanin, 2017: 22 v.d.).

Tanımların çeşitli yönlerden robotları ele almasının nedeni robotların tek tip olmamasından kaynaklanmaktadır. Her robotu ya da silah sistemini öne çıkaran hem avantaj hem de dezavantajlar bulunmaktadır. Literatürde genel olarak yer verilen tanım DoD ve HRW tarafından kullanılan birinci grup kapsamındaki tanımlardır (Ersoy, 2018: 20 v.d.; Leys, 2018: 51 v.d.; Scharre, 2020: 73 v.d.).

Genel kabul gören tanımın robotların sınıflandırılmasında kullanılması ise *OODA (Observe – Orient- Decide – Act / Gözlemle -Odaklan – Karar ver – Harekete Geç)* döngüsü adı verilen bir döngüye dayanmaktadır. Esasen OODA döngüsü YZ ve OSS öncesi dönemde, ABD Hava Kuvvetleri'nde pilot olarak görev yapan ve aynı zamanda bir askeri stratejist olan John Boyd tarafından geliştirilmiş bir teoridir. Teoriye göre sadece askeri alanda değil, tüm karar alma birimlerinde OODA döngüsü işlemektedir. Döngünün zamanını kısaltan ve

rakibinin/döngüsünü kıran taraf kazançlı çıkar. YZ döngünün zamanını kısaltma anlamında OODA teorisine katkı sunmaktadır. Bunun ötesinde OSS sınıflandırmasında da OODA döngüsü içinde insanın konumu belirleyici olmaktadır. İnsanın döngüdeki konumuna göre üç tür OSS olduğu kabul edilmektedir: i) İnsanın döngü içinde olduğu yarı otonom sistemler *(human in the loop)*, ii) insanın döngünün üstünde olduğu denetimli otonom sistemler *(human on the loop)* ve iii) insanın döngü dışında olduğu tam otonom sistemler *(human out of the loop)* (Ersoy, 2018; Leys, 2018; Scharre, 2020).

Döngünün içinde insanın var olması sistemi yarı otonom hale getirir. Otonom sistemler OODA döngüsü ile benzer biçimde sez - karar ver- uygula döngüsü içinde hareket ederler. Yarı otonom bir sistem çevreyi algılar ancak harekete geçemez. Harekete geçme kararını insan verir. İnsanın verdiği karar makine tarafından uygulanır. Yarı otonom sistemlerin tipik örneği, angajman kuralları ve hava savunma sistemi radarlarıdır. Tehdit tanımlaması yapıldıktan sonra radar alarm verir ve insan tarafından harekete geçmesi kararlaştırırsa, angajman kurallarına göre ihlali gerçekleştiren nesne ya da insan hedefe karşı eyleme geçilir (Scharre, 2020: 58). Bu sistemin faydasına yönelik olarak klasik Yarbay Petrov örneği verilebilir.

1983 yılının Eylül ayı dönemin iki süper gücü arasında gerilimin çok yüksek olduğu bir dönemdi (Barrass, 2016: 16; Scharre, 2020: 23). Çünkü; Ruslar hava sahalarını ihlal ettiği gerekçesiyle bir Amerikan uçağını düşürerek, biri ABD milletvekili olmak üzere 269 kişinin ölmesine neden olmuşlar ve bir misilleme yapılmasından endişe duyuyorlardı. Bu endişeyi gidermek için Oko isimli bir uydu temelli erken uyarı alarm sistemi kurdular. 23 Eylül 1983 gecesi Yarbay Petrov'un görevli olduğu radar sistemi ABD'nin, SSCB'ye karşı bir nükleer füze ateşlediği uyarısını verdi. Teknik olarak Petrov'un yapması gereken üstlerine haber verip, karşı nükleer saldırı başlatılmasını istemekti. Ancak Petrov ilk etapta sisteme güvenmemiş, beklemeyi tercih etmişti. Ardından sistem ikinci füzenin fırlatıldığı uyarısını vermiş, ardından füze saldırısı uyarısı vererek toplamda 5 füzenin fırlatıldığını göstermişti. Petrov sadece sisteme güvenmemiş, kara radarları ile iletişime geçmeyi tercih etmişti. Kara radarlarının füze algılamaması durumu karmaşıklaştırmış, saldırı altında olup olmadıklarını tespit etmeyi güçleştirmişti. Petrov üstlerini arayıp sistemin hata verdiğini bildirmişti. Gerçekte olan şey bir nükleer saldırı değil, doğan güneş ışınlarının uydu sistemini yanıltmasından ibaretti. Yarı otonom sistemde karar verme yetkisinin bir insanda olması adeta bir faciayı önlemişti (Say, 2021: 144; Scharre, 2020: 23.vd).

İnsanın döngünün üstünde olması durumu, diğer bir deyişle denetimli otonom sistemler kendi başlarına sez - karar ver - uygula döngüsünü tamamlayabilecek niteliktedirler. Bununla

birlikte döngüyü ve robotu gözlemleyen bir insan vardır ve döngünün herhangi bir aşamasında insan müdahalesi mümkündür (Scharre, 2020: 58).

İnsanın döngü dışı bırakıldığı sistemler ise bir kez başlatıldıktan sonra insan operatörle iletişime geçmeden ve insanın sonradan müdahalesi olmadan sez – karar ver – uygula döngüsünü gerçekleştirirler (Scharre, 2020: 59). Tam otonom silah sistemlerinin tehlikelerini işaret etmek amacıyla katil robotlar, öldürücü otonom silah sistemleri gibi isimler de kullanılmaktadır. University of California at Berkeley 'den Stuart Russell[12] bir konferansında hali hazırda var olan tam otonom silah sistemlerine üç örnek göstermektedir. Bunlar kara mayınları, Samsung Sentry Robot ve İsrail yapımı Harop füzeleridir (CITRIS, 2016).

Kara/deniz mayınları tam otonom silah sistemlerinin en ilkel türüdür. Çünkü bir kere kurulduktan sonra insan müdahalesi olmaksızın, özgülendiği amacı gerçekleştirecek biçimde tasarlanmıştır. Genellikle kara/deniz sınır boylarında yasa dışı insan ya da gemi geçişlerini engellemek amacıyla kullanılmıştır. Üzerine basılmasıyla aktif hale gelmekte ve patlamasının etkisiyle, mayını etkinleştiren insan ya da nesneyi yok etmektedir. Kara mayınları 1997 yılında imzaya açılıp, imza tarihinden 2 yıl sonra yürürlüğe giren Ottawa Sözleşmesi[13] ile yasaklanmıştır. Türkiye'nin de 2003 yılında onaylayarak taraf olduğu sözleşmeye, (Aralık, 2021 itibariyle) 164 devlet taraftır. Çalışmada incelenen ABD ve Çin sözleşmeyi imzalamamış, taraf da olmamışlardır (UN, 1997).

Samsung Sentry Robot (SGR-A1), Güney Kore – Kuzey Kore arasındaki askerden arındırılmış bölgenin Güney Kore tarafını gözetlemek ve güvenliğini sağlamak amacıyla üretilmiştir.[14] 2006 yılında üretileceği duyurulup 3 yıl sonra üretilen SGR- A1 tam otonom ve yarı otonom olmak üzere iki ayrı modda çalıştırılabilmektedir. Robot izleme, ses algılama, ateş etme özelliklerine sahiptir (Verbruggen & Boulanin, 2017: 42 v.d). SGR – A1 üreticileri ateşleme kararını vermek için bir insana ihtiyaç duyulduğunu bildirerek, yarı otonom sistem

[12] Stuart Russell, I. Bölümde YZ'nin teknik kısmı açıklanırken baş ucu kitabı olarak kullanılan Artificial Intelligence: A Modern Approach isimli kitabın yazarıdır. Yaklaşık 30 yıldır YZ üzerine çalışan fizikçi, bilgisayar bilimcidir. Ayrıca Dünya Ekonomi Forumu'nun YZ-Robotik komisyonu başkan yardımcısıdır.

[13] Ottawa Sözleşmesi: Sözleşmenin tam adı ***"Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction"*** Oslo'da yapılan konferansın ardından Ottawa'da imzaya açıldığı için Ottawa Sözleşmesi olarak da anılmaktadır.

[14] Çok güvenilir bir kaynak olmamak ile birlikte, bir web sayfasında yer alan bilgilere göre Güney Kore'nin SGR-A1 öncesi sınır güvenliği şu şekilde sağlanmaktaydı. Anılan iki ülke arasındaki askerden arındırılmış bölgenin sınırı yaklaşık 250 km'dir. Sınırın Güney Kore tarafında, her 50m'de 1 tane nöbet noktası yer almakta, her nöbet noktasında 2 tane nöbetçi görevlendirilmekte ve günde 12 vardiya bulundurulmaktaydı. Yaklaşık olarak günde 5.000 insanın koordinasyon ve aktif nöbet tutması ile korunan bir bölgenin güvenliğinin otomasyona aktarılması ekonomik olarak kazançlı görülmüştür. Bkz. https://www.globalsecurity.org/military/world/rok/sgr-a1.htm (erişim tarihi: 20.12.2021).

olduğunu ifade etmişlerdir (Green, 2015). Ancak gerek uzman inceleme raporları (Liu, 2012: 631), gerekse Stuart Russell'in ifadesine dayanarak SGR-A1'in tam otonom kategoride olduğunu kabul etmek gerekir.

SGR – A1'i tam otonom kategoride değerlendirmeyi gerektiren en önemli özelliği, askerden arındırılmış bölgeye giren herkesi dost-düşman ayrımı yapmaksızın, düşman görmesidir (Lin et al., 2008: 19). Kızılötesi sensörleri kullanarak yaklaşık 4 km (2.5 mil) mesafeden gelen insanları algılama yeteneğine sahip olan SGR-A1, bölgeye zorla girmeye çalışan kişileri, yaklaşık olarak 455 metreden (500 yarda[15]) daha fazla yaklaştıklarında tehdit olarak algılamaktadır. Tehdidi bertaraf etmek için iki seçeneğe sahiptir: ya alarm çalmakta ya da ateş açmaktadır (Krishnan, 2009: 72). SGR-A1 2010 yılında yerini Super aEgis II 'ye bırakarak kullanımdan kaldırılmıştır (*retired*) (Verbruggen & Boulanin, 2017: 44). Super aEgis II, SGR-A1 ile benzer çalışma prensibine sahip olup, gece ve gündüz görme mesafesi, atış kalitesi gibi nitelikler bakımından güçlendirilmiştir (Bkz. http://www.dodaam.com/eng/sub2/menu2_1_4.php *Super aEgis II*).

Russell'in tam otonom silah sistemleri kapsamında değerlendirdiği üçüncü robot İsrail yapımı Harop füzeleri diğer ismi ile Harpy dronlarıdır. Bu silah sistemi yarı gezici mühimmat füze sistemi, yarı insansız hava aracı olarak tasarlanmıştır ("The IAI is a disposable half-UAV, half-missile drone system with inherent surveillance capabilities," 2020). Gezici mühimmat sistemleri, belirli bir alan üzerinde hareket ederek potansiyel hedefler arayan ve bulduklarında onları imha eden sistemlerdir (Scharre, 2020: 78). Harpy dronları angajman öncesi insan tarafından herhangi bir hedef belirlenmeden çalışan sistemlerdir. Bu yönüyle yarı-otonom sistemlerden ayrılır. Harpy dronlarının havada kalabilme süresi yaklaşık iki buçuk saattir. 500 km civarında bir araziyi tarama kapasitesine sahiptir. Harpy dronları ile insan operatör arasındaki ilişki şu şekildedir: Harpy dronunu fırlatan insan, genel bir alanda hangi düşman radarlarını tahrip edeceğine karar verir, Harpy ise bu radarlardan hangisini tahrip edeceğine karar verir (Scharre, 2020: 79).

OSS bir sürecin sonucudur. Tarihsel tecrübelerin yazılan kodlara ve eklenen donanımlara aktarılması ile oluşturulmuştur. 1861 yılında Amerikan iç savaşı sırasında, savaş alanında çok fazla insan bulunduğu ve ölümlerin de savaş alanındaki insan sayısı ile ilişkili olduğunu varsayan Gatling, yükleme ve ateşleme için otomasyon kullanan modern makineli tüfeklerin öncüsü olan Gatling silahını geliştirmiştir. Gatling öncesi silahlar dakikada 3 mermi

[15] Yarda bir uzunluk ölçü birimidir. 1 yarda yaklaşık olarak 0.91 metre, 3 fit ve 36 inç uzunluğa eşittir.

atabilirken, Gatling silahı dakikada yüz kattan daha fazla mermi atabilme kapasitesine sahipti (Scharre, 2020: 64-65). Bir silah üretme motivasyonu savaş alanında daha az insana ihtiyaç duyulmasını sağlamak suretiyle ölümleri azaltmak şeklinde ifade edilirken, makineli tüfeklerin tahrip gücünün etkisiyle neden olduğu insan yaralanmaları ve ölümleri eskiye oranla anlamlı biçimde artmıştır. Otonom silah sistemlerinin de insansız mücadeleyi mümkün kılarak, daha az insanın ölümüne ya da yaralanmasını sağlamak bakımından yararlı olacağını savunmak oldukça güçtür.

Geleneksel silah sistemlerinin gerektirdiği uzmanlık bilgisi, örgütlenme biçimi ve askeri doktrinlerin OSS'ler için mevcut haliyle uygulanması mümkün değildir. Hem askeri personelin nitelik ve yetkinliklerinde OSS'leri kapsayacak biçimde bir değişim hem de askeri doktrinlerde OSS'nin gerektirdiği esneklik ve yetki devrinin politika ve strateji düzeyinde ortaya konması gerekmektedir. OSS bir teknolojik yenilik olarak askeri doktrin ve örgütlenme biçiminde değişiklikleri zorunlu kıldığı için YZ-RMA dalgasının teknolojik unsuru olarak kabul edilmelidir. Bir diğer ifadeyle, YZ-RMA dalgasının üzerine kurulduğu teknolojilerden bir tanesi OSS'lerdir.

2. OSS'ye Karşı Etik ve Hukuki Kaygılar

Öldürücü etkiye sahip tam otonom silah sistemleri hem hukuki açıdan hem de etik boyutuyla eleştirilmektedir. Tam otonom silah sistemlerinin yasaklanması amacıyla gerçekleştirilen en ciddi girişim, 13 Kasım 2017 tarihli bir açık mektup hazırlanması ve Geleneksel Silahlar Sözleşmesinin gözden geçirme toplantısında sunulmasıdır (Wareham et al., 2017). Bu mektup öncesinde de benzer amaçla kamuoyuna duyurulan mektuplar da bulunmaktadır[16]. 2017 tarihli mektupta kampanyayı yürütenler, üzerinde anlamlı bir insan kontrolü olmayan robotların yasaklanmasını istemişlerdir. Kampanyanın tam otonom silah sistemlerine *Lethal Autonomous Weapons Systems (Öldürücü Otonom Silah Sistemleri)* diyerek *LAWS* kısaltması kullanması da anlamlıdır. Çünkü uluslararası hukuka vurgu yaparak argümanlarını oluşturmaktadırlar.

Kampanya kapsamında tam otonom silahların yasak silahlar kapsamına alınması önerilmektedir. Geleneksel Silahlar Sözleşmesi'nin 1995 tarihli protokolüyle, üretilmeden ya da kullanıma geçmemesine rağmen önleyici bir biçimde yasaklanan kör edici lazer silahlarını

[16] Autonomous Weapons: An Open Letter From AI&Robotic Researchers, Aralarında Stuart Russell, N. Nilsson, Elon Musk, Stephen Hawking, Steve Wozniak gibi YZ-Robotik alanında ünlü isimlerin de yer aldığı 100'den fazla YZ-Robotik araştırmacısı ve 60'ın üstünde sivil toplum kuruluşu kampanyaya katılmıştır. https://futureoflife.org/2016/02/09/open-letter-autonomous-weapons-ai-robotics/ (erişim tarihi : 20.12.2021)

örnek göstererek, tam otonom silahlar üretilip, kullanılmadan da yasaklanabileceği görüşünü savunmaktadırlar (Wareham et al., 2017).

Akademik çevrelerce de konu tartışılmaktadır. Bu tartışmalarda ileri sürülen argümanları üç grup altında toplamak mümkündür[17]. İlk argüman, uluslararası insancıl hukukun ya da diğer adlandırmasıyla silahlı çatışmalar hukukunun kurucu metinlerinden biri kabul edilen 1949 tarihli Cenevre Sözleşmesi'nin 1977 tarihli ek protokolü m.36'ya dayanmaktadır. Madde hükmüne göre sözleşmeye taraf olan devletler, yeni bir silah ya da araç geliştirecekleri zaman, geliştirmeyi planladıkları silahın anılan sözleşmeye ya da diğer uluslararası insancıl hukuk kurallarına aykırı bir yönünün bulunup bulunmadığını değerlendirme yükümlülüğü altına girmektedirler (Garcia, 2018: 4; Marchant et al., 2011: 297; UN, 1977: 258).

İkinci argüman savaş/çatışma yürütülürken uyulması gereken kurallar *(Jus in Bello)* kapsamında oluşturulmaktadır. Buna göre *Jus in bello* çerçevesinde *ayırt edebilme* ve *orantılılık* olmak üzere iki ilke bakımından konu tartışmaya açılmaktadır. Ayırt edebilme ilkesi savaşçı ile sivillerin ayırt edilebilmesini zorunlu gören ilkedir. Savaş sırasında sivillerin korunması ve savaşın öldürücü ya da yaralayıcı etkilerinden korunmalarını gerekli görür. Orantılılık ilkesi ise kuvvet kullanmayı ortaya çıkartan "haklı neden" ve bu nedeni ortadan kaldırmak için geliştirilen amaçla orantılı bir kuvvetin kullanılması gerektiğini ifade eden ilkedir (Galliott, 2015: 83 v.d.).

Üçüncü argüman silah üstünde anlamlı bir insan kontrolünün bulunup bulunmadığı sorusu etrafında şekillenerek yukarıda anılan orantılılık ilkesinin ihlal edildiği iddiasındadır. Bu görüşe göre; öldürme gücüne sahip olan robotlar ne kadar kuvvet kullanılmasının yeterli olacağını ayırt edebilecek kapasitede olmadığı gibi, saldırının sivillere vereceği zararları da hesaplayamazlar (ÖZER: 262-263; Sharkey, 2012: 119 v.d.; Verbruggen & Boulanin, 2017: 73 v.d.).

Noel Sharkey bir tam otonom silah sisteminin hukuka uygunluğu bakımından beş aşamalı bir değerlendirme kriteri sunmaktadır. Buna göre beş durum saptar;

[17] Kökenlerini Orta Çağ Haklı Savaş teorisinden alan Uluslararası İnsancıl Hukuk iki soruna odaklanır. İlki *Jus ad bellum* yani savaşın haklı bir nedene dayanması ilkesidir. İkincisi ise *Jus in bello*, diğer bir deyişle savaş/çatışma sırasında uyulacak kuralların haklılığıdır. Bkz. Ereker, F. A. GÜVENLİK YAZILARI. https://www.researchgate.net/profile/Uluslararasi-Iliskiler-Konseyi/publication/336926680_Hakli_Savas/links/5dbb1db2299bf1a47b06fb83/Hakli-Savas.pdf ve Walzer, M. (2017). *Haklı Savaş Haksız Savaş* (M. Doğan, Trans.). Alfa.
OSS üzerine yürütülen akademik tartışmalar savaşın haklı nedene dayanması (jus ad bellum) ile ilgilenmemekte, sivillerin korunması başta olmak üzere savaşta uygulanacak kurallar (jus in bello) kapsamında tartışmalar yürütülmektedir.

- Herhangi bir saldırı öncesi insanın, hedef hakkında kastının olması.
- Programın hedefler listesi sunması ve insanın saldırı için seçim yapması,
- Programın hedefi seçmesi, saldırı öncesi insanın onaylaması,
- Programın hedefi seçmesi, insanın veto etmek için kısıtlı zamanının olması
- İnsan müdahalesi olmadan, programın hedefi seçmesi ve saldırıyı başlatması.

Sharkey'e göre ilk iki durum kabul edilebilirdir. Üçüncü durum eğer insanın onay vermesi için yeterli zamanı varsa kabul edilebilir. Son iki durum ise kaza riskleri nedeniyle kabul edilemezdir (Sharkey, 2014: 31).

Tam otonom silah sistemlerinin, etik ve hukuki ihlaller oluşturacağına ilişkin kaygılar genel olarak, bu kategorideki silahların ayırt edici özelliği olan insandan bağımsız ateşleme yetkisinin neden olacağı risklere odaklanmaktadır. Sadece saldırı amacıyla değil, savunma amacıyla kullanılmaları halinde de sivillerin, çevrenin zarar görmesi ya da uluslararası insancıl hukuka aykırı olarak savaşçıların gereksiz acı çekmesine neden olabilecek potansiyele sahiptir. Bununla birlikte, uluslararası kuruluşlar nezdinde açıklanan kaygıları gidermeye yönelik anlamlı bir sonuç elde edilemediği gibi, yakın gelecekte elde edilmesi de kolay değildir. Çünkü OSS, özellikle güçlü devletler açısından ekonomik, politik ve askeri açıdan avantajlı bir silah sistemidir. Bir diğer neden teknolojinin çifte kullanım imkanı sunmasıdır. Geliştirme sürecinde tespit edilmesi ve müdahale edilmesi teknik olarak mümkün olan nükleer silahların aksine, tam otonom silah sistemlerinin geliştirme sürecinde tespiti oldukça zordur. Bu zorluk hem silahın yarı otonom seviyeden tam otonom seviyeye ne zaman ve ne şekilde aktarılacağının tespiti noktasında hem de gerekli olan ara bilgi ve donanımların diğer ekonomik amaçlı YZ ürünlerinden de elde edilebilecek olmasından kaynaklanmaktadır.

Uluslararası kuruluşlar aracılığıyla bir uzlaşının öngörülebilir gelecekte mümkün olmaması, devletlerin tam otonom silah sistemleri bakımından da bir yarışa gireceği şeklinde yorumlanmamalıdır. Başka bir deyişle, teknolojinin daha üst sürümlerinin geliştirilebilmesi karşısında bizatihi teknolojinin kendi kısıtları da bulunmaktadır. Özellikle III. bölümde değinileceği üzere incelenen devletlerin bu yöndeki çalışmalarında sürü dronlar ayrı bir önem kazanmaktadır. Sürü dronların etkin görev ifa edebilmesi için birbirleriyle iletişime geçme kapasitelerinin olması gerekir. Bu gereklilik birtakım zorlukları beraberinde getirmektedir. Tam otonom silah sistemlerinin geliştirilmesine yönelik çalışmalar devam etmekle birlikte hızlı bir tam otonom silahlanma yarışı kolay değildir. Çünkü bir yandan I. bölümde yer verildiği gibi YZ'yi besleyen çip, işlemci, hafıza gibi ara parçaların daha büyük amaçları gerçekleştirecek

biçimde geliştirilmesi gerekmekte; diğer yandan ise tam otonom sistemlerin birbirleriyle iletişim kuracağı ağların güvenliğinin nasıl sağlanacağı belirsizlikler içermektedir. Bu belirsizliğin kaynağı ve nedenlerini incelemek için siber güvenlik konusuna bakmak ve güvenlik açıklarını incelemek gerekir.

OSS üzerindeki etik ve hukuki kaygıların ortaya konması ve çözüm yollarının aranması stratejik rekabetin bir diğer boyutunu oluşturmaktadır. Devletlerin kendi gücünü ve egemenlik alanını artırırken rakiplerini sınırlandırma arzularının yöntemlerinden bir tanesi de uluslararası hukuk düzenlemeleridir. İki büyük gücün birbirlerine karşı OSS alanında böylesi bir sınırlandırma kapasitesi şu ana kadar oluşmamıştır. Dolayısıyla ABD ve Çin'in uluslararası hukuk kuralları aracılığıyla birbirlerini sınırlandırmasını stratejik rekabetin bir boyutu olarak kabul etmek için yeterli neden yoktur. Ancak bir uluslararası hukuk normunun rakibini sınırlandırmasa da hangi devletin önerisiyle şekillendiği ve uluslararası toplum tarafından kabul edildiği devletin prestiji bakımından önemlidir. Bu açıdan bakıldığında devletlerin geliştirdikleri önerilerle prestij kazanma amaçlarını da stratejik rekabetin bir boyutu olarak kabul etmek mümkündür.

C. Siber Güvenlik

Bu başlık üç alt başlıktan oluşmaktadır. İlk olarak siber güvenliğe ilişkin kavramlar tanımlanacak, ardından siber güvenlikte yapay zeka uygulamalarına değinilecektir. Üçüncü bölümde ise siber güvenlik ile uluslararası güvenlik ilişkisi kurularak, devletlerin hangi tehditlerle karşı karşıya oldukları örnek saldırılara yer verilerek ortaya konacaktır.

Uluslararası ilişkilerde stratejik rekabetten bahsedebilmek için, menfaat sağlamaya elverişli somut veya soyut varlıklar üzerinde bir uyuşmazlık olması gerekir. Siber güvenlik yeni bir egemenlik alanı olarak düşünülürse büyük güçlerin rekabeti için uygun bir ortam oluşturur. Bu yeni alanda egemen olmak bir yandan rekabet eden devletin çıkarlarını korumaya ve geliştirmeye imkan sağlarken diğer yandan rakibinin bu alanda tam egemenlik kurmasını da engellemektedir. Bu nedenlerle siber uzay ve siber güvenlik YZ-RMA dalgasının altında yatan ikinci teknoloji olarak değerlendirilebilir ve ABD-Çin stratejik rekabetinin bir boyutunu oluşturur.

1. Tanım ve Siber Güvenlik Kavramı

İnternetin toplumsal hayata girmesi, ilişkilerin düzey ve boyutlarının da internet ortamında ve internet hızında gerçekleşmesini beraberinde getirmiştir. Web 1.0 temel bir serverdan yüklenen kaynakların diğer kullanıcılar tarafından görüntülenmesi imkanı sunarken, web 2.0

kullanıcıların doğrudan veri yükleyebilmesini mümkün kılmıştır. İnternet ortamına, gerek özel hayata ilişkin gerekse kamusal yaşama ilişkin verilerin girilmesi ve bu ortamlarda yayılması beraberinde bilginin güvenliği sorununu ortaya çıkarmıştır.

Eldeki çalışmanın incelediği neredeyse tüm kavramlar gibi; içinde siber kelimesi geçen, güvenliğe, ekonomiye ya da bu ilişkilerin gerçekleştiği ortama dair üzerinde uzlaşılmış kavramsal tanımlar geliştirmek oldukça zordur. Bu nedenle literatürde yapılan tanımlar ilk önce siber kavramına açıklık getirmekte, ardından internet ve ağlar üzerinden ilişkilerin gerçekleştiği alan olarak siber uzayı tanımlamakta, daha sonra da siber güvenliğe ilişkin tanımlar geliştirilmektedir. Bu çalışmada da benzer sistematik takip edilecektir.

Siber kelimesi sözlük anlamıyla, 'internet başta olmak üzere elektronik iletişim ağlarıyla bağlantılı olan' anlamına gelmektedir (Oxforddictionary, 2021). Kavramsal olarak ise herhangi bir kavramın elektronik iletişim ağlarıyla ilgili olan boyutunu vurgulamak için kullanılan bir önektir (Nye Jr, 2010: 3). Siber uzay ise *" ...insanların birbirine bağlı bilişim sistemleri ile etkileştiği ve birbirine bağlı bilişim sistemlerinin birbiri arasında ya da insanlarla iletişim içinde olduğu fiziksel olmayan alan(dır)..." (Bıçakçı, 2014: 106)*. Bu tanımdan anlaşılacağı üzere siber uzay tanımından kastedilen husus birbiriyle bağlantı içinde olan bilişim sistemleri olarak değerlendirilmektedir. Bir diğer çalışmada siber uzay şu şekilde tanımlanmıştır: *" ...elektrik ve elektromanyetik bir operasyonel alan olup bilgi oluşturma, değiştirme ve kullanmayı mümkün kılan, farklı ve benzersiz özellikleriyle birbirine bağlı ve bilgi ekosistemlerinde mevcut olan küresel bir alandır." (Kuehl 2009'dan akt. Akyeşilmen, 2018: 56; Nye Jr, 2010: 3).*

Akyeşilmen (2018: 54 v.d.), siber uzay kavramını daha geniş bir kapsamda ele alarak bileşenlerine vurgu yapmakta, yeni bir tanım getirmek yerine gerek literatürde gerekse devletlerin strateji belgelerinde yapılan tanımların eksik yönlerini vurgulamaktadır. Akyeşilmen'in ortaya koyduğu bileşenler insan, bilgi, mantıksal çerçeve *(yazılımlar)* ve fiziksel altyapı *(donanımlar)* olmak üzere dört tanedir. Yapılacak bir tanımın bu dört bileşeni de kapsaması gerektiğini ifade ederek, insan unsurunu dahil etmeyen tanımları eksik olarak nitelemektedir. Köker (2021: 129) ise yukarıda yer verilen tanımlardan farklı olarak birbirinden bağımsız bilgi sistemlerini de tanıma dahil etmektedir. Daha anlaşılır ve kapsayıcı bir tanım ise şu şekildedir: *"içerisinde bilginin çevrimiçi olarak saklandığı, paylaşıldığı ve iletildiği bilgisayar ağlarının (ve arkalarındaki kullanıcıların) alemidir* (Singer & Friedman, 2018: 29).

Tanımlardan anlaşıldığı üzere siber uzay, bir ağ üzerinden birbiriyle etkileşim içinde olan ya da olma olasılığı bulunan elektronik cihazlar ve onların kullanıcılarından oluşur. Temelde siber uzayda depolanan ya da dolaşan ve korunması gereken en önemli unsur bilgidir. Dolayısıyla siber güvenlik ilk olarak bilginin güvenliğini amaçlar. Bu bilgi kişi, devlet ya da kuruluşlara ait olabilir. Akyeşilmen (2018: 55) ve Bıçakçı (2014: 107 v.d) 'nın da isabetle altını çizdiği gibi; siber uzayın bileşenleri / katmanları siber güvenliğin de çerçevesini çizmektedir. Başka bir deyişle, siber güvenlik, siber uzayı oluşturan insan, bilgi, yazılımlar ya da fiziksel altyapılara yönelen saldırılara karşı alınan tedbirlerden oluşmaktadır.

2. Siber Güvenlik - YZ İlişkisi

Siber uzayda YZ uygulamaları incelendiğinde, siber güvenlik ile YZ ilişkisinin çift yönlü bir ilişki olduğu çıkarımını yapmak mümkündür.Yani YZ, hem kötücül amaçlarla saldırı aracı olarak kullanılmaya elverişlidir hem de olan/olası saldırılara karşı güvenlik sağlama aracı olarak kullanılmaktadır. Bu başlık altında öncelikle her birisi YZ kullanılarak ya da kullanılmadan doğrudan insan tarafından yapılan ve siber uzayda tehdit yaratan siber saldırı türlerine yer verilecektir. Ardından siber saldırılardan korunma amacıyla YZ'nin kullanım yöntemleri aktarılacak, son olarak da YZ'nin kötücül kullanım yöntemleri ve riskleri açıklanacaktır. Devletlerin bir yandan bilgi güvenliğini sağlaması diğer yandan siber uzay alt yapısını kullanarak yürüttükleri ticari kapasitelerini korumaları ancak siber güvenlik alanında etkin bir politika geliştirmeleri ile mümkündür. Sunduğu fırsatlar kadar karşı karşıya bıraktığı riskleri de barındıran siber uzay hem YZ-RMA dalgası çerçevesinde devletleri bu alanda strateji ve politika oluşturmaya davet etmekte hem de ABD-Çin rekabetine yeni bir stratejik rekabet sahası açmaktadır. Bu nedenlerle siber güvenlik YZ-RMA dalgasının bir unsuru olarak kabul edilerek ve bu kapsamdaki ABD-Çin politikaları incelenmeye değer görülmelidir.

Fiziksel dünyada gerçekleştirilen suçların, siber uzayda faaliyet gösteren araçlarla veya bu araçlara karşı gerçekleştirilmesine siber suç denilebilir (Akyeşilmen, 2018: 102). Siber suçlar oldukça farklı yöntemlerle işlenebilmektedir. Bunlardan en sık başvurulan birkaç tanesini örnek olarak açıklamak mümkündür: Oltalama, kötücül yazılımlar, botnet, hizmeti engelleme (DoS/DDoS) saldırıları, gelişmiş kalıcı tehdit saldırıları (APT) (Akyeşilmen, 2018: 102; Eren, 2017: 34).

Oltalama internet kullanıcısına, genellikle bankadan ya da müşterisi bulunduğu finans kuruluşundan gönderilen bir maile benzer formatta mail atılarak, kurban olarak seçilen kişinin mailde bulunan linke tıklaması ve bilgileri doldurması istenerek gerçekleştirilen bir siber saldırı

türüdür. Saldırının amacı kişiye ait bilgileri çalmak ve bu bilgilerle haksız kazanç elde etmektir (Eren, 2017: 36). Çoğunlukla kurbanın bulunduğu ülke dışında bir ülkenin serverları kullanıldığı için, failin tespiti ve cezalandırılması mümkün olmaz.

Kötücül yazılım, kullanıcıların haberi olmadan bilgisayarlarına sızmak ve bilgisayarlarına zarar vermek için kullanılan yazılımlardır. Bu yazılımların bulaştırıldığı bilgisayarlar aynı zamanda başka bir kullanıcı tarafından da kontrol edilebilmekte, gerçek kullanıcısının iradesi olmaksızın farklı işlerde kullanılabilmektedir. Kötücül yazılımlara örnek olarak truva atı, virüsler, solucanlar, reklam içerikli ve casus yazılımlar verilebilir. (Eren, 2017: 38 v.d.). Alman menşeili bir kuruluş olan AVTEST Bağımsız Bilişim Teknolojileri Enstitüsü, 2019 yılında 140 milyondan fazla yeni kötücül yazılım tanımladı. Bu rakam yaklaşık olarak bir dakikada 266 yeni kötücül yazılımın tanımlanması anlamına gelmektedir (Zeadally et al., 2020: 23818).

Oltalama ve kötücül yazılım ve daha da çeşitleri olan siber saldırı türlerinin hedefi genellikle bireysel kullanıcılardır. Ancak çalışmanın konusu bakımından daha önemli olan devletlere yönelik saldırılar için botnet, DoS/DDoS ve APT saldırıları ayrı bir önem taşımaktadır.

Botnet saldırıları, kullanıcının bilgisayarına kötücül yazılımlar yerleştirildikten sonra bilgisayarın "zombi" olarak adlandırılan ve uzaktan kontrol edilerek başka saldırılarda araç olarak kullanılmasıyla yapılan bir siber saldırıdır. Zombiye çevrilmiş olan her bir bilgisayar bot olarak adlandırılır, bu zombileştirilmiş bilgisayarların bir merkezden kontrol edilmesiyle oluşturulan ağa ise botnet denir. Botnet merkezi, asıl saldırıyı planladığı hedefe gerçek kullanıcılarının haberi olmaksızın bu zombi bilgisayarları kullanarak saldırı düzenler. Farklı motivasyonlarla saldırılar gerçekleştirilmesi mümkün olmakla birlikte, çalışmanın konusu bağlamında botnet saldırılarının öne çıkan kullanım amacı devletlerin kritik altyapılarına sabotaj düzenlemek için kullanılmalarıdır (Eren, 2017: 48 v.d.).

Hizmet engelleme DoS/DDoS[18] saldırıları bir kamu kurum ya da kuruluşunun veya şirketin elektronik ortamda sunduğu bir hizmeti kullanılamaz hale getirmek amacıyla yapılmaktadır. Botnetler, DDoS saldırılarının düzenlenmesinde etkin olarak kullanılmaktadırlar. Bu tür saldırıların çalışma mantığı, hizmet sunulan server bant genişliğinin

[18] DoS (Denial of Service – hizmeti engelleme), DDoS ise (Distributed Denial of Service – dağıtılmış hizmeti engelleme) anlamına gelmektedir. İki siber saldırı türü arasındaki fark, saldırıya katılan bilgisayar sayısında ortaya çıkmaktadır. DDoS saldırılarında, botnetler kullanılarak binlerce bilgisayar aynı anda saldırı gerçekleştirmektedir.

taşıyabileceği yükün çok üstünde bir hizmet talebinin eş zamanlı olarak sisteme yönlendirilmesidir. Sistem kapasitesinin üstünde bir yükle karşılaşınca çalışamaz hale gelmektedir. En sık gerçekleştirilen saldırı türüdür (Eren, 2017: 51 v.d.).

Gelişmiş kalıcı tehdit (APT) saldırıları çoğunlukla ulusal güvenlik, finans gibi sektörlerin ağlarına yetkisiz olarak girip, uzun süre ağda kalarak bu ağ ve kuruluşa zarar verme amacıyla gerçekleştirilir. APT saldırılarının başarılı olabilmesi için üç koşulu birden sağlaması gerekir. Bu üç koşul şu şekilde özetlenebilir: i) uzun bir süre kalmak amacıyla ağa yerleşmek, ii) ağdaki güvenlik sistemine karşı uyum sağlamak ve iii) kararlı bir biçimde sonuca ulaşmak için gerekli etkileşim seviyesini korumak (Eren, 2017: 56).

Siber saldırı türlerini sınırlı sayıda kabul etmek ya da siber suç – siber saldırı ayrımını yapabilmek her zaman mümkün olmamaktadır. Bunun da ötesinde saldırıya katılan hangi bilgisayarın kurban hangisinin fail olduğunu tespit etmek de oldukça güçtür. Bu güçlüğün bir sonucu olarak, saldırılara karşı caydırıcı tedbirler geliştirmek de çoğu zaman istenen amaca ulaşmayı sağlamakta yetersiz kalmaktadır. Bu nedenlerle, saldırı amacına ulaşamadan bertaraf edilmelidir. Bunun yöntemi ise siber güvenlik araçlarının etkin kullanımıyla mümkündür.

Botnet ve DoS/DDoS başta olmak üzere siber saldırılara karşı YZ temelli siber güvenlik sistemleri geliştirilmektedir. Yapay Sinir Ağları, Uzman Sistemler, Makine Öğrenmesi ve Derin Öğrenme gibi YZ teknikleri kullanılarak geleneksel siber güvenlik yöntemleri güçlendirilmektedir. Bu tür siber güvenlik sistemlerinin temel amacı makine öğrenmesi, derin öğrenme gibi teknikleri kullanarak, hangi hizmet talebinin gerçek kişiden hangisinin saldırıya katılan bilgisayardan yöneltildiğini tespit etmektir (Şeker, 2020: 111 v.d). Bu tespitlerin mümkün olması halinde, hizmet sunucusu saldırganların hizmet taleplerini doğrudan reddedebilme imkanı kazanacaktır.

Yapılan çalışmalarda yazılım tanımlı ağ çevresindeki ağ protokollerinin istatistiksel verilerinden çıkarılan 68 özellik tanımlanmış ve derin öğrenme algoritması kullanılarak DoS saldırılarını bulmak amaçlanmıştır. DoS saldırıları %95.65 oranında bulunabilmiştir. Bir diğer çalışmada 20 özellik tanımlanmış, derin öğrenme aracılığıyla %99.88 doğruluk oranında DoS saldırıları yakalanmıştır (Zeadally et al., 2020: 23826).

İnsanların bilgiye ulaşma, iletişim ve etkileşim olanaklarını olağanüstü bir hızda artırarak avantajlar sağlayan internet ve bilişim teknolojileri, saldırıların kurbanı olma riskini de beraberinde getirmiştir. YZ teknolojileri yeni tehditlere karşı siber güvenlik tedbirleri

sunabilmektedir. Ancak YZ'nin kötü amaçlarla kullanılması riski de ciddi tehditler barındırmaktadır.

YZ'nin kötü niyetli kullanım yöntemlerini inceleyen bir çalışmada (Brundage et al., 2018: 23 v.d.) üç güvenlik alanı tanımlanmış ve bu üç alanda YZ'nin kötü niyetli kullanılma risklerine yer verilmiştir. Çalışmada belirlenen üç alan; dijital güvenlik, fiziksel güvenlik ve siyasal güvenlik alanlarıdır. Çalışmanın bulguları ve saptadığı YZ'nin kötü niyetli kullanım yöntemleri genel hatlarıyla özetlenebilir.

Dijital güvenlik alanında sosyal mühendislik saldırıları olarak adlandırılan; web sayfaları, e-mailler veya link bağlantıları üzerinden hedefteki kurban ile iletişime geçerek güvenini kazanma ve sonrasında bilgilerini çalma görevleri otomasyona aktarılarak makinelere yaptırılabilir. Yazılım kodlarının güvenlik açıklarını bulmak için YZ destekli kodlar oluşturulabilir. Hakleme görevleri daha karmaşık bir otomasyon sürecine aktarılarak; hedef seçimi ve özelleştirilmesi, hedefin davranışlarındaki değişikliklere yanıt verme gibi görevler YZ'ye yaptırılabilir. En uygun hedeflerin belirlenmesi için makine öğrenmesi teknikleri kullanılabilir. İnternet üzerinde yapılan her işlem bir ayak izi bırakmakta ve bu izler kullanıcının davranış kalıpları hakkında da veri sağlamaktadır. Makine öğrenmesi teknikleri bu verileri işleyerek, saldırının amacına uygun kişileri saptayabilme yeteneğine sahiptir. Bilgi güvenliği konusunda, veri zehirleme saldırıları kullanılarak kullanıcının makine öğrenmesi modellerinde arka kapı açmak ya da modeli bozmak mümkündür (Brundage et al., 2018: 24 v.d.).

Fiziksel güvenlik alanında YZ temelli sistemlerin terörist amaçlarla yeniden işlevlendirilmesi mümkündür. Örneğin, dronlar kullanılarak patlayıcıların hedefe ulaştırılması ya da otonom araçlarda kazalara sebep olacak değişiklikler yapmak yeniden işlevlendirmedir. Sürü saldırıları adı verilen, otonom robot sistemlerinin dağıtılmış ağları makine hızıyla eşgüdümlenerek, daha geniş alanlar izlenebilir ve koordineli saldırılar düzenlenebilir. Fiziksel ortamda, saldırıyı düzenleyenden daha uzak bir mesafede saldırı düzenlenmesi imkanı doğmaktadır (Brundage et al., 2018: 27 v.d.).

Siyasal güvenlik alanında ise; devletler muhalefeti baskılamak amacıyla otomatik izleme platformları kullanabilirler. Gerçekçi video ve sesler üretilerek sahte haber ve rapor hazırlanabilir. Bireylerin oy verme davranışlarına etki etmek amacıyla, hiper-kişiselleştirilmiş dezenformasyon kampanyaları yürütülebilir. Bilgi reddi saldırılarıyla bilgi kanallarına saldırı düzenlenerek, daha fazla gerçek bilgiye ulaşılması yavaşlatılabilir ya da engellenebilir (Brundage et al., 2018: 28 v.d.).

YZ faydaları olduğu kadar riskleri de olan bir teknolojidir. Çünkü YZ'nin çalışma alanı olan siber uzay, adeta belirsizlikler ülkesidir. Hangi tehdidin nereden, kim tarafından geldiğini tespit etmek çoğu zaman mümkün olmaz. YZ'nin buradaki rolü, hem güvenlik hem de kötü amaçlı kullanımında, devasa büyüklükteki verileri işleyerek YZ'yi kullanan kişinin/grubun amacına uygun sonuçlar elde etmektir. YZ ve siber güvenlik kullanılarak düzenlenen saldırıların uluslararası ilişkiler bakımından anlamı nedir? Bu soruyu cevaplayabilmek için konu bağlamındaki örnek saldırılara bakmak yerinde olacaktır.

3. Siber Güvenlik- Uluslararası Güvenlik İlişkisi: Yeni Tehditler ve Örnek Olaylar

Siber uzayda yasadışı faaliyet gösteren kişi ya da gruplar genel olarak hacker olarak adlandırılıp, faaliyetlerinin amaçlarına göre şapka rengi cinsinden betimlenmektedirler. Bireysel olarak ya da bir grup halinde hareket eden kişilerin amaçları, bir ideolojiyi yaymak, herhangi bir kamu politikasını protesto etmek ya da bir uluslararası örgütün eylemi veya eylemsizliğine tepki göstermek olabilmektedir. Bireysel ya da bir grup halinde siber uzayda yasa dışı faaliyet gösteren gruplar, bu alanı güvensiz hale getirmektedir.

Siber uzayda gerçekleştirilen yasadışı faaliyetleri uluslararası güvenlik bakımından daha önemli bir konuma yükselten husus ise, doğrudan devletler tarafından ya da devletlerin desteklediği hacker grupları tarafından diğer devletlere yönelik saldırılar düzenlenmesidir. Bu saldırılardan en çok bilinenler ve niteliği itibariyle ayrı bir önem taşıyanları şunlardır: 2007 yılında Estonya'ya yapılan DoS ve DDoS saldırıları, Aynı yıl İsrail'in Suriye'ye karşı gerçekleştirdiği Orchard saldırısı, 2008 yılında Gürcistan'a yapılan saldırılar 2010 yılında İran'a karşı yapılan Stuxnet saldırısı, 2016 yılında Rusya'nın ABD seçimlerine müdahale ettiği iddiaları (Akyeşilmen, 2018: 239 v.d. ; Akyeşilmen & Kurnaz, 2020: 14 v.d.). Orchard ve Stuxnet saldırılarının yöntem ve sonuçlarına bu başlık altında detaylı olarak yer verilecektir. Sayılan diğer saldırılara bir şekilde Rusya'nın adının karışmış olması nedeniyle, bu saldırılar III.C.3 başlığı altında incelenecektir.

Stuxnet saldırısı üzerinde muğlak iddiaları içinde barındıran, İran'ın nükleer tesislerine yönelik olarak yapılmış bir saldırıdır. Saldırının gerçekleştirilebilmesi için özel bir kurtçuk/virüs yazılımı hazırlanmış ve küresel internet bağlantısına bağlı olmayan İran tesislerine bulaştırılmıştır. Bulaştırma yöntemi kesin olarak bilinmemekle birlikte, tesiste çalışan bir personelin flaş belleğine bulaştırılıp bu flaş bellek aracılığıyla da tesise sokulduğu tahmin edilmektedir. Stuxnet saldırısının diğer siber saldırı türlerinden farklı olarak sadece ağ ya da bilgisayara zarar verme amacı taşımamasıdır (Akyeşilmen, 2018: 243; Say, 2021).

Stuxnet yazılımı dünya tarihinde bilinen fiziksel makinelere zarar veren ilk yazılımdır. Şöyle ki, yazılımın bulaştığı bilgisayarın kontrol ettiği makine üzerindeki hakimiyetini engellemekte aynı zamanda, yönetici bilgisayardaki hata uyarısını da kamufle edebilmektedir. Yazılımın fiziksel makinelere zarar vermesi, kontrolü ele geçirdikten sonra mümkün hale gelmektedir. Reaktörün hızını çok yüksek seviyeye çıkarma talimatı vermekte, maksimum seviyeye ulaşınca ani fren komutu girmektedir. Bu yöntem reaktörün fiziki hasarına sebep olmakta ve reaktörü kullanılamaz hale getirmektedir. Rakamlar değişiklik göstermekle birlikte, bir görüşe göre 10.000 reaktörün 1.000 tanesini, diğer bir görüşe göre ise 8.000 reaktörden 5.000 tanesini devre dışı bırakmıştır (Akyeşilmen, 2018: 244) .

Yapısı itibariyle tahmini olarak 50.000 satır kod ile yazılan, kendini belirli bir sürede yok etmeye programlı olan ve kod içine tekrar kod yazılarak oluşturulan yazılımın devlet destekli bir proje olma olasılığı çok yüksektir. Destekleyen devletlerin ABD ve İsrail olduğu yönünde kanaat oluşmuştur (Akyeşilmen, 2018: 243-244). Siber uzayda tasarlanıp, fiziksel alanda sonuç doğuran, devletlerin egemenlik yetkileri hilafına önemli bir müdahale örneği oluşturmaktadır.

İran'ın muhtemeldir ki en iyi korunan, küresel ağ bağlantısı kullanmayan bir tesisine dahi böyle bir saldırının başarıyla düzenlenebilmiş olması bir yandan siber güvenliğin önemini ortaya koymakta, diğer yandan devletler arası rekabet ve güç mücadelesinin siber ortamda da devam ettiğini göstermektedir. Ayrıca stuxnet saldırısının önemli bir göstergesi de, bilişim ağlarına dışardan müdahale etmenin bir şekilde mümkün olabildiğidir.

Orchard saldırısı, İsrail tarafından Suriye hava sahasına girip nükleer silah üzerine çalışıldığı iddia edilen bir tesisi bombalaması ve bu saldırıyı düzenlerken hava savunma sistemlerine yakalanmaması biçiminde gerçekleşen saldırıdır. Suriye Hava savunma sistemlerine saldırı düzenleyerek gerekli şifreleri (I ve O) gönderen İsrail, radar ekranına görünmesini istediği görüntüyü yerleştirebilmiştir (Akyeşilmen & Kurnaz, 2020: 16). Görünüş itibariyle bir elektronik harp tekniği olduğu anlaşılan saldırıda; geleneksel elektronik harpten farklı olarak radarlar körleştirilmemiştir. Radarların bağlı olduğu bilgisayara erişim sağlanarak görüntü değiştirilmiştir.

4. OSS ve Siber Güvenlik Konularının RMA Bağlamında Değerlendirilmesi

Yukarıda açıklandığı üzere RMA, ortaya çıkan bir teknolojinin doktrinel, operasyonel ya da stratejik yönlerden ele alınıp askeri alana uyarlanması için yapılan çalışmalardan oluşmaktadır. Askeri alanın birinci önceliği güvenlik olup, güvenlik ile

ilişkilendirilebilecek teknolojiler üzerine RMA çalışmaları yürütmek mümkündür. Hem OSS hem de Siber Güvenlik doğrudan güvenlik ile ilişkilendirilebilecek teknolojilerden oluşmaktadır. OSS çatışma alanı dahil öldürücü etkiye sahip bir güvenlik aracı iken, Siber alanda yapılan faaliyetler bilgi başta olmak üzere verilerin ve hizmetlerin amaca uygun yapılmasını sağlama ya da engelleme amaçlarından birine özgülenmektedir. Dolayısıyla bu iki alan da üzerinde RMA çalışması yürütmeye elverişli alanlardır.

RMA dalgalarında gözlemlenen hususlar bağlamında OSS ve Siber Güvenlik konusu incelendiğinde; uluslararası ortamın yapısı, rakiplerin kapasitesi ve tehdit tanımlamaları gibi konulara değinmek gerekir. OSS'ler büyük güçlerle birlikte diğer orta büyüklükteki güçler ve küçük devletlerin de rekabet ettiği bir alan haline gelmiştir. Bu tür sistemlerin ticari amaçlarla yaygınlaşması uluslararası ortamı etkilemektedir. Bunun yanısıra RMA çalışması yürütecek devletin uluslararası ortam algısı, özellikle de tehdit algısı, yapılacak çalışmaların niteliğini doğrudan etkileyecek önemli bir husustur. Rakiplerin kapasitesi ise jeopolitik gerçeklikler ışığında etkisini göstermektedir. Örneğin Pasifik Bölgesi'nde Çin tarafından konumlandırılacak bir OSS, ABD için tehdit anlamına gelirken; Avustralya'nın sınırlarına yerleştireceği daha güçlü OSS'ler kaygı nedeni olarak değerlendirilmeyecektir. Diğer yandan böylesi bir güvenlik sisteminin gerekliliği konusu da jeopolitik konum bağlamında ortaya çıkmaktadır.

Siber Güvenlik konusu ise niteliği gereği zaman ve mekan sınırlılıklarına takılmamaktadır. Siber uzayda faaliyet gösteren her aktör hem tehdit hem de kurban olabilecek durumdadır. Stratejik bilgiler dahil devletlere ilişkin veriler ve siber ortamda sunulan kamusal hizmetler açık bir hedef niteliğindedir. Dolayısıyla siber alan son RMA dalgası için görece daha önemli bir çalışma alanı haline gelmektedir. Üzerine operasyonel ya da taktik stratejiler oluşturulmaya imkan veren bir teknoloji olarak siber uzay, hem internet temelli çalışan fiziksel güvenlik araçlarının etkinliği hem de siber uzayın bizatihi kendi güvenliği için askeri alana uyarlanması için önem taşımaktadır.

Özetle hem OSS hem de siber güvenlik son RMA dalgasının odak noktasında yer alan teknolojilerdir. Bu nedenle de büyük güçlerin bu alanda geliştireceği doktrinler ya da operasyonel yenilikler aynı zamanda ilgili gücün iç ve dış politikası bakımından da öngörülerde bulunmaya imkan tanıyacaktır.

Bir teknolojinin RMA bağlamında değerlendirilebilmesi için üzerinde politika ve strateji geliştirmenin mümkün olup olmadığı, yani teknolojinin yönetilmesinin mümkün

olup olmadığı önem kazanmaktadır. Hem OSS hem de Siber güvenlik üzerinde politika ve strateji geliştirmeye elverişli olduğu hatta bu geliştirmeleri yapmayı gerekli kıldığı için YZ-RMA dalgasının teknik altyapısı olarak kabul edilmelidir. Öte yandan ABD-Çin stratejik rekabetinde açtıkları yeni mücadele alanları nedeniyle herbir ülke için incelenmeleri önem kazanmaktadır. Çünkü bu teknolojiler üzerinde devletlerin geliştirdikleri politika ve stratejilerinden yola çıkarak iki devletin birbirlerini nasıl konumlandırdıklarını anlamak mümkün olacaktır.

III. BÖLÜM : BÜYÜK GÜÇ SİYASETİNDE YAPAY ZEKA : ABD ve ÇİN ÖRNEĞİ

II. Bölümde Askeri Devrim (MR) ve Askeri Alanda Devrim (RMA) kavramları açıklanmıştır. Ayrıca Son RMA dalgasının altında yatan teknoloji olarak OSS ve Siber Güvenlik konularına yer verilmiştir. YZ destekli güvenlik araçlarının MR-RMA yaklaşımlarının hangisi kapsamında değerlendirilebileceği sorusunu cevaplayabilmek için, iki kavramsal çerçeve arasındaki temel farklılığı oluşturan öngörülebilirlik, kontrol edilebilirlik, operasyonel ya da taktik stratejilerin doktrin boyutuyla ele alınıp alınmadığı konularının değerlendirilmesi gerekmektedir.

Bu bölümde ABD ve Çin'in YZ politikaları, RMA bağlamında incelenecektir. Her bir devlet incelemesi aynı dört alt başlık şeklinde tasarlanmıştır. İlk başlıkta strateji belgelerindeki ifadeler ve/veya devlet yetkililerinin konuşmaları analiz edilerek ilgili devletin, YZ temelli güvenlik araçları geliştirmekteki motivasyonunun ne olduğunu ortaya koymak amaçlanmıştır. Devlet incelemelerinin diğer üç alt başlığı ise sırasıyla OSS, Siber Güvenlik ve RMA başlıklarıdır. Bu başlıklarda ilgili devletin sahip olduğu ve geliştirmekte olduğu OSS ve siber güvenlik politikaları incelenerek, RMA kapsamında nitelenebilecek doktin ya da kavramların oluşturulup oluşturulmadığı araştırılacaktır.

A) Amerika Birleşik Devletleri (ABD)

Uluslararası politikadaki varlığını ve gücünü, II. Dünya Savaşı sonunda Hiroşima ve Nagazaki'ye attığı nükleer bomba ile ortaya koyan ABD, askeri teknoloji ile uluslararası politikadaki güç arasındaki kopmaz bağın bilinciyle politikalar geliştirmektedir. ABD savunma sanayisi ile ticari ürünler arasında başarılı işbirlikleri kurarak karşılıklı bir beslenme ortamı yaratmıştır. Bu işbirliği neticesinde geliştirdiği teknolojiler hem savunma sanayisinde öncü adımlar atılmasını sağlamış hem de üretilen bilgiler sivil yatırımlarda kullanılarak ABD ekonomisine katkı sunmuştur. ABD'nin ulusal strateji belgeleri incelendiğinde; güvenlik, ekonomi ve teknoloji üzerine sürekli bir vurgu yapıldığı görülmektedir (WhiteHouse, 2010, 2015a, 2017).

Dönemsel olarak tehdit tanımlaması değişiklik gösterse de, değişmeyen husus ABD'nin kendini dünya lideri olarak tanımlaması ve bu konumunu korumak amacıyla politikalar üretmesi olmuştur. YZ özelinde de geliştirilen stratejiler ekonomi, güvenlik ve dünya liderliği temaları etrafında kurgulanmıştır.

1. ABD'de Devletin Yapay Zekaya Yönelik Yaklaşımları

ABD Savunma Bakanlığı *(Department of Defense - DoD),* 2012 yılında yayınladığı 3000.09 sayılı direktif ile silah sistemlerinde otonomi konusunu ele almıştır. YZ- uluslararası güvenlik ilişkisi ile doğrudan ilgili ilk belge olan bu belgenin hazırlanma amacı, silah sistemlerindeki otonom ve yarı otonom işlevlerin kullanımı ve geliştirilmesi için politika ve sorumlulukları belirlemek olmuştur. Direktifte belirtilen bir diğer amaç ise, direktife konu olan silah sistemlerinin istemsiz nişan almalarına yol açabilecek başarısızlıklarının sonuçlarını ve başarısızlık olasılıklarını minimize etmek için bir kullanım kılavuzu hazırlamaktır. Direktifte tam otonom ve yarı otonom silah sistemleri de tanımlanmıştır. Metinden anlaşıldığı kadarıyla ABD, otonom silah sistemleri ifadesini tam otonom silah sistemleri için kullanmakta, yarı otonom silah sistemlerini ayrıca tanımlamaktadır. Buna göre, bir önceki bölümde yer alan tanımlarla uyumlu biçimde insan müdahalesinin, hedef seçme ve nişan alma döngülerinde yer alıp almamasına göre silah sistemlerini sınıflandırmaktadır. Direktifin genelinde, insan müdahalesinin önemi ve savaş hukuku kurallarına uyma yükümlülüğü vurgulanmaktadır (DoD, 2012a).

ABD'nin YZ ve güvenlik politikasını asıl ortaya koyan, takip eden yılların strateji belgelerine ve politikalarına öncülük eden açıklamalar, Savunma Bakanı Chuck Hagel'in bir konuşması[19] ile gündeme gelmiştir (Hagel, 2014). Hagel'in konuşması literatürde, ABD'nin Third Offset Stratejisi (3OS)[20] olarak anılmaktadır (Dombrowski, 2015; Fiott, 2016; Louth & Taylor, 2016). Anılan konuşmanın ana teması, savunma sanayisinin modernize edilmesi için gerekli olan bütçe ve özel sektör ile işbirliği yapılmasının gerekliliğidir. Bununla birlikte çalışmanın konusu bakımından öne çıkan en önemli vurgu Hagel'in şu sözlerinden anlaşılmaktadır: *" Biz on yıldan fazla bir süredir istikrar operasyonlarına odaklanırken, Rusya ve Çin gibi ülkeler ordumuzun teknolojik üstünlüğünü köreltmek için, ileri savaş uçakları, denizaltılar, hem daha uzun menzilli hem de daha isabetli füzeleri sahaya çıkarıyorlar. Ayrıca, yeni gemisavar ve havadan havaya füzeler, karşı-uzay, siber elektronik savaş, denizaltı ve hava*

[19] Söz konusu konuşma, 15 Kasım 2014 tarihinde, Reagan Ulusal Savunma Forumu açılış konuşmasıdır. Konuşmanın yazılı metin formatı kamuoyuyla paylaşılmıştır.

[20] Stratejinin resmi adı Defence Innovation Initiative'dir. "Offset" kelimesi dengeleme kavramına işaret etmektedir. Third "Offset" ise ABD siyasi tarihindeki üçüncü dengeleme stratejisini ifade etmek amacıyla kullanılmaktadır. İlk "Offset", 1950'lerde Başkan Eisenhower tarafından ortaya konan ve Varşova Paktı'nın konvansiyonel güçlerine karşı nükleer caydırıcılık amaçlayan stratejisidir. İkincisi ise, 1970'lerde Savunma Bakanı Harold Brown tarafından açıklanan, "Long-Range Research and Development Planning Program" kapsamında geliştirilen ve günümüzde de kullanılmaya devam eden yeteneklerin büyük çoğunluğunu ifade eder. Bkz. Hagel, C. (2014). Secretary of Defence Speech. In. Simi Valley, CA: Reagan National Defense Forum, Louth, J., & Taylor, T. (2016). The US Third Offset Strategy: Hegemony and Dependency in the Twenty-First Century. *The RUSI Journal*, *161*(3), 66-71.

saldırı yeteneklerini geliştiriyorlar" (Hagel, 2014: 3-4). Hagel'in sözlerinden açıkça anlaşıldığı gibi 3OS'nin motivasyonu Çin ve Rusya'nın askeri teknolojideki ilerlemelerini dengelemektir.

Savunma Bakanı'nın konuşmasından yaklaşık iki buçuk ay sonra, Bakan Yardımcısı Robert (Bob) Work, CNAS[21] organizasyonunda bir konuşma yaparak 3OS'nin çerçevesini, amaçlarını ve ilk iki stratejiden farklarını ortaya koymuştur (Work, 2015). Konuşmasına o dönemdeki güncel tehdit tanımlamalarıyla başlayan Work, Rusya'nın Kırım'ı işgali başta olmak üzere Doğu Avrupa üzerindeki agresif politikaları, Afrika'daki Ebola salgını ve Orta Doğu'daki IŞID saldırılarını başlıca tehditler olarak ifade etmiştir (Work, 2015: 4). Ayrıca *"Çin'in Doğu ve Güney Çin Denizi'ndeki kışkırtıcı faaliyetleriyle uğraşıyoruz"* demek suretiyle, Pasifik bölgesindeki tehditlere ve Çin'in stratejideki yerine de değinmiştir (Work, 2015: 6-7).

Work, Savunma Bakanlığı'nın 2014 Quadrennial Defence Review isimli belgede ortaya koyduğu 5 stratejik önceliğin, 3OS için de önemini koruduğunu ifade etmiştir. Bu beş stratejik öncelik şunlardır (Work, 2015: 7):

- *"Asya Pasifik Bölgesini yeniden dengelemek,*
- *Avrupa'da ve Orta Doğu'da güvenlik ve istikrar için güçlü bağlılığı sürdürmek,*
- *Küresel karşı terörizm kampanyalarını sürdürmek,*
- *Temel ittifakları ve ortaklıkları güçlendirmek,*
- *Temel modernizasyon çabalarına öncelik vermek."*

Bakan Yardımcısı'nın ifadelerinden Asya Pasifik Bölgesi'nde Çin'e karşı, Doğu Avrupa'da Rusya'ya karşı, Orta Doğu'da devlet dışı terör örgütleri ve Rusya'ya karşı politikalar geliştirirken, mevcut ittifakların güçlendirilmesine ve askeri modernizasyona önem verildiği görülmektedir.

Askeri modernizasyon kapsamında 3OS gerekliliğini ortaya koymak için amacıyla, nükleer silahlardaki hızlı gelişmeler, yeni gemisavarlar, karşı uzay yetenekleri ve siber kapasiteler, elektronik savaş yetenekleri gibi yeni nesil savunma/saldırı araçlarının ABD'nin geleneksel askeri gücüne karşı çıkmak için tasarlandığını iddia etmiştir (Work, 2015: 9) Çin'in geçen 10 yıllık sürede askeri gücünü neredeyse her yıl iki katına çıkarması, Rusya ve Çin'in çok hızlı bir tempoda çok ileri yetenekler geliştirmesi, Çin'in kendi kaynaklarını harcamadan,

[21] CNAS: Center for a new American Security. Detaylı bilgi için bkz. https://www.cnas.org/ (e.t.30.12.2021)

ABD'nin Ar-Ge projelerini çalarak geliştirmesi yeni tehditler olarak ifade edilmektedir (Bitzinger, 2017; Louth & Taylor, 2016; Work, 2015: 10).

3OS'in hazırlanma gerekçesi, *"21.yy'da ABD'nin askeri üstünlüğünü sürdürmek"* ifadesiyle dile getirilmiştir (Work, 2015: 10). Bu amacı gerçekleştirmek için yatırım yapılan alanlar ise geleneksel askeri araçların güçlendirilmesinin yanı sıra; *"...siber yetenekler, insansız denizaltı araçları, ileri deniz mayınları, ileri havacılık, yüksek hızlı saldırı silahları, yüksek enerji lazerleri, elektro manyetik raylı toplar."* Şeklinde belirtilmiştir (Work, 2015: 11) . Çin'e karşı girişilen en önemli üstünlük mücadelesi, anti erişim *(anti access)* ve inkar ağları silah sistemlerine *(area of denial network weapon systems)*[22] karşı ilerleme çalışmalarıdır (Work, 2015: 14,21).

Work, ilk iki strateji ili 3OS'yi karşılaştırarak, yeni dönemin güçlüklerini de belirtmiştir. Bu kapsamda üç temel farklılık saptamaktadır. Bu farklılıklar şöyle özetlenebilir (Work, 2015: 15):

- 3OS çok daha zorlayıcı bir zamansal bileşene sahip olacak,
- Soğuk Savaş yıllarında olduğu gibi tek ve yatıştırılamaz bir hasımdan ziyade; Kuzey Kore ve İran gibi küçük bölgesel devletlerden, Rusya ve Çin gibi büyük ilerlemiş devletlere, devlet dışı düşmanlardan ileri yeteneklere sahip aktörlere birçok potansiyel rakip bulunmaktadır.
- İlk iki strateji için gerekli görülen askeri yetenekler askeri laboratuvarlarda geliştirilirken; robotik, görselleştirme, biyoteknoloji, minyatürleştirme, büyük veri, 3-D yazıcı gibi teknolojiler ticari sektör tarafından geliştirilmektedir.

3OS ile ortaya konan ana argümanlar Çin ve Rusya'nın askeri teknolojilerini modernize etmelerine karşılık olarak, Amerikan askeri gücünün de modernize edilmesinin, 21.yy'da ABD'nin askeri üstünlüğünü sürdürmek ve çıkarlarını korumak için hayati olduğu iddiasına dayanmaktadır. Ayrıca yeni teknolojilerin askeri laboratuvarlardan değil, özel sektör girişimlerinden besleniyor olması güvenlik araçlarının mülkiyeti ve devletlerin meşru şiddet kullanma tekeli[23] bağlamında tartışılması gereken bir diğer husus olarak öne çıkmaktadır. Bu tartışmaya, çalışma ile ilgili olduğu ölçüde, IV. Bölümde yer verilecektir.

[22] Anılan iki sistem Çin başlığı altında ele alınacaktır.

[23] Devletlerin meşru şiddet kullanma tekelinin erozyona uğraması, özel orduların kurulması ve görev ifa etmesi gibi geleneksel devlet ve uluslararası ilişkiler yapısının temel varsayımlarına karşıtlık içeren gelişmelerin detaylı bir analizi için bkz. Balta, E. (2021). *Küresel Güvenlik Kompleksi* (3 ed.). İletişim.

2. Otonom Silah Sistemleri

ABD, askeri gücünü teknolojik gelişmişliğine borçlu olduğunun bilincinde hareket ederek, ilk nükleer bombaları attığı günden itibaren teknolojisini sürekli geliştirmiş bir devlettir. Bu kapsamda herhangi bir ulusal strateji belgesini milat kabul edip sonrasında OSS geliştirilmeye başlandığını tespit ve iddia etmek oldukça zordur. Çünkü 21.yy askeri teknolojileri aslında köklerini II. Dünya Savaşı sırasında kullanılan elektronik harp teknikleri, savaş uçakları, güdümlü füzeler gibi askeri araçlardan almaktadır. Değiştirilip, güçlendirilen yönleri ise genellikle, insansız olarak aynı faaliyetlerin yapılabilmesi, hesaplama ve planlama süreçlerinde YZ tekniklerinin kullanılması olmuştur. Tüm güvenlik araçlarının modernizsasyon evrelerini kronolojik olarak sıralamak[24], çalışmayı kapsamından çıkaracağı için bu bölümde özellikle insan makine işbirliği kapsamında geliştirilen araçların genel avantaj ve dezavantajlarına ve sürü dronları teknolojisine yer verilecektir. ABD'nin OSS üzerinde 3OS stratejisini geliştirmesi konunun RMA bağlamanına taşınmasına imkan veren en önemli girişimidir. Çünkü OSS'yi stratejik bir alan olarak görmekte, bu konuda strateji geliştirmekte ve insan-makine işbirliği kavamını ortaya atarak yeni bir askeri doktrin çerçevesinde askeri örgütlenmesini kurgulamaktadır.

İlk bölümde yer verildiği gibi, kural tabanlı uzman sistemlerin çalışabilmesi için makinelere aktarılacak birikmiş tecrübelerin varlığı gerekir. Makine öğrenmesi kapsamında da makinelerin tecrübesini geliştireceği saha deneyimi ayrıca önem kazanmaktadır. Dolayısıyla ABD'nin yeni nesil güvenlik araçları üretiminde en büyük avantajı, özellikle 11 Eylül sonrasında sürekli olarak dünyanın çeşitli bölgelerinde, sahada savaş halinde olmasıdır (Darıcılı, 2020: 60).

İnsan makine işbirliği ifadesinden kast edilen yarı otonom silah sistemlerini de içine alan, ayrıca planlama, görüntüleme, analiz gibi destek hizmetleri bakımından da YZ'nin insanlara karar verme süreçlerinde yardım etmesini ifade eden bir kavramdır. Bu yarı otonom sistemleri ve insan makine işbirliği örneklerini ele almadan önce, ABD'nin tam OSS'ye sahip olan devletlerden biri olduğunu ifade etmek[25] ve sahip olduğu denetimli otonom sistemlere değinmekte yarar vardır. Soğuk savaş döneminde ABD'nin geliştirdiği *Gemisavar Tomahawk Füzesi (TASM)*, Sovyet gemilerinin muhtemel rotalarına doğru fırlatıldığında, ilgili bölgede

[24] Askeri amaçlı geliştirilen ve kullanılan otonom sistemler hakkında detaylı bilgi için bkz. Galliott, J. (2015). *Military Robots Mapping the Moral Landscape*. Ashgate (e-book).

[25] Sayıları en az 7 olan OSS sahibi devletler şunlardır: ABD, Çin, Rusya, Birleşik Krallık, Fransa, İsrail, Güney Kore. Bkz. Rohrlich, J. (2019, 08.05.2019). Report: Kill the idea of "killer robots" before they kill us. https://qz.com/1614684/killer-robots-must-be-stopped-pax-tells-the-world/

radar sinyali araması ve Sovyet gemisi bulması durumunda da vurması amacıyla tasarlanmıştı. 1990'ların başlarında donanma envanterinden çıkarılmasına rağmen TASM, hiç kullanılmamış olsa da ilk tam otonom silah sistemidir (Scharre, 2020: 80-81). ABD, 90'lı yıllarda *Tacit Rainbow* ve *LOCAAS*[26] isimli iki deneysel gezici mühimmat projesi üzerinde çalışmaya başladı. *Rainbow*, yukarıda değinilen *Harpy* ile aynı mantıkta kurgulanmış ve kara radarlarını hedef alan bir sistem olarak düşünülmüştü. *LOCAAS* ise daha zor bir amaçla ortaya konmuş, düşman tanklarını bulup yok etmesi planlanmıştı. Fakat ikisi de kullanıma girmeden, geliştirme aşamasında iptal edildi (Scharre, 2020: 81-82).

2011 yılına gelindiğinde ABD, savunma alanında otonomiye geçiş yol haritasının aşamalarını ortaya koydu (DoD, 2011: 89). Buna göre sırasıyla insan kontrollü, insan temsilli, insan denetimli ve son olarak tam otonom biçiminde ilerleyecek 4 aşamalı bir süreç dahilinde tam otonomiye ulaşılması planlanmıştır (Scharre, 2020: 44). Yol haritasının açıklanmasından iki yıl sonra ABD Deniz Kuvvetleri, *X-47B dronu*'nu otonom bir biçimde denizde bulunan uçak gemisine indirdi. 2014 yılında otonom bir helikopter, doğaçlama olarak iniş alanı bulup, inmeyi başardı. Bir yıl sonra *X-47B* havada ilk otonom yakıt ikmalini yaparak tarihe geçmiştir (Scharre, 2020: 45).

ABD'nin denetimli OSS araçlarına da örnek olarak, deniz güvenliğinde *Aegis savaş sistemi* ve *Phalanks Yakın Silah Sistemi*; kara güvenliği için *Patriot* sistemleri gösterilebilir. Sistemlerin çalışma mantığı önceden hangi tehditlerin vurulacağı, hangilerinin görmezden gelineceği tanımlandıktan sonra sistemin otonom olarak çalıştırılmaya başlanması ve savunmanın gerçekleştirilmesine dayanır. Bu tür sistemler yarı otonom ya da denetimli otonom olarak çalıştırılabilen farklı modlara da sahiptir, sistemin denetimli modda çalıştırıldığı ya da tamamen denetimli olan sistemlerde, sistemin komutlara doğru tepkiler vermemesi halinde insan müdahalesi ile kapatılması mümkündür (Scharre, 2020: 77).

Denetimli otonom sistemlerin üstlendikleri asıl işlev, olası ani saldırılara karşı hızlı tepki vermektir. Dolayısıyla daha fazla otonominin gerekçesi daha hızlı savunma yapabilmektir. Bu da denetimli OSS'leri savunma karakterli bir yapıya çevirmektedir.

Yarı OSS'ler ise en yaygın kullanılan sistemlerdir. Temel olarak aracın uzağında bulunan bir insanın kontrolüyle çalışırlar. İHA'lar, SİHA'lar en bilinen örnekleridir. ABD'de *Predator* ve *Reaper dronları* otonomi seviyeleri düşük olan, insan operatörlerce yönetilen

[26] LOCAAS: Low Cost Autonomous Attack System - Düşük Maliyetli Otonom Saldırı Sistemi

güvenlik araçlarına örnek olarak gösterilebilir. *Air Force Global Hawk* ve *Army Grey Eagle* otonomi seviyeleri daha yüksek yarı otonom sistemlerdir (Scharre, 2020: 44).

ABD'nin gerek yarı otonom sistemleri kullanması gerekse de insan makine işbirliği modelini uygulamasının ilk örneklerine 1991 Körfez Savaşı dönemlerinde rastlanılmaktadır. Bu dönemde YZ çalışmalarına daha çok, destek hizmetleri bakımından önem verilmekteydi. ABD'nin operasyon yönetmek için asker ve mühimmat sevkiyatı planlamasında yaşanan aksaklıkları gidermek amacıyla *DARPA (Defense Advanced Research Project Agency – İleri Savunma Araştırma Proje Ajancı)* tarafından YZ destekli bir planlama programı hazırlaması istendi. *DARPA, DART (Dynamic Analysis and Replanning Tool – Dinamik Analiz ve Yeniden Planlama Aracı)* isimli projeyi geliştirdi. Bu projenin Körfez Savaşı'nda ve sonraki 5 yılda, ABD için sağladığı ekonomik tasarruf, geçmiş 30 yılda YZ'ye harcanan bütçeyi telafi etmiş ve ABD'yi ekonomik olarak kazançlı konuma geçirmiştir (Branch, 2018: 27; Say, 2021: 90) . Aynı Körfez Savaşı'nda ABD ordusu tarafından, İsrail'den satın alınan İHA'lar ve mayın temizleme amacıyla geliştirilen insansız kara araçları kullanılmıştır. Singer'in (2009: 28) ifadesiyle Körfez Savaşı, insanlık tarihinde ilk defa insanların insan olmayanlara teslim olduğu bir savaş olmuştur.

İnsan makine işbirliğinin başarılı bir örneği olan DART projesi ve insansız araçların savaş alanında sağladığı avantajlar, YZ geliştirme çalışmaları ve askeri düzeyde kullanımını teşvik etmiştir. Örneğin, ABD'nin Irak'a müdahalesinin ilk dönemlerinde yarı otonom sistemlerin sayısı oldukça az iken, 2009 yılına gelindiğinde Irak'ta ABD'ye ait 5.300 İHA, 12.000 civarında da bomba imha ya da istihbarat toplama gibi işlevler yüklenen insansız kara aracı bulunmaktaydı (Balta, 2021: 36).

ABD'nin insan makine işbirliği kapsamında en öne çıkan projelerinden bir tanesi de *Maven Projesi*'dir. Maven projesi, ABD Savunma Bakanlığı tarafından yönetilen, 130'un üzerinde özel sektör işletmesinin katkısıyla genişleyen ve bilgisayarla görüntüleme başta olmak üzere, YZ teknikleriyle askeri teknolojiyi güçlendirmeyi amaçlayan bir projedir (Council, 2019: 37). ABD, Maven Projesi'ni Suriye ve Irak operasyonlarında aktif olarak kullanmak suretiyle, terör hedeflerini bulabilen algoritmalar geliştirmiştir. Makine öğrenmesi tekniği ile çalışan algoritmaların tespit ettiği hedefler, uzaktan kontrol edilen SİHA'lara bildirilmekte ve hedefler imha edilmektedir (Darıcılı, 2020: 59). Maven Projesi'nin geliştirilme çalışmalarında Google'da dahil olmak üzere önde gelen teknoloji şirketleri paydaş olarak yer almıştır. Fakat Google ve Maven Projesi'ni birlikte anmanın daha çarpıcı bir nedeni; Google çalışanlarının şirketleri ile Savunma Bakanlığı arasındaki anlaşmayı öğrendikten sonra, katil robotlara katkı

sunmak istemedikleri gerekçesiyle tepki göstermek amacıyla mektup yayınlamaları ve bunun üzerine Google'ın 2019 yılında biten sözleşmeyi yenilemeyeceğini açıklamasıdır (Lanier, 2018).

Maven-Google olayı güvenlik araçlarındaki mülkiyet ve geliştirme sürecinde rol üstlenen aktörler bakımından yaşanan dönüşümün önemli bir göstergesidir. Devletler tek başlarına karar alma ve uygulama yeteneklerini belirli bir ölçüde kaybetmekte, devlet dışı aktörler güvenlik alanında da söz sahibi olmaya başlamaktadır.

ABD'nin operasyonlarında yarı OSS'leri taarruz amacıyla kullanması da uluslararası hukuka aykırılık oluşturduğu gerekçesiyle eleştirilmektedir. Eleştiriler hem *jus ad bellum* hem de *jus in bello* kapsamında şekillendirilmektedir. Özellikle *jus in bello* bağlamında, dron operatörlerinin ateşleme kararını verirken insani duygulardan daha uzakta olarak, bir video oyunu oynuyormuşçasına karar verdikleri iddia edilmektedir. Ayrıca, hedeflerin sivil-savaşçı ayrımı yapma kapasitesinin ölçülebilir olmadığı ve gerekli olan kuvvet kullanma sınırının kontrol edilebilirliği üzerindeki şüpheler ileri sürülen diğer argümanlardır (Taşkesen, 2020: 289 vd.).

ABD'nin YZ ve güvenlik alanında geliştirme sürecinde olduğu bir diğer proje ise *sürü dronlar* projesidir. Sürü dronlar tek merkezi beyine bağlı birden fazla dronun fırlatıldıktan sonra kendi aralarında iletişim kurmak suretiyle, özgülendikleri amaca ulaşmak için iş bölümünü planlayıp faaliyetlerini gerçekleştirmeleri mantığına dayanır. Karar verme sürecinin nasıl şekilleneceği/şekillendiği henüz çok basit seviyede tasarlanan algoritmalar ile belirlenmektedir. Sürü dronların geliştirilme ihtiyacı, her dron için bir operatör gerekliliğini ortadan kaldırmak istenmesinden doğmaktadır. Bu projenin başarılı olması, ekonomik kaynaklar ve insan kaynağı bakımından avantaj sağlamasının yanı sıra, belirlenen hedefe daha çevik ve etkili saldırılar düzenlenmesini de mümkün kılacak olmasıdır (Scharre, 2020: 47-48).

ABD Savunma Bakanlığı, 2016 yılında 103 drondan oluşan bir *sürü dron* tanıtımını yaptı. Sadece hava sahasında değil, aynı zamanda deniz sahasında da sürü dron teknolojisi geliştirilmektedir. 2014 yılında yapılan bir tatbikatta 5 bot bir sürü halinde görevlendirilmiş ve görev olarak şüpheli araçları araştırmaları istenen dronlar, bu görevin ötesine geçerek şüpheli aracın önünü kesmiş ve ablukaya almışlardır (Scharre, 2020: 50).

Sürü halinde hareket eden dronların kendi kararlarını alma aşamasına varmaları halinde, hangi durumda hangi kararı verebilecekleri öngörülebilir olmaktan uzaktır. Amaca özgülendikten sonra bu amacı gerçekleştirmek için meşru-gayrı meşru sınır ayrımını yapıp

yapamayacakları belirsizdir. İnsanlara göre YZ'nin daha yaratıcı ve öngörülemez kararlar ve amaca ulaşmak için alternatif yollar bulduklarına dair en çarpıcı örnek olarak, Traveller isimli oyun yarışmasında, Doug Lenat tarafından geliştirilen *Eurisko* programının taktik yaratıcılığı ve başarısı gösterilebilir[27].

Sürü dronların birbiriyle iletişim kurması ve karar alma süreçleri için ortak bir bağlantı gerekmektedir. Bu bağlantının güvenliğinin nasıl sağlanacağı, yazılıma yönelik bir saldırı ile dost-düşman tanımlarının değiştirilmesine karşı nasıl tedbirler alınacağı henüz çözülebilmiş sorunlar değildir. Bu nedenle de fırlatıldıktan sonra tam otonom olarak çalışıyor olsalar da, aslında mevcut sürü dronlar denetimli otonom sistemlerdir. Çünkü beklenmeyen durumda, insan müdahalesi gereklidir ve sistemler bu şekilde kurgulanmışlardır. Sürü dron teknolojisi başta olmak üzere, OSS'ler için en büyük tehdit siber güvenlik konusunda toplanmaktadır. Devletler siber ağların güvenliğini sağlamadan, güvenlik açıkları ve öngörülemezlik nedenleriyle daha ileri teknolojilere geçiş yapmayı tercih etmeyecektir. Bir diğer sorun ise, her alanda dronlar arası iletişimi sağlayacak ağ alt yapısının bulunmamasıdır. ABD'nin OSS alanında geliştirdiği strateji belgeleri ve yol haritaları mevcuttur. Bu belgeler ABD nazarında OSS'yi stratejik bir teknoloji konumuna getirmektedir. Oluşturulan politikalar ve stratejiler RMA kapsamında konuyu ele almak için gerekli koşulları sağlamaktadır. Özellikle sürü dron teknolojisi ile yeni bir örgütlenme modeline geçiş görülmektedir.

3. Siber Güvenlik

ABD, 2010 yılı Ulusal Güvenlik Strateji Belgesi'nde siber güvenlik konusuna yer vererek, konuyu ulusal bir güvenlik sorunu seviyesinde değerlendirmiştir. Belgede ABD'nin

[27] Traveller belirli bütçe ve kurallar dahilinde bir filo kurarak, rakibin filosunu yenerek bir üst tura geçmenin amaçlandığı bir oyundur. Lenat, 1981 yılında düzenlenen ulusal turnuvaya katılmak için Eurisko'yu kullandı. Oyunun kurallarını programa ekledikten sonra kendi kendine oynayan ve kazanç yolları arayan Eurisko çarpıcı bir şekilde "oyunun kurallarını değiştirelim ve kendimizi galip ilan edelim" gibi çözümleri de içeren kazanç stratejileri hesaplıyordu. Lenat insan doğasının kabul etmeyeceği, insan zekasıyla doğru ve uygulanabilir olmadığı basitçe anlaşılabilen çözüm önerilerini programdan siliyordu. Eurisko, tüm bütçesini küçük torpidobotlara hacayarak bir donanma kurmuştu. Gerçek dünyada güçsüz araçlardan oluşan bir donanma ile güçlü bir donanmayı yenebileceğini hesaplamak insan aklına aykırıdır. Ancak oyunun kuralları gereği, taraflardan birinin donanması yok olduğunda diğer tarafın en az bir aracı kalması kazanmaya yetiyordu. Küçük torpidobotların sayısının çok olması ve aynı bütçeyle güçlü gemileri almak isteyen yarışmacıların sayıca daha az gemi alabiliyor olması Eurisko'nun 1981 şampiyonu olmasına yetmişti. Çünkü rakiplerin büyük gemileri yok olduğunda, küçük torpidobotlardan hala ayakta kalanlar oluyordu.

Yarışma kurallarında değişiklik yapılarak 1982 turnuvası düzenlendi. Kurallara Eurisko'nun stratejisini işe yaramaz kılacak biçimde donanmanın "çeviklik değeri" puanlamaya dahil edildi. Böylelikle kalabalık filo kurmanın avantajını ortadan kaldırmak istediler. Ancak Eurisko yeni kurallara göre yeniden çalıştırılıp, bu sefer yine kalabalık filolar kurmuş ve yara alan gemilerini kendisi batırarak donanma çeviklik ortalamasını yükseltmeyi strateji olarak belirlemişti. Bu da 1982 şampiyonluğunu getirmiştir. Say, C. (2021). *50 Soruda Yapay Zeka*. 7 Renk.

liderliği ve gücünün kaynağı olarak gösterilen teknolojinin aynı zamanda yıkıcı ve bozucu etkileri olduğu da ifade edilmektedir. Günlük hayatın ve kamu güvenliğinin önemli bir kısmının elektrik şebekelerine bağlı olarak sürdürüldüğü saptamasının ardından, potansiyel hasımlarının bu kritik altyapılara büyük ölçekte zarar vermek için siber zayıflıkları kullanabileceği belirtilmiştir. ABD'nin ekonomik rekabet yeteneğinin temeli olarak internet ve e-ticaret gösterilmiş, ancak siber suçlar sonucunda şirketlerin ve tüketicilerin, fikri mülkiyet hakları ihlalleri de dahil olmak üzere yüz milyonlarca dolar zarara uğradıkları ifade edilmiştir. Tehditlerin kaynağı geniş bir yelpazede tanımlanarak, bireysel suçlular, hacker grupları, terör örgütleri ve gelişmiş devletler potansiyel tehdit olarak değerlendirilmiştir. Siber güvenlik kapsamında iki temel mücadele yöntemi belirlenmiştir. Bunlardan ilki insana ve teknolojiye yatırım yapmak diğeri ise ortaklıkları güçlendirmektir (WhiteHouse, 2010: 27-28).

ABD, 2010 yılında Siber Komutanlığı *(cybercom)* kurmuştur[28]. Siber Komutanlık beş temel amacı gerçekleştirmektedir. Bunları şu şekilde özetlemek mümkündür (Singer & Friedman, 2018: 184):

- Geleneksel ordunun kara, hava ve denizde yaptığı gibi siber uzayı bir "harekat alanı" olarak değerlendirip, faaliyetler gerçekleştirmek,
- Siber uzayda başarılı olmayı sağlayacak gerekli güvenlik konseptini oluşturmak ve uygulamak,
- Özel sektör ve diğer kurumlar gibi paydaşlarla yeni ortaklıklar geliştirmek,
- Uluslararası ortaklar ile yeni ortaklıklar geliştirmek,
- Siber uzayda ordunun savaş ve kazanma usullerini belirleyip teşvik edici yeni yetenekler geliştirmek.

Sıralanan amaçları gerçekleştirmek için Siber Komutanlığın üç yeni siber güç yaratması ve kullanması kararlaştırılmıştır. Buna göre oluşturulacak olan yeni siber güçler şunlardır; orduya ait bilgisayar ağlarını savunmakla görevli "siber korunma güçleri", sahada görev yapan askerlere destek sağlayacak olan ve bölgesel olarak örgütlenen "çatışma görev kuvvetleri", son olarak da kritik altyapıların korunmasından görevli olan "ulusal görev kuvvetleri" (Singer & Friedman, 2018: 184).

ABD, 2010 yılından sonra bir dizi strateji belgesinde siber güvenliğe giderek artan düzeyde önem ve yer vermekle birlikte, politikaların temel motivasyonu savunma odaklı olarak

[28] Detaylı bilgi için bkz. https://www.cybercom.mil/About/History/

belirlenmiş ve ısrarlı bir biçimde uluslararası işbirliğinin gerekliliği vurgulanmıştır (Selçuk, 2020: 71 v.d.; Soni, 2020; WhiteHouse, 2010: 27-43). Çünkü siber uzayda saldırının kimden geldiğini tespit etmek çoğu zaman mümkün olmamaktadır. Doğası gereği anonim ve anarşik olan siber uzayda etkili savunma yapabilmek, geniş veri paylaşımı ve ortaklık gerektirmektedir. Başka bir deyişle, devletler hem diğer devletlerden hem de özellikle devlet dışı gruplardan gelen saldırılardan korunmak için siber uzayda işbirliğine zorunlu olarak ihtiyaç duymaktadırlar.

Siber uzayda ortaya çıkan uyuşmazlıklar ve saldırılar çoğunlukla yine siber uzayda çözümlenmektedir. Ancak ABD kaynaklı bir raporda geçen ifadeler, siber uzaydaki saldırılara fiziksel ortamda da karşılık verilebileceğini düşündürmektedir. Raporda geçen ifade tam olarak şudur: *"Eğer bir siber saldırı geleneksel bir ordunun saldırısının sebep olacağı, ölüm, hasar, yıkım veya yüksek seviyede bozulma yaratıyorsa, güç kullanımı değerlendirmesi için misillemeye layık olabilecek bir aday olur"* (Singer & Friedman, 2018: 186). Siber saldırının fiziksel saldırı ile karşılanabileceği düşüncesini kuvvetlendiren bir diğer ifade ABD ordu subaylarından bir tanesine aittir. Şöyle der subay: *" Eğer elektrik şebekemizi kapatırsanız, belki de bacalarınızın birinden içeri bir füze göndeririz"* (Singer & Friedman, 2018: 186).

Bu çalışmanın hazırlandığı dönemde ABD tarafından bir siber saldırıya karşılık olarak fiziksel güç kullanılmış değildir. Ancak alıntılanan ifadeler, bu durumun ne denli mümkün olduğunu gösterecek açıklıktadır. Dolayısıyla ABD'nin siber saldırıya karşı, siber savunma yöntemlerinin tatmin edici düzeyde sonuçlar vermediği durumların meydana gelmesi halinde, fiziksel güç kullanacağı yönünde bir çıkarım yapmak mümkündür. Bu durumda yine siber uzayın en temel sorunu olan failin tespiti ve ispatı zorluğu gündeme gelmektedir. Bir önceki bölümde açıklanan botnet ya da DDoS saldırılarında kullanılan zombi bilgisayarların bulunduğu ülke sınırları ya da internet ağına bağlı olduğu ülke, söz konusu saldırıdan sorumlu tutularak, fiziksel saldırının hedefi olabilir mi? Bunun mümkün olmadığı varsayıldığında, ABD'nin siber saldırıya karşı fiziksel güç kullanma iradesi uygulama alanı bulamayacaktır.

İsnat etme probleminin yoğun bir biçimde yaşandığı siber uzayda ABD neredeyse en yüksek dozda Çin'i ve Rusya'yı sorumlu tutan ve hedefe koyan açıklamalar yapmaktadır (Selçuk, 2020: 82). Singer ve Friedman'ın (Singer & Friedman, 2018: 189) aktardığına göre; ABD Kongresi bir raporunda Çin'i *"ABD'deki siber ihlallerin en aktif ve inatçı faili"* olarak tanımlamıştır.

ABD'nin gerek açıklamaları gerekse de söylemleri Çin'e odaklanmakta ve fikri mülkiyet haklarını ihlal ettiği gerekçesiyle suçlamaktadır. Bir yönüyle fiziksel kullanma tehdidinde

bulunması, diğer yönüyle açık bir hedef göstermesi siber güvenliği uluslararası güvenliğin öncelikli bir çalışma alanı seviyesine yükseltmektedir. Sadece akademik çalışmalar değil, aynı zamanda uluslararası politika bağlamında da konu gündeme gelmiştir. 2015 yılında ABD ile Çin arasında siber saldırılara karşı mücadele için bir anlaşma yapmışlardır. Anlaşmaya göre; fikri mülkiyet ve ticari bilgi hırsızlıkları başta olmak üzere siber suçlar taraflarca araştırılacak, veriler toplanacak ve diğer tarafla paylaşılacaktır (WhiteHouse, 2015b).

4. ABD ve Askeri Alanda Devrim

ABD'nin RMA çalışmaları 1980'li yıllarda Sovyet teorisyenlerinin MTR kavramı çerçevesinde elektronikle ilişkili teknolojiler kapsamında geliştirdikleri yaklaşımların takip edilmesi ile başlamıştır (Martyanov, 2019: 72 v.d.). İstihbarat seviyesinde başlayan çalışmalar 1990'lı yıllara gelindiğinde Savunma Bakanlığı'na bağlı olarak kurulan ONA *(Office of Net Assesment)* ofisi ile kurumsallaşmıştır. ONA de Sovyet MTR çalışmalarını takip etmiş ve teknolojiye vurgu yapan MTR kavramı yerine; örgütsel, operasyonel ve insan yönetiminde bir değişime vurgu yapan RMA kavramını kullanmaya başlamıştır. Bu kapsamda yayınlanan bir ONA raporu, RMA'nın büyük askeri değişim için birleştirilmesi gereken dört anahtar unsuru ortaya koymuştur. Bu unsurlar: i) teknolojik değişim, ii) askeri sistemlerin gelişimi, iii) operasyonel inovasyon ve iv) örgütsel inovasyondur (Raska, 2021: 463). Bu unsurlar Krepinevich tarafından tanımlanan MR'nin unsurlarıdır. MR-RMA tartışması 1990'lı yıllarda ortaya çıkmış ve yukarıda da değinildiği gibi MR büyük askeri değişimin büyük stratejik yönünü esas alırken; RMA, Murray ve Knox'un çalışmalarında yer verdiği gibi, doktrin, taktik, usul ya da teknoloji değişikliklerini içeren bir kavram olarak gelişimine devam etmiştir (Murray & Knox, 2001; Raska, 2021: 463). ONA Anrew Marshall'in öncülüğünde, özellikle soğuk savaş yıllarında ABD-SSCC arasındaki güç mücadelesinin stratejik boyutu üzerine çalışmalar yapmış ve stratejiler üretmiştir (Krepinevich & Watts, 2015).

Marshall 1996 yılında hazırladığı raporda ve özellikle de 2000'lerin başından itibaren ABD'nin stratejisini Avrupa'dan Çin'e yöneltme yönünde düşünceler geliştirmiştir. Çin'in hem ekonomik olarak hem de yeni askeri teknolojileri uyarlama konusundaki ilerlemesini dengelemek bu dönemde Marshall düşüncesinin ve ONA stratejilerinin temelini oluşturmuştur (Krepinevich & Watts, 2015: 227 v.d.). Marshall bu dönemde üç temel denge stratejisi tanımlamıştır (Krepinevich & Watts, 2015: 230-231) :

- Asya bölgesinde askeri dengeye odaklanan bölgesel değerlendirme yapmak ve Çin'in yükselişine karşı önlem ihtiyacını vurgulamak,

- Alan engelleme ve erişim engelleme (A2/AD)[29] çevrelerinde işlevsel bir güç projeksiyonu değerlendirmesi yapmak,
- Vietnam Savaşı'ndan sonra ortaya çıkan gerçekçi muharebe eğitiminde ABD'nin avantajlarının dayanıklılığını değerlendirmek.

ABD'nin Çin'i dengeleme ve yükselişine karşı önlem alma ihtiyacı aslında RMA motivasyonlarından birini oluşturan tehdit algısına karşılık gelmektedir. Çin'i yükselen bir tehdit olarak tanımlamak, eldeki imkanları ve yeni teknolojileri bu tehdidi bertaraf edecek biçimde kullanmayı gerektirmiştir. Marshall'ın önerdiği stratejilerden YZ ile en yakın ilişkili olanı şüphesiz ki A2/AD ile mücadele girişimi olmuştur.

ABD'nin RMA çalışmalarının en öne çıkan boyutları ikinci Körfez Savaşı sırasında gösterdiği performanstır. Bu savaştaki ABD başarısını Murray ve Knox (2001: 189) *"bir RMA reklamı"* olarak tanımlamaktadırlar.

ABD'nin YZ kapsamındaki RMA çalışmaları doktrin ve stratejik boyutlarıyla incelendiğinde, yukarıda detaylı olarak ele alınan 3OS stratejisi doktrin boyutunu ortaya koymaktadır. Bu stratejide insan-makine işbirliği vurgusu yapılmış olup, sonrasındaki çalışmalarla tam otonom güvenlik araçlarına kademeli geçiş için yol haritaları düzenlenmiştir.

ABD kara, hava ve denizde YZ destekli araçları geliştirip askeri teknolojiye uyarlamanın yanısıra karar verme süreçlerinde de YZ'den faydalanarak taktik ve ekonomik avantajlar sağlamaktadır (Payne, 2018). Bu yönüyle askeri sistemin örgütlenmesi bakımından da bir değişim içinde olduğu görülebilmektedir.

Bu tez çalımasında odaklanılan temel husus YZ etkisiyle gelişen güvenlik araçlarının MR-RMA ayrımında nerede konumlandırılması gerektiğini saptamak ve ABD ile Çin üzerinden konuyu incelemektir. ABD'nin ortaya koyduğu stratejiler ve politikalar OSS ve siber güvenliğe stratejik bir önem yüklediğini ve aynı zamanda bu bağlamda Çin'i stratejik rakip olarak tanımladığını göstermektedir. ABD ile Çin'in konu bağlamında stratejik rakip olarak tanımlanmasına ilişkin soruya en açıklayıcı yanıt 1996'da Marshall'ın ONA'da ortaya attığı görüşlere bakmak gerekir (Krepinevich & Watts, 2015: 225-226). Marshall bu yıllarda ABD'nin politikalarını Avrupa yerine Asya'ya yöneltmesi ve Çin'i dengelemesi gerektiğini

[29] Bir devletin rakip ya da düşmanlarının ulaşmasını istemediği alanlarda kullanılmak üzere geliştirilen ve genellikle yeni teknolojilere dayanan bir tür güvenlik aracı. Detaylı bilgi için bkz. https://trguvenlikportali.com/ders-10-a2-ad-doktrini/

vurgulamıştır. Dolayısıyla düşünsel boyutuyla birlikte yaklaşık çeyrek yüzyıldır ABD Çin'i stratejik rakip olarak konumlandırmaktadır.

ABD, OSS ve Siber güvenlik alanında dünya liderliği vizyonuyla hareket ettiği için Çin'i de kapsayan rakiplerine karşı üstünlük kurmayı amaçlamaktadır. Bu kapsamda geliştirdiği teknolojilerle Asya'da Çin'i dengelemek ve Çin'in A2/AD politikasını etkisizleştirmek amaçlarına yönelmiştir. Buradan hareketle ABD'nin stratejik rakibine yönelik politikalarını YZ temelli yeni güvenlik araçları üzerine inşa ettiği sonucuna ulaşmak mümkündür. Çünkü bu teknoloji iki devlet arasındaki rekabeti tetikleyen bir niteliğe sahiptir.

B) Çin Halk Cumhuriyeti (Çin)

Çin yüzyılın başlarından itibaren yükselen bir güç olarak uluslararası politika sahnesine giriş yapmış, özellikle ucuz iş gücünün sağladığı avantajdan yararlanarak doğrudan dış yatırım çekebilmiş ve bu sayede ekonomik olarak gelişmiş bir ülkedir. Çin'e çalışmada yer verilmesinin nedeni ekonomik gücü ve teknolojik gelişmişlik kapasitesi bakımından YZ yatırımlarını yapabilen bir ülkelerin başında gelmesidir. Diğer taraftan ABD'nin karşısında Pasifik Bölgesi'nde dengeleyici pozisyonda olabilecek kapasitede bir ülkedir.

Çin'in YZ alanında ortaya koyduğu stratejik vizyon ve bu vizyonu uygulamak için geliştirdiği politikalar, uluslararası sistem üzerinde etkili olabilecek büyüklükte ve önemdedir. Özellikle ekonomik ilişkiler bağlamında öne çıkan Çin politika ve yatırımları, YZ teknolojilerinin çifte kullanım özelliği göz önünde bulundurulduğunda, ulusal ve uluslararası güvenlik boyutlarında da incelemeye değer nitelikte bir öneme sahiptir. Bir önceki bölümde ABD politikaları incelenirken, ilgili dokümanlarda sıklıkla adı geçen iki ülkeden birisinin Çin olması, Çin'in inceleme konusu yapılmasının bir diğer nedenidir. Buna ek olarak YZ-RMA dalgasının ilk 5 dalgadan farklılaşan bir yönü yukarıda değinildiği üzere, ABD'nin güçlü bir rakip ile karşı karşıya kalmış olmasıdır. Bu yönüyle de ABD-Çin arasında RMA bağlamında stratejik rekabet olup olmadığının sorgulanabilmesi için Çin'in konu bağlamındaki politika ve stratejileri incelenmelidir.

Çin 2013 yılından itibaren ulusal düzeyde YZ geliştirme niyetini ve amaçlarını ortaya koyan bir dizi belge yayınlamıştır (Roberts et al., 2021: 60). 2015 yılında Çin Devlet Konseyi *(ÇDK)* tarafından yayınlanan İnternet + kullanım kılavuzu, aynı yıl yayınlanan ve 10 yıllık bir planı içeren 2025 vizyonu ve 2016 yılında Çin Komünist Partisi Merkez Komitesi tarafından yayınlanan 13. beş yıllık plan bu bir dizi ulusal nitelikteki belgelerden bazılarıdır (Roberts et al., 2021: 60).

Çin'in uluslararası bir aktör olma iddiasıyla YZ alanına girişi ise 2017 yılında ÇDK tarafından yayınlanan *"Yeni Nesil YZ Geliştirme Planı – (YNGP)"* çerçevesinde olmuştur. Bu planın kapsam, amaç ve stratejileri Çin'in YZ'ye yüklediği anlamı ve YZ teknolojilerinden beklentilerini anlayabilmek için değerli bir kaynaktır.

1. Çin'de Devletin Yapay Zekaya Yönelik Yaklaşımları

YNGP[30], YZ teknolojisinin bileşenleri ve bu bileşenlerin geliştirilebilmesi için gerekli adımlar, ekonomik gelişim için yatırım yapılması gereken endüstriler, güvenli ve elverişli bir zeki toplum inşa etmek, YZ alanında sivil-asker entegrasyonunu güçlendirmek, güvenli ve verimli bir zeki altyapı sistemi kurmak, yeni nesil YZ alanında bilim ve teknoloji projeleri planlamak gibi konu başlıkları etrafında kurgulanmış bir plandır (State Council, 2017).

YNGP kapsamında stratejik hedefler üç aşamalı olarak belirlenmiştir. Bu hedefleri şu şekilde özetlemek mümkündür (State Council, 2017: 5 v.d):

- 2020 yılına kadar YZ'nin teorisinde ve teknolojisinde önemli bir ilerlemeye ulaşmak. Bu kapsamda büyük veri, karşı-ortam istihbaratı, sürü zekası, hibrit güçlendirilmiş zeka ve otonom zeka sistemleri ilerlemenin hedeflendiği teknolojiler olarak belirlenmiştir. Bu teknolojiler aracılığıyla; uluslararası alanda YZ endüstrisi rekabetinde ilk derecelere girmek hedeflenmiştir. Bu hedefi gerçekleştirmek için, temel YZ alanlarına 150 Milyar Yuan[31], YZ ile ilişkili diğer teknoloji alanlarına ise 1 Trilyon Yuan yatırım yapılması planlanmıştır.
- 2025 yılı itibariyle Çin YZ alanında büyük bir atılım yapmayı başaracaktır. Yeni nesil YZ, zeki üretim, tıp, tarım, ulusal savunma yapısı gibi alanlarda temel YZ alanlarının ekonomik büyüklüğü 400 Milyar Yuan'dan fazla, ilgili diğer alanların ekonomik büyüklüğü 5 Trilyon Yuan'dan fazla olacaktır.
- 2030 itibariyle, Çin'in YZ teorisinde, teknolojilerinde ve uygulamalarında dünyada lider seviyeye ulaşmak ve Çin'i YZ inovasyon merkezi yapmak.

Anılan planda belirlenen hedefler ekonomik ve teknolojik üstünlüğü ele geçirmek amacını göstermektedir. Bu planın uygulanması süreci Bilim ve Teknoloji Bakanlığı koordinasyonuna bırakılmıştır (Roberts et al., 2021: 60-61). 2012-2017 yılları arasında Çin

[30] Çalışmada kaynak olarak planın İngilizce çevirisi kullanılmıştır. New America kuruluşu adına çeviriyi yapanlar şunlardır: Rogier Creemers, Graham Webster, Paul Triolo ve Elsa Kania.
[31] 150 Milyar Yuan yaklaşık olarak 23,6 Milyar dolara karşılık gelmektedir.

tarafından ABD'deki YZ sektörlerine, toplamda 641 farklı anlaşma ile yaklaşık 19 Milyar dolar tutarında yatırım yapılmıştır. Bu durum ABD Dış Yatırım Komitesi tarafından şüpheli bulunmuş ve Çin'in YZ temelli stratejik sektörlere yatırımı engellenmiştir (Wang & Chen, 2018: 254-255). Çin açısından ABD'ye yatırım yapmanın başlıca avantajı, kendi ülkesinde yetişmiş insan kaynağının eksikliğini gidermektir. Çin bu konudaki dezavantajını gidermek için, lisansüstü seviyede eğitim programları başlatmış ve yerel insan kaynağı gücünü artırmayı amaçlamıştır. Örnek olarak Beihang Üniversitesi ve Çin YZ Teknoloji Akademisi bünyesinde açılan lisansüstü programlar gösterilebilir (Kania, 2017: 11)

Çin, Planın uygulanması sürecinde önde gelen şirketler arasında yarışma düzenleyerek, her sektörde bir Çin firmasını dünya ölçeğinde rekabet edebilecek güce ulaştırmak için desteklemiştir. Bu kapsamda, Baidu firması otonom sürüş, Alibaba akıllı kentler ve Tencent firması tıbbi teşhisler için bilgisayarla görme alanında seçilip desteklenmiş özel sektör firmalarıdır (Roberts et al., 2021: 61).

Hem YNGP öncesi doğrudan dış yatırımlar hem de Planın uygulanması süreci ekonomi ve eğitim üzerine şekilleniyor gibi görünse de, aslında bu alanlarda yapılan neredeyse her çalışma, YZ teknolojilerinin çifte kullanım avantajı sayesinde, askeri teknolojilerde de kaldıraç etkisi yaratmaktadır (Kania, 2017: 11). Takip eden bölümde Çin'in öne çıkan YZ temelli güvenlik araçlarına ve tam OSS'nin risklerine karşı tutumuna yer verilecektir.

Çin'in YZ üzerine geliştirdiği politika ve stratejilerin varlığı bizatihi konuyu RMA bağlamı içine yerleştirmektedir. Çünkü hem YZ temelli güvenlik araçlarına stratejik bir önem atfederek askeri doktrin ve örgütlenmesini şekillendirmekte hem de YZ'yi ticari bir araç olarak kullanmak suretiyle ABD ile arasındaki rekabete yeni bir boyut kazandırmaktadır.

2. Otonom Silah Sistemleri

Çin'in, İsrail'den satın aldığı Harpy dronları üzerinde ters mühendislik yapmak suretiyle, kendi tam otonom Harpy sistemlerini ürettiği iddia edilmektedir (Scharre, 2020: 78). Tam OSS geliştirdiği bilinmekle birlikte, Çin bu tür silahlara karşı başlatılan kampanyalara da kısmen destek vermiştir. Desteğin koşulu, ya da başka bir deyişle, Çin'in OSS'lere yönelik kaygılara karşı cevabı, kullanımının yasaklanması ancak üretiminin ve geliştirilmesinin yasaklanamayacağı yönündedir (Campaign to Stop Killer Robots, 2019: 2). Çin'in bu yaklaşımı, *"İlk Kullanıma Hayır (No First Use)"* sözleriyle formüle edilerek, nükleer silahlar üzerindeki uluslararası uzlaşı ile analoji kurulmuştur. Çin'in, askeri alanda agresif bir biçimde YZ geliştirmesine rağmen, böyle bir uluslararası söylem geliştirmesi, askeri amaçlı YZ

kullanımını perdelemek ve politik düzeyde propaganda stratejisi olarak yorumlanmıştır (Roberts et al., 2021: 63-64).

Çin'in askeri düzeyde YZ geliştirilmesi ve kullanılması politikaları, Halk Kurtuluş Ordusu (HKO) tarafından yürütülmektedir. HKO resmi sözlüğünde YZ silahları şu şekilde tanımlanmaktadır: *"düşman hedefleri otomatik olarak izlemek, ayırt etmek ve imha etmek için YZ ile desteklenen; çoğunlukla bilgi toplama ve yönetim sistemleri, kural temelli sistemler, karar sistemlerine yardım, görev icra etme sistemleri gibi sistemlerden oluşan bir silahtır." (Kania, 2017).* Tanımdan da anlaşılacağı üzere, Çin YZ silahlarını geniş anlamda değerlendirmekte; insan karar alıcılara destek sunan yarı otonom sistemlerden, tek başına hedef tespit edip imha edebilen tam OSS'lere kadar tüm silah türlerine aynı tanım içinde yer vermektedir.

HKO araştırmacılarının öngörülerine göre; geleceğin savaşlarının kara, deniz, hava ve uzay fark etmeksizin tamamının insansız sistemler tarafından çok yönlü olarak gerçekleştirilecektir (Kania, 2017: 22). Gerek Devlet Başkanı Xi Jinping'in *" giderek artan şiddetli uluslararası askeri rekabet ortamında sadece yenilikçiler kazanır"* sözleri gerekse de HKO'nun *"savaştan önce kazanmak"* yaklaşımı Çin'in askeri teknolojilerini modernize etme motivasyonunu göstermektedir (Roberts et al., 2021: 63). Bu söylem ve yaklaşımlara uygun olarak Çin askeri gücü, YZ desteğiyle modernize edilmekte; kara, hava, deniz ve uzay güvenliği için insansız sistemler geliştirilmektedir.

Çin, 3OS'e benzer biçimde insan makine işbirliğinin daha belirgin olduğu sistemler geliştirmektedir. TYW-1, HKO deniz kuvvetleri ve hava kuvvetleri tarafından keşif amaçlı kullanılan bir İHA sistemidir. Sistemin temel özelliği yüksek derecede otonomiye sahip olmasıdır. Bağımsız olarak kalkış ve iniş yapabilmekte olup, izleme ve hedefe taarruz yapmak için minimum düzeyde insan müdahalesi gerektirmektedir (Kania, 2017: 22-23).

Çin'in insansız deniz ve deniz altı araçları da bulunmaktadır. Özellikle Doğu ve Güney Çin Denizi güvenliğini ve bu bölgedeki Çin çıkarlarını korumak amacıyla geliştirilen ve kullanılan insansız araçlara örnek vermek gerekirse; *Jinghai, SeaFly ve D3000 stealty insansız savaş gemisi* araçları sayılabilir. *Jinghai* otonom olarak denizde seyrüsefer yapabilme ve karşılaştığı engellerden kaçınabilme yeteneklerine sahiptir. *SeaFly* karşılaştığı engellerden nasıl kurtulacağını öğrenebilen algoritmalarla donatılmıştır. *D3000* ise, deniz yüzeyindeki savaş görevlerine ve denizaltı savarlara kilitlenme yeteneğine sahiptir (Kania, 2017: 24). İnsansız denizaltı araçlarına örnek olarak da Haiyi (Sea Wing) gösterilebilir. Haiyi, Güney Çin

Denizi'ndeki bilimsel araştırmalarda kullanılmasına ek olarak, çoklu sensörleri sayesinde yabancı denizaltıları keşfedebileceğini de gösteren üç aylık bir deniz altı keşif görevinde kullanılmıştır (Kania, 2017: 25).

Çin insansız kara araçları ve tanklar da geliştirmektedir. Ayrıca füze sistemlerinde de yarı otonom ve denetimli otonom sistemlere sahiptir. Bu sistemlerin otonomi dereceleri değişkenlik göstermekle birlikte, açık kaynaklarda henüz tam otonom olarak çalıştırıldığını gösteren bir bilgi bulunmamaktadır (Kania, 2017: 25).

Çin OSS ticareti de yapan bir ülkedir. 2020 yılı verilerine göre dünyada satışı yapılmış olan OSS'lerin %90'ı Çin şirketleri tarafından üretilmiş olan sistemlerdir (Kania, 2020: 7). 2019 yılında ABD Savunma Bakanı Mark Esper'in yaptığı bir açıklamada, Çin'in Orta Doğu'ya tam otonom özelliğe sahip olanları da içeren silah sistemleri sattığını iddia etmiştir (Kania, 2020: 5). Bu yönüyle de Çin'in ürettiği ve satışını yaptığı silah sistemlerinin devlet dışı aktörler, özellikle de terör örgütleri tarafından kullanılabilme riski bulunmaktadır.

Çin'in sürü dronlar geliştirme çalışmaları da bulunmaktadır. Scharre (2020: 49-50), ABD'nin 103 drondan oluşan sürü drone tanıtımından hemen sonra, Çin'in de rekabette varlığını göstermek için daha yüksek sayıda 119 drondan oluşan bir sürü ile gösteri yaptığını ifade etmektedir. *Caihong-5* yüksek irtifa ve uzun dayanıklılık özelliğine sahip bir İHA'dır. Aynı zamanda çoklu drone görevleri için, diğer İHA'lar ile takım oluşturma kapasitesine de sahiptir (Kania, 2017: 22).

Çin mevcut teknolojisini güçlendirmek ve daha ileri silah sistemleri üretme projeleri de yürütmektedir. Bu projelerde izlenen temel yaklaşım, ABD'nin yürüttüğü 3OS kapsamında temel alınan insan makine işbirliği yaklaşımına benzer biçimde, sivil-asker birleşimi yaklaşımıdır. Bu kapsamda HKO Askeri Bilimler Akademisi ile Tianjin Binhai YZ Sivil-Asker Birleştirme Merkezi arasında ortaklık kurularak, daha ileri araştırmaların temel eğilimi belirlenmiştir (Darıcılı, 2020: 60; Kania, 2020: 4).

Çin'in OSS'lere yönelik yaklaşımı ve geliştirdiği sistemler kendi ordusu tarafından doğrudan sahada, bir çatışma ya da savaş ortamında kullanılmadığı için ABD'ye oranla sistemlerin eksiklerini ve hatalarını bulup düzeltme konusunda daha dezavantajlı konumdadır. İhracatını yaptıkları sistemler ile geri bildirim ve güncelleme çalışmaları yürütüyor olsalar da, daha etkin veriler toplamak için yakın gelecekte Çin'in bölgesel ya da küçük çaplı çatışmalarda doğrudan yer alarak silah sistemlerini deneyeceği öngörülebilir. Çin'in mevcut teknolojilerinin

daha çok savunma odaklı olduğu görülmekle birlikte, karar destek sistemleri başta olmak üzere sahip olduğu yarı otonom sistemler saldırı için de elverişlidir.

3. Siber Güvenlik

Çin'in internet ile tanışması ve ağ alt yapılarını kurup geliştirecek politikalar üretmesi 1980'li yıların sonlarına doğru gerçekleşmiştir. Çin'den gönderilen ilk e-mail, 1987 yılında İsviçre'ye gönderilmiştir (Pekcan, 2020: 207). Ülke içerisinde yeni teknolojileri geliştirmek ve uygulamak amacıyla uyumlu olarak, internet alt yapısı da yaygınlaştırılmıştır. 2000'li yılların başında internet ve ağ alt yapısını yönetecek kamu kuruluşları kurulmaya ve yasal statüleri belirlenmeye başlanmıştır. Örneğin Sanayi ve Bilgi Teknolojileri Bakanlığı bünyesinde, bir sivil toplum örgütü statüsünde bulunan *" Çin Ulusal Bilgisayar Ağı Acil Müdahale Teknik Ekibi",* kurulmuş ve temel görevi Çin'in ulusal ağlarındaki kötücül yazılımları tespit etmek ve gerekli tedbirleri almaktır (Pekcan, 2020: 210). Çin'de internetin yaygınlaşması beraberinde "sorunları" da getirmiştir. Toplumsal muhalefetin, belirli konularda örgütlediği protestolarda, interneti örgütlenme amacıyla kullandığı görüşü, Çin yönetimini konu özelinde tedbirler almaya itmiştir. Özellikle Hong Kong ve Falun Gong[32] (Falun Dafa) protestoları Çin'in internet üzerindeki sansür uygulama iradesini kuvvetlendirmiştir (Pekcan, 2020: 208 v.d.).

Çin uluslararası alanda, kendi ülkesindeki internet ve sansür uygulamalarını pekiştirecek ve meşru bir zemine taşıyacak girişimlerde bulunmuştur. BM Genel Kurulu'na sunduğu taslakta *"devletlerin siber uzaydaki egemenlik hakkı"*na saygı duyulmasını istemiştir. Bu talep, ABD başta olmak üzere Batı Devletleri tarafından kabul görmemiş ve eleştirilmiştir. Rusya ise Çin'in talebini yerinde bulmuş ve desteklemiştir. Çabalar siber uzayda tam devlet egemenliği yönünde olsa da, BM'den bu yönde bir karar çıkmamıştır (Pekcan, 2020: 210-211).

Siber uzayın askeri amaçlı kullanımı konusunda da Çin'in girişimleri mevcuttur. HKO'ye bağlı olarak sanal "Mavi Ordu" kurulmuştur. Bu sanal ordunun amacını ortaya koymak için HKO Ulusal Savunma Üniversitesi Mensubu Prof. Zhang Shaozhon yaptığı açıklamada, mavi ordunun hackerlardan oluşmadığını aksine yasal bir statüsü bulunduğunu

[3232] Falun Dafa: Li Hongzi tarafından 1992 yılında bulunmuş olan bir uygulamadır. Falun Dafa için yapılan tanım şöyledir: *"yapılan bazı egzersizler ile evrenin en yüksek nitelikleri olan doğruluk-merhamet-hoşgörüye (Zhen-Shan-Ren) asimile olmayı hedefleyen bir disiplindir."* Uygulamanın protesto boyutuna ulaşması Çin yönetiminin Falun Dafa'yı yasaklama kararı üzerine başlamış, siber güvenlik ile ilişkisi ise protestocuların internet ağları üzerinden örgütlenmiş olmasıdır. Pekcan, C. (2020). Çin Halk Cumhuriyeti'nin Siber Güvenlik Politikası. In F. Köksoy (Ed.), *Yeni Küresel Tehdit Siber Saldırılar* (pp. 205-226). Nobel.

ifade etmiştir (Pekcan, 2020: 215-216). HKO bünyesinde yaklaşık 130.000 atamalı personel istihdam edilmektedir. Bu personellerin önemli bir kısmı, ABD'deki Siber Komutanlık benzeri bir birim olan *Pekin Kuzey Bilgisayar Merkezi*'nde faaliyet göstermektedir. *"Bilgisayar ağı savunma, saldırı ve istismar sistemleri tasarlama ve geliştirme"* gibi alt birimler halinde örgütlenmiştir (Singer & Friedman, 2018: 192). HKO'ya bağlı Stratejik Destek Gücü makine öğrenmesi ve büyük veri analizi tekniklerini kullanarak, siber yeteneklerini geliştirmiştir. DDoS saldırılarını örüntü izleme, istatistiksel analiz ve makine öğrenmesi teknikleriyle bulan ve saldırıların etkisini hafifleten yöntemler geliştirmişlerdir. Çin kuruluşlarından 54. Araştırma Enstitüsü, sistemlere girişleri yakalayan, derin sinir ağlarına dayalı bir sistem geliştirmiş ve patentini almıştır (Kania, 2017: 27).

ABD'nin siber saldırılar bakımından hedef gösterdiği Çin, yaptığı açıklamalarda asıl olarak siber saldırıların mağdurunun kendisi olduğunu, kendisine yöneltilen saldırıların çoğunluğunun ABD kaynaklarından geldiğini ifade etmektedir (Singer & Friedman, 2018: 190). Rakamlara bakıldığında bu iddianın doğruluk payı da oldukça yüksektir. Çünkü, paylaşılan rakamlara göre 10-19 milyon civarında Çin bilgisayarının yabancı hackerlar tarafından yönetilen botnetler içinde yer aldığı ileri sürülmektedir. Ancak Çin'in bu saldırılara maruz kalmasının nedeni olarak lisanslı olmayan yazılım kullanmaları ve orijinal yazılımların sahip olduğu güvenlik araçlarından mahrum olmalarıyla açıklanmaktadır (Singer & Friedman, 2018: 189-190).

Çin'in siber uzayda adının geçtiği en önemli konu ise siber casusluk ve fikri mülkiyet haklarını ihlal ettiği yönündeki iddialardır (Singer & Friedman, 2018: 189). Çin'in YZ alanında hızlı bir sıçrama yakalamasının yöntemi olarak siber hırsızlık/casusluk gösterilmektedir. ABD başta olmak üzere, Avustralya, Filipinler ve Hong Kong gibi devletlerin yürüttüğü Ar-Ge projelerine, bilimsel ve ticari bilgilere, siber saldırılar aracılığıyla ulaşıp, bu devletlerden önce projeleri gerçekleştirdiği iddia edilmektedir (Roberts et al., 2021: 63).

ABD söylemleriyle Çin'i hedef gösterse de, 2013 yılında Edward Snowden'in sızdırdığı belgeler, ABD'nin Çin'e karşı siber saldırı düzenlediğini kamuoyuna duyurmuştur. Bu duyuru ardından Çin medyasında dikkat çekici düzeyde şu sözler yer almıştır: *" Siber saldırıların kurbanı olarak uzun zamandır masumu oynamaya çalışan ABD'nin, çağımızın en büyük kabadayısı olduğu ortaya çıkmıştır." (Singer & Friedman, 2018: 190-191).* İki devletin de birbirlerine karşı suçlayıcı söylemlerde bulunduğu, muhtemelen de karşılıklı operasyonlar gerçekleştirdiği, ancak bu iddiaların çok azının ispatlanabiliyor olması siber uzayın karmaşık yapısını göstermektedir.

Çin'in genel olarak YZ stratejisi, özelde de siber güvenlik konusundaki stratejisi, geleneksel bir Çin stratejisi olan *trump-card (Shashoujian)*[33] stratejisi olarak tanımlanmaktadır. Buna göre; Çin, ABD ile açık rekabete girişmeyi değil, savaş zamanlarında hayati avantajlar elde etmek, barış zamanlarında ise inandırıcı düzeyde bir caydırıcılık sağlayacak yetenekler geliştirme yönünde politikalar izlemektedir (Pekcan, 2020: 219; Roberts et al., 2021: 62).

Çinli bir subayın şu sözleri, Çin ve ABD'nin siber uzaydaki konumunu açıklamakla birlikte, bizatihi siber uzayın doğasını da ortaya koymaktadır: *" ABD'nin elinde büyük taşlar var ancak penceresinde de cam tabaka var. Çin'in elinde büyük taşlar var ancak penceresinde cam tabaka var. Belki de bu yüzden üzerinde anlaşabileceğimiz konular var."* (Singer & Friedman, 2018: 196). Bu sözler, bir teknolojinin sağladığı avantajlar ile beraberinde getirdiği risklerin, uluslararası politika yapım sürecindeki etkisini göstermektedir. Özel olarak siber uzay, genel olarak ise askeri kullanıma elverişli öncü teknolojiler; uluslararası sistem bakımından krizlere sebep olsa da, gücün dengelenmesi için gerekli şartları da kendi içerisinde oluşturmaktadır. Stratejik düzeyde rekabet eden iki hasım, kendi çabalarıyla güvenliklerini sağlayabilecekleri eşiği aştıklarında, işbirliğini zorunlu bir seçenek olarak görmektedirler.

4. Çin ve Askeri Alanda Devrim

YZ teknolojileri kapsamında ortaya koyduğu çalışmalar ile ABD'ye meydan okuyan bir pozisyona yerleşen Çin'in RMA bağlamındaki çalışmalarını incelemek, geliştirdiği strateji ve politikalara yer vermek iki devlet arasındaki stratejik rekabetin sorgulanması bakımından gerekli görülmektedir. Çin'in güvenlik ve RMA bağlamında özellikle YZ ve Robotik alanlarındaki çalışmalar 1980'lerin ortalarına rastlasamaktadır (Kania, 2021: 534). Bunun ötesinde 1990'ların ortalarında geliştirmeye başladığı A2/AD (erişim ve alan engelleme) stratejisi, temel olarak ABD ile stratejik rekabetin esaslı bir konusunu oluşturmuştur (Krepinevich & Watts, 2015: 236). Erken sayılabilecek bir dönemde RMA çalışmaları yürüten Çin, milenyumun başından 2014 yılına kadar savaş ve savaş alanına ilişkin stratejilerini "bilgilendirme / informatised" çerçevesinde yürütmüştür. 2014 yılında ise Xi Jinping YZ temelli teknolojilerin askeri alana uygulanmasını içeren yeni RMA dalgasında Çin'in hızla yerini almasının önemini vurgulamıştır. Böylece Çin askeri alanını bilgilendirme paradigmasından "zekileştirme / intelligentised " paradigmasına yönlendirmiştir (Kania, 2021:

[33] Shashoujian (trump-card): Eski Çin devlet başkanı Jiang Zemin döneminde ortaya atılan bir stratejidir. Kelime anlamı olarak iskambil oyunundaki "koz" anlamındadır.

515). Bu kapsamda 2015 yılında onaylanan Çin Askeri Stratejisi insansız, uzun soluklu, zeki ve gizli silah ve ekipmanlara önem vermiştir. Çin'in bu yöndeki stratejisi ABD'nin 3OS stratejisi ile ilişkilidir. Çünkü Çin, ABD'nin 3OS ile yeni nesil farklılıklar yaratmasından endişelenmiştir (Kania, 2021: 521).

Çin 2014 yılından 2019 yılına kadar bir dizi RMA girişiminde bulunmuştur. Bu girişimlerin bir kısmı siber güvenliğe ilişkin tedbirler, bir kısmı HKO örgütlenmesine ilişkin uygulamalar bir kısmı ise OSS'lere yönelik stratejilerden oluşmaktadır. Kronolojik olarak bu gelişmeleri şöyle özetlemek mümkündür (Kania, 2021: 522):

- 2014 yılında Çin Adalet Bakanlığı 5 Çinli hakkında siber casusluk suçlamasıyla işlem başlattı.
- 2015'te bir yandan ABD ile Çin arasında Güney Çin Denizi üzerinde gerilim ortaya çıkarken, diğer yandan Xi Jinping HKO'nun reformlarda yeni evreye geçme planını duyurdu. Ayrıca aynı yıl hem HKO Stratejik Destek Gücü hem de HKO Roket gücü kuruldu.
- 2016 Ağustosunda Çin Dünyanın ilk kuantum uydusu olan Micius'u fırlattı. YZ Ar-Ge Stratejik Planı yayınlandı.
- 2017 yılında Yukarıda detaylarından bahsedilen Yeni Nesil YZ Geliştirme Planı yayınlandı. Jinping askeri alanın zekileştirilme sürecinin hızlandırılması yönünde HKO'ya çağrıda bulundu. Bu yılın sonunda ABD Ulusal Güvenlik Stratejisi Çin'i revizyonist bir güç olarak tanımladı.
- 2018 yılında Yeni Ulusal Savunma Stratejisi büyük güç rekabetine odaklandı.
- Çin Ulusal Savunma Bakanlığı "Yeni Çağda Çin'in Ulusal Savunması" isimli raporu yayınladı. Çin askeri geçit töreninde dronlar, hipersonik füzeler yeni nükleer yetkinlikleri de içeren yeni nesil silahlar gösterildi.

Çin, RMA çalışmalarının kavramsal çerçevesini asker-sivil birleşimi bağlamında oluşturmuştur (Kania, 2021: 525). Bunun önemi örgütsel düzeyde yaşanan değişimin görünür hale gelmesidir. Salt askeri sektör eliyle yaşanan bir dönüşümden ziyade, YZ teknolojisinin ruhuna da uygun olarak özel sektör sürece dahil edilmiştir. II. Bölümde YZ teknolojilerinin çifte kullanım özelliğinden ve ticari amaçlara uygunluğuna yer verilmişti. Çin de bu yaklaşıma uygun davranmaktadır.

Çin'in RMA stratejileri ile kurumsal düzeyde ilgilenen birim HKO Stratejik Destek Gücü'dür. Çin'in uzay, siber, elektronik ya da psikolojik savaş stratejileri bu birim

tarafından yönetilmektedir. Bu birimin altında da bilim ve teknoloji çalışmalarıyla görevli birimler kurulmuştur (Kania, 2021: 526).

Çin RMA kapsamında kavramsal olarak da C4ISR kavramını ortaya atmış ve bu kavram ile komuta, kontrol, iletişim, bilgisayar, istihbarat, izleme ve keşif yeteneklerini vurgulamaktadırlar.

IV. BÖLÜM : TARTIŞMA VE BULGULAR

Çalışmada tartışmaya açık olan ve cevap aranan sorular şunlardır: YZ destekli askeri teknolojiler Askeri Devrim (MR) kapsamında mı, Askeri Alanda Devrim (RMA) kapsamında mı değerlendirilmelidir? Bu soruyla amaçlanan temel husus YZ temelli güvenlik araçlarının literatürdeki konumunu tanımlamaktır. Bu soruya verilecek cevap ile birlikte söz konusu yeni güvenlik araçlarının öngörülebilirlik ve yönetilebilirlik seviyesi saptanarak, uluslararası ilişkilerin gelişimi ve yorumlanmasına katkı sunmak amaçlanmıştır. OSS ve Siber Güvenlik RMA'nın son dalgası olarak kabul edilebilir mi? OSS ve Siber güvenlik RMA'nın son dalgasına teknik altyapı oluşturmanın ötesinde incelenen devletlerin politikalarının inceleme sınırlarını çizmesi bakımından önem taşımaktadır.

Çalışmanın en temel sorusu ise "ABD ve Çin YZ-RMA bağlamında stratejik rakip olarak kabul edilebilir mi?" sorusudur. OSS ve siber güvenlik mevcut gelişmişlik düzeyiyle öngörülebilirlik ve yönetilebilirlik sınırları içinde kalmaktadır. Nitekim iki devletin de geliştirdiği politika ve stratejiler bu alanın yönetilebilir olduğunu, tedbir alınması gereken riskler bulunduğunu, yani öngörülebilir olduğunu, göstermektedir. İki devletin birbirlerini konumlandırdıkları yer bakımından soruya yaklaşıldığında, stratejik rakip tanımlaması yerinde bir tanımlamadır. Çünkü ABD, Marshall'ın katkılarıyla 1996 yılından beri Çin'i gündeminde tutmakta, Çin ise ABD'nin dünyadaki mevcut hakim konumuna meydan okuyan konumundadır. Bu konu YZ-Uluslararası İlişkiler açısından değerlendirildiğinde ise YZ'nın uluslararası ilişkilere yeni bir konu olarak eklendiğini, bu alandaki gelişmelerin devletlerin dış politika yapım ve uygulamaları bakımından göz önünde bulundurulması gerektiğini söylemek mümkündür.

II. Bölümde açıklandığı üzere MR büyük askeri değişimleri konu edinmektedir. RMA ise ortaya çıkan bir teknolojinin doktrinin oluşturularak askeri alana uyarlanması anlamına gelmektedir. RMA politik ve stratejik yönü daha ağır basan bir kavramsallaştırmadır. YZ teknolojilerini hem ABD hem de Çin askeri alana uyarlayabilmek için strateji belgeleri ve konuya özgü doktrinler, kavramlar geliştirmiş, örgütsel değişimi de içeren boyutlarda söz konusu teknolojileri askeri alana uygulamışlardır. Dolayısıyla YZ destekli teknolojileri RMA kapsamında ele almak gerekir. Bir diğer deyişle RMA alanında stratejik rakiptirler ve bu nedenle YZ tamamen siyasal ve stratejik bir konudur.

RMA dalgaları dönemsel olarak ortaya çıkan teknolojilerin, dönemin kısıtlılıkları ve ihtiyaçları da göz önünde bulundurularak, askeri alana uyarlanması anlamına gelmektedir. OSS ve Siber güvenlik son dönem güvenlik ihtiyaçlarının önde gelen çalışma alanlarından biri

olduğu gibi askeri alanda kullanımları da mevcuttur. Başka bir deyişle OSS doğası gereği askeri alana özgü olarak geliştirilirken, sivil alanda geliştirilen siber güvenlik politikalarının askeri alana uyarlanması da mümkündür.

ABD ile Çin'in konu bağlamında stratejik rakip olarak tanımlanmasına ilişkin soruya en açıklayıcı yanıt 1996'da Marshall'ın ONA'da ortaya attığı görüşlere ve ardından karşılıklı olarak geliştirilen stratejilerde birbirlerini konumlandırmalarına bakmak gerekir (Krepinevich & Watts, 2015: 225-226). Marshall 1996 yılında ABD'nin Avrupa yerine Asya'ya yönelmesi gerektiğini ve yükselen Çin'i dengelemenin önemini vurgulamıştır. Çin ise aynı yıllarda A2/AD stratejisini uygulamış ve gerek istihbarat toplama amacıyla gerekse de saldırı amacıyla Çin anakarasına davetsiz misafir girişine yönelik tedbirler almıştır. ABD'nin 3OS stratejisine karşılık Çin Yeni Nesil YZ geliştirme planını açıklamış ve uygulamaya koymuştur. Çin'in askeri alanda yaptığı modernizasyon çalışmalarının ardından ABD Çin'i revizyonist ilan etmiştir. Bütün bu karşılıklı hamleler birlikte değerlendirildiğinde YZ-RMA kapsamında Raska'nın belirttiği gibi Çin ve ABD'nin stratejik rakip olduğunu söylemek mümkündür.

Çalışmanın bulguları şu şekilde özetlenebilir: YZ destekli güvenlik araçları MR kadar büyük ve yaygın etkiye sahip olmadığından ve aynı zamanda RMA kapsamında değerlendirilebilmek için gerekli stratejik, örgütsel ve doktrinel değişimleri sağladığı için RMA kapsamında değerlendirilmesi gerekir.

RMA'nın son dalgası olarak OSS ve Siber güvenlik kabul edilebilir. Çünkü bu teknolojiler güvenlik konusuyla doğrudan ilgili olup, askeri alana RMA kapsamında uygulanması mümkün olan teknolojilerdir.

Çin ve ABD YZ-RMA bağlamında stratejik rakip olarak kabul edilebilir. Çünkü geliştirdikleri stratejiler karşılıklı olarak güç ve üstünlük mücadelesi yürütüldüğünü göstermektedir.

SONUÇ

YZ destekli teknolojilerin askeri alana etkilerini konu edinen bu tez çalışmasında ilk olarak YZ kavramsal düzeyde açıklanmış ve takip eden bölümde MR-RMA kavramları ve farkları vurgulanmıştır. RMA dalgalarına yer verilerek, söz konusu dalgaları tetikleyen olayları saptamak amaçlanmıştır. OSS ve Siber Güvenlik konularına yer verilmiş ve bu teknolojilerin askeri alana uygulanması yönünde gerçekleştirilen uygulamalar aktarılmıştır. III. Bölümde ABD ve Çin'in YZ, RMA, OSS ve Siber Güvenlik çerçevesindeki politikaları incelenmiştir.

Bu çalışmayla cevap aranan temel sorular: i) OSS ve Siber güvenlik RMA dalgası yaratabilecek güçte teknolojiler midir? ii) YZ ile ortaya çıkan teknolojilerin askeri alana etkileri MR-RMA tartışmasında nerede konumlandırılmalıdır? iii) ABD ve Çin YZ-RMA bağlamında stratejik rakip olarak kabul edilebilirler mi?

Açık kaynaklar, akademik yayınlar, ilgili rapor ve strateji belgeleri incelenerek, ABD ve Çin'in konuya ilişkin politikaları ortaya konmuştur. OSS ve Siber güvenliğin RMA dalgasını tetikleyecek güçte teknolojiler olduğu görülmüştür. Çünkü bu teknolojiler askeri alana uygulanmak amacıyla RMA çalışmalarına konu edilmişlerdir. MR-RMA ayrımında YZ'nin konumu RMA olarak değerlendirilmiştir. Bunun iki temel nedeni bulunmaktadır. İlk olarak YZ'nin güvenlik üzerindeki etkileri, henüz MR boyutunda sonuçları olan bir evrede değildir. İkinci neden ise RMA'nın belirleyici özelliği olan askeri alana uyarlama konusunda doktrin, taktik, stratejik ve örgütsel bakımdan yenilikler barındırma kriterini YZ karşılamaktadır. ABD ve Çin YZ politikalarını ve bu politikaların askeri alana uygulanması yönündeki çalışmalarını ortaya koyarken, doktrin ve stratejik değişimlere yer vermişlerdir.

ABD ve Çin YZ-RMA bağlamındaki stratejilerini oluştururken belirli düzeyde birbirlerini rakip olarak konumlandırmışlar ve dengeleme amacı gütmüşlerdir. Bu nedenle anılan devletlerin YZ-RMA bağlamında stratejik rakip olduğu söylenebilir.

KAYNAKLAR

Acar, O. (2020). *Yapay Zeka Fırsat Mı, Yoksa Tehdit Mi?* Kriter.

Acemoglu, D., & Restrepo, P. (2018). Artificial intelligence, automation, and work. In *The economics of artificial intelligence: An agenda* (pp. 197-236). University of Chicago Press.

Akyeşilmen, N. (2018). *Disiplinlerarası Bir Yaklaşımla Siber Politika & Güvenlik*. Orion.

Akyeşilmen, N., & Kurnaz, İ. (2020). Küresel Siber Güvenlik: Kavramsal ve Kuramsal Bir Analiz. In F. Köksoy (Ed.), *Yeni Küresel Tehdit Siber Saldırılar* (pp. 3-32). Nobel.

Balta, E. (2021). *Küresel Güvenlik Kompleksi* (3 ed.). İletişim.

Barrass, G. (2016). Able Archer 83: What Were the Soviets Thinking? *Survival*, *58*(6), 7-30.

Beduschi, A. (2020). International migration management in the age of artificial intelligence. *Migration Studies*.

Bıçakçı, S. (2014). NATO'nun gelişen tehdit algısı: 21. yüzyılda siber güvenlik. *Uluslararası İlişkiler Dergisi*, *10*(40), 100-130.

Bissio, R., & WATCH, S. (2018). Vector of hope, source of fear. *Spotlight on Sustainable Development*, 77-86.

Bitzinger, R. (2017). US-China Competition, the Third Offset Strategy, and Implications for the Global Arms Industry. *SITC Research Briefs*(2017-12).

Bostrom, N. (2014). *Superintelligence : paths, dangers, strategies* (First edition. ed.). Oxford University Press.

Branch, W. A. (2018). *Artificial Intelligence and Operational - Level Planning: An Emergent Convergence*. https://apps.dtic.mil/sti/pdfs/AD1070958.pdf

Brundage, M., Avin, S., Clark, J., Toner, H., Eckersley, P., Garfinkel, B., Dafoe, A., Scharre, P., Zeitzoff, T., & Filar, B. (2018). The malicious use of artificial intelligence: Forecasting, prevention, and mitigation. *arXiv preprint arXiv:1802.07228*.

Campaign to Stop Killer Robots. (2019). *Country Views on Killer Robots*. Retrieved 30.12.2021 from https://www.stopkillerrobots.org/wp-content/uploads/2019/10/KRC_CountryViews_25Oct2019rev.pdf

Cassella, C. (2021). *Brain Implant Gives Blind Woman Artificial Vision in Scientific First*. Science Alert. Retrieved 01.11.2021 from https://www.sciencealert.com/a-brain-implant-has-allowed-a-blind-woman-to-see-simple-2d-shapes-and-letters

CITRIS. (2016). *Lethal Autonomous Weapons*. https://www.youtube.com/watch?v=JYQ7p3pWwr4

Clarke, R. (2019). Why the world wants controls over Artificial Intelligence. *Computer Law & Security Review*, *35*(4), 423-433.

Cockburn, I. M., Henderson, R., & Stern, S. (2019). The impact of artificial intelligence on innovation. *The economics of artificial intelligence: An agenda*, 115-152.

Copeland, B. J. (2004). Chess. In B. J. Copeland (Ed.), *The essential turing* (pp. 562-575). Oxford University Press.

Corea, F. (2019). *An Introduction to Data Everything You Need to Know About AI, Big Data and Data Science* (Vol. 50). Springer. https://doi.org/doi.org/10.1007/978-3-030-04468-8

Council, N. S. T. (2019). *2016-2019 Progress Report: Advancing Artificial Intelligence R&D*. https://www.nitrd.gov/pubs/AI-Research-and-Development-Progress-Report-2016-2019.pdf

Cummings, M., Roff, H. M., Cukier, K., Parakilas, J., & Bryce, H. (2018). Artificial Intelligence and International Affairs. *Chatham House Report*, 7-18.

Darıcılı, A. B. (2020). The Impact Of Artificial Intelligence Management Upon International Security. *Savunma Bilimleri Dergisi*, *19*(37), 49-72.

Dechter, R. (1986). Learning while searching in constraint-satisfaction problems.

Denk, E. (2019). Taş Çağından Günümüze Güvenliğin Dönüşen Ontolojisi. *Güvenlik Yazıları Serisi*, *2*(Eylül). https://doi.org/10.13140/RG.2.2.28747.13608

Autonomy in Weapon Systems, (2012a). https://www.esd.whs.mil/Portals/54/Documents/DD/issuances/dodd/300009p.pdf

DoD. (2012b). *Autonomy in Weapon Systems*. Retrieved from https://www.esd.whs.mil/portals/54/documents/dd/issuances/dodd/300009p.pdf

DoD, U. (2011). *Unmanned Systems Integrated Roadmap*. Washington DC: White House Retrieved from https://irp.fas.org/program/collect/usroadmap2011.pdf

Doğan, Ü., & Alaca, A. İ. S. (2020). Yapay Zeka Uyulamaları ve Büyük Veri. In A. B. Darıcılı (Ed.), *Güvenlik Teknoloji ve Yeni Tehditler* (pp. 383-421). Nobel.

Dombrowski, P. (2015). *America's Third Offset Strategy: New Military Technologies And Implications For The Asia Pasific*.

Ekmekci, P. E., & Arda, B. (2020). History of Artificial Intelligence. In *Artificial Intelligence and Bioethics* (pp. 1-15). Springer.

El Naqa, I., & Murphy, M. J. (2015). What is machine learning? In *machine learning in radiation oncology* (pp. 3-11). Springer.

Elmas, Ç. (2018). *Yapay Zeka Uygulamaları*. Seçkin.

Ereker, F. A. GÜVENLİK YAZILARI. https://www.researchgate.net/profile/Uluslararasi-Iliskiler-Konseyi/publication/336926680_Hakli_Savas/links/5dbb1db2299bf1a47b06fb83/Hakli-Savas.pdf

Eren, M. (2017). *Avrupa Birliği'nin Siber Güvenlik Politikası*. Beta.

Ersoy, Ç. (2018). *Robotlar, Yapay Zeka ve Hukuk*. Onikilevha.

Fernández, E., Alfaro, A., Soto-Sánchez, C., González-López, P., Ortega, A. M. L., Peña, S., Grima, M. D., Rodil, A., Gómez, B., & Chen, X. (2021). Visual percepts evoked with an Intracortical 96-channel microelectrode array inserted in human occipital cortex. *The Journal of Clinical Investigation*.

Fiott, D. (2016). Europe and the Pentagon's third offset strategy. *The RUSI Journal*, *161*(1), 26-31.

Frey, C. B., & Osborne, M. A. (2017). The future of employment: How susceptible are jobs to computerisation? *Technological Forecasting and Social Change*, *114*, 254-280. https://doi.org/https://doi.org/10.1016/j.techfore.2016.08.019

Galliott, J. (2015). *Military Robots Mapping the Moral Landscape*. Ashgate (e-book).

Garcia, D. (2018). Lethal artificial intelligence and change: The future of international peace and security. *International Studies Review*, *20*(2), 334-341.

Georgiadou, E., Angelopoulos, S., & Drake, H. (2020). Big data analytics and international negotiations: Sentiment analysis of Brexit negotiating outcomes. *International Journal of Information Management*, *51*, 102048. file:///C:/Users/Hp/Downloads/1-s2.0-S0268401219309454-main.pdf

Georgieff, A., & Milanez, A. (2021). What happened to jobs at high risk of automation? https://www.oecd-ilibrary.org/docserver/10bc97f4-en.pdf?expires=1637615374&id=id&accname=guest&checksum=A10D223E5B209E9CC35C1C5EF3D3F647

Geva, N., Mayhar, J., & Skorick, J. M. (2000). The cognitive calculus of foreign policy decision making: An experimental assessment. *Journal of conflict resolution*, *44*(4), 447-471.

Gray, C. S. (2005). *Strategy For Chaos: Revolutions in Military Affairs and the Evidence of History*. Taylor & Francis e-Library.

Green, A. V.-. (2015, 01.03.2015). The Foreign Policy Essay: The South Korean Sentry - A "Killer Robot" to Prevent War. https://www.lawfareblog.com/foreign-policy-essay-south-korean-sentry%E2%80%94-killer-robot-prevent-war

Grosz, B. J., Altman, R., Horvitz, E., Mackworth, A., Michael, T., Mulligan, D., & Shoham, Y. (2016). *Report of the 2015 Study Panel."Artificial Intelligence and Life in 2030." One Hundred Year Study on Artificial Intelligence.* . https://ai100.stanford.edu/

Hagel, C. (2014). Secretary of Defence Speech. In. Simi Valley, CA: Reagan National Defense Forum.

Hawksworth, J., Berriman, R., & Goel, S. (2018). Will robots really steal our jobs? An international analysis of the potential long term impact of automation. *PricewaterhouseCoopers, http://pwc. co. uk/economics, access, 13*. https://www.pwc.com.tr/tr/gundemdeki-konular/ekonomi/otomasyon-mevcut-isleri-nasil-sekillendirecek.pdf

Heath, D., Allum, D., & Square, P. (1997). *The Historical Development of Computer Chess and its Impact on Artificial Intelligence* (Deep Blue Versus Kasparov: The Significance for Artificial Intelligence, Issue.

Hiippala, T. (2017). Recognizing military vehicles in social media images using deep learning. 2017 IEEE International Conference on Intelligence and Security Informatics (ISI),

Hoffman, F. G. (2017). Will war's nature change in the seventh military revolution? *The US Army War College Quarterly: Parameters*, *47*(4), 19-31.

HRW. (2012). *losing Humanity The Case Against Killer Robots*. https://www.hrw.org/report/2012/11/19/losing-humanity/case-against-killer-robots

Hudson, V. M., & Day, B. S. (2019). *Foreign policy analysis: classic and contemporary theory*. Rowman & Littlefield.

Hudson, V. M., & Vore, C. S. (1995). Foreign policy analysis yesterday, today, and tomorrow. *Mershon International Studies Review*, *39*(Supplement_2), 209-238.

The IAI is a disposable half-UAV, half-missile drone system with inherent surveillance capabilities. (2020, 10.12.2020). *Military Factory*. https://www.militaryfactory.com/aircraft/detail.php?aircraft_id=1288

Johnson, L. K. (1977). Operational Codes And the Prediction of Leadership Behaviour: Frank Church at Mid-Career. In M. G. Hermann. (Ed.), *A Psychological Examination of Political Leaders.* Free Press.

Kania, E. B. (2017). Battlefield singularity. *Artificial Intelligence, Military Revolution, and China's Future Military Power, CNAS*.

Kania, E. B. (2020). 'AI Weapons' in China's Military Innovation. *Brookings Institution, April*. https://www.brookings.edu/wp-content/uploads/2020/04/FP_20200427_ai_weapons_kania_v2.pdf

Kania, E. B. (2021). Artificial intelligence in China's revolution in military affairs. *Journal of strategic studies*, *44*(4), 515-542.

Kasparov vs Deep Blue. Retrieved 24.08.2021 from https://www.chessgames.com/perl/chesscollection?cid=1014770

Köker, A. E. (2021). *Çatışma ve Savaş İkileminde Siber Dünya*. Urzeni.

Krepinevich, A., & Watts, B. (2015). *The last warrior: Andrew Marshall And The Shaping Of Modern American Defence Strategy*. Basic Books.

Krepinevich, A. F. (1994). Cavalry to computer: The pattern of military revolutions. *The National Interest*(37), 30-42.

Krishnan, A. (2009). *Killer Robots: Legality and Ethicality of Autonomous Weapons*. Ashgate (e-book).

Kurzweil, R. (2005). *The singularity is near: When humans transcend biology*. Penguin.

Lanier, T. C. (2018, 01.06.2018). Google backs down from controversial Air Force AI Project. *Fedscoop*. https://www.fedscoop.com/reports-google-backs-controversial-air-force-ai-project/

Leys, N. (2018). Autonomous weapon systems and international crises. *Strategic Studies Quarterly*, *12*(1), 48-73.
Lin, G.-M., Nagamine, M., Yang, S.-N., Tai, Y.-M., Lin, C., & Sato, H. (2020). Machine learning based suicide ideation prediction for military personnel. *IEEE journal of biomedical and health informatics*, *24*(7), 1907-1916.
Lin, P., Bekey, G., & Abney, K. (2008). *Autonomous Military Robotics : Risk, Ethics and Design*.
Liu, H.-Y. (2012). Categorization and legality of autonomous and remote weapons systems. *International Review of the Red Cross*, *94*(886), 627-652.
Louth, J., & Taylor, T. (2016). The US Third Offset Strategy: Hegemony and Dependency in the Twenty-First Century. *The RUSI Journal*, *161*(3), 66-71.
Manyika, J., Lund, S., Chui, M., Bughin, J., Woetzel, J., Batra, P., Ko, R., & Sanghvi, S. (2017). Jobs lost, jobs gained: Workforce transitions in a time of automation. *McKinsey Global Institute*, *150*. https://www.mckinsey.com/~/media/mckinsey/industries/public%20and%20social%20sector/our%20insights/what%20the%20future%20of%20work%20will%20mean%20for%20jobs%20skills%20and%20wages/mgi-jobs-lost-jobs-gained-report-december-6-2017.pdf
Marchant, G. E., Allenby, B., Arkin, R., & Barrett, E. T. (2011). International governance of autonomous military robots. *Colum. Sci. & Tech. L. Rev.*, *12*, 272.
Martyanov, A. (2019). *The (real) revolution in military affairs*. SCB Distributors.
Mayor, A. (2020). *Gods and robots: myths, machines, and ancient dreams of technology*. Princeton University Press.
McCarthy, J. (2007). *What is Artificial Intelligence?* Stanford University. http://jmc.stanford.edu/articles/whatisai/whatisai.pdf
McCarthy, J., Minsky, M. L., Rochester, N., & Shannon, C. E. (2006). A proposal for the dartmouth summer research project on artificial intelligence, august 31, 1955. *AI magazine*, *27*(4), 12-12.
McCarthy, J., Minsky, M. L., Rochester, N., & Shanon, C. E. (1955). *A Proposal For The Dartmouth Summer Research Project On Artificial Intelligence*. http://jmc.stanford.edu/articles/dartmouth/dartmouth.pdf
Mintz, A. (1993). The decision to attack Iraq: A noncompensatory theory of decision making. *Journal of conflict resolution*, *37*(4), 595-618.
Mintz, A. (2004). How do leaders make decisions? A poliheuristic perspective. *Journal of conflict resolution*, *48*(1), 3-13.
Mintz, A., Geva, N., Redd, S. B., & Carnes, A. (1997). The effect of dynamic and static choice sets on political decision making: An analysis using the decision board platform. *American Political Science Review*, *91*(3), 553-566.
Moor, J. (2006). The Dartmouth College artificial intelligence conference: The next fifty years. *AI magazine*, *27*(4).
Murray, W. (1997). *Thinking about revolutions in military affairs*.
Murray, W., & Knox, M. (2001). *The dynamics of military revolution, 1300-2050*. Cambridge University Press.
Nilsson, N. J. (2010). *Yapay Zeka* (M. Doğan, Trans.). Boğaziçi Üniversitesi Yayınevi.
Nissen, L. R., Tsamardinos, I., Eskelund, K., Gradus, J. L., Andersen, S. B., & Karstoft, K.-I. (2021). Forecasting military mental health in a complete sample of Danish military personnel deployed between 1992-2013. *Journal of Affective Disorders*, *288*, 167-174.
Nye Jr, J. S. (2010). *Cyber power*.
Oxforddictionary. (2021). *Oxford Dictionary*. https://www.oxfordlearnersdictionaries.com/definition/english/cyber?q=cyber

ÖZER, A. SAVAŞLARDA ÜÇÜNCÜ DEVRİM OTONOM SİLAH SİSTEMLERİ VE İNSANCIL HUKUK.
Payne, K. (2018). Artificial intelligence: a revolution in strategic affairs? *Survival*, *60*(5), 7-32.
Pekcan, C. (2020). Çin Halk Cumhuriyeti'nin Siber Güvenlik Politikası. In F. Köksoy (Ed.), *Yeni Küresel Tehdit Siber Saldırılar* (pp. 205-226). Nobel.
Poole, D. L., & Mackworth, A. K. (2010). *Artificial Intelligence: foundations of computational agents*. Cambridge University Press.
Raska, M. (2021). The sixth RMA wave: Disruption in military affairs? *Journal of strategic studies*, *44*(4), 456-479.
Rich, E., Knight, K., & Nair, S. B. (2009). *Artificial Intelligence*. Tata McGraw-Hill.
Roberts, H., Cowls, J., Morley, J., Taddeo, M., Wang, V., & Floridi, L. (2021). The Chinese approach to artificial intelligence: an analysis of policy, ethics, and regulation. *AI & SOCIETY*, *36*(1), 59-77.
Rohrlich, J. (2019, 08.05.2019). Report: Kill the idea of "killer robots" before they kill us. https://qz.com/1614684/killer-robots-must-be-stopped-pax-tells-the-world/
Russell, S., & Norvig, P. (2021). Artificial Intelligence: A Modern Approach, Global Edition 4th. *Foundations*, *19*.
Say, C. (2021). *50 Soruda Yapay Zeka*. 7 Renk.
Schaeffer, J., Burch, N., Björnsson, Y., Kishimoto, A., Müller, M., Lake, R., Lu, P., & Sutphen, S. (2007). Checkers is solved. *science*, *317*(5844), 1518-1522. https://science.sciencemag.org/content/317/5844/1518.long
Scharre, P. (2020). *İnsansız Ordular : Katil Robotlar, Otonom Silahlar ve Makine Savaşaları* (K. A. Çetinalp, Trans.). Kronik.
Schrodt, P. A. (1988). Artificial intelligence and formal models of international behavior. *The American Sociologist*, *19*(1), 71-85. https://link.springer.com/content/pdf/10.1007/BF02692375.pdf
Schrodt, P. A. (2019). Artificial intelligence and international relations: An overview. *Artifical Intelligence and International Politics*, 9-31.
Schwab, K. (2017). *Dördüncü Sanayi Devrimi* (Z. Dicleli, Trans.). Optimist.
Searle, J. (1980). Minds, brains, and programs. *Behavioral and brain sciences*, *3*(3), 417-457.
Selçuk, Z. (2020). Amerika Birleşik Devletleri'nin Siber Güvenlik Politikası. In F. Köksoy (Ed.), *Yeni Küresel Tehdit Siber Saldırılar* (pp. 71-86). Nobel.
Shannon, C. E. (1950). XXII. Programming a computer for playing chess. *The London, Edinburgh, and Dublin Philosophical Magazine and Journal of Science*, *41*(314), 256-275.
Sharkey, N. (2012). Killing Made Easy: From Joysticks to Politics. In P. Lin, K. Abney, & G. A. Bekey (Eds.), *Robot Ethics The Ethical And Social Implications of Robotics* (pp. 111-128). MIT Press.
Sharkey, N. (2014). Autonomous Weapons and Human Supervisory Control. Autonomous Wepon Systems: Technical, Military, Legal And Humanitarian Aspects, Geneva, Switzerland.
Silver, D., Hubert, T., Schrittwieser, J., Antonoglou, I., Lai, M., Guez, A., Lanctot, M., Sifre, L., Kumaran, D., & Graepel, T. (2017). Mastering chess and shogi by self-play with a general reinforcement learning algorithm. *arXiv preprint arXiv:1712.01815*.
Simon, H. A., & Newell, A. (1958). Heuristic problem solving: The next advance in operations research. *Operations research*, *6*(1), 1-10.
Singer, P. W. (2009). Military robots and the laws of war. *The New Atlantis*(23), 25-45.
Singer, P. W. (2009). *Wired for war: The robotics revolution and conflict in the 21st century*. Penguin.
Singer, P. W., & Friedman, A. (2018). *Siber Güvenlik ve Siber Savaş*. Buzdağı

Snow, C. P. (2005). *İki Kültür* (T. Birkan, Trans.; 4. ed.). TÜBİTAK.
Soni, V. D. (2020). Challenges and Solution for Artificial Intelligence in Cybersecurity of the USA. *Available at SSRN 3624487*.
State Council, C. (2017). *A Next Generation Artificial Intelligence Development Plan*. Retrieved from https://d1y8sb8igg2f8e.cloudfront.net/documents/translation-fulltext-8.1.17.pdf
Super aEgis II. http://www.dodaam.com/eng/sub2/menu2_1_4.php
Şeker, E. (2020). Yapay Zeka Tekniklerinin/Uygulamalarının Siber Savunmada Kullanımı. *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, *6*(2), 108-115.
Taşkesen, S. (2020). Sınırların Belirsizleşmesi: Dron Teknolojileri Temelli Saldırılar. In A. B. Darıcılı (Ed.), *Güvenlik, Teknoloji ve Yeni Tehditler* (pp. 277-300). Nobel.
TURING, A. M. (1950). I.—COMPUTING MACHINERY AND INTELLIGENCE. *Mind*, *LIX*(236), 433-460. https://doi.org/10.1093/mind/LIX.236.433
Türkkan, A. Z., & Özdaş, M. R. (2021). Yapay Zeka ve Jeopolitik 4.0 : Yapay Zekanın 21. Yüzyıl Güvenlik Anlayışına Etkisi. In Ö. İyigün & M. K. Yılmaz (Eds.), *Yapay Zeka Güncel Yaklaşımlar ve Uygulamalar* (pp. 289-323). Beta.
Protocol Additional to The Geneva Conventions of 12 Agust 1949, And Relating to the Protection of International Armed Conflicts (Protocol I), (1977). https://www.un.org/en/genocideprevention/documents/atrocity-crimes/Doc.34_AP-I-EN.pdf
Convention on the Prohibition of the Use, Stockpiling, Production and Transfer of Anti-Personnel Mines and on their Destruction, (1997). https://treaties.un.org/Pages/ViewDetails.aspx?src=TREATY&mtdsg_no=XXVI-5&chapter=26&clang=_en
Unmanned Aircraft Systems. (2017). https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/673940/doctrine_uk_uas_jdp_0_30_2.pdf
Verbruggen, M., & Boulanin, V. (2017). Mapping the development of autonomy in weapon systems.
Walker, S. G. (1981). The correspondence between foreign policy rhetoric and behavior: Insights from role theory and exchange theory. *Behavioral Science*, *26*(3), 272-280.
Walker, S. G., Schafer, M., & Young, M. D. (1998). Systematic procedures for operational code analysis: Measuring and modeling Jimmy Carter's operational code. *International studies quarterly*, *42*(1), 175-189.
Walzer, M. (2017). *Haklı Savaş Haksız Savaş* (M. Doğan, Trans.). Alfa.
Wang, Y., & Chen, D. (2018). Rising sino-US competition in artificial intelligence. *China Quarterly of International Strategic Studies*, *4*(02), 241-258.
Wareham, M., Kayser, D., & Sharkey, N. (2017). Process on Killer Robots Lacks Focus and Goal. In C. t. s. k. robots (Ed.).
WhiteHouse. (2010). *National Security Strategy*.
WhiteHouse. (2015a). *National Security Strategy*.
WhiteHouse. (2015b). *President Xi Jinping's State Visit to the United States*. Retrieved 31.12.2021 from https://obamawhitehouse.archives.gov/the-press-office/2015/09/25/fact-sheet-president-xi-jinpings-state-visit-united-states
WhiteHouse. (2017). *National Security Strategy*.
Work, B. (2015, 28.01.2015). *The Third US Offset Strategy and Its Implications for Partners and Allies* Wasington, DC, CNAS. https://warontherocks.com/2015/01/video-the-third-u-s-offset-strategy-and-its-implications-for-partners-and-allies/
Zeadally, S., Adi, E., Baig, Z., & Khan, I. A. (2020). Harnessing artificial intelligence capabilities to improve cybersecurity. *Ieee Access*, *8*, 23817-23837.

ÖZET

YAPAY ZEKA ULUSLARARASI İLİŞKİLERDE ASKERİ ALANDA DEVRİM MİDİR? ABD VE ÇİN REKABETİ ÜZERİNDEN BİR DEĞERLENDİRME

SEMİH AYSAL

Bu çalışmada; yeni bir teknoloji olarak ortaya çıkan, bireysel, toplumsal ve kurumsal düzeylerde insan hayatına etkileri olan Yapay Zeka (YZ)'nın, askeri alana uyarlanmasına ilişkin politikalar ABD ve Çin örnekleri üzerinden incelenmektedir. Çalışmada cevap aranan temel sorular şunlardır: "YZ'nin askeri alana uygulanması bağlamında ortaya çıkan teknolojiler MR-RMA bağlamında hangi kavram kapsamında ele alınmalıdır?, OSS ve Siber güvenlik RMA dalgasını tetikleyecek güçte teknolojiler midir?, ABD ve Çin arasında YZ-RMA bağlamında stratejik bir rekabet var mıdır? Çalışmada Türkçe ve İngilizce olarak yayınlanmış olan akademik kaynaklar, uluslararası örgüt raporları strateji belgeleri doküman analizi yöntemiyle incelenmiştir. Çalışmanın temel bulgusu YZ'nin askeri alana uygulanmasının RMA kapsamında konumlandırmak gerekmektedir.

Anahtar Kelimeler: *Yapay zeka, Askeri Devrim,Askeri Alanda Devrim, Otonom Silah Sistemleri, Siber Güvenlik.*

ABSTRACT
IS ARTIFICIAL INTELLIGENCE A REVOLUTION IN MILITARY AFFAIRS IN INTERNATIONAL RELATIONS? AN ANALYZE ON THE USA AND CHINA COMPETITION

SEMİH AYSAL

In this study; Policies regarding the adaptation of Artificial Intelligence (AI), emerging as a new technology and having effects on human life at individual, social and institutional levels, to the military field are examined through the examples of the USA and China. The main questions that are sought to be answered in the study are: "Which concept should the emerging technologies in the context of the application of AI in the military field be considered in the context of MR-RMA?, Are OSS and Cyber security technologies strong enough to trigger the RMA wave?, Is there a Strategic competition between the USA and China in the context of AI-RMA. In the study, academic resources published in Turkish and English, international organization reports, strategy documents were examined by document analysis method. The main finding of the study is that the application of AI to the military field should be positioned within the scope of RMA.

Key Words: *Artificial Intelligence, Military Revolution, Revolution in Military Affairs, Autonomous Weapon Systems, Cybersecurity.*