



T.C.

UFUK ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER ANABİLİM DALI

ULUSLARARASI İLİŞKİLER PROGRAMI

**ABD-ÇİN REKABETİNİN SİBER GÜVENLİK BAĞLAMINDA
ORTADOĞU'YA YANSIMALARI**

YÜKSEK LİSANS TEZİ

NURBANU KESGİN

TEZ DANIŞMANI

PROF. DR. CEM KARADELİ

ANKARA

2022

T.C.
UFUK ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ
SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER ANABİLİM DALI
ULUSLARARASI İLİŞKİLER PROGRAMI

**ABD-ÇİN REKABETİNİN SİBER GÜVENLİK BAĞLAMINDA
ORTADOĞU'YA YANSIMALARI**

YÜKSEK LİSANS TEZİ

NURBANU KESGİN

TEZ DANIŞMANI
PROF. DR. CEM KARADELİ

ANKARA

2022

BİLDİRİM

Hazırladığım tezin/raporun tamamen kendi çalışmam olduğunu ve her alıntıya kaynak gösterdiğimi taahhüt eder, tezimin/raporumun kâğıt ve elektronik kopyalarının Ufuk Üniversitesi Sosyal Bilimler Enstitüsü arşivlerinde aşağıda belirttiğim koşullarda saklanmasına izin verdiğimi onaylarım:

- Tezimin/Raporumun tamamı her yerden erişime açılabilir.

18.02.2022

NURBANU KESGİN

ADAMA



Canımdan çok sevdiğim anne ve babama...

TEŞEKKÜR

Tez çalışmamda bana yol göstermiş ve yönlendirmiş, desteğini hiçbir zaman esirgememiş olmakla birlikte tezimi teslim edemeden vefatıyla bizleri yasa boğan değerli Hocam Prof. Dr. Celalettin Sencer İmer'e teşekkürü bir borç bilirim. Ayrıca çalışmaya devam ettiğim değerli Hocam Prof. Dr. Cem Karadeli'ye; çalışmam süresince desteklerini esirgemeyen, bana gece gündüz demeden yardımcı olan, tüm yoğunluklarının arasında bana çalışmamda eşlik eden, yükümü benimle sırtlayan sevgili eşim Emre Kesgin'e; bugüne kadar bana maddi manevi desteklerini esirgemeyen canım babam Cemalettin Akcan ve canım annem Selma Akcan'a; desteklerini her daim hissettiğim kardeşlerim Ramazan, Burçe ve Hakan Akcan'a; sorularımı sıkılmadan yanıtlayan iş arkadaşlarıma ve yanımda olan herkese sonsuz teşekkürlerimi sunarım.

Son olarak, 2013 yılının Eylül ayında tanıştığım; daha tanıştığım ilk günden bana bu alanı sevdiren, hastalıklarla boğuştuğu zamanlarda dahi yaşadıklarını öğrencilerine hissettirmeden derslerine devam eden, kendisini ülkesine adanmış, sayesinde attığım her adımda kendime "*Vatanım, ailem ve kendim için ne yaptım?*" sorusunu yönelttiğim, beni her koşulda bir anne gibi destekleyen, hayatıma dokunan, arkamda olan; tanıdığım en zarif, kusursuz insanların başında gelen, 2018 yılında kaybettiğimiz canım Hocam Prof. Dr. Oya Akgönenç Muğisuddin'e minnettarım. Kendisini tanıma fırsatım olduğu için çok ama çok şanslıyım. Sonsuz sevgi ve teşekkürler...

Tezimin bu alanda çalışma yapan tüm araştırmacılara ve insanlığa yararlı olması ümidiyle...

ÖZET

Kesgin, Nurbanu. ABD-Çin Rekabetinin Siber Güvenlik Bağlamında Ortadoğu'ya Yansımaları, Yüksek Lisans Tezi, Ankara, 2022.

Soğuk Savaş'ın sona ermesi, güvenlik çalışmalarının farklı bir yöne doğru ilerlemesine; yaşanan teknolojik gelişmeler ve küreselleşme olgusu da siber güvenlik alanının doğmasına ve gelişmesine neden olmuştur. İnternet ağının 21. yüzyılda yaygınlaşması ve dünyanın artık sanıldığıının aksine fazlasıyla küçülmesi, devletlerin farklı güvenlik endişeleri yaşaması ve güvenlik sistemlerinde güncellemeler yapmak zorunda kalması ile sonuçlanmıştır. Oluşan güvensizlik ortamı devletlerin ulusal güvenlik stratejileri açısından birtakım teknolojik ihtiyaçları gündeme getirmiştir. Bu da teknolojik alanda dünya devi olan ABD, Çin gibi devletlerin rekabetinin siber güvenlik alanına taşınmasına sebep olmuştur. Oluşan bu rekabet ise dünyanın kritik öneme sahip ülkelerinden Ortadoğu'ya yansımaktadır. Bu bağlamda çalışma; ABD ile Çin arasında yaşanan rekabeti, rekabetin bir diğer alanı olan siber rekabeti ve bu rekabetin Ortadoğu'ya yansımalarını yaşanan son gelişmeler ışığında irdelemiştir.

Anahtar Sözcükler: Siber Güvenlik, Ulusal Güvenlik, Rekabet, ABD, Çin, Küresel Güçler, Ortadoğu.

ABSTRACT

Kesgin, Nurbanu. The Reflections of the USA-China Competition to the Middle East in the Context of Cyber Security, Master Thesis, Ankara, 2021.

The end of the Cold War caused the security studies to move in a different direction, and the technological developments and the phenomenon of globalization led to the emergence and development of the cyber security field. The widespread use of the Internet in the 21st century and contrary to popular belief, the highly shrinking of the world, have resulted in states having different security concerns and having to make updates in their security systems. The resulting insecurity environment has brought some technological needs to the agenda in terms of the national security strategies of the states. This has caused the competition of states such as the USA and China, which are world giants in the field of technology, to move to the field of cyber security. This competition is reflected in the Middle East, which is one of the critically important regions of the world. In this context, the study examines the competition between the USA and China, cyber competition, which is another area of competition, and the reflections of this competition on the Middle East in the light of recent developments.

Keywords: Cyber Security, National Security, Competition, USA, China, Global Powers, Middle East.

İÇİNDEKİLER

Sayfa No:

BİLDİRİM	i
ADAMA	ii
TEŞEKKÜR	iii
ÖZET	iv
ABSTRACT	v
İÇİNDEKİLER	vi
SİMGELER VE KISALTMALAR DİZİNİ	viii
GRAFİKLER DİZİNİ	x
ŞEKİLLER DİZİNİ	xi
GİRİŞ	1
1. BÖLÜM	5
GÜVENLİKTE YENİ AŞAMA: SİBER GÜVENLİK	5
1.1. Güvenlik Kavramı	5
1.2. Güvenliğin Dönüşümü.....	6
1.3. Siber Güvenliğin Gelişimi.....	7
1.4. Siber Alandaki Tehditler ve Saldırılar	10
1.5. Siber Alanda Hissedilen Güvensizlik.....	13
2. BÖLÜM	14
ABD-ÇİN REKABETİNİN ARKA PLANI VE BOYUTLARI	14
2.1. Rekabetin Tarihsel Süreci	14
2.1.1. Çin'in Yükselişi	15
2.1.2. ABD'nin Düşüşü.....	16
2.2. Rekabetin Geleneksel Boyutları.....	18
2.2.1. Siyasi Boyut.....	18
2.2.2. Ekonomik Boyut.....	21
2.2.3. Askerî Boyut	28
2.2.4. Kültürel Boyut	31
3. BÖLÜM	32
GENİŞLEYEN REKABET ALANI: SİBER ALANDA MÜCADELE	32
3.1. Yeni Rekabet Sahası: Teknolojik Gelişmeler ve Siber Alan.....	32
3.2. Ulusal Güvenlik Politikalarında Siber Güvenlik	38

3.2.1. ABD ve Çin'in Siber Güvenlik Politikaları	40
3.2.1.1. ABD'nin Siber Güvenlik Politikası.....	41
3.2.1.2. Çin'in Siber Güvenlik Politikası	45
4. BÖLÜM	54
SİBER REKABETTE YENİ BÖLGE: ORTADOĞU	54
4.1. İsrail ve İran Bağlamında Siber Rekabet.....	55
4.2. Körfez Bölgesi Bağlamında Siber Rekabet	62
SONUÇ	69
KAYNAKÇA	71
ÖZ GEÇMİŞ.....	82



SİMGELER VE KISALTMALAR DİZİNİ

%	: Yüzde işareti
AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
AGİT	: Avrupa Güvenlik ve İşbirliği Teşkilatı
APEC	: Asya Pasifik Ekonomik İşbirliği
ASEAN	: Güneydoğu Asya Uluslar Birliği
BAE	: Birleşik Arap Emirlikleri
BM	: Birleşmiş Milletler
BMGK	: Birleşmiş Milletler Güvenlik Konseyi
CIA	: ABD Merkezî İstihbarat Servisi
ÇHC	: Çin Halk Cumhuriyeti
ÇKP	: Çin Komünist Partisi
DHS	: İç Güvenlik Bakanlığı
DTÖ	: Dünya Ticaret Örgütü
FBI	: Federal Soruşturma Bürosu)
GSYH	: Gayri Safı Yurt İçi
İHA	: İnsansız Hava Aracı
KİK	: Körfez İşbirliği Konseyi
KOEP	: Kapsamlı Ortak Eylem Planı
LNG	: Sıvılaştırılmış Doğal Gaz
NATO	: Kuzey Atlantik Anlaşması Örgütü

NIPC : Ulusal Altyapı Koruma Merkezi

RSFSC : Rusya Sovyet Federatif Sosyalist Cumhuriyeti

SSCB : Sovyet Sosyalist Cumhuriyetler Birliđi

UGS : Ulusal Güvenlik Stratejisi



GRAFİKLER DİZİNİ

Sayfa No:

Grafik 1: 1990-2020 Yılları Arasında Çin'in GSYH Büyümesi (Yıllık %)	15
Grafik 2: Dünya Bankası Verilerine Göre 2020 Yılı Satın Alma Pariteli GSYH'ye Göre En Yüksek Değere Sahip Ülkeler	25
Grafik 3: Dünya Bankası Verilerine Göre ABD ve Çin'in 2020 Yılı Ekonomi Büyüme Oranları	26



ŞEKİLLER DİZİNİ

Sayfa No:

Şekil 1: 2020 Yılı İtibarıyla ABD'nin Dünya Çağında Askerî Varlığı.....	28
Şekil 2: Ortadoğu Coğrafyası.....	54



GİRİŞ

Soğuk Savaş'ın sona ermesinin akabinde yaşanan gelişmeler güvenlik çalışmalarının farklı bir yöne doğru evrilmesine neden olmakla birlikte yaşanan teknolojik gelişmeler ve küreselleşme olgusu fazlasıyla girift ve gelenekselden uzak bir güvenlik algısı meydana getirmiştir. Soğuk Savaş dönemindeki iki kutuplu düzenin yerini çok kutuplu düzene bıraktığına inanılan yeni dönemin daha güvenli olacağı fikri oluşmuşsa da sonuç beklenilenin tam tersi şekilde gerçekleşmiştir.

Soğuk Savaş'ın sonrasında iki kutuplu dünya düzeni yalnızca Amerika Birleşik Devletleri'nin (ABD) başat aktör olduğu bir düzen oluşturmuş ve bu esnada kutuplardan ayrılan taraflar oluşan boşluktan fırsat bularak gelişme göstermeye başlamıştır. Sovyet Sosyalist Cumhuriyetler Birliği'nin (SSCB) yıkılması ile oluşan bu boşluk kendisini en çok Güney ve Orta Asya'da hissettirmiştir. Özellikle komünist yapının böylesine bir çöküş yaşaması, SSCB ile belirli dönemlerde ayrışma yaşayan Çin Halk Cumhuriyeti'nin (ÇHC)* kapitalizm ile tanışmasına ve yavaş yavaş kapital sisteme ayak uydurmasına vesile olmuştur.

1979 yılında ABD ile diplomatik ilişkilerin yeniden kurulması, ülkeye gelen yabancı yatırımlar, nüfusun yüksek oluşu, ucuz iş gücü gibi etkenler Çin ekonomisini bir anda farklı boyutlara taşımıştır. Mevcut potansiyelini “Çin Rüyası” politikalarıyla birleştiren ve zaman içinde gelişme gösteren Çin, ABD'nin karşısında yükselen bir güç olarak konumlanmıştır. 2001 yılında küresel ticarete katkısı %4 olan Çin'in aynı yıl, Dünya Ticaret Örgütü'ne (DTÖ) dâhil olmasıyla birlikte süper güç olması için önündeki tüm engeller aşılmıştır. Çin bu tarihten itibaren tüm dünya ile ticari ilişkiler kurabilir hale gelmiştir. ABD'de ise bu durum başlarda olmasa da zaman içinde “Çin tehdidi” algısı olarak karşılık bulmuş; Çin'in gelişimi karşısında var olan gücüyle mevcut olanı daha da ileriye taşıma gayretine girişmiştir. 11 Eylül 2001 tarihinde gerçekleşen terörist saldırıları, takip eden on yıllar boyunca “terörizme karşı savaş” olarak Amerikan dış politikasına hâkim olmuşsa da ABD, zaman zaman sinyallerini verdiği Çin tehdidi meselesini 2018 yılında dönemin güç rekabeti dönemi olduğunu resmen ilan etmek suretiyle ortaya koymuştur. Ülkesinin yeni ulusal savunma stratejisini açıklayan ABD

* Çalışmada ÇHC ifadesi yerinden bundan sonra “Çin” ifadesi kullanılacaktır.

Savunma Bakanı James Mattis'in belirlenen yeni stratejide Washington'un önceliğinin "terörizm değil Çin ve Rusya gibi güçlerle rekabet" olacağını açıklaması esasen meselenin ABD açısından nasıl değerlendirdiğini gözler önüne sermiştir. Benzer şekilde ABD Başkanı Joe Biden da henüz başkanlık makamına seçilmeden önce Çin'i ABD'nin en önemli rakibi olarak işaret etmiştir. Bu kapsamda ABD, Çin'in yüklenen bir güç konumunda olmasını "en büyük" tehdit olarak ortaya koymuştur.

ABD ve Çin, olası bir anlaşmazlık karşısında hazır vaziyette bulunma çabasıdadır. Ancak bu hazırlık yalnızca geleneksel güvenlik anlayışıyla sıcak çatışma, askerî üstünlük ve gelişim olarak algılanmamalıdır. Teknolojik gelişmeler; askerî, ekonomik, ticari tüm rekabet alanlarını farklı bir boyuta taşımıştır. Günümüz dünyasında neredeyse her şey bilgisayar ortamında yürütülmekte ve kontrol edilmektedir. Bu nedenle en büyük tehdit siber alan dediğimiz alanda yoğunlaşmaktadır.

1980'li yıllardan itibaren iletişim ve ulaşım teknolojilerindeki gelişmeye bağlı olarak hızlı bir değişim yaşanmaktadır. Küreselleşme ile ifade edilen bu değişimde ülkeler birbirlerine başta ekonomi, güvenlik, enerji, kültür olmak üzere çeşitli alanlarda birbirlerine daha bağımlı hale gelmişlerdir. Yine bu dönemde eskinin askerî odaklı tehditlerine ek olarak siber saldırılar gibi yeni tehditler ortaya çıkmıştır.

Mevcut tüm alanların teknolojik gelişmeler ile entegre hale getirilmesi, devletlerin bu duruma olan güvenlik zafiyetini ortaya çıkarmıştır. Çünkü geline nokta, gelişmiş ülkeler kritik altyapıları ileri düzey bilgi teknolojileri ile korunmaktadır. Bu durum da onları siber saldırı tehdidi altında bırakmaktadır. Teknolojiyi verimli kullanarak rakiplerine üstünlük sağlayan ülkelere yönelik enerji, finans, temel altyapı hizmetleri, elektrik, savunma gibi alanlarda siber saldırı kaçınılmazdır ve tam anlamıyla güvenliğin kusursuz olarak sağlanması gerekmektedir. Siber savaşın gelecekte en önemli üstünlük mücadelesi olacağını öngören devletler bu alanda çalışmaktadır.

Dünyanın süper gücü olarak gösterilen ABD ve Çin arasında teknoloji alanında bir rekabet yaşanmaya başlamıştır. İki büyük ekonomi devinin rekabeti ise küresel ve bölgesel etkileri de beraberinde getirmiş; rekabet bu anlamda ABD ve

Çin ile iş birliği geliştiren/geliştirmeyen pek çok aktöre tesir etmiştir. ABD ve Çin'in siber güvenlik bağlamındaki rekabetinin en belirgin yansımaları ise Ortadoğu'da gözlemlenmektedir.

Çalışmanın amacı, Soğuk Savaş sonrası oluşan tek kutuplu dünya düzenin zaman içinde çok kutuplu dünya düzenine evrilmesinin bunun yanı sıra küreselleşme ve teknolojik gelişmelerin, başta askerî, siyasi, ekonomik ve teknolojik alanlarda birer rakip olan ABD-Çin rekabetinin siber güvenliğe nasıl yansıdığını ve bu yansımanın Ortadoğu'da nasıl karşılık bulduğunu anlamaya çalışmaktır. Söz konusu iki ülke ile siber güvenlik açısından ilişkiler geliştiren Ortadoğu ülkelerinden İsrail, İran, Suudi Arabistan, Birleşik Arap Emirlikleri (BAE) ve Katar'ın meselede nasıl konumlandığıyla birlikte iş birlikleri ve anlaşmazlıkları ortaya koyabilmektir.

Çalışma dört bölüm olarak oluşturulmuştur. İlk bölümde güvenlik ve siber güvenliğin kavramsal çerçevesi ortaya konulduktan sonra siber güvenliğin gelişimi, siber alandaki tehdit, saldırı ve güvensizlik durumu ortaya konulmuştur. Çalışmanın ikinci bölümünde ABD-Çin rekabetinin arka planı ve boyutları ele alınmıştır. Bu bölümde ayrıca söz konusu iki ülke arasındaki geleneksel rekabetin boyutları olan siyasi, ekonomik ve askerî alanlara değinilmiştir. Çalışmanın üçüncü bölümünde ABD-Çin rekabetinin taşındığı yeni alan olan siber alan ve bu alana ilişkin güvenlik adımları analiz edilmiştir. Öte yandan tarafların siber güvenlik konusundaki çalışmaları incelenmiştir. Çalışmanın dördüncü ve son bölümünde ise bahsi geçen bu ülkelerin siber alandaki rekabetinin Ortadoğu nasıl yansıdığı ele alınmıştır. Bu bağlamda siber alanda öne çıkan İsrail, ABD-İsrail müttefikliğinin karşısında konumlanan ve buna karşın Çin'e yakın bir pozisyonda yer alan İran ve son olarak hidrokarbon rezervlerinin ekonomik avantajını siber alana aktarmaya çalışmak suretiyle iş birliklerine açık olan Körfez ülkelerinin rekabetten ne şekilde etkilendiği son dönem gelişmeler ışığında irdelenmiştir. Çalışmanın sonuç bölümünde ise ana konu olan ABD-Çin rekabetinin siber güvenlik bağlamında Ortadoğu'ya yansımalarına ilişkin değerlendirmelere dayanılarak çeşitli karşılaştırmalarla varılan sonuçlara değinilmiştir.

Çalışmada ABD-Çin rekabetinin siber güvenlik bağlamında Ortadoğu'ya yansımaları ortaya konulması için tarihsel analiz metodu kullanılmış ve bu konuda yazılmış eser ve makaleler incelenmiştir. Çalışmanın hipotezi; ABD ile

Çin'in günümüzde devam eden rekabetinin siber güvenliğe kaydığı ve Ortadoğu'ya bu rekabetin yansıdığıdır. Hipotezin çalışma sonunda doğru olup olmadığı elde edilen veriler ışığında değerlendirilecektir.



1. BÖLÜM

GÜVENLİKTE YENİ AŞAMA: SİBER GÜVENLİK

1.1. Güvenlik Kavramı

Güvenlik, hayatın hemen hemen her alanında bugüne kadar var olmuş ve bundan sonraki süreçte de var olacak bir kavramdır. Daimî olan bu kavram aynı zamanda konusuna göre insan, çevre, ulusal gibi farklı alanlarda da karşılık bulmaktadır. Kavram, zaman içerisinde kullanma alanları ve üzerine yüklenen anlam bakımından değişikliğe uğrasa da bir insanın yemek yemesi veya uyuma ihtiyacı kadar kritik bir önem taşıdığı için varlığını her zaman sürdürmüştür (Kula ve Çakar, 2015, s.197).

Güvenlik kavramı konusunda birçok tanım bulunmakla birlikte disiplin içerisindeki temel teorik yaklaşımlar tarafından farklı hassasiyetler ve değerlendirmelere göre ele alınmıştır. Uluslararası ilişkiler ve güvenlik çalışmaları alanlarında yoğun bir şekilde üzerinde çalışılan güvenlik kavramı en temel biçimiyle, “herhangi bir korkunun olmaması ve güvende hissetme durumu” şeklinde ifade edilebilmektedir. Güvenliği daha çok askerî unsurlar ışığında değerlendiren realistler için dış politika ulusal güvenlik meseleleri etrafında şekillenmektedir. Bu bağlamda askerî ve siyasi meseleler “yüksek politika (high politics)”; ekonomi, sağlık, çevre ve diğer meseleler ise “alçak politika (low politics)” olarak nitelendirilmiştir. (Oğuzlu, 2007, s.14). Realist anlayışa göre yalnızca *güç* ile sağlanabileceği öne sürülen güvenlik kavramı neorealistler tarafından ise realistlerden çok da uzak olmayan biçimlerde ortaya koyulmuştur. Niccolò Machiavelli iyi yönetimle, Hans Morgenthau varlığını sürdürmekle, Kenneth Waltz, Edward Carr ve realist görüşe sahip diğer düşünürler askerî kapasite ve güç dengesi ile güvenli olunacağını ileri sürmüştür (Brauch, 2012, s.168-169). Bu durumda ise karşılıklı şekilde ve anarşik düzenin bir sonucu olarak kapasite artırımı yapan devletlerin arasında yaşanan güvensizlik algısı da John H. Herz tarafından *güvenlik ikilemi* olarak ortaya konulmuştur.

Sıklıkla birbirleri yerine kullanılabilen idealizm ve liberalizm ise güvenliğe ilişkin meselelerde realistlerden farklı argümanlar öne sürmüştür. Liberallere göre güvenliğin asıl sağlayıcı unsuru devletlerin yönetim biçimidir ve eğer bir devlet

totaliter rejime sahipse savaşa meyilli, demokratik rejime sahipse barış yanlısı olmaktadır (Arı, 2010, s.364-373). Öte yandan konstrüktivizme göre ise devletlerin tarihsel ve kültürel geçmişlerinin oluşturduğu kimlikler, güvenliğe dair algıları belirleyen unsurlardır. Devletlerin sahip olduğu kimlikler birbirlerini tehdit olarak algılayıp algılamamalarına neden olmaktadır (Wendt, 2003, s.96-138).

1.2. Güvenliğin Dönüşümü

I. Dünya Savaşı sonrası uluslararası ilişkiler disiplinin esas alanlarından biri olan güvenlik kavramı, ağırlıklı olarak II. Dünya Savaşı sonrasında irdelenmeye başlanmıştır (Burchill ve Linklater, 2012, s.18). II. Dünya Savaşı sonrası dönemde, savaşın geride bıraktığı yıkımın tekrar yaşanmaması noktasında uluslararası güvenliğin nasıl sağlanacağı meselesi cevap aranan soruların başında gelmiştir. II. Dünya Savaşı'nın akabinde ise ABD ve SSCB'nin öncülüğünde Batı ve Doğu Bloku olarak kutuplaşmanın yaşanmaya başladığı ve söz konusu iki blokta yer almayan *Bağılantısızlar* isimli grubun olduğu yeni bir dönem başlamıştır. "Soğuk Savaş" olarak adlandırılan bu dönemde, güvenlik anlayışında belirleyici unsur askerî güvenlik olmuştur. Bu bağlamda ABD ve SSCB, güvenliklerini sağlamak için NATO (Kuzey Atlantik Antlaşması Örgütü) ve Varşova Paktı gibi örgütler kurmuşlardır (Evans ve Newnham, 2007). Bu dönemde devletler güvenliklerini tek başında değil bir ittifak sistemi içinde sağlamaya çalışma yoluna gitmişlerdir (Dedeoğlu, 2008, s.38).

Öte yandan ABD'nin II. Dünya Savaşı esnasında Japonya'nın Hiroşima ve Nagazaki şehirlerine düzenlediği atom bombası, nükleer silahların uluslararası güvenlikte kullanıldığı bir dönem başlatmış ve Soğuk Savaş süresince de yıkıcı etkisi Japonya tecrübesinde gözler önüne serilen kitle imha silahları, Doğu ve Batı Blokları arasında belirleyici ve caydırıcı bir etki yaratmıştır. Zaten bu nedenledir ki taraflar arasındaki savaş *soğuk* olarak adlandırılmıştır. Tehdidin son derece net ve sabit olduğu bu dönemde tehdit özneleri devletler olmuştur ve savaş süresince güvenlik öncelenerek askerî ve savunma odaklı harcamalara ağırlık verilmiştir.

Soğuk Savaş dönemi sonrası ise hemen hemen her alanda mevcut düzene kıyasla farklı değişimlerin yaşandığı yeni bir dönem başlamıştır. Soğuk Savaş süresince net, tahmin edilebilir ve yalın bir tehdit algısı ve güvenlik anlayışı

hâkim olmuşsa da yeni dönemde bu durum yerini oldukça girift, tahmin edilebilirliğin zayıfladığı ve değişen bir yapıya bırakmıştır. Ayrıca iki kutuplu dünya düzeninin sona ermesi ve tehdit algısının yalnızca devletlerarasında olmanın da ötesine geçmesi ile birlikte tüm dünya bir mücadele alanı olarak ortaya çıkmaktadır.

Teknolojik gelişmeler ve küreselleşme ile birlikte daha geniş bir yelpazeye sahip olan güvenlik kavramı içerisinde birçok yeni alan ortaya çıkmış ve konjonktürel olarak önemi artmıştır (Brauch, 2012, s.169-175). Ulusal güvenliğin bir alt kolu olan siber güvenlik kavramı da Soğuk Savaş sonrası dönemde zamanla daha önemli bir alan haline gelerek devletlerin özel olarak strateji geliştirdikleri bir politikaya dönüşmüştür.

Soğuk Savaş sonrasını takip eden dönemde özellikle ABD’de 11 Eylül 2001 saldırılarının gerçekleşmesi, ulusal güvenliğin kapsamının ve algısının değişmesi güvenliğin yalnızca fiziksel ve askerî saldırılar karşısında alınan önlemler anlamına gelmediği bir yaklaşıma dönüşmüştür. Bu yeni yaklaşım kapsamında ulusal güvenlik içerisinde siber saldırılar, terör, salgın hastalıklar ve ekonomik gelişmelerin engellenmesi de ulusal güvenliğin bir parçası haline gelmiştir. Ulusal güvenlik kapsamında devletlerin önemli verilerinin korunması hususu da önem kazanmış; devletler için önem teşkil eden enerji, ulaşım, finans, sağlık gibi kritik altyapılar ile ilgili olarak siber suçlara ve tehditlere karşı siber politikalar geliştirilmiştir.

1.3. Siber Güvenliğin Gelişimi

Soğuk Savaş’ın yaşandığı süreçte güvenliğin kaynağı olarak Doğu ve Batı Bloku’ndan oluşan iki kutuplu güç dengesi sistemi görülmekteydi. Bu dönemde güvenlik algısı daha çok askerî güvenlik alanında yoğunlaşmış ve taraflar karşılıklı olarak sert politikalar geliştirmiştir.

Soğuk Savaş’ın sona ermesi neticesinde ise iki kutuplu sistem algısı, yerini tek kutuplu ve sonraki süreçte çok kutuplu sisteme bırakmış; güvenlik tehditlerinde farklılaşma yaşanmış ve buradan hareketle güvenlik anlayışında değişiklikler meydana gelmiştir. Ekonomik sorunlar, küresel salgınlar ve hastalıklar, uluslararası terör tehdidi ve çevresel problemlerin bu yeni güvenlik

biçiminde öne çıkan temel kavramlar olmasına binaen güvenliğin boyutunda da bir genişleme meydana gelmiştir. Güvenlik anlayışının bu şekilde genişlemesi ve çeşitlenmesine küreselleşme ve bu sayede hız kazanan teknolojik gelişmeler de eklenince "siber uzay (cyberspace)" adı altında yeni bir alan ortaya çıkmıştır. Bu sürecin diğer bir uzantısı ise *güvenlik ihlalleri*dir. Nitekim siber uzayda bilgisayar sistemleri ve dijital ağların kullanımının bir sonucu olarak siber saldırı ve siber terör gibi tehditlerin varlığı ve güvenlik ihlalleri ortaya çıkmıştır. Bu sorun, başlarda teknik bir konu olarak değerlendirilmiş ancak akabindeki dönemlerde söz konusu tehditlerin siber alan ile ilişkili yapısı sonucunda ilginin siber güvenliğe kaymasına da neden olmuştur. Komplike yapısı itibarıyla siber alanın kontrol edilmesinin çok zor ve hatta imkânsız olduğunu söylemek mümkündür. Bu bağlamda, siber alandaki tehditlerin bu denli çok yönlü ve kolaylıkla gerçekleştirilebiliyor olması, siber güvenliğin önemini ortaya koymaktadır.

Siber güvenliği, siber uzayda sağlanan güvenlik olarak düşünmek yanlış olmayacaktır. Siber uzay, fizikî donanımlar aracılığıyla ortaya çıkarılan bir alan olsa da somut bir alan değildir. Aynı zamanda siber uzay sadece internetle birlikte var olan bir alan da değildir. İnternete bağlı olmayan bilgisayarlar ya da farklı ağlar da siber alan oluşturabilmektedir. Öte yandan siber uzay, birden fazla soyut olgunun bir araya gelmesinden de oluşabilmektedir. Yazılımlar, bilgiler ve ağlar buna örnek olarak verilebilecektir (Clark vd., 2014). Bir diğer deyişle siber uzay, "tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan bir ortam" olarak tanımlanabilecektir. Kavram, 1980'li yılların başında ilk kez bilim kurgu romanlarıyla meşhur William Gibson tarafından kullanılmıştır (Kara, 2013, s.4). Birleşik Krallık'ın siber güvenlik strateji belgesinde ise siber uzay, "bilgileri saklamaya, düzenlemeye ve birbiri arasında alışveriş yapmaya imkân veren; bilgisayar, internet ve diğer sistemleri içeren altyapısal ve sektörel sistemleri destekleyen, dijital ve interaktif bir bağlantı ağı" (The Information Security Arm of GCHQ, 2012, s.3) olarak tanımlanmıştır.

1990'lı yıllarda internet ağına bağlı olan bilgisayar sistemlerinde ortaya çıkan güvenlik sorunları neticesinde siber güvenlik kavramı literatüre kazandırılmıştır. Söz konusu dönemde bu kavram daha çok bilgisayar sistemlerindeki verilerin, dosyaların ve bilgilerin güvenliğine olan riskleri ifade etmek için kullanılmaktaydı. Siber alanın güvenli olabilmesi için bilgi güvenliği

yönetim sistemi standardında olduğu gibi bilginin gizliliğinin (confidentiality), bütünlüğünün (intergrity) ve erişilebilirliğinin (availability) sağlanması gerekmektedir (Aslay, 2017, s.25). Fakat artık siber güvenliği ilgilendiren alanların genişlemesi ve çeşitlenmesi neticesinde siber güvenlik sadece bilgi güvenliği ile sağlanmış olmamaktadır. Teknolojide kat edilen gelişmeler siber alanın hayatımızın her alanına yerleşmesine neden olmuştur. Dolayısıyla siber alanın kapsamı ve ilgili olduğu mecralar da genişlemiştir.

Siber güvenliğin daha önceden devletler tarafından çok önemsenmediğini söylemek yanlış olmayacaktır. Çünkü siber güvenlik konusu, devletlerin nezdinde güvenlik tehditlerini oluşturacak ve bu tehditlerin de milli güvenliği tehdit edecek bir alan olarak değerlendirilmemiştir. ABD’de yaşanan 11 Eylül terör saldırıları ve sonrasında Madrid ve Londra gibi şehirlerde gerçekleşen terör saldırılarında siber güvenlik açıklarının kullanıldığı fark edilmiş ve bu olayların ardından siber güvenliğe olan ilgi artmıştır. Bahsi geçen eylemlerde ilk kez siber saldırılardaki tehlikenin boyutunun ne denli büyük olabileceği anlaşılmıştır. Bu eylemler sonucunda, siber alandan gelen bir saldırının da silahlı terör eylemlerindeki gibi etkisinin çok büyük olacağı, yıkıcı sonuçlar doğuracağı, suçsuz insanların hayatlarına mal olacak zararlar verebileceği gibi tehlikeli durumların doğabileceği anlaşılmıştır (Dupont, 2013, s.67-80).

Siber güvenliğin, ulusal güvenlik bağlamındaki tehdidine ilişkin fikirlerin oluşmasında 2007 yılı önemli bir dönüm noktası olmuştur. Bu tarihte, Estonya’ya karşı gerçekleştirilen ve Rusya kaynaklı olduğu iddia edilen siber saldırıların sonucunda ortaya çıkan hasarlarla siber güvenliğin aynı zamanda ulusal güvenlik için bir tehdit olabileceği düşüncesi güçlenmiştir. Talinn Meydanı’nda konuşlanmış olan ve SSCB döneminden kalan Bronz Askerî Heykeli’nin yerinin değişmesinin sonucu olarak Estonya ve Rusya arasındaki gerilim artmış ve bu gerilimin etkileri siber alanda da görülmüştür (Darıcılı, 2015, s.414). Estonyalı Ruslar, bir NATO müttefiki olan ve her türlü hizmeti internet aracılığı ile sağlama olanağına sahip Estonya’nın bilişim sistemlerine bir ay boyunca saldırarak Estonya’da hayatı hemen hemen durdurma noktasına getirmişlerdir. Söz konusu saldırılar dünyanın çeşitli yerlerinden, birçok farklı merkezden koordineli bir biçimde gerçekleştirilmiştir. Saldırıların sonucu olarak Estonya’da en çok kullanılan internet siteleri, hükûmet hizmetlerinin sağlandığı devlete ait altyapı sistemleri,

bankacılık ve finans sistemleri vs. hedef alınarak verilen zarar artırılmıştır. Kapsamlı, geniş kullanım alanı olan, gelişmiş bir internet ağına ve bu ağlarla birlikte büyük bir organizasyona sahip olan Estonya bunun yanında siber alandan gelen saldırı, risk ve tehditlere karşı da güçsüz ve savunmasız bir hale gelmiştir (Eren, 2017, s.36-37).

Yaşadığımız dönemde savunma, sanayi, eğitim, sağlık, ulaşım ve sosyal hayatın bir parçası olan siber teknolojiler aynı zamanda bu alanların tehdit ve saldırılara açık hale gelmesine yol açmıştır. Bu da siber güvenliğin önemini artırmış ve başta yalnızca teknik bir konu olarak değerlendirilen bilgisayar sistemlerinin hayatımıza bu derece entegre olması, siber güvenliğin sağlanması gerektiği düşüncesini ilk zamanlardan bugüne kadar bir zorunluluk olarak ortaya konmuştur (Johnson, 2015, s.26-29). Dolayısıyla devletler bu konuda önlemler almak ve adımlar atmak durumunda kalmaktadır. Siber saldırılar ve hatta *siber savaşlar* olarak tabir edebileceğimiz sızma faaliyetleri sonucunda devletler artık bu konuda birçok çalışma yapmakla birlikte hem siber güvenlik politikası ve altyapısı oluşturmak hem de bu alanla bütünleşmiş savunma sistemleri oluşturmak zorunda kalmaktadır. Siber güvenliği sağla(ya)mayan devletlerin aksi takdirde ekonomik ve askerî alanlardaki varlıkları siber alandan gelen tehditlere karşı güçsüz, açık ve savunmasız bir hâl almaktadır. Buradan hareketle; NATO, BM (Birleşmiş Milletler), AB (Avrupa Birliği), AGİT (Avrupa Güvenlik ve İş Birliği Teşkilatı) gibi uluslararası kurum ve kuruluşlar nezdinde ve ülkelerin tek başlarına bu konuda oluşturdukları politikalar ve savunma sistemleri ile siber güvenlik mekanizmaları kurulmakta ve kullanılmaktadır (Yılmaz ve Sağıroğlu, 2013, s.159).

1.4. Siber Alandaki Tehditler ve Saldırılar

Bilginin önem kazandığı, teknolojinin gelişmesiyle birlikte yeniliklerin ve bilgi sistemlerinin hayatımıza girmeye başladığı 1990'lı yıllardan sonra uluslararası ilişkilerde tehdit olgusunun değişmesi gerektiği anlaşılmıştır. Hayatın her alanına bilgi sistemleri dâhil olmuş; internet, çevrim içi (online) alışveriş, çevrim içi eğitim gibi birçok unsur bilgi sistemlerinin konusu olmuştur. Hem devletler nezdinde hem de bireylerin yaşamlarında kültürden eğlenceye, araştırmadan savunmaya, sağlıktan eğitime kadar birçok alanda bilgi sistemlerinin büyük etkileri görülmüştür. İnsan hayatını bu denli etkileyen yeni

teknolojilerin ortaya ıkmasıyla beraber yapısal reformların da onu takip etmesi hep kaçınılmaz olmuştur. Fakat bu reformlar ve değışimler her zaman olumlu ve iyi sonuçlar doğurmamış; bazı tehditleri, riskleri ve sorunları da beraberinde getirmiştir. Bu olumsuzlukların başında ise *siber saldırılar* yer almaktadır.

Siber saldırılar, siber alanda hedef olan bilgisayar işletim sistemlerini zarara uğratmak amacıyla yapılan eylemlerden oluşmaktadır. Bir diğer ifadeyle siber saldırı, “politik veya stratejik bir amaç için bir bilgisayar sisteminin işlevselliğine müdahale etmek için kodun kullanılması” anlamına gelmektedir (Kello, 2013, s.19). Bir işletim sistemindeki hatalar veya sistemsel arızaların sebebiyet verdiği zararlar siber saldırı olarak tanımlanmamaktadır ancak siber saldırıların sonuçlarının tamamını siber alanda görmek mümkün değildir. Siber saldırı sonucunda ortaya ileri vadede zararların da ıkması mümkündür; ekonomik, siyasal, sosyal, kültürel ya da devlet sistemlerine etki eden zararlar da görülebilmektedir. Bu saldırılar doğrudan ve dolaylı olarak ortaya çıkmaktadır. Doğrudan yapılan siber saldırılarda hedef sistemin yok edilmesi ve çalışamaz duruma gelmesi amaçlanırken dolaylı yollardan gerçekleştirilen siber saldırılarda hedef sistemin işlevselliğinin azalması, önlenmesi ve zarar görmesi amaçlanmaktadır. (Kello, 2013, s.19-20). Siber saldırıları diğer saldırılardan ayıran sahip olduğu diğer bir özellik ise siber alanın coğrafya ve fiziki dünyadan daha da büyük bir yapıya sahip olmasıdır. Siber saldırganlar, bu tarz sınır ve kısıtlamalarla karşı karşıya kalmaksızın başka ülkelere veya o ülkelerin vatandaşlarına daha geniş bir alandan saldırı düzenleyebilmektedir. Netice itibarıyla, söz konusu saldırganlar olası bir siber saldırı ile hedeflenen ülke ve saldırının gerçekleştiği ülke arasında uluslararası boyutlara ıkabilecek krizlere neden olabilmektedir. Siber alanın özelliği sayesinde saldırganlar kimliklerini de gizleyebilmektedir ve fiziksel hasarın öncelendiği klasik saldırı anlayışından farklı olarak siber saldırılarda suçlunun belirsizliği sebebiyle cezanın gerçekleşmesi de zorlaşmaktadır.

Siber alanın bu durumu ele alındığında Mary Kaldor'un eski ve yeni savaş ayrımını da göz önünde bulundurmak gerekmektedir. Kaldor'a göre eski tip savaşlarda savaşan taraflar düzenli ordular olurken, yeni tip savaşlarda ise devlet ordularının yanında silahlı dış organizasyonlar, paralı askerler ve farklı gruplar da savaşların tarafı olabilmektedir. Bunun dışında eski savaşlarda hedef ideolojik

veya jeopolitik nedenlerden kaynaklanırken bunun yeni tip savaşlarda kimlik temelli olduğu görülmektedir. Ancak eski ve yeni tip savaşların birçok ortak noktası vardır. Bunlardan biri, savaşan tarafların kimliklerinin bir durumda bilinip bilinmemesidir (Kaldor, 2012, s.1-14).

Bir diğer açıdan, siber uzayda bahsi geçen eski savaş ve yeni savaş ayrımının dışında bir durum daha vardır. Siber uzayda oluşan, bazı durumlarda siber savaşlara sebebiyet verecek kadar ciddi sonuçlara yol açabilecek siber saldırılar incelendiğinde görülecektir ki bu alanda eski tip savaşlarda olduğu gibi düzenli ordular yoktur, yeni tip savaşlarda olduğu gibi kimlikler de açık ve belirgin değildir. Siber saldırılarda diğerlerinden farklı olarak hangi durumların savaş olarak lanse edilebileceği de kolayca belirlenememektedir. Siber saldırılarda saldırganların kimlikleri tam olarak belirli değildir, saldırganlar devlet dışından da olabilmektedir. Yapılan saldırıların gerçekleştirildiği ağlar sebebiyle; saldırının nereden, nasıl ve kimler tarafından yapıldığı tam olarak tespit edilememekte ve saldırının bir savaş ilanı olup olmadığı da kesin bir şekilde ortaya konamamaktadır (Brenner, 2010, s.3).

Yeni tehditlerin ve saldırı algısının değiştiğini anlamak için 11 Eylül 2001 tarihinde fazlasıyla yıkıcı sonuçları olan terör saldırıları ve 2007 yılında Estonya'ya yönelik gerçekleştirilen saldırıları dikkate almak gerekmektedir. Bu saldırılar siber kaynaklı saldırılardır ve sonuçlarının ne kadar yıkıcı etkileri olduğunu görmek mümkündür (Kurnaz, 2016, s.63). Estonya, internet ağı ve internet güvenliği açısından örnek gösterilen ve farklı alanlarda birçok hizmeti internet üzerinden sunan bir ülkedir. Fakat Estonya 2007 yılından sonra birçok siber saldırıya maruz kalmış ve uzun bir süre vatandaşlarına bu hizmetleri sunamamıştır. Yaşanan bu durum da hayatın büyük oranda aksamasına sebep olmuştur. Çünkü gerçekleştirilen saldırı ile devletin sistemlerinin yanı sıra ekonomi, güvenlik ve medyayı etkileyen sistemler de dâhil olmak üzere altyapılara büyük zararlar verilmiş ve çalışmaları engellenmiştir. Dolayısıyla, siber alanın günümüz dünyasıyla her açıdan iç içe hale gelmesi, siber saldırıların ne ölçüde yıkıcı sonuçlar doğurabileceğini ve meselenin ne kadar önemli olduğunu ortaya koymuştur.

1.5. Siber Alanda Hissedilen Güvensizlik

Siber güvenlik konusunu ele aldığımızda *siber güvensizlik* ifadesi üzerinde de durmak gerekmektedir. Siber terör, siber saldırı ve siber casusluk olarak kendini gösteren faaliyetler siber güvensizlik terimi ile ifade edilebilmektedir. Kritik alanlar, bilgisayar sistemleri, telekomünikasyon altyapıları ve internet platformlarına yönelik gerçekleştirilen eylemler ve sızma faaliyetleri siber terör olarak adlandırılırken, siber saldırılar ulus devletlerin başka bir devletin ağlarına ve kritik altyapılarına zarar vermek amacıyla bilgi teknolojisini kullanması yoluyla meydana gelmektedir. Gizli bilgi ve belgelerin bilgi teknolojilerini kullanarak elde edilmesi için ise siber casusluk ifadesi kullanılmaktadır (Seemaa vd., 2018, s.125). Ancak devletlerin dışında siber saldırılar farklı aktörler, gruplar ve şahıslar tarafından da yürütülebilmektedir.

Ekonomi, eğitim, sağlık, ulaşım, hükûmet faaliyetleri gibi kritik altyapıların korunması için siber güvenlik büyük önem arz etmektedir. Dolayısıyla siber saldırganlar devletlerin kritik altyapılarına büyük zarar verebilecek potansiyele sahiptir (Clemente, 2013, s.1-8).

Ayrıca hem devletlerin hem de kişilerin özel ve gizli kalması gereken bilgi ve belgelerinin gizliliği de siber güvenlik ile sağlanmaya çalışılan bir diğer konudur. Tüm bunlarla beraber; meydana gelen siber saldırılar, zafiyetler, siber güvenlik alanında alınan önlemler ve yaşanan birçok siber sorunlar hem devletler hem de kişiler için siber güvensizlik ifadesini de ön plana çıkarmaktadır.

2. BÖLÜM

ABD-ÇİN REKABETİNİN ARKA PLANI VE BOYUTLARI

2.1. Rekabetin Tarihsel Süreci

ABD-Çin ilişkileri 18. yüzyıldan beri süregelmektedir. Bölgede meydana gelen savaşlar, Çin'deki kültür değişiklikleri ve sonrasında oluşan değişimler sebebiyle sürekli inişli çıkışlı bir değişim yaşansa da iki ülke arasındaki bu ilişki, günümüze kadar devam etmiştir. Tarih boyunca iki ülke arasındaki ilişkilerin temel niteliği ticari bir özellik taşımıştır. Bugün, dünyanın en büyük iki ekonomisine sahip olan ABD ve Çin'in aralarındaki finansal ve ticari ilişkilerin boyutu ve niteliği küresel boyutta ciddi önem arz etmektedir. Bu ilişkiler iki ülkeyi farklı pozisyonlarda ve farklı dönemlerde karşılıklı bağımlılık içine sokmuştur. 18. yüzyılın son çeyreğinden bu yana süren ABD-Çin ilişkilerinde meydana gelen kırılmalar ve bunların aşılma süreci tüm dünya için önemli gelişmelere neden olmuştur. Özellikle ivme kazanarak gelişen ekonomisi dolayısıyla Çin'in küresel bir dünya ticaret devi haline gelmesi ABD'nin dikkat ve gayretini üzerine çekmiştir.

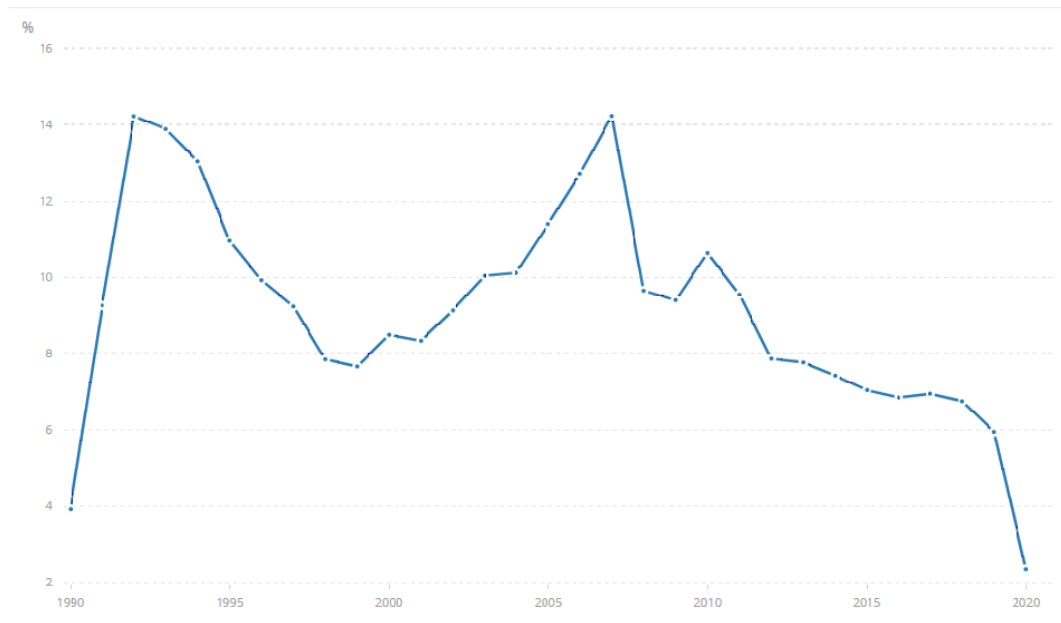
Özellikle Soğuk Savaş döneminin sona ermesiyle ABD ile Çin arasındaki anlaşmazlıklar yerini yumuşamaya bırakmış; 1999'dan itibaren iki ülke arasındaki ticari ilişkiler gelişmeye başlamıştır. Bunlarla birlikte ABD, Çin'in girişine ilişkin çekinceli tavrına son vermiş ve Pekin, DTÖ'nün bir üyesi olmuştur (Shirk, 2007, s.25). 11 Eylül 2001 tarihinde ABD'de gerçekleşen terör saldırıları iki ülke arasındaki ilişkiler için önemli bir dönüm noktası olmakla birlikte bu dönemde ABD, saldırıların ardından Çin'e yönelik politikalarında farklılaşmaya gitmiş ve Çin'i destekler bir tavır sergilemiştir. Buradan hareketle, Çin ve ABD terörizme karşı iş birliğine ve görüş birliğine varmıştır.

İki ülke arasındaki ilişkilerin tarihsel boyutunu ele aldığımızda dönem içerisinde Çin'in yükselişi ve ABD'nin düşüşü rekabetin ortaya çıkış serüvenini özetlemek için yeterli olacaktır. Bu noktada Çin'in büyümesinin çoğunlukla ticari ve ekonomik açıdan gerçekleştiğini; buna karşın ABD'nin düşüşünün ise çoğunlukla küresel düzeyde birtakım yanlış siyasi hamleler ile prestij kaybetmek suretiyle gerçekleştiğini söylemek yanlış olmayacaktır.

2.1.1. Çin'in Yükselişi

Köklü ve zengin tarihi, özgün bir uygarlık yapısına sahip olan Çin, yaklaşık olarak son 30 yıl içerisinde hızla büyüyen ekonomisi ile birlikte dünyada son zamanlarda en çok dikkat çeken ülke konumuna yerleşmiştir. 19. yüzyılda Batılı ülkelerde yaşanan hızlı gelişmelere ayak uyduramayan Çin, dünya siyasetinde arka plana itilmiş ve hatta bazı topraklarını kaybetmişse de Çin eski Devlet Başkanı Mao Zedung'nun ardından başa geçen Deng Xiaoping ile gündeme gelen "sosyalist piyasa ekonomisi" modeli, Çin'in kısa sürede yükselişe geçmesine imkân sağlamıştır (Sandıklı, 2009, s.663).

Farklı ekonomik modeller deneyen Çin'de bu dönemde yabancı sermaye girişleri ve dış ticaret önemli hale gelmiş ve güçlü bir bankacılık sisteminin temelleri atılmıştır. Yıllar içinde daha fazla dış yatırım yaparak, teknoloji taklidi ve ithalatı gerçekleştirmek suretiyle ABD ile arasındaki gelişmişlik uçurumunu kapatmıştır. Çin, ticari ve ekonomik problemler yaşamışsa da bunların üstesinden gelmeyi bilmiştir. Nihayet 2007 yılına gelindiğinde Çin'deki büyüme oranı tarihinin en yüksek oranı olan %14,23'e ulaşmıştır (Grafik 1). Yıllar içinde, Çin büyük bir ekonomik değer yaratarak ABD'nin ardından dünyanın ikinci büyük ekonomisi konumuna gelmiştir.



Grafik 1: 1990-2020 Yılları Arasında Çin'in GSYH Büyümesi (Yıllık %)

Kaynak: <https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG?locations=CN+-CN&end=2020&locations=CN&start=1990>

Dış politikada temkinli bir büyüme stratejisi izleyen Çin, ölçülü ve dikkatli davranıp ABD ve Batı dünyasını korkutmadan ekonomik ve askerî alandaki gelişimini tamamlamayı, Tayvan'ı bünyesine katmayı, Ortadoğu'da söz sahibi olarak artan enerji ihtiyacını karşılamayı ve yeni enerji pazarlarına girmeyi; Şanghay İşbirliği Örgütü, Güneydoğu Asya Uluslar Birliği (ASEAN) ve Asya Pasifik Ekonomik İşbirliği (APEC) gibi uluslararası kurumların aracılığı ile bölgede barış içerisinde kendi üstünlüğünü sağlamayı kendisine amaç edinmiştir. Çin tüm bu amaçları doğrultusunda süper güç olarak konumlanma arzusu taşıırken, güçlü pozisyonunu kaybetmek istemeyecek süper güç ABD ile tam anlamıyla güçlenmeden bir çatışma ortamına girmekten dolayı çekinceye sahip olmuştur. Çin eksikliklerine rağmen dünya liderliği konusunda hamleler yapmaya başlamıştır ve bu hamlelerini özellikle ekonomik ve teknolojik alanı ve potansiyellerini kullanarak halen devam ettirmektedir. Bu bağlamda öne sürülen “Bir Kuşak Bir Yol Girişimi (One Belt One Road (OBOR) veya Belt and Road Initiative (BRI) olarak geçmektedir)” ve “Made In China 2025”, Çin'in başat güç olma noktasında önde gelen atılımlarındandır. Öte yandan, alanlardaki hamleleriyle yükselişinde günden güne ilerleyen Çin'in güçlendikçe otoriter siyasal ve yarı devletçi ekonomik modelini dünyaya dayatabilecek olması, kendisinin yükselişi ile ilgili en büyük çekincelerin başında gelmekte ve ABD tarafından bu meselenin altı sıklıkla çizilmektedir.

2.1.2. ABD'nin Düşüşü

Çin'in yükselişinin yanı sıra ABD'nin düşüşü de gündemde yerini koruyan bir mesele olarak karşımıza çıkmaktadır. Soğuk Savaş'ın galibi olarak mevcut düzenin tek süper gücü olarak lanse edilen ABD, “Kızıl Tehlike”yi yanı Sovyet tehlikesini geride bırakmış; uluslararası ve bölgesel organizasyonlar aracılığıyla bu gücü muhafaza etme ve genişletebilme arayışlarına yönelmiştir. Ancak yaşanan 11 Eylül 2001 saldırılarının ardından izlediği saldırgan politikalar sonucunda ABD, dünya siyasetindeki tek güç olma avantajını elinden kaybetmeye başlamıştır. Peş peşe Afganistan ve Irak'ta gerçekleşen savaşlar ile “teröre karşı savaş”ın yönünün İslam ülkelerine karşı savaş yani “Yeşil Tehlike” olarak algılanması durumu ABD'nin hem Ortadoğu'da hem de diğer bölgeler nezdinde prestij kaybı yaşamasına sebep olmuş; bahse konu olan bölgede

kendisinin nefret edilen, güvenilmez, ayrımcı bir devlet olarak konumlandırılmasına yetmiştir.

2000'li yıllardan sonra iktidardaki yeni muhafazakâr çevreler uluslararası hukuk ve müttefiklik ilişkilerine de zarar verecek şekilde kendi çıkarlarını ön planda tutmuşlardır. Bu durum da ABD'nin dünya siyasetinde prestij kaybetmesine ve müttefikleri ile olan ilişkilerinin zarar görmesine sebebiyet vermiştir. Ayrıca 11 Eylül saldırılarının etkisi ile başlayan terörizmle mücadele önlemleri çok sert bir şekilde sürdürüldüğünden dolayı ABD'nin yumuşak güç profili bir anlamda kaybolmuş; bu durum demokrasisine ve imajına zarar vermiştir. Bunlarla birlikte devam eden süreçte ABD ulusallaşmaya ve aynı zamanda küresel gücünü de kaybetmeye devam etmiştir. Dönem dönem izolasyon politikasını izleyen ABD, saldırılardan sonra da güvenlik önemlerini artırarak ve hatta fazlasıyla ileri giderek ülke içinde Müslümanlara karşı olumsuz davranışlar sergilemiştir.

Teröre karşı savaş açtığını ilan eden; 2001 yılında Afganistan'a, 2003 yılında ise Irak'a askerî müdahale gerçekleştiren ABD için her şey daha kötüye gitmeye başlamıştır. Afganistan müdahalesi 20 yıl sürecek bir savaş, çok sayıda ölüm, yerinden edilme ve ekonomik maliyet getirmekten başka bir işe yaramamıştır. Irak müdahalesi sonrası ise İran bölgedeki etkisini artırmış, aynı zamanda işgal döneminde ABD ve İngiliz askerlerinin birtakım eylemleri, işkenceleri ve saldırıları İslam dünyasında büyük tepki almıştır. Akabinde uluslararası bir sivil toplum kuruluşu olan Wikileaks tarafından başta Irak ve İran'a ilişkin gizli yazışmaların sızdırılması da ABD için büyük bir prestij ve güven kaybı oluşturmuştur. Ancak ABD sözde Arap Baharı dönemindeki demokrasi yanlısı tutumuyla bir nebze de olsa kaybettiği imajını tekrar kazanmaya başlıyor mu sorusu akıllara gelirken 2021 yılında, tam 20 yıl sonra Biden yönetimin Afganistan'dan çekilmesi ve ülkede yeniden Taliban'ın yönetimi devralması hadisesi ABD'yi uluslararası arenada ciddi bir prestij kaybına uğratmıştır.

Etkisini hız kaybetmeden devam ettiren bu rekabet kapsamında, ABD'nin askerî ve güvenlik alanlarında güçlü adımları bulunurken Çin; ekonomi, siyasi, ticaret ve yumuşak güç mekanizmalarında girişimlerde bulunmaktadır. Öte yandan Çin'in askerî ve güvenlik alanındaki girişimlerine Güney ve Doğu Çin Denizi'nde artan askerî hareketliliği de önemli bir örnek olarak öne çıkmaktadır.

Tayvan ve Hong Kong merkezli meseleler ile Doğu ve Güney Çin Denizi'ndeki askerî hareketlilik sebebiyle önümüzdeki dönemde iki ülke arasında gerginliğin artarak devam etmesi öngörülmektedir. ABD ve Çin arasında; siber saldırılar konusu, ticaret savaşları, 5G teknolojisinin gelişimi, Çin'in artan ekonomi-politik nüfuz alanı gibi konuların yanı sıra son dönemde ülkelerin koronavirüs aşısını bulma yarışı, hızlanan ideolojik rekabet, virüsün ekonomiye açtığı zararı telafi etmede kimin etkin rol alacağı gibi yeni konular da gündeme gelmiştir.

2.2. Rekabetin Geleneksel Boyutları

ABD ve Çin rekabetinin geleneksel boyutlarını siyasi, ekonomik, askerî ve kültürel olarak dört ayrı başlıkta inceleyebiliriz.

2.2.1. Siyasi Boyut

Çin'in ekonomik anlamda yükselmesi ile birlikte dünya siyasetinde daha fazla söz sahibi olması da kaçınılmazdır. ABD Silahlı Kuvvetlerine hizmet eden bir düşünce kuruluşu olan Research And Development tarafından hazırlanan raporda Çin'in dış siyasette izlediği ilkeler; büyük bir savaşın çıkmaması için gayret etmek, ekonomik büyümeyi sürdürmek, ABD'nin zayıflaması ile paralel olarak Çin'in bir lider adayı konumunda bulunacağı yeni bir düzenin inşası, Afrika ve Ortadoğu'daki enerji kaynaklarının temini ve enerji güvenliğinin tesisi, doğal felaketler, terör, salgın hastalıklar, güvenlik tehditleri gibi riskler için iş birlikleri yapılması ve kamuoyundaki *Çin tehdidi* kavramının *Çin yükselişine* dönüşmesi çerçevesindedir (Medeiros, 2009).

2010'lu yıllarda Çin, uluslararası siyasette daha ağırlıklı biçimde yer almayı tercih etmiştir (Karadeli, 2021, s.18). Ancak Çin'in henüz süper güç olmak için yeterli siyasi birikime sahip olmadan bu hedefi önüne koyması onun için önemli bir dezavantaj olmuştur. Ayrıca her ne kadar gelişim kat etse de Çin'deki üniversitelerin sosyal bilimler alanları ABD ile mücadele edecek seviyede değildir. Çin'in kalabalık ve niteliksiz nüfusu da ABD karşısında bir dezavantaj gibi görülebilecektir. Ayrıca ABD'nin Arap Ayaklanmaları konusunda ülke hakkında algıyı kırmak ve bozulan imajı düzeltmek adına çok daha farklı bir dış politika izlediği de bilinmektedir. Dış politika konusunda Çin'i artı konuma yükselten unsur; ülkeler arasında egemenlik, toprak bütünlüğü ve eşitlik ilkelerini

savunmasıdır. Bu sebeple, demokratik sistemleri tam oturmamış ve sınır sorunu olan ülkeler Çin ile daha yakın ilişkiye girme potansiyeline sahiptir. Fakat demokratik bilincin gelişmesi, sivil toplum faaliyetleri ve iletişim ağının güçlenmesi ile Çin'in bu duruma daha hızlı ayak uydurması gerekmektedir. ABD'nin dış politikadaki avantajı ise Soğuk Savaş dönemindekinden farklı olarak, halk hareketlerine ve demokrasiye sahip çıkması ve daha kabul gören bir rejim modeline sahip olmasıdır.

Barack Obama'nın ABD'de Başkan olarak göreve başlamasının ardından Çin için *önemli bir ortak ve rakip* tanımlarını kullanması iki ülke ilişkilerinin ticari ve ekonomik boyutunun dışında siyasi boyutunu da gündeme getirmiştir. Obama'nın Çin ile ilişkilerinde izlediği yol, Çin'in yükselişine karşı ülkesinin çıkarlarını koruyarak etki alanını genişletmek amacıyla Asya Eksenli Stratejisini hayata geçirmek olmuştur. Bu dönemde ABD-Çin ilişkilerinin başlıca konularını; bölge ülkeleriyle olan ilişkiler, anlaşmazlıklar ve sorunlar da oluşturmuştur. İran'a karşı uygulanmak istenen yaptırımları Çin'in BM'de veto etmesi sonucu iki ülke arasında önemli sorunlar doğmuştur. Doğu Türkistan ve Tibet sorunlarına Çin'in karışmamasını istemesine rağmen ABD'nin bu konuları uluslararası arenaya taşımak istemesi gerginliklere sebep olmuştur. ABD Savunma Bakanlığı tarafından Çin'in 30 yıl içerisinde üst düzey bir güç olmak için modern bir düzenli ordu kurma çabaları (Maizland, 2020) ve konuya ilişkin açıklamaları da ilişkilerin gerilemesinin bir başka nedenidir. Öte yandan 23 Kasım 2013 tarihinde Çin yeni bir hava savunma sahası ilan etmiştir. Bu ilanı reddeden ABD ise hava sahası içerisinde bombardıman uçaklarını uçurmuş ve bu durum da iki ülke arasında ciddi sorunlara sebep olmuştur ("ABD ve Çin arasında siber gerilim", BBC News Türkçe, 2013). Çin için deniz ve hava ulaşım yollarının güvenliği, ticaretini sürdürebilmesi, ihracat yapabilmesi, ham madde ve enerji ihtiyacını sağlayabilmesi, sosyal dengeyi koruyabilmesi, ekonomisini büyütebilmesi için oldukça önemlidir. Bu anlamda Güney Çin Denizi'ndeki Çin varlığı ve yapay adalar konusu da iki ülke arasındaki gerginliğin bir diğer boyutu olmuştur.

Farklı gerginlikler ve sorunlar yaşansa da Çin ve ABD yönetimi arasında diplomatik bir kopukluk olmamıştır ancak 2016 yılının Kasım ayında Donald Trump'ın ABD Başkanı olması sonucu iki ülke arasında ilişkileri bozacak bazı gelişmeler yaşanmıştır. Trump'ın Tayvan lideri ile yaptığı telefon görüşmesi Çin

tarafından şiddetle kınanmış ve bunun sonucunda iki ülke arasında ciddi bir gerginlik meydana gelmiştir. Trump; Çin'i bir numaralı düşman olarak görmüş, Çin üretiminde olan ürünlere büyük vergiler uygulayacağını söylemiş ve ticaret savaşını alevlendirmişse de sonradan söylemlerinin aksine bazı adımlar atmıştır.

Tayvan meselesi, iki ülkenin siyasi ilişkilerinde git gide yükselen tansiyonu artıran unsurlardan biri haline gelmiştir. Tayvan'ı kendi topraklarının bir parçası olarak gören ve Tayvan'daki emellerine ulaşmak için bu alanda askerî kapasitesini devamlı artıran Çin'e karşı ABD, Tayvan'ın yanında yer almaktadır. Biden ise Tayvan meselesi hakkında gerilimi artıracak bir açıklama yapmış, egemenliğini kabul etmesi için Çin'in Tayvan'a siyasi ve askerî baskılarını artırdığını ve olası bir müdahale durumunda ABD'nin tutumunun nasıl olacağı sorusu üzerine ise ABD'nin Tayvan'a destek vereceğini ifade etmiştir ("Biden, Tayvan'ı Çin'e karşı koruyacaklarını açıkladı", Deutsche Welle, 2021). 2021 yılının Mart ayında ABD'nin Alaska eyaletinde Biden yönetimi ve Çin arasında yapılan ilk üst düzey görüşmelerde de taraflar gerilmiş ve Tayvan meselesinin de konuşulduğu görüşmede karşılıklı sert suçlamalar yöneltilmiştir.

ABD yeni Başkanı Joe Biden, göreve gelmeden önce uluslararası siyaset çerçevesinde liberal uluslararası düzeni canlandırmayı vadetmiştir. ABD'yi Paris İklim Anlaşmasına geri taşıyarak, Dünya Sağlık Örgütü ve Birleşmiş Milletler İnsan Hakları Konseyi üyeliğini yeniden hayata geçirerek, Avrupa ve Asya tarafındaki müttefiklerle daha sıkı ilişkiler kurarak bu alanda önemli hamleler de yapmıştır. Fakat kurumsal düzenin canlandırılması aynı zamanda ABD'nin en büyük rakibi olan Çin'in de bu düzene entegre edilmesini kapsamaktadır. Bu iki ülke arasındaki rekabeti sona erdirecek bir hamle değildir ancak ABD'nin Çin'i uluslararası liberal düzenin bir kâr ortağı haline getirmesi Çin'in aynı zamanda bu düzenin kurallarına uyması ve ABD liderliğini kabul etmesi anlamına da gelmektedir. Dolayısıyla ABD'nin hedefi Çin ile sürdürdüğü mücadelede kendine avantaj oluşturacak alanlar inşa etmektir. Bu şekilde ABD, Çin'in yükselişini herhangi bir çatışmaya yol açmadan durdurabileceğini ya da bu yükseliş karşısında manevra kabiliyeti kazanacak bir zaman elde etmeyi düşünmektedir. Dolayısıyla ABD'nin hedefleri doğrultusunda uluslararası siyasette liderliğini belirli bir süre daha sürdüreceği beklenmektedir.

Biden; seçim döneminde Trump'ın özellikle Çin'e karşı uyguladığı stratejileri eleştirmiş, Trump yönetiminin Çin'e ve İran'a yönelik gerginleştirdiği ilişkileri iyileştirecek ve gerilimleri düşürecek yollar bulacağını vadedmiştir. Son dönemde ABD ve Çin arasındaki tırmanan gerilimler dikkate alındığında ise Biden'ın, söylemlerinin tam aksine bir yol izleyeceğini de söylemek mümkündür. ABD tarafından yapılan açıklamalara ve hayata geçirilen hamlelere bakıldığında Biden yönetiminin Çin ile çatışmacı tutumunun süreceği de söylenebilecektir (Aslan, 2021).

Ekonomisi günden güne güçlenen, askerî ve teknolojik yatırımlarını hızlandıran Çin ise son dönemde ABD liderliğinde şekil almış dünya ekonomisini sorgulamaya ve kendi projesini inşa etmeye başlamıştır. Benzer şekilde, Çin'in dünya liderliğine yükselme kararının da ABD ile olan ilişkilerini tırmandırmaya devam ettiği söylenebilecektir. Netice itibarıyla, Biden yönetimi dış politikasına ve Çin yönetiminin talep ve hedeflerine bakıldığında; barış, iş birliği ve rekabet temalı bir gelecek veya dünya ekonomisinin bloklara bölüneceği ve bazı çatışmalara da sahne olacağı bir geleceğin mümkün olduğunu söylemek yanlış olmayacaktır ("ABD ve Çin: Rekabetleriyle geleceği şekillendirecek iki süper güç", BBC News, 2021).

Çin her geçen gün farklı alanlarda gerçekleştirdiği atılımlarla ABD ile olan mücadelesinde güç kazanmakta ve bu mücadeleyi hızlandırmaktadır. Tüm bu gelişmeler de dünyanın en büyük iki ekonomisi olan ABD ve Çin arasındaki gerilimlerin tırmanmasına doğrudan veya dolaylı olarak sebebiyet vermektedir. 2 yıldan fazla bir süredir yaşanan koronavirüs pandemisi meselesi son dönemde iki ülke arasındaki yeni bir mücadele alanı olarak başlamış ve devam etmektedir. Koronavirüs sürecinde Çin'in söylemlerinin sertleşmesi, ABD'ye karşı sert eleştirilerde bulunması, farklı alanlarda gücünü sağlamlaştırmaya çalışması Çin'in büyük güç olma yolunda yeni bir yol kat ettiği şeklinde değerlendirilebilir.

2.2.2. Ekonomik Boyut

Gelişen Çin ekonomisi, ABD'nin Çin'e olan bağımlılığını artırmıştır. Hızla küreselleşen dünyada; ABD'nin bağımlılığının artması, ABD-Çin arasında ticarete dayalı yaşanan gerilimin de ivme kazanmasına yol açmıştır. Küresel bir ticaret devi olarak konumlanmaya başlayan Çin, gün geçtikçe kazandığı bu konumu

sağlamlaştırmak üzere gayret göstermektedir. Bu bağlamda, ABD'nin Çin ile gerçekleştirdiği ticaret verilerine bakıldığında ABD'nin dış ticaret açığı 1991 yılında 12.691 milyar dolar iken bu rakam 2021 yılına gelindiğinde 355.301 milyar dolara yükselmiştir (CENSUS, 2021). Öte yandan Çin hem kalabalık nüfusu hem teknoloji yatırımları hem de üretim tesisleri ile ABD için önemli bir pazar konumuna gelmiştir. Aynı zamanda önemli oranda Çinli vatandaş, Batı markalarına karşı ilgi duymakta ve Çin pazarı artık güçlü markalar için bir fırsat oluşturmaktadır. Ancak yine de Çin'in düşük maliyetli ürünleri, bireyleri ve devletleri cezbetmekte ve bu durum ABD'nin rahatsızlığını artırmaktadır.

2021 yılı hesaplamalarına göre 1.4126 milyarlık nüfusu ile dünya nüfusunun yaklaşık %18'sini oluşturan Çin, dünyanın en kalabalık ülkesi konumunda yer almaktadır. Aynı zamanda ABD'den sonra dünyanın en büyük ikinci ekonomisi olan Çin, 2021 yılı itibarıyla 16,9 trilyon dolar ile küresel gayri safi yurt içi (GSYH) hasılanın %17,9'undan sorumludur (Neufeld, 2021). Çin; 1900'lü yıllarda kurduğu özel ekonomik bölgelerde, sahip olduğu nüfus üstünlüğünü iş gücü olarak değerlendirmiş ve düşük maliyetli üretimler yaparak üretilen bu ürünlerin ihracatıyla verimliliğini kısa sürede artırmıştır. Ucuz mallar ile Batı pazarında yer alabilen Çin, ekonomisini yaptığı ihracatla geliştirmiştir. Bunun yanı sıra, ithal ürünlerin pahalılığı Çin'de sahte ürün üretiminin ve akabinde ihracatının yapıldığı bir alan oluşturmuş ve zaman içinde bu alan gelişmiştir. 2019 yılı itibarıyla dünyadaki sahte ürünlerin %85'inin Çin'den geldiği öngörülmektedir (Tiley ve Bower, 2020).

1998 yılında DTÖ'ye girmesi için Çin'i destekleyen ABD, 2001 yılında DTÖ'ye katılan Çin'in ekonomik büyümesinden ve dünya ihracatındaki yerinden rahatsız olmakla birlikte sahte ürün meselesini Çin ekonomisi üzerinde bir baskı unsuru olarak kullanmaya çalışmıştır. ABD, meseleye ilişkin olarak 2013 yılında Çin'e karşı telif hakları davası açarak Çin'i DTÖ'ye korsan ürün çoğaltması iddiasıyla şikâyet etmiştir. ABD'nin ticaret açığı Çin'e siyasi baskı yapmasını beraberinde getirmiştir. Yine aynı dönemde, ABD'nin ticaret açığı 240 milyar dolara ulaşmış, bunun sebebi olarak da Çin para birimi olan Yuan'ın değerinin çok düşük olması öne sürülmüştür. Washington yönetimi, önlem olarak Çin'den ithal edilen ürünlere uygulanan gümrük tarifelerini yükselteceğini söylemiştir ve bu hamle, *kur savaşları* da denilen bir mücadeleyi ortaya koymuştur. Yaşanan

gelişmeler karşısında Çin ise Yuan'ın değerini zorla yükseltmek amacıyla ABD'de bir yasa kabul edilmesine karşı çıktıklarını belirtmiş ve aksi durumda Çin ve ABD arasında ticaret savaşlarının başlayacağını ifade etmiştir.

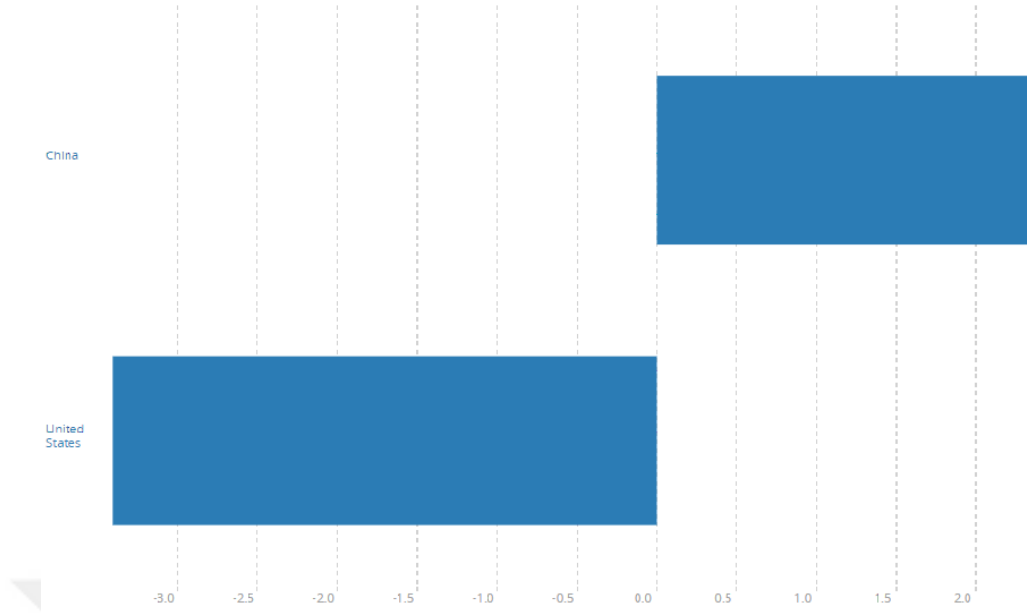
Çin, 2013 yılında en iddialı politikalarından olan ve kara yolları ile okyanusların dâhil edildiği “Modern İpek Yolu – Bir Kuşak Bir Yol Girişimi”ni öne sürmüştür. Çin Devlet Başkanı Xi Jinping'in 2013'ün sonlarına doğru Orta Asya ve Güney Asya ülkelerine gerçekleştirdiği bir dizi ziyaret söz konusu projeyi duyurmuştur. Bu proje ile birlikte Çin, yoksulluğu azaltacağı ve istihdamı artıracığı iddiaları ile proje kapsamındaki ülkelere olan yatırımlarını desteklemiştir. Çin, dünya genelinde onlarca ülkenin altyapı projelerine söz konusu girişim dolayısıyla 1 trilyon dolardan fazla yatırım yapmış ve başta ABD olmak üzere rakiplerinin dikkatlerini üzerine çekmeyi başarmıştır (Tiley ve Bower, 2020). 2015 yılında ise Çin, “Made In China 2025 (MIC2025)” hedefleri ile *ucuz iş gücü merkezi* olmaktan ziyade *teknoloji ve inovasyon merkezi* olarak küresel düzeyde güçlü ve büyük bir üretici olmayı hedeflediğini ortaya koymuştur (Aytekin, 2021, s.155-156). Bu bağlamda, Pekin hükûmeti söz konusu plan doğrultusunda yapay zekâ, havacılık, uzay, bilişim gibi stratejik pek çok alanda elde ettiği başarıyla tüm dikkatleri üzerine çekebilmiştir. Dünyanın ihracat devi haline gelen Çin, 2019 yılının sonlarından beri dünyayı etkisi altına alan koronavirüs pandemisinin tüm olumsuz şartlarına rağmen 2021 yılında 6 trilyon dolarlık ihracat gerçekleştirmiştir (“Çin'in ihracatı 2021 yılında yüzde 30 arttı”, 2022). Öte yandan 2021 yılında Çin'in ihracatının önemli bir kısmı telefon, bilgisayar gibi yüksek teknolojlili ürünlerden oluşmaktadır (OEC, 2021).

2016 yılının sonlarında ABD'de başkan seçimleri sebebiyle ekonomide bir belirsizlik söz konusu olmuşsa da seçimlerin ardından küresel ekonomideki belirsizlik ve ABD'nin ekonomi politikalarındaki belirsizlikler de azalmaya başlamıştır. Ancak zaman içinde ABD-Çin arasındaki dış ticaret açığının ABD aleyhine ivme kazanması, seçimde Donald Trump'ın altını çizdiği bir mesele olmakla birlikte Trump'ın seçim vaatleri arasında yer almış ve Trump hükûmeti tarafından söz konusu ticaret açığının kapatılması noktasında çeşitli programlar uygulanmaya başlamıştır. Bu kapsamda, 2017 yılının sonlarına doğru ABD Başkanı Trump'ın ithalat yaptığı ülkelere aldıkları ürünleri azaltmaya yönelik açıklamaları hem küresel politikada hem de ABD ticaret politikalarında

belirsizliklerin tekrar tırmanmasına sebebiyet vermiştir. Öte yandan 2017 yılında Çin'in ABD için bir tehdit olduğunun ortaya koyulmasını müteakip 2018 yılından itibaren Çin'den gelen ürünlere ek gümrük vergileri getirilmeye başlanmış, ekonomik belirsizlikler de artmaya devam etmiştir. ABD ve Çin arasındaki *ticaret savaşları*, ABD Başkanı Trump'ın Mart 2018'de Çin'den ithal edilen bazı ürünlere yaptığı ilave tarifeler neticesinde ivme kazanmıştır. Söz konusu savaşlarda; soya fasulyesinden otomotiv parçalarına, teknoloji şirketlerinden Çin'in teknolojiye yerleşme programı olan "Made in China 2025" ve kritik teknolojilerin üretilmesi sürecine dâhil edilen nadir elementlere kadar pek çok ürün iki ülke arasında koz olarak kullanılmıştır (Çopur, 2020).

2019 yılında Huawei konusunun gündeme gelmesiyle birlikte küresel ekonomideki belirsizlik ve ABD ticaret politikaları belirsizliği en yüksek seviyelere ulaşmıştır. Trump yönetimi tarafından 15 Mayıs 2019'da ulusal tehlike hali ilan edilerek alınan kararlar doğrultusunda ABD firmalarının Çin'in önde gelen telekomünikasyon şirketlerinden Huawei'nin teknolojisini kullanılması ve Amerikan mallarının Çin firmalarına satışı yasaklanmıştır (Pham, 2019). Böylelikle, süregelen ticari anlaşmazlıklar teknoloji savaşları ile yeni bir boyuta taşınmış ve Birleşik Krallık'ın Avrupa Birliği'nden ayrılması (Brexit) süreci, bu belirsizliği daha da tırmandırmıştır. Fakat 2019 Eylül ayında yürürlüğe girecek olan ek yaptırımlar bir müddet ertelenmiş ve devamında ise kaldırılmış; böylelikle küresel ekonomi politikalarındaki belirsizlik biraz da olsa azalmıştır. ABD ve Çin arasında 2020'nin ocak ayında birinci faz anlaşması yapılmış ve iki ülke arasındaki ticari savaşların bitmesi amaçlanmıştır.

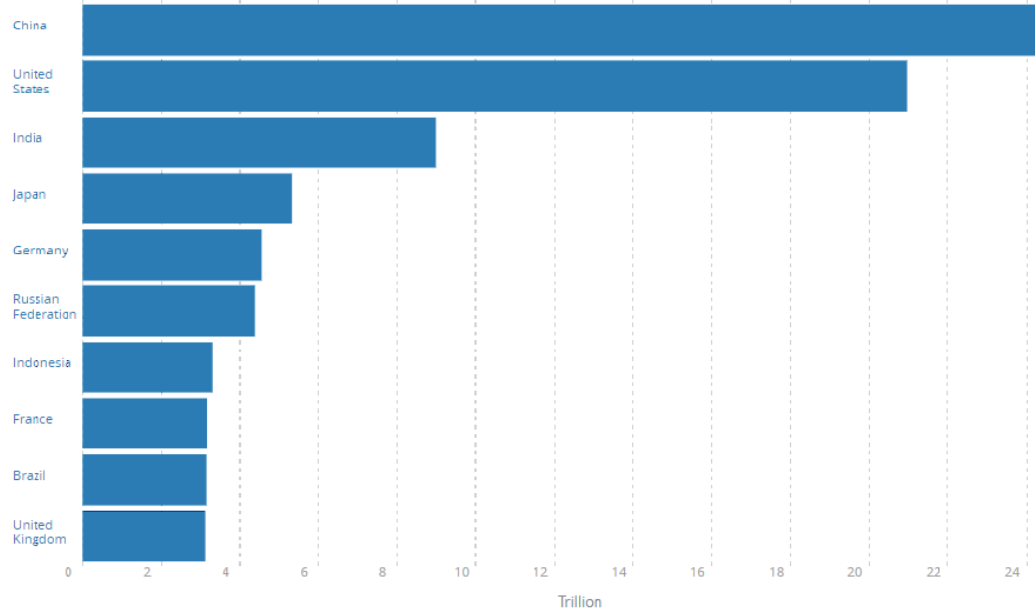
Özellikle geçtiğimiz 15 yıl, Çin'in uluslararası alanda hem gücünü hem de ekonomik ağırlığını artıran bir dönem olmuştur. Satın alma gücü paritesine göre Çin, dünyanın en büyük ekonomisi konumuna gelmiştir (Grafik 2).



Grafik 2: Dünya Bankası Verilerine Göre 2020 Yılı Satın Alma Pariteli GSYH'YE Göre En Yüksek Değere Sahip Ülkeler

Kaynak: <https://data.worldbank.org/indicator/ny.gdp.mktp.pp.cd?locations=CN-US-IN-JP-RU-DE-ID-BR-GB-FR>

Piyasa fiyatlarına göre bir değerlendirme yapıldığında ise on yıl içinde ABD'yi geçme olasılığı gözler önündedir. ABD ekonomisi, 2020 yılında yaklaşık %3,5 oranında küçülme yaşarken, Çin ekonomisi ise yaklaşık %2,4 oranında bir büyüme kat etmiştir (Grafik 3). İki ülke arasındaki ekonomik rekabeti bu rakamlar da kısaca özetlemekte ve farkı ortaya koymaktadır.



Grafik 3: Dünya Bankası Verilerine Göre ABD ve Çin'in 2020 Yılı Ekonomi Büyüme Oranları

Kaynak: <https://data.worldbank.org/indicator/NY.GDP.MKTP.KD.ZG?end=2020&locations=CN-US&start=2020&view=bar>

Dünya ekonomisinde Çin'in ABD'ye oranla ağırlığının daha da arttığını örnekleyen bir başka gelişme ise Çin'in dünya ticareti içindeki payıdır. 2000'li yıllardan bu zamana kadar dünya ticareti içindeki payını düzenli bir şekilde artıran Çin birinci sırayı almıştır. Böylelikle Çin piyasaları diğer ülkeler açısından da önemli hale gelmiş, Çin piyasalarına rağbet artmıştır. 2004-2019 yılları arasında ABD'nin ithalatı %71 oranında artmış, 1,5 trilyon dolardan 2 trilyon 650 milyar dolara yükselmiştir. Yine aynı dönemde Çin'in ithalatı ise %257 oranında artmış, 561 milyar dolardan 2 trilyon dolara yükselmiştir (ABD ve Çin: Rekabetleriyle geleceği şekillendirecek iki süper güç, 2021).

Kredi verme anlamında da Çin'in önemi son 20 yılda büyük oranda artış göstermiştir. Harvard Business Review'daki bir araştırmaya göre Çin 150'den fazla ülkeye kredi veren bir ülke konumundadır ve 1,8 trilyon dolarlık bu kredilerle birlikte dünya hasılasının %5'ine sahip olmuştur (Horn vd., 2020).

Koronavirüs dönemi tüm dünya ekonomisinde olduğu gibi Çin ve ABD ekonomisinde de yeni bir dönemin başlangıcı olarak kabul edilmektedir. Salgın sebebiyle iki ülkenin ekonomisi de zorluklarla mücadele etmektedir. ABD tarihindeki en yüksek işsizlik oranları, Çin'de ise 30 yıldan sonra ilk defa 2020 yılının ilk çeyreğinde en düşük büyüme oranı ortaya çıkmıştır. Çin kaynaklı çıkan Koronavirüs sonrası dönemde tedarik zincirinin Çin'den başka ülkelere geçmesi

tartışmaları da bu ülkelerin ekonomik dengelerinde önemli bir yer tutmaktadır. Fakat ABD-Çin ekonomilerindeki bağımlılık iki ülke ilişkilerinde sıcak çatışma risklerinden kaçınılmasını da sağlamaktadır.

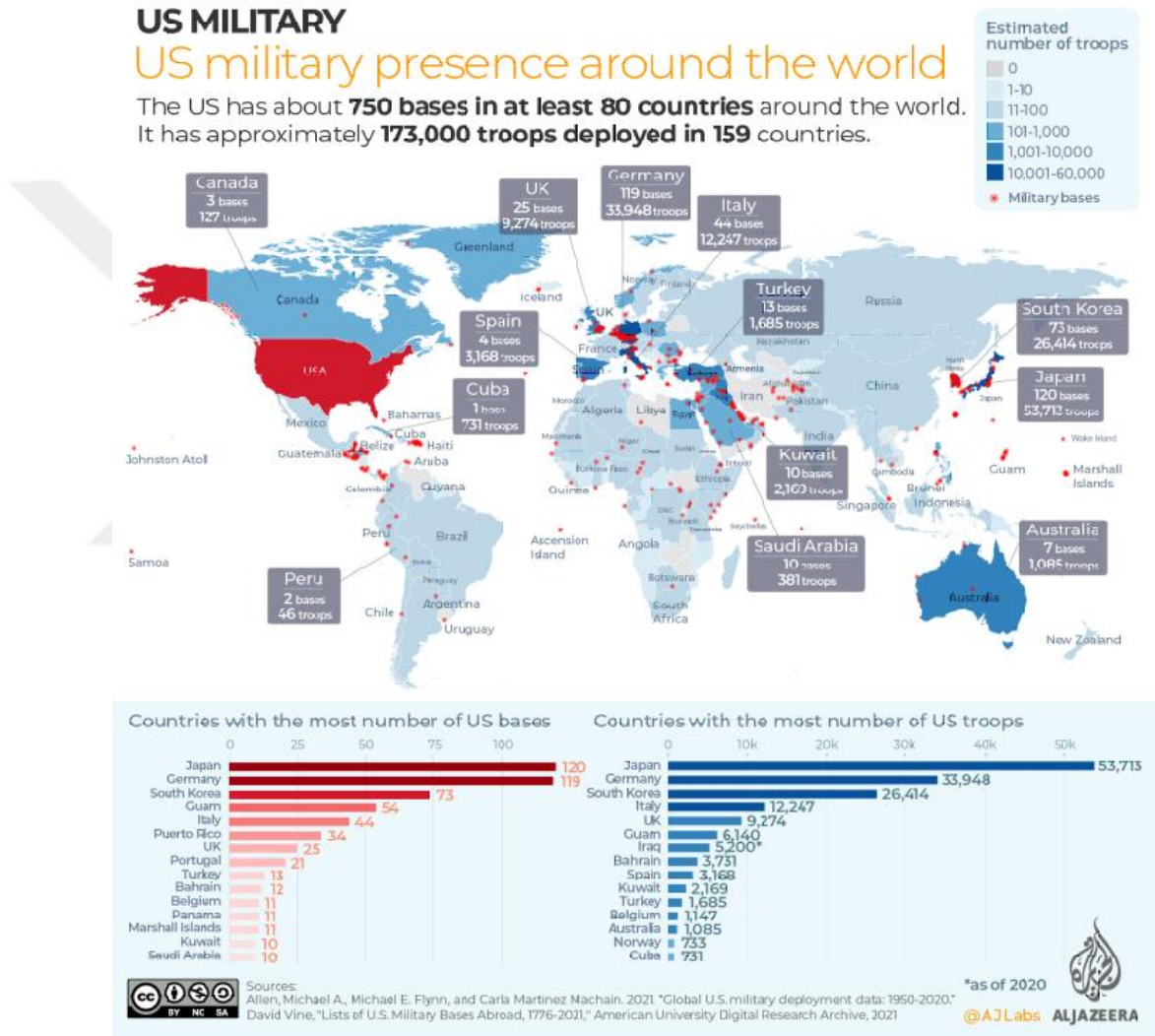
Diğer bir taraftan, koronavirüs krizi dünya ekonomisinde büyük bir durgunluğu meydana getirmişken Çin bu salgını hızlı bir şekilde kontrol altına alarak koronavirüs aşısını (Sinovac-CoronaVac vaccine) üretmiş ve sağlık ekipmanları piyasasında hâkim konuma gelmiştir. Aynı zamanda, salgın döneminde ekonomisi çok zor duruma düşen 77 ülkenin borçlarını da ertelemiştir. Fortune Global 500 şirket listesi içerisinde 2021 yılında 143 Çin menşeli şirket yer almıştır (Çin'den 143 şirket Fortune Global 500 listesine girdi, 2020). ABD ve Çin arasında hızla değişen ekonomik gelişmeler Çin lehine değişmeye devam etmektedir.

2021 yılında ABD-Çin İş Konseyi (USCBC), Oxford Economics ile birlikte "ABD-Çin Ekonomik İlişkileri: Kritik Dönemeçte Önemli Bir Ortaklık" isimli bir rapor yayımlanmıştır. Bu raporda, ABD'nin Çin ile olan ticaretinden fayda gördüğü ve 2019'da Çin'e yapılan ihracatın ABD'deki 1,2 milyon kişinin işine katkı sunduğu belirtilmiştir. Raporda, iki ülke arasındaki ticaret savaşının zararlarından bahsedilmiş ve Trump yönetimi zamanında başlayan ticaret savaşlarının ekonomiye fayda vermediği tam aksine ABD ekonomisini zayıflattığı ve tahminen 245 bin kişinin işini kaybetmesine yol açtığı ifade edilmiştir (Zengin, 2021). Raporda aynı zamanda bazı öngörülerde de bulunulmuş ve ticaret savaşının devam etmesi durumunda ABD'nin gayrisafi yurt içi hasılasının önümüzdeki beş yıllık periyotta 1,6 trilyon dolar azalabileceği, 2022'de 732.000 ve 2025'te de 320.000 kişinin işini kaybedebileceği söylenmiştir (The US-China Business Council vd., 2021, s.4).

Özetle, Çin pazarı gerek bölge ülkeleri gerekse genel itibarıyla zaman içinde dünya ekonomisi açısından önemli hale gelmiş ve hızlı artışla ABD'yi yakalamıştır. Öyle ki, artık Çin ekonomisinin ABD ekonomisini geçip geçemeyeceği değil ne zaman geçeceği tartışılmaya başlanmıştır.

2.2.3. Askerî Boyut

ABD, dünya üzerinde diğer ülkelere oranla çok büyük bir savunma harcamasına ve yüzlerce üsse sahiptir (Şekil 1). Bu durum, tüm dünyaya yayılmış olan askerî gücü çok aşırı olan ABD'nin ekonomik gücünün azalmasına sebebiyet vermiştir. Büyük bir cari açığa sebep olan bu harcama kolu sonucunda ekonomik sorunların doğmasıyla birlikte askerî gücün azalması da bir sonuç olarak gündeme gelmiştir.



Şekil 1: 2020 Yılı İtibarıyla ABD'nin Dünya Çapında Askerî Varlığı

Kaynak: <https://www.aljazeera.com/news/2021/9/10/infographic-us-military-presence-around-the-world-interactive>

ABD'nin 2017 yılında yayınladığı Ulusal Savunma Stratejisi'nde bundan sonra büyük güçler rekabeti döneminin başladığı açıkça ilan edilmiştir. Trump yönetimi tarafından Çin, açıkça siyasi ve ekonomik bir düşman olarak kabul edilmekle birlikte Çin'in, ekonomik araçlarla ve askerî tehditlerle, diğer devletleri ikna ettiği ve onlara siyasi ve güvenlik gündemini kabul ettirdiği öne sürülmüştür.

ABD'nin yeni Başkanı Joe Biden ise başkan seçilmeden önce yaptığı açıklamalarda ve 2020 yılında Foreign Affairs dergisinde yayımlanan yazısında, Çin için "ABD'nin en önemli rakibi" tanımlamasını yapmıştır. Biden yönetiminde ABD Savunma Bakanı olan Lloyd Austin de "Çin en büyük tehdittir çünkü yükselen bir güçtür" ifadesini kullanmıştır.

Çin'in günden güne askerî harcamalarını artırdığı, bu alanda büyük yatırımlar yaptığı, güçlendiği ve deniz gücünde büyük bir gelişme kat ettiği bilinmektedir. Bununla birlikte son dönemde Güney ve Doğu Çin Denizi'nde askerî hareketliliğinin arttığı da gözlemlenmektedir. ABD'nin de hem deniz hem de hava alanında varlığını devam ettirdiği bu bölge, iki ülkenin askerî açıdan birbirlerine en çok yakın olduğu ve sıcak çatışma ihtimalinin de en yüksek olduğu bölge olarak görülmektedir. Çin son dönemde askerî harcamalarına büyük ölçüde ağırlık vermişse de yine de hala ABD'nin gerisindedir. 2019 verilerine göre Çin 252 milyar dolar askerî harcamaya sahipken bu miktar ABD için 778 milyar dolar seviyelerindedir (SIPRI, 2021).

Son dönemler ele alınacak olursa, tarihin farklı dönemlerinde inişli çıkışlı bir seyir izleyen Çin-ABD ilişkilerinin Soğuk Savaş döneminden sonra en gergin zamanlarının yaşandığı söylenebilecektir. ("Çin-ABD ilişkilerinde Soğuk Savaş'tan beri en gergin dönem", TRT Haber, 2021). Çin hem son zamanlarda balistik füze denemeleri yapmaya hem de savunma eğitimi için Amerikan uçak gemisinin taklit bir modelini inşa etmeye başlamıştır. Gitgide büyüyen ve güçlenen Çin ile dünyada süper güç olarak gösterilen ABD arasındaki gerginlikler Joe Biden'ın başkan seçilmesinin ardından tırmanışa geçmiştir. İki ülke arasındaki ilişkilerinin yeniden gerilmesinin temel sebeplerinin başında ise Çin'in Tayvan'a yönelik savaş tehdidi ve ABD'nin Tayvan safında yer alması gelmektedir. ABD Sağlık Bakanı'nın Tayvan'a ziyaret gerçekleştirmesi, 40 yıl sonra yapılan ilk resmî temas olarak hem büyük bir önem arz etmekte hem de Tayvan'a olan desteği gözler önüne sermektedir. ABD Başkanı Joe Biden da Çin'in Tayvan'a saldırması durumunda Tayvan'ı koruyacaklarını ifade etmiştir ("Biden, Tayvan'ı Çin'e karşı koruyacaklarını açıkladı", Dünya, 2021). Çin ise Biden'ın bu mesajına karşı yanıtsız kalmamış ve savaş uçaklarını Tayvan hava sahasına göndermiştir.

Ardından Tayvan, adada ABD askerlerinin varlığından ve orduların eğitildiğinden bahsetmiştir. Tayvan Savunma Bakanlığı bir rapor hazırlayarak Pekin yönetimi ile olan gerilimden bahsetmiş ve Çin'in *gri alan* olarak ifade edilen bir savaş başlattığını öne sürmüştür. Raporda Çin'in Eylül 2020'den Ağustos 2021'in sonuna kadar toplamda 554 defa hava sahası ihlali yaptığının ve Çin'in Tayvan'ın stratejik havalimanları ve limanlarını bloke edebilecek güce sahip olduğundan da bahsedilmiştir (Kurunç, 2021). Bu sayı, 2021 yılında toplam 950 olarak kaydedilmiştir (Wang, 2021). Tayvan tarafından hazırlanan bu rapor gerilimi tırmandırmış ve Çin hipersonik füze testleri ile yanıt vermiştir. Çin ordusunun hipersonik testleri yapacağı ABD tarafından da doğrulanmıştır.

Henüz böyle bir test gerçekleştirmeyen ABD için bu gelişme büyük endişelere sebebiyet vermiştir. Tarihin gördüğü en büyük jeostratejik güç değişimine şahit olduklarını ifade eden ABD Genelkurmay Başkanı, Çin'in Tayvan'a saldırabileceklerini düşünmediklerini fakat saldırı durumunda Tayvan'ı koruyacak güce sahip olduklarını da belirtmiştir (Clark, 2021). Son olarak Çin'in ABD'ye ait uçak gemilerine benzer hedeflerle silahlarını test ettiği ortaya çıkmıştır.

ABD uçak gemisinin taklit modelleri uydudan görüntülenmiş, bu modellerin Sincan Uygur bölgesindeki Taklamakan Çölü'nde inşa edildiği ortaya çıkmıştır. Bu görüntüleri yayınlayan ABD Donanma Enstitüsü tarafından bölgenin balistik füze eğitimi için kullanıldığı iddia edilmiştir (Sutton ve LaGrone, 2021). Çin'in, kendisine ait teknolojik bilgileri çaldığını sıklıkla yineleyen ABD, 2022 yılının Ocak ayında Güney Çin Denizi'ne düşen F-35C hayalet avcı uçağına ilişkin çalışmalarda bulunmuştur. Uçağın Çin tarafından ele geçirilmemesi için geniş güvenlik önlemleri alan ABD hükûmeti, Güney Çin Denizi'nin tamamı üzerinde hak iddia eden Çin hükûmetinden önce 110 milyon dolara mal olan yüksek teknoloji donanımlı uçak enkazına ivedi şekilde ulaşmak için çalışma başlamıştır.

Son dönemde giderek popülaritesi artan ve dünyada daha fazla söz sahibi olmaya başlayan Çin, ordusunda modernleşme hamlelerine hız vermiş ve nükleer cephanesini de güçlendirmiştir. Ayrıca yeni nesil savaş teknolojileri ile de bu alanda yeni atılımlar gerçekleştirmiştir. Bu durum da ABD ile yaşanan gerilimde kritik gelişmeler olarak ortaya çıkmıştır.

2.2.4. Kltrel Boyut

Geleneksel rekabetin bir diğr ayađı da kltrel rekabettir. lkeler zerinde son derece etkili bir yumuřak gç olan kltr, ABD ve Çin gibi sper gç olma gayreti iinde olan devletler kritik nem tařıtmaktadır. Çin tarihi itibarıyla ABD'ye nazaran ok gçl ve kkl bir kltre sahiptir. Kendine has bir kltr olmasına ve merak uyandırmasına rağmen Çin bu konuda ABD'nin dnyadaki kltrel etkisi karřısında zayıf kalmaktadır. Son zamanlarda Asya'ya ynelik ilgi artmıř olsa da bu durum daha ok Gney Kore'nin dizileri ve "K-Pop (Korean Pop)" adı verilen pop mzik tarzı ile Japonya'nın anime film, dizi ve oyunlarına yneliktir. ABD ise Hollywood sineması, dnya apında dinlenen mzik listeleri, řarkıcıları, oyuncularını, yemek kltr, giyim tarzı ve markaları ile Çin'e karřı bu rekabet alanında ciddi bir stnlk saėlamaktadır.

3. BÖLÜM

GENİŞLEYEN REKABET ALANI: SİBER ALANDA MÜCADELE

3.1. Yeni Rekabet Sahası: Teknolojik Gelişmeler ve Siber Alan

ABD-Çin arasındaki rekabetin geleneksel dinamiklerini incelediğimizde artık son dönemde ülkelerin politikalarına, hamlelerine, uluslararası ilişkilerine yaptığı etki kaçınılmaz olan teknoloji de ön plana çıkmaktadır. Ülkeler; teknoloji yatırımlarıyla diğer ülkeler için ciddi bir tehdit olabilmekte, teknolojik hamleler ile rakip ülkelerin savunma mekanizmalarına zarar verilebilmektedir. Dolayısıyla dünya siyasetinde söz sahibi olmak isteyen ülkeler için teknoloji, özellikle 21. yüzyıldan itibaren geniş kapsamlı bir rekabet alanı olarak ortaya çıkmaktadır. Dünya kamuoyunu yönlendirme ve psikolojik üstünlük sağlamaya da yol açan ve güçlü ülkeler arasındaki rekabetin artık en önemli ayaklarından birisi olan teknolojik rekabete, Soğuk Savaş dönemindeki ABD ve SSCB arasında gerçekleşen uzay rekabetini örnek olarak göstermek mümkündür.

ABD yönetimini kaygılandıran ve dünya ekonomisinde büyük etki yaratan Çin'in ekonomik gelişimi; bilgisayar, uzay çalışmaları, yapay zekâ gibi teknolojik gelişmelerle daha da güçlenmiştir. ABD ve Çin arasında karmaşık bir ekonomik ve finansal ilişkinin yanı sıra karşılıklı teknolojik bağımlılık ilişkisi de bulunmaktadır. İki ülke arasındaki rekabetin en yoğunlaştığı alanlardan birisi stratejik teknolojiler olmuştur (Whalen ve Alcantara, 2021).

ABD'nin ekolojik üstünlüğünü koruma gücü öncelikli olarak teknoloji alanındaki liderliğini korumasıyla bir tutulmaktadır. 2014 yılında 3. Dengeleme Modelini açıklayan Pentagon, teknolojik gelişmelerle siber alanda ve uzayda Çin karşısında üstünlük sağlamayı ve Çin'deki teknolojik gelişmeleri yavaşlatmayı hedeflemektedir. Diğer taraftan Çin'in; yapay zekâ, kuantum bilgisayar, uzay ağlarındaki ulaşım, nükleer enerji, havacılık çalışmaları, hipersonik füze teknolojileri, güvenlik ve istihbarat sistemleri, savaş yöntemleri ile ilgili teknolojiler gibi konularda hızlı bir şekilde yaptığı atılımlar öne çıkmaktadır. Bu çalışmalar arasında otonom silahların gelişmesini kolaylaştıran ve insansız savaş araçlarının da ötesinde bir teknolojiye sahip olan yapay zekâ, teknolojik rekabetin önemli bir alanı olarak göze çarpmaktadır (Allison ve Schmidt, 2020).

Enerji bağımsızlığı olasılığını artıran teknolojiler, düşman merkezlerin sızamayacağı haberleşme olanakları, bilgi işlem alanındaki çalışmalar ve Çin'in uzay çalışmaları alanında hızlı bir şekilde attığı adımlar, teknoloji ve uzayı bu rekabetin içine almaktadır. Aynı zamanda bu teknolojik rekabet; iki ülke arasındaki kaynak rekabeti, ticaret yolları üzerindeki denetim hâkimiyeti ve coğrafyaları paylaşma rekabetini de tetiklemektedir. Tüm bu gelişmeler ışığında; ABD, Çin'deki teknolojik gelişmeleri engellemeye, ekonomik gücü ile Çin'in diğer ülkeler üzerinde etki kurmasının önüne geçmeye çalışmaktadır. Bunlara rağmen teknolojik gelişmelerini engelleyecek girişimleri etkisiz kılmaya önem veren Çin, teknolojik gelişmeleri hızlandıracak ve askerî kapasitesini artıracak şekilde bir kaynak kullanımı uygulamaktadır. Çin'in yeni teknolojilere ulaşmasını engellemeye çalışan ABD ise bazı Çin teknoloji şirketlerinin ABD'deki çalışmalarını sınırlamakta ve yasaklamaktadır; Çin de ülkesindeki yabancı şirketlere, özellikle teknoloji alanında çalışan şirketlere, benzer sınırlandırmalar getirerek bu şirketlerin ürettiği büyük veri kaynaklarını da denetim altında tutmaktadır (Yıldızoğlu, 2021).

ABD, 2012 yılında Çin menşeli önemli şirketlerden Huawei ve ZTE'nin Pekin hükûmeti ve ordusu için çalıştığından şüphelenerek söz konusu şirketlerin ABD'de birleşme ve satın alımlarını yasaklamıştır (Wolf, 2012). 2018 yılına gelindiğinde ise Washington yönetimi, casusluk endişelerini öne sürerek devlet kurumlarında ya da devlet kurumlarıyla çalışan iştiraklerde ve ordu hareketlerinin takip edilebileceği endişesi ile dünya çapındaki ABD askerî üslerindeki tüm mağazalarda Huawei ve ZTE'ye ait cep telefonlarını ve diğer telekomünikasyon ekipmanlarının satışının yasaklanması doğrultusunda emir vermiştir (Tomlinson ve Miles, 2018). Son olarak ABD Federal Soruşturma Bürosu (FBI), 2022 Pekin Olimpiyat Oyunları kapsamında Çin'de tüm sporcularına siber güvenlik nedeniyle kişisel cihazlarını evde bırakmalarını veya geçici telefon kullanmalarını tavsiye etmiştir (LeBlanc ve Lillis, 2022).

Güvenlik algısının güçlendiği, ülkelerin birbirlerini güvenlik konusunda tehdit ettiği bu dönemde silahlı savaşlar kadar büyük sonuçlar doğurabilecek, devletlerin gizli bilgi ve belgelerinin açığa çıkmasına sebebiyet verecek, ulusal güvenliği tehlike altına alabilecek yeni bir savaş alanı olan siber savaş kavramı doğmuştur. Teknolojinin gelişimi ve ülkelere sağladığı avantajların yanı sıra siber

teknolojiler ile savunma, sanayi, eğitim ve ekonomi gibi alanlarda bir tehdit algısı da oluşmuş, ülkeler siber alanda güvenliği sağlamanın aynı zamanda ulusal ve toplumsal güvenliği sağlamak olduğu düşüncesini geliştirmiştir. Birçok alanda rekabet eden ve birbirine üstünlük sağlamaya çalışan ABD ve Çin için de siber alan büyük bir mücadele alanı olarak ortaya çıkmıştır.

ABD-Çin rekabetinde siber güvenlik kavramının yanı sıra siber savaş kavramı da gün yüzüne çıkmıştır. Uluslararası güçlerin rekabeti artık yeni bir arenaya taşınmış ve sanal dünyada siber savaş da gündeme gelmiştir. ABD-Çin arasındaki siber savaşlar ve bu alanda verilen mücadeleler son dönemde birçok gelişmeyle somutlaşmıştır. Çin, mavi ordu adlı bir süper elit siber savaşçı birliğine sahip olduğunu duyurmuştur. Bunun ardından da ABD'nin yeni savunma stratejisi gün yüzüne çıkmıştır. Pentagon bir strateji açıklamış ve siber saldırıların savaş ilanını kabul edilebileceğini belirtmiştir. Bu duyurudan bir gün sonra ise Google, Çinli bilgisayar korsanları (hacker) tarafından düzenlenen bir saldırı sonucu üst düzey ABD'li ve Güney Koreli devlet yetkililerinin bilgilerinin çalındığını açıklamıştır. Yüzlerce kişinin Gmail hesaplarına ait bilgilerin çalınması da siber saldırılar ve siber güvenlik konusunda ülkeler arasındaki gerginliğin artmasına sebebiyet vermiştir. Artık siber saldırılar ülkelerin uluslararası güvenliğini büyük ölçüde tehdit edecek ciddi bir savaş unsuru olarak ortaya konmuştur (King, 2011).

2013 yılına geldiğimizde ise ABD ve Çin arasındaki siber gerilim tırmanışa geçmiştir. Yıllık raporunda ilk defa Çin'in resmî bilgisayarlara erişerek ABD'nin gizli bilgilerini çalmaya çalıştığını ileri süren Pentagon; bu raporda Çin'in ABD'nin diplomasi, ekonomi ve savunma programları ile alakalı istihbarat bilgilerini ele geçirmek için siber kapasitesini kullandığını ifade etmiştir. Bu iddiaları ve suçlamaları reddeden Çin ise açıklamaların ABD'nin güvensizliğini gösterdiğini söylemiştir. O dönemin Obama yönetimi siber saldırı konusunda Çin'i ilk kez resmen suçlamıştır. Pentagon, ABD Kongresi'ne yaklaşık 100 sayfalık bir rapor sunmuş ve bu raporda 2012'de ABD'nin dünya üzerindeki sahip olduğu birçok bilgisayar sistemine girildiği iddia edilmiştir. Pentagon bir önceki yıl yayınladığı raporda da Çin tarafından saldırıların gerçekleştiğini ifade etmiş fakat doğrudan hükûmet tarafından gerçekleştiğini belirtmemiştir. Ancak bu sefer saldırıların bir kısmının direkt Çin hükûmetine ve ordusuna dayandırılabilceği ifade edilerek suçlama kararı alınmıştır. O dönemde ABD'deki siber saldırıların

tamamına yakınında Çin'in ismi geçmiş ve siber casusluk faaliyetlerinin %90'ının Çin merkezli olduğu tahmin edilmiştir. Bu iddiaların ardından ABD yönetiminin Çin için ekonomik yaptırımlar getireceği ileri sürülmüştür. ABD'li bazı yetkililer Çin tarafından gerçekleştirilen siber casusluk faaliyetleri sebebiyle bazı para cezaları ve ticari yaptırımlar getirmeyi düşündüklerini ifade etmiştir. Pentagon'un o dönemdeki raporunda Çin ordusunun modernize edildiğinden de bahsedilmiş, Çin'in askerî kapasitesine de işaret edilmiştir. Aynı zamanda raporda Çin'in balistik füze, anti-uzay silah ve askerî siber sistemler için yaptığı yatırımın arttığı da belirtilmiştir. Pentagon yetkilisi David Helvey, bu yaptırımlar sayesinde Çin'in askerî operasyon kapasitesinin ve bölgedeki hak iddialarının da arttığını söylemiştir ("ABD ve Çin arasında siber gerilim", BBC News Türkçe, 2013).

2019 yılına gelindiğinde iki ülke arasında Huawei meselesi, büyük bir krize yol açmıştır. ABD ve Çin arasındaki rekabette ticaret savaşları ve siber savaşlar kritik öneme sahiptir ve bu bağlamda ise teknolojik rekabet ön plana çıkmaktadır. ABD Başkanı Donald Trump döneminde başlayan ticaret savaşları Çin'den çelik ithalatına %25, alüminyum ithalatına ise %10 ek gümrük vergisi getirilmesi ile devam etmiştir. ABD Başkanı Donald Trump, 22 Mart 2018 tarihinde yaptığı açıklamada "Şu anda dünya ile 800 milyar dolarlık bir ticaret açığımız var. Diyelim ki Çin ile 500 milyar dolar var, ancak dünya ile toplamda 800 milyar dolar. Bu, ticaret açığının yarısının Çin'in teşkil ettiği anlamına gelir. Dolayısıyla bununla ilgileneceğiz" ifadelerine yer vermiştir. Çin menşeli telekomünikasyon şirketi Huawei'ye karşı sürdürülen ABD politikaları da bu mücadelenin önemli bir ayağını oluşturmuştur. 2011 yılından beri Huawei'nin ABD pazarında etkin olmaması için birçok girişimlerde bulunulmuş, Huawei'nin ABD'nin teknolojisini çaldığı ve teknolojik casusluk faaliyetlerinde bulunduğu iddia edilmiştir. FBI Başkanı Christopher Wray, 28 Ocak 2019 tarihindeki konuşmasında, "Huawei ayrıca, bilinçli ve sistematik olarak bir Amerikan şirketinden değerli fikrî mülkiyet çalmaya çalıştı. Bu nedenle zor kazanılmış, zaman alan araştırmaları atlatıp adil olmayan bir pazar avantajı elde etti" ifadelerine yer vermiştir. 2012 yılındaki istihbarat raporunda ise Huawei için casusluk faaliyetlerinde bulunduğu dair maddeler yer almıştır. Çinli şirketler Huawei ve ZTE'nin faaliyetleri ile alakalı hazırlanan raporda şöyle bir madde bulunmaktadır: "Kanıtlar gösteriyor ki, Huawei, ABD'deki şirket ve kuruluşların zihinsel birikim haklarını ihlal etmiş bulunmaktadır." Tüm bu gelişmelerin ardından ABD'de Ağustos 2018 tarihinden itibaren hükûmet

görevlilerinin Huawei ve ZTE markalarına ait cihazları kullanmaları yasaklanmıştır. Huawei Mali İşler Direktörü Ming Vancou, Kanada'da İran yaptırımlarını deldiği gerekçesiyle yargılanmış, ABD kefaletle serbest bırakılan Vancou'nun iadesini istemiştir. Buna karşılık Çin ise ulusal güvenliği tehdit ettiği gerekçesiyle Kanadalı iş adamı Michael Spavor ve diplomatlık yapmış olan Michael Kovrig'i tutuklamıştır. 5G teknolojisine de ciddi yatırımlar yapan Huawei, dünya genelinde en çok satılan telefonların başında gelmektedir. Çin'in ve Huawei'nin bu alanda yaptığı atılımlar da Huawei markasının üzerindeki baskıların sebeplerinden birisidir. 26 Ocak 2019 tarihli New York Times haberine göre ABD, Çin ile girdiği 5G yarışında kendi taraflarına hâkim olmaya çalışarak Huawei'nin 5G projelerine destek vermemesi için bazı ülkelere baskı yapmıştır. Tüm bunların aksine Huawei ise casusluk iddialarını kabul etmemiş, 15 Ocak 2019 tarihli Reuters haberinde Huawei kurucusu, "Çin için casusluk yapmadıklarını" söylüyor ifadeleri yer almıştır ("ABD Huawei'yi neden hedef alıyor?", Anadolu Ajansı, 2019).

2020 yılına geldiğimizde koronavirüs salgını ile birlikte ABD ve Çin arasında hem yeni bir gerginlik hem de yeni siber saldırı iddiaları gündeme gelmiştir. ABD Güvenlik ve İstihbarat Servisleri tarafından Çin'in koronavirüs aşısı ve tedavisi için çalışmalar yürüten laboratuvarlara siber saldırılar düzenleyip önemli bilgileri çalmaya çalıştığı duyurulmuştur. FBI ve ABD Siber Güvenlik Teşkilatı, konuyla ilgili olarak bir açıklama yapmış ve Çin destekli bilgisayar korsanlarının gerçekleştirdiği siber saldırıların soruşturulduğunu belirtmiştir. FBI ve ABD Siber Güvenlik Teşkilatı bazı ilaç şirketlerinin de siber saldırılarda hedef alındığını iddia ederek bu şirketlere gerekli önlemleri almaları hakkında uyarılarda bulunmuştur. Çin'e oranla koronavirüs vakalarının sayısında kat ve kat artış gösteren ABD'de Trump yönetimi, Çin'i birçok kez koronavirüs salgınının kaynağı konusunda şeffaf olmamakla suçlamış, buna karşılık Çin ise iddiaları reddetmiştir ("Koronavirüs: ABD istihbaratı 'Çin'in siber saldırılarını' soruşturduğunu açıkladı", BBC News Türkçe, 2020).

İki ülke arasında savaş diye tabir edilen gerginliklere sebep olan siber faaliyetlerden bir diğeri ise geçtiğimiz yıl Microsoft ve Çin arasında gerçekleşmiştir. Amerikan teknoloji şirketi Microsoft; ABD'deki birçok kurum, kuruluş ve şirketin e-posta hesaplarına Çin'in siber saldırı düzenlediğini iddia

etmiştir. BBC'nin haberine göre Microsoft bu iddiasında siber saldırı düzenleyenlerin "devlet destekli, oldukça yetenekli ve bilgili" olduğunu da vurgulamıştır. Microsoft, Hafnium isimli bir hacker grubunun; birçok farklı araştırmacının, firmanın, kurumun, şirketin ve sivil toplum kuruluşunun hesaplarına saldırdığını duyurmuştur. Konu ile alakalı Çin Dışişleri Bakanlığı Sözcüsü Vang Vinbin "Çin, ilgili medya ve şirketlerin profesyonel ve sorumlu bir tavır benimsemesini, siber saldırıların karakterlerini temelsiz tahmin ve suçlamalar yerine yeterli kanıtlara dayanarak belirlemesini umuyor" şeklinde açıklama yapmıştır (Kabakçı, 2021).

Teknoloji alanında yoğun bir rekabet içerisinde olan ABD ve Çin ilişkilerini zora sokacak bu gelişme ABD'nin Microsoft'a yapılan siber saldırıdan Çin'i resmen sorumlu tutmasıyla daha da ciddi bir boyut kazanmıştır. Beyaz Saray yönetimi kamuya bir duyuru yaparak bu siber saldırıdan Çin'i sorumlu tutmuş, Adalet Bakanlığı da buna benzer bir açıklama yapmıştır ("US blames China for hacks, opening new front in cyber offensive", CNN Politics, 2021).

Çin ise bu açıklamalara tepki göstererek iddiaları reddetmiştir. ("Çin, siber saldırı iddiasını reddetti", Dünya, 2021). Çin Dışişleri Bakanlığı sözcülerinden Cao Licien, ülkesinin siber güvenlik saldırılarının tamamına karşı çıktığını, Çin'in de bu saldırılarla mücadele ettiğini belirtmiş ve hiçbir siber saldırıyı desteklemediklerini söylemiştir. Hatta Licien de ABD Merkezî İstihbarat Servisi'nin (CIA) 11 yıldan fazladır Çin'in uzay araştırma tesislerine, endüstrisine, internet şirketlerine ve kurumlarına siber saldırılar düzenlediğini ileri sürmüştür. Bu saldırıların ulusal ve ekonomik güvenliği ciddi şekilde sarstığını söyleyen Licien, Çinli kuruluşların ABD'nin siber saldırılarından etkilendiğini dile getirmiştir ("China denies hacking Microsoft, calls allegations 'groundless' and 'irresponsible'", France 24, 2021).

İki ülke arasındaki rekabetin en şiddetli yaşandığı alanların başında gelen teknolojik gelişmelerin bir diğer boyutu da çip sektörü olmuştur. 2021 yılının haziran ayında yürürlüğe giren ABD Yenilikçilik ve Rekabet Yasası ile çip sektörüne 52 milyar dolarlık bir destek yapılması, ABD'nin Asya piyasasındaki bağımlılığının azalması hedeflenmektedir. Ayrıca bu yasa ile yapay zekâ ve kuantum alanında da 120 milyar dolarlık bir teknolojik yatırım hedeflenmektedir. ABD'nin bu hamlelerine ise teknolojik alanda büyük sıçramalar gösteren Çin; 5G

teknolojisi, klonlama, yarı iletkenler, kuantum, yapay zekâ, robot teknolojileri gibi sektörlerde büyük atılımlar yaparak ABD'yi tedirgin etmektedir. İki ülke arasında teknoloji firmalarını da içrisine alan bu kavgada Çin'in süreci daha iyi yöneterek kendi teknoloji sektöründe kontrolü eline aldığı ve ülkenin kalkınması lehine kullandığı söylenebilir (Kozanoğlu, 2021).

Teknolojik rekabette Çin'in üstünlüğünü ortaya koyan bir gelişme de ABD Savunma Bakanlığının bilgisayar yazılım sistemlerinden sorumlu yetkilisi Nicolas Chaillan tarafından ifade edilmiştir. Bu rekabette Amerika'nın teknolojik gelişiminin çok yavaş olduğunu öne süren Chaillan, "Çin'in ABD'yi geçmesini izlemeye dayanmam" diyerek görevinden istifa etmiştir ("Eski Pentagon yetkilisi: ABD Çin'e karşı siber savaşı kaybetti", TRT Haber, 2021). İngiltere'nin Financial Times gazetesine konuşan Chaillan, konu ile ilgili "15-20 yıl içinde Çin'le rekabet ve mücadele edemeyecek bir konumda olacağız. Bence bu şimdiden belli. Çin, gelecekte dünyayı domine edecek. Medyadan jeopolitiğe her alanda, bu durum değişmeyecek. Bazı hükûmet birimlerinde, ABD'nin siber savunması anaokulu düzeyinde" ifadelerini kullanmış ve bu rekabette ABD'nin kaybeden taraf olduğunu belirtmiştir (Klawans, 2021).

3.2. Ulusal Güvenlik Politikalarında Siber Güvenlik

Ulusal güvenlik politikası temel anlamıyla; bir milletin hak ve menfaatlerini korumak, askerî ve sivil kaynaklarının tamamını ve bu kaynakların araçlarını toplu ve koordineli olacak biçimde savunma görevlerinde kullanmak ve millî çıkarları muhafaza etmek amacıyla kullanılmasını amaçlayan bir plandır. Her ülkenin gizli ya da açık şekilde bir ulusal güvenlik politikası vardır. Açık olan ulusal güvenlik politikalarını ilgili belge, veri ve planlardan okumak ve anlamak mümkünse de gizli olan politikalar için aynı yöntem uygulanamamaktadır. Bu nedenle gizli politikalar ancak devletlerin güvenlikleri ile ilgili attıkları adımlara göre yapacağı hamleleri ve göstereceği reaksiyonları öngörmek ve gözlemlemek suretiyle okunabilecektir (Doyle, 2007, s.624). Örneğin Soğuk Savaş döneminde ABD ve Rusya Sovyet Federatif Sosyalist Cumhuriyeti'nin (RSFSC) güvenlik politikaları temel hatlarıyla birbirlerine karşı geliştirilmiştir. Ancak Soğuk Savaş sonrası dönemde ABD nezdinde tehlike tek bir odakta toplanmamaktadır.

21. yüzyılda artık siber güvenlik, ulusal güvenliği yakından ilgilendiren ve bu konuda hayata geçecek adımları ve ortaya konan politikaları etkileyen bir unsur olmuştur. Devletler artık ulusal güvenlik politikalarını oluştururken siber güvenlik faktörünü de hesaba katmak durumundadırlar. Bu bağlamda siber güvenliğin ehemmiyeti ile ilgili olarak PEW Araştırma Merkezi (PEW Research Center) tarafından bir araştırma yapılmıştır. 2014 yılında yapılan bu araştırmaya göre, araştırmaya dahil olan 1600 teknoloji uzmanından yaklaşık 1100 tanesi 2025 senesine kadar şiddetli bir maddi hasar ve can kaybına mal olacak bir savaşın olacağını düşünmektedir (Rainie vd., 2014'ten akt. Kshetri, 2016, s.54). Bu ve bunun gibi durumlar siber güvenliğin ulusal güvenlik bağlamındaki yüksek risk potansiyelini ortaya koymakta ve devletlerin bu konuya yönelik politikalar oluşturmalarını ve siber güvenliği ciddi şekilde ele almalarını gerekli kılmaktadır. Siber güvenlik konusunu ulusal bir açıdan inceleyen Cavelti (2014) ise siber güvenlik açıklarının her geçen gün arttığını ve bu doğrultuda kişilerin ve devletlerin siber güvenliğinin azaldığını öne sürmektedir. Uluslararası çaptaki büyük firmaların tüketiciyi merkeze koyan yaklaşımları ve vatandaşların bireysel özgürlük taleplerinin olmasının karşısında devletlerin her zamanki riskli ve kritik altyapıları koruma politikaları ile siber güvenliğe ulusal bir güvenlik unsuru olarak yaklaşma eğilimleri siber güvenlik konusunda bir ikilem oluşturmaktadır. Bu ikilemin temeli vatandaşların özgürlük alanı ile devletlerin güvenliğinin çatıştığı noktalardır. Devletler, ulusal güvenlik politikalarında önemli ve kritik altyapılarını koruma ve siber güvenliği artırmak suretiyle güvenlik açıklarının azaltılması ve bu amaçla katı ve net kurallar koymak üzere adımlar atmaya hedefler. Bireyler ise kendi özgürlüklerini korumak ve siber uzaydaki hareket alanlarını en serbest şekilde korumak istemektedirler. İşte ikilem bu iki durumdan kaynaklanmaktadır. Liberal görüşün etkisiyle, uluslararası şirketler de bu durumda bireylerin tarafında durmaktadır. Devletler için siber uzayda vatandaşlara ve firmalara, özellikle ağ sistemleriyle ve yazılımla ilgili çalışan firmalara, tanınan serbestlik bazı riskler taşımaktadır çünkü bu serbestlik beraberinde ulusal güvenlik açısından genişleyen ve büyüyen güvenlik açıklarını da beraberinde getirmektedir. Bu ikileme çözüm olarak devletler de ulusal güvenlik politikalarında siber güvenliği ele alırken bireylerin de önceliklerini göz önünde bulundurarak adım atmak durumunda kalmaktadır.

Siber güvenlik alanında yaşanan sıkıntıların sonucunda meydana gelen aksaklıklar, devletleri siber güvenlik konusunda daha tedbirli olmaya ve güvenlik önlemlerini artırmaya yönlendirmiştir. Siber güvenlik zafiyetleri sonucu sadece teknik olarak değil diplomatik, siyasi ve ekonomik olarak da sorunların meydana geldiği görülmektedir. Devletlerin gizli verilerinin ele geçirilmesi, paylaşılması, devletlerin ağ sistemlerine sızılması sonucu meydana gelen sorunlar devletlerarasında savaşımlara dahi sebebiyet verecek güçtedir. Devletlerarasında yaşanan krizlerin yanı sıra siber saldırıya maruz kalan ülkeler, bu saldırıların izlerini silmek ve buna karşın yeni düzenlemeler yapmak için bazı ekonomik sıkıntılar da yaşamaktadır. Teknik alanda bir saldırıya maruz kalınması sonucu güvenlik sistemlerinin ve verilerin zarar görmesiyle birlikte gizli verilerin yayılması, ülkeler arası siyasi ve diplomatik krizleri de meydana getirebilmektedir. Ulusal bilgileri, devlet adına gizli belgeleri, kişisel verileri koruyan bir alan olarak değerlendirilen siber alan, ülkelerin önemli değerleri arasındadır. Sadece ulusal güvenliği sağlamak değil ticari kimliği korumak ve rekabet gücünü sağlamak amacıyla da önem arz eden siber güvenlik, ülkelerin geleceğine de etki ettiği için ayrı bir önem arz etmektedir (Sağıroğlu, 2018, s.36-37).

Dolayısıyla ülkeler; ulusal anlamda kendi menfaatlerini korumak, kritik altyapıları ile kamusal bilgilerin gizliliğini sağlamak, gizli kalması gereken sistemleri güvende tutmak ve ülkede yaşayan vatandaşların özgürlüklerini sağlamak, bilgileri korumak için farklı siber güvenlik politikaları oluşturmakta ve bu konuyla alakalı stratejiler uygulamaktadırlar. Öte yandan farklı dönemlerde meydana gelen ve elektronik ortamlardaki verilerin ele geçirilmesi, zarara uğratılması, gizliliğinin ve bütünlüğünün zarar görmesi ile sonuçlanan siber ataklar ve saldırılar devletlerin politikalarını şekillendirmiş ve bu konuda yeni adımlar atılmasını, yeni stratejiler geliştirilmesini, çeşitli önlemler alınmasını sağlamıştır.

3.2.1. ABD ve Çin'in Siber Güvenlik Politikaları

Teknolojik gelişmeler ve küreselleşmenin beraberinde getirdiği değişimle birlikte siber alandan daha çok söz edilmeye başlanmıştır. Söz edilmenin de ötesinde güç kontrolünün artık bilgisayar ortamına taşınması ile küresel düzeyde oyun belirleyici olmanın bir gereği olarak siber alanda gelişmişlik, bir diğerinden daha iyi olma ve güçlü siber güvenlik altyapılarına sahip olma şartına bağlı hale

gelmiştir. Önemi günden güne artan siber güvenlik, bilgi ve iletişim güvenliği olarak adlandırılırken ilerleyen seneler içerisinde bu konuda yapılan oluşumlarla bilişim güvenliği önlemlerinin bir parçası konumuna gelmiştir. Özellikle son yıllarda siber güvenlik, askerî ve sivil kurumların en üst düzey yönetimlerinin içerisine dâhil edilmiş ve önemle icra edilmesi gereken bir alan olmuştur.

Ülkelerin siber güvenlik konusunda farkındalık kazanması ve daha güçlü siber güvenlik altyapıları oluşturması birçok farklı etkene bağlıdır. Ulusal güvenliklerini tam anlamıyla sağlamak ve önem verdikleri korunması gereken altyapıları muhafaza etmek isteyen ülkeler, geleneksel güvenlik yöntemlerinin yanında gelişen teknolojileri ve bu teknolojilerle birlikte yeniden şekil alan kritik altyapıları da göz önünde bulundurarak siber güvenlik konusundaki gücünü değiştirebilir. Kapsamı ve ilgilendirdiği alanlar bakımından geniş bir yelpazeye sahip olan siber güvenlik, ülkelerin fiziki ve ekonomik güçlerinden daha da kapsamlı bir güvenliği ifade etmektedir. Özellikle günümüz dünyasının başat güçlerinden ABD ve Çin, başat olma durumlarını koruyabilmek ve hatta ekonomik, teknolojik vb. alanlarda daha çok gelişebilmek maksadıyla siber güvenliklerini sağlamak, sağlamlaştırmak ve geliştirmek için fazlasıyla efor sarf etmektedirler.

3.2.1.1. ABD'nin Siber Güvenlik Politikası

Gerek sahip olduğu askerî kapasite gerek teknoloji ve sanayi alanlarındaki potansiyel ve gelişim gerekse diğer pek çok alanda sahip olduğu üstünlük nedeniyle başat aktör olarak görülen ABD, siber güvenlik alanında da yaşanan gelişmelerden hareketle stratejiler geliştirme yönünde çalışmalarını hızlandırmıştır. Özellikle Soğuk Savaş sonrası dönemde siber güvenlik ulusal güvenliğin temel taşlarından birisi olmuş ve özellikle 11 Eylül saldırılarının ardından ABD, siber güvenliği daha çok dikkate alarak önemli bir politika sahası olarak görmüştür.

1986'dan beri, başkanların her yıl bir Ulusal Güvenlik Stratejisi (UGS, National Security Strategy – NSS) sunmaları istenmiştir (Historical Office, Office of the Secretary of Defense, x). Son yıllarda, kısmen UGS ile bağlantılı olan diğer türden ulusal stratejilerin de çoğaldığı gözlemlenmektedir. UGS, “ulusal çıkarlarını savunan ve geliştiren hedeflere ulaşmak için -askerî veya değil- devlet

gücünün tüm araçlarının eşgüdümlü kullanımına yönelik bir ulusun planını" temsil etme amacını taşımaktadır. Bu bağlamda ABD, siber güvenlik konusunda da kurumsal altyapı oluşturmaya başlamıştır. Başkan talimatları ve siber alandaki stratejik planlamalar siber güvenlik politikalarının belirlenmesinde etkin rol almıştır. 1995 senesinde, siber güvenlik alanındaki gelişmeleri konu eden ilk resmî belge niteliğine sahip başkan direktifi yayımlanmıştır.

ABD’de güvenlik politikalarını şekillendirmek üzere çalışmalar yapılırken aynı zamanda kurumsal alanda da bazı gelişmeler olmuş ve buna paralel olarak 1998 yılında FBI bünyesinde, siber saldırılara cevap verebilmek için ve altyapıya yönelik tehditlerin bilgi aktarımının sağlanmasını amaçlayan Ulusal Altyapı Koruma Merkezi (NIPC) kurulmuştur. Atılan bu adımdan da görülebileceği gibi ABD için siber tehdit algısı siber suçlara ve tehditlere yönelik tedbirlerle alakalıdır (Demirel, 2012, s.91). Fakat 11 Eylül saldırılarının ardından asimetrik tehditlerin de öne çıkması ile siber güvenlik algısında değişim yaşanmış ve siber güvenlik artık ulusal güvenliğin bir parçası olarak değerlendirilmeye başlanmış, bu konu 2002’de kurulan İç Güvenlik Bakanlığı (The Department of Homeland Security-DHS) kapsamına alınmıştır (Demirel, 2012, s.92).

ABD’de, FBI ve DHS’nin de içinde bulunduğu siber güvenlik politikası ile ilgili faaliyet gösteren kurumlardan oluşan üçlü bir yapı vardır ve bu yapı, alt kurumlarının yürüttüğü faaliyetlerle birlikte siber güvenlik stratejisine şekil verir. Bu üçlü yapının bir diğer ayağı da Savunma Bakanlığıdır. ABD’nin siber güvenlik hamleleri, uygulamaları, çalışmaları ve stratejileri hakkında temel oluşturan ve ABD’nin resmî siber organizasyonu olarak da bilinen bu üçlü yapı, kurumsal altyapı dayanağı özelliği taşımaktadır (Darıcılı, 2017, s.7). ABD’nin siber güvenlik algısındaki askerî yönünü teşkil eden ve içindeki kurumlar sebebiyle siber güvenlik stratejisinin önemli bir ayağını oluşturan Savunma Bakanlığının karargâhı, 11 Eylül saldırılarında zarar gören merkezlerden birisi olan Pentagon’dur. Savunma Bakanlığının barındırdığı kurumlardan; şifre çözme, veri analizi, karşı istihbarat gibi çalışmalar yapan ve 1952’de kurulan Ulusal Güvenlik Ajansı (National Security Agency-NSA) bu konuda önem arz etmektedir (Darıcılı, 2017, s.8). Savunma Bakanlığına göre siber uzay, ciddi riskler taşıyan bir savaş alanıdır. Savunma Bakanlığı bu görüşünü “Siber Uzay Harekâtları için Ulusal Askerî Stratejisi” belgesi ile de resmî hale getirmiştir. Bu belge ile siber uzay;

elektromanyetik enerjinin kullanıldığı ağ sistemlerinden oluşan bir fiziksel etki alanı olarak ifade edilmiştir ve yine bu alanda hareket serbestliğini sağlamak için ABD Hava Kuvvetleri Siber Komutanlığı kurulmuştur (Akyazı, 2013, s.218). Siber güvenlik konusunda FBI'ın rolü ise casusluk faaliyetlerine karşı istihbarat oluşturarak savunma mekanizması geliştirmesi ve önlemler almasıdır. Bu konuda FBI'ı önemli kılan unsur, siber saldırılara karşı koyma görevidir. Siber Ulusal Güvenlik Bölümü ve Siber Suç Bölümü de FBI kapsamında olan birimlerdir (Darıcılı, 2017, s.10).

ABD'deki siber güvenlik politikası ile ilgili çalışmalar yürüten üçlü yapının bir diğer ayağı olan DHS ise terörle mücadele konusunda yetkili olan kuruluştur. 2002 senesinde yürürlüğe konan Kamu Güvenliği Yasası kapsamında kurulan DHS, siber güvenlik anlamında; siber güvenliği daha da güçlendirmek, önemli altyapıları korumak, kritik kaynakların direncini korumak ve hükûmetin iletişim gücünün sürdürülebilirliğini sağlamak için çalışır (Başa, s.33). Acil müdahale yeteneği de olan DHS'de temel sorumluluğa sahip birim, Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezidir. Ülkedeki siber olayları izleyen birim aynı zamanda özel ve resmî birimler arasındaki iletişim ve iş birliğini de sağlamaktadır (Darıcılı, 2017, s.9).

2003 yılı ABD'de siber güvenlik anlamında önemli bir yıldır. O senede yayınlanan "Secure Cyberspace" (Güvenli Siber Uzay) belgesi siber güvenlikle ilgili yayınlanan ilk belge özelliğini taşımakla birlikte, bu belgede "siber güvenlik" teriminden daha çok "güvenli siber uzay" terimi geçmektedir. Bu belgeye göre siber uzay; kritik altyapıların işleyişini sağlayan ve birbiriyle bağlı olan birçok bilgisayar, sunucu, modem, anahtar ve kablolardan oluşan alandır. (The White House, 2003, s.vii). Ulusal Güvenliğin Sağlanmasına Yönelik Ulusal Strateji (National Strategy for Homeland Security) ile Kritik Altyapıların ve Değerli Varlıkların Fiziki Olarak Korunmasına Yönelik Ulusal Strateji (National Strategy for the Physical Protection of Critical Infrastructures and Key Assets) belgesinin uygulama bölümü olarak hazırlanan Güvenli Siber Uzay belgesi, siber güvenlik hakkındaki ulusal ve federal kurumların direktiflerini içeren; devlet ile yerel yönetim kurumlarının, özel firmaların, sivil toplum kuruluşlarının ve vatandaşların birlikte siber güvenliği geliştirmek için yapacağı hamleleri belirleyen bir belgedir.

Bu belgede ulusal güvenliğin tesisi için beş öncelik bulunmaktadır. Bunlar; ulusal siber uzay güvenliği karşılık sistemi, ulusal siber uzay güvenliği tehditlerini ve güvenlik açığını savunma programı, ulusal siber uzay güvenliği farkındalık ve geliştirme programı, hükûmetin siber uzayını güvenlik altına alma ve koruma, ulusal güvenlik ve uluslararası siber uzay güvenliği iş birliğidir. 2011, 2013 ve 2015 yıllarında da ABD'nin siber güvenlik politikası ile alakalı başka önemli belgeler de yayınlanmıştır.

Tüm bu gelişmeler ile birlikte, siber güvenlik konusunda öncü bir ülke olan ABD'nin bu politikada oluşturduğu milli siber altyapılar siber bağımlılığı en düşük seviyede tutarken, diğer yandan kritik altyapıların çoğunlukla siber altyapılara bağlı olması ABD'nin siber savunma fonksiyonunu zayıflatmaktadır.

Sonuç itibarıyla, ABD'de siber güvenliğe yönelik gözle görülen değişimler genel olarak 2000'li yılların başlarında olmuştur. Siber güvenliği sağlamak üzere devlet kurumlarının kapasitelerinin artırılması ve gelebilecek siber tehditlere karşı ülkenin savunma sistemlerinin güçlendirilmesi için son yıllarda somut adımlar atılmıştır. Ortaya koyulan belgelerde, siber güvenlik hakkındaki politika önerilerinin ABD'ye karşı siber güvenlik saldırıları ve siber bağımsızlık ile alakalı olduğu görülmektedir.

Donald Trump ile başlayan 2017 sonrası ve yeni dönem olarak ele alınan dönemde ise her alanda olduğu gibi siber güvenlik alanında da bazı değişiklikler yaşanmıştır. Yeni dönemde 1,5 milyar dolarlık bir yatırım kritik altyapıların korunması için siber güvenliğe ayrılmış ve ayrıca her bakanlığa kendi siber güvenliğini koruması sorumluluğu verilmiştir ("Trump'tan Devrim", 2017). Siber saldırılara karşı daha saldırgan adımlar atılmasının öngörülmesi sebebiyle, 2018 yılında imzalanan Ulusal Siber Güvenlik Stratejisi Belgesi "saldırgan" ifadesi ile tanımlanmıştır. Siber konularda suçlu olan kişilere karşı ihbar ve yasal işlemler konularında daha etkili sistemler kurulması gerekliliği öne çıkmış ve bu konuda ABD'nin küresel üstünlük kurması, siber güvenliğin sağlanmasında bazı ölçütler oluşturarak bu ölçütlere küresel düzeyde uyulmasının sağlanması için çalışmalar yapılması önemsenmiştir ("Trump'tan Daha", 2018). Bu belgede siber alan, Amerika'da yaşayan halk için "*ekonomi ve savunma ile iç içe bir alan*" olarak nitelendirilmiştir. Siber güvenlik ve savunmanın birlikte ve etkili bir şekilde çalışması gerektiği konusuna önem verilmiş ve gerektiğinde bilişim sistemlerine

karşı kullanılan zararlı yazılımların ABD'ye karşı kullanılması durumunda cezalandırmaların yapılacağı ifade edilmiştir (The Department of Homeland Security, 2018, s.6).

Bu dönemde diğer dönemlerde de olduğu gibi olası tehditleri minimum seviyeye indirmek, siber tehditlere karşı ulusal güvenlik programını geliştirmek, gelebilecek ulusal saldırılara engel olmak, eğer böyle bir durum gelişirse uluslararası alanda ses çıkarmak ve tepki oluşturmak, kritik alt yapıları ve federal hükûmetin bilgi sistemlerini muhafaza etmek amaçlanmıştır (The Department of Homeland Security, 2018, s.3). Tehditlere karşı yapılabilecek eylemler ile alakalı genel olarak, kamu ve özel sektör arasında iş birliği kurulması ve siber uyarı ağlarının daha da geliştirilmesinden söz edilmektedir. Önlemlerle alakalı ise yazılım açıklarını kapatma, ilgili hukuki düzenlemeler yapma, aciliyet sistemlerinin güvenliğini sağlama gibi konular öne çıkmaktadır (The White House, 2003). Belgede aynı zamanda kritik altyapılar hakkında yedi önemli alandan bahsedilmiştir. Bunlar; enerji ve güç, ulaşım, iletişim, sağlık, ulusal güvenlik, finans ve bilgi teknolojileri alanlarıdır (The White House, 2018, s.10).

ABD'nin siber güvenlik hakkındaki önceliklerini içeren bir diğer önemli kaynak da Savunma Bakanlığı Siber Strateji Belgesi'dir. Bu belgede Rusya ve Çin'in önemli tehditler olduğu belirtilmiştir. Belgede, Rusya ve Çin gibi ABD'nin varlığına ve güvenliğine karşı tehdit unsuru olan ülkelere daha fazla ağırlık verileceği belirtilmiştir. Herhangi bir çatışma veya kriz durumu anında bilgi elde etmek ve askerî siber kapasiteyi artırmak için siber uzay operasyonlarının gerçekleştirileceğinden de bu belgede bahsedilmiştir. Güvenliğin, sistemlerin ve ağ bağlantılarının güçlendirilmesi de gelecek için planlanan adımlardan ve stratejilerden biridir (The Department of Defence, 2018, s.1). Siber stratejiler devamlı bir gelişim halindedir ve ABD'nin güvenlik gündeminde her geçen gün daha üst sıralarda yer almaktadır. ABD'ye göre hükûmet uygulamalarının ve ciddi bir öneme sahip olan hizmet dağılımlarının daha güvenli olması siber uzay ile sağlanabilmektedir (The Department of Homeland Security, 2018, s.27).

3.2.1.2. Çin'in Siber Güvenlik Politikası

"Siber güvenlik" kavramı yerine "bilgi güvenliği" ya da "ağ güvenliği" kavramını daha çok kullanan Çin'de, 2017 senesinde yürürlüğe giren Siber

Güvenlik Kanunu, siber terimini kısmen içerse de siber güvenlikle alakalı konular bilgi güvenliği olarak işlenmiştir. Bunun sebebi Çin kültürü ve Çin'in Batı edebiyatına karşı antipatisi ile açıklanabilir. Çin kültüründeki inanca göre bilgi birikimi bir güçtür ve Çin'in stratejisinin temelinde de geleneksel gücün bilgiye dayalı güce dönüşümü yatmaktadır (Patton, 2016, s.9). Bilgi güvenliği kavramını kullanan Çin aynı zamanda ideolojik bir tavır alarak ABD'ye ve Batı edebiyatında yer alan siber kavramına karşı da bir tutum ortaya koymaktadır (Darıcılı ve Özdal, 2018, s.11).

Kavramların dışında Çin'in net bir siber güvenlik tanımının olmadığı görülmektedir. Fakat Çin siber güvenliği geniş kapsamlı bir şekilde ele almaktadır (Akyeşilmen, 2018, s.114). Kaynaklardan yapılan açıklamalara bakıldığında Çin'in siber güvenlik anlayışının diğer devletlerin görüşleri ile paralel olduğu söylenebilecektir. Çin'in siber güvenlik düşünceleri arasında; internetin ulusal güvenlik, ticaret, sosyal ve bireysel çıkarlara karşı zararlarından ve zarar verici etkilerinden korunmanın sağlanması vardır. Devletin ve toplumun savunma kapasitesi, ekonomik anlamda güçlü bir şekilde rekabet etme yeteneği, sosyal normların muhafaza edilmesi, kişilerin mahremiyeti ve vatandaşların güvenliği bu bahsedilen çıkarlar arasındadır (Swaine, 2013, s.3).

Siber savunma alanına önemli yatırımlar yapan ülkelerin başında gelenlerden biri olan Çin, en büyük rakibi ABD'nin aksine stratejilerinde daha kapalı bir tavır sergilemektedir. Dolayısıyla ABD'nin Çin'e yönelik tehdit algıları, şeffaflık eksikliği nedeniyle artmaktadır. Bu bağlamda dönemin ABD Milli Savunma Uzmanlarından Steve Hildreth tarafından yazılan "Siber Savaş (Cyberwarfare)" başlıklı bir ABD Kongre Araştırma Servisi raporuna göre Çin, teknolojik olarak üstün rakiplerin askerî yeteneklerini etkisiz hale getirmek için "Net Force" adlı stratejik bir bilgi savaş birimi geliştirmektedir. Çin, söz konusu konsepti çeşitli üniversitelerde, akademilerde ve eğitim merkezlerinde eğitilmiş bilgisayar uzmanlarından oluşan güçlü bir ekiple takip etmektedir. 1997'den beri ise yıllık olarak büyük eğitim tatbikatları gerçekleştirmektedir. Öte yandan Çin, bu görevler için gençleri eğitmeye büyük önem vermiştir (Hildreth, 2001, s.12).

Günden güne gelişen ve henüz potansiyeline tam anlamıyla ulaşmamış olan Çin, yalnızca geleneksel savunma yöntemleri ve fazla sayıda asker ile bir savaşı kazanmanın mümkün olmadığını anlamış; kısmen daha küçük bir ordu

kurarak yeni teknolojiye yatırım yapma kararı almıştır (Clarke ve Knake, 2011, s.32-33). Çin ordusu albaylarından olan Qiao Liang ve Wang Xiangsui tarafından 1999 senesinde yayımlanan ve teknolojik gelişmelerin savaş gidişatında nasıl bir etki yarattığının altını çizen “Sınırsız Savaş (Unrestricted Warfare)” adlı eser, Çin’in bu düşüncelerinin ilk açık kaynak olarak göstergesi olarak dikkat çekmektedir. 1990’lı yıllardan itibaren Çin, daha küçük bir ordu ve daha gelişmiş bilgi sistemlerine yönelik çalışmalar yürütmüştür (Spade, 2012, s.14-15).

Çin rakiplerine karşı siber saldırı kapasitesini artırarak yalnızca fiziki dünyada yapılan savaşların üstünlük için yeterli olmadığını kabul etmiştir. Özellikle ABD ve Rusya gibi güçlü rakipleriyle siber alanda mücadele edebilmek için önemli çalışmalar yapmaktadır. Güçlü virüsler ve kötü amaçlı yazılımlar (malware) oluşturarak düşmanlarının kritik alt yapılarını çökertmeyi amaçlamaktadır. Çin, siber savaşa karşı aldığı bu önlemlerinde yalnız değildir. Gelişmiş teknolojiye sahip diğer devletler de benzer şekilde kendi önlemlerini almaktadırlar.

1990’lı yıllardan sonra siber güvenlik stratejilerine hız veren Çin, ilk başta savunma amaçlı başladığı politikalarına daha sonra saldırı amaçlı olarak devam etmiştir ve Çin’in siber güvenlik stratejileri bu konuda analiz ettiği siber güvenlik tehditleri ile şekillenmiştir. Çin’de ilk resmî bilgi teknolojileri girişimi 1986 senesinde “Devlet Ekonomik Bilgi Yönetimine Öncü Küçük Grup” isimli yapıyla başlamıştır. Daha sonra “Devlet Bilişim Öncü Grubu” ve bu grubun altında çalışması amacıyla 2003 yılında da “Devlet Ağı ve Bilgi Güvenliği Koordinasyon Küçük Grubu” kurulmuştur. “İnternet Güvenliği ve Bilgilendirme için Merkezi Öncü Küçük Grup” adında bir organizasyon da 2014 yılında kurulmuştur. Bu kuruluşun faaliyetlerinin yönlendirilmesi Çin başkanları tarafından kararlaştırılmış, yönetimin siber uzay gelişmelerine verdiği önem ortaya konmuştur. Kurulan tüm bu organizasyonlar Çin’in bilgi teknolojilerini geliştirmeyi amaç edinmişlerdir (Darıcılı ve Özdal, 2018, s.12-14).

Çin’in siber güvenlikle ilgili yayınladığı strateji ve planlardan ilki 2003 yılında yayımlanan “Doküman 27” olmuştur. Bu dokümanla Çin, bilgi teknolojisini bir ekonomik fırsat kaynağı ve aynı zamanda bir güvenlik sorunu olarak ele almıştır. Bu belge ile kritik altyapıların korunması için aktif bir savunma politikası oluşturmak amaçlanmış ve aynı zamanda dinamik gözlemlleme, gelişimi

destekleme, devlet organları ve ekonomik bilgilerin yönetimi grubuyla iş birliği yapmak suretiyle siber güvenlik politikalarını şekillendirmek hedeflenmiştir (Raud, 2016, s.11).

Bilgi teknolojisindeki savunmasızlığını açık bir şekilde anlayan Çin, bu savunmasızlığı azaltmayı amaçlamıştır (Janeliūnas ve Tumkevič, 2020, s.129). 2006 yılında oluşturulan “Bilim ve Teknolojide Gelişim için Orta ve Uzun Vadeli Ulusal Program”da ise 21. yüzyılda bilim ve teknoloji devriminin hızlı bir şekilde ilerlediği ve bu durumun ekonomik ve sosyal görüşlerde köklü değişiklikleri meydana getirdiği belirtilmektedir. Çin’in; bilginin, teknolojinin ve AR-GE çalışmalarının önemli rol aldığı bu dönemde yenilik odaklı bir ülke inşa etmeyi hedeflediği gözlemlenmektedir (Clarke ve Knake, 2011, s.32-33).

2010 yılında yayınlanan Savunma Raporu’nda siber güvenliğin ulusal savunma sisteminde önemli bir yere sahip olduğundan bahsedilmektedir. Bunun dışında, siber alanın gelişmesi ve güçlenmesi için önemli yatırımlar yapılacağı da vurgulanmaktadır. Çin’in siber casusluk yapabilmesi, siber alanda rakip devletlerin verilerine ulaşabilmesi ve ülkelerin internet tabanlı şirketlerinin altyapısına siber saldırılar düzenleyebilmesi, Çin yönetiminin siber alan konusunda önemli bir güce ulaştığını göstermektedir.

2012 yılında, bilgiye erişimde ve bilginin kullanılmasında devletlerin arasındaki rekabetin arttığına dikkat çeken Devlet Konseyi Bilgi Ofisi, “Yeni Politika Görüşü” isimli bir belge duyurmuştur. Çin’in gelişmiş ülkelerle arasında bir eşitsizliğin var olduğu, hükûmetin endüstri alanıyla bilgi paylaşımının düşük seviyede olduğu, teknolojinin yabancıların kontrolünde olduğu, bilgi ve ağ güvenliğinde yetersiz kalındığı ve yeni teknolojinin hızlı bir şekilde büyüdüğü hususlarına değinilmektedir. Bu sorunların çözülmesi ve eksikliklerin giderilmesi için ciddi adımlar atılması gerektiği vurgulanmaktadır (Segal, 2012).

Çin, siber güvenlik konusunda ulusal güvenlik kapasitesini güçlendirmesi ile birlikte rakip ülkeler için risk ve tehdit oluşturabilecek kozlara da sahip olmuştur. Örneğin, ABD Kongresi’nde Amerikalı teknoloji şirketlerine Çin tarafından gerçekleştirilen siber saldırıların tartışmaya açılması ve 2014 yılında ABD’nin Çinli hackerlar tarafından casusluk faaliyetlerinde bulunduğunu vurgulamasıyla Pekin-Washington arasında gerginlikler yaşanmıştır (Göçöğlu ve

Aydın, 2019, s.245). Ayrıca, 2015 senesinde yayınlanan “Beyaz Kitap” adlı raporda da siber uzay konusundan bahsedilmiş ve konunun önemi açık bir şekilde ortaya koyulmuştur (Korhan, 2018, s.61).

Çin’in siber alan ile ilgili hazırladığı bir diğer resmî belge de 2017 yılında uygulamaya konulan Siber Güvenlik Kanunu’dur. Bu kanun ile bilgi teknolojileri vasıtasıyla karşılaşılabilecek tehditlerin engellenmesi ve bireylerin, toplumun, kamunun ve özel kurumların çıkarlarının korunması hedeflenmektedir. Verilerin korunduğu, çalınması veya değiştirilmesine karşılık bazı sistemlerin oluşturulduğu, kanuna aykırı eylemlerde bulunanların ise cezalandırılacağı açıklanmaktadır (Creemers vd., 2018).

Siber güvenlik kanunun ilk maddesi “Hukuk kapsamında siber uzay egemenliğini ulusal, sosyal ve kamu menfaatlerini koruyarak; vatandaşların, tüzel kişilerin ve diğer kuruluşların yasal haklarının ve çıkarlarının korunmasıyla birlikte toplumun bilgilendirilmesini sağlayarak gelişimini temin etmek” şeklindedir (Creemers vd., 2018). Bu ifadeden de anlaşılacağı üzere, devletin bir kurumuna yapılan siber saldırı ulusal güvenliği tehdit ederek devletin tüm kurumlarına ve finans sektörüne zarar verebilir. Dolayısıyla siber güvenliğin sağlanması ulusal güvenliğin tüm alanda sağlanması anlamına gelmektedir. Bu anlamda siber saldırı tehlikesini göz önünde bulunduran Pekin, siber güvenlik tedbirleri ile ulusal güvenliği korumaya çalışmaktadır.

Pekin, siber alana özel ekiplerle ayrı bir önem veren ve bu konuda büyük yatırımlar yapan küresel bir aktördür. Ayrıca Çin, internet yönetiminin hükûmetin kontrolünde olması gerektiğini düşünen bir devlettir. Fakat siber alan, ulus-devletlerle birlikte devlet dışı aktörlerin de yer aldığı bir ortamdır. Bu sebeple Pekin, çeşitli kısıtlamalar getirerek siber alanda gücü elinde tutmaya çalışmakta ve bu konuda gündemde yer almaktadır.

Çin’in siber güvenlik politikası incelendiğinde; kendi milli siber ağlarını kullanarak, uluslararası arenalarda yaygın olan ağları yasaklayarak veya sınırlandırarak güçlü bir savunma mekanizması geliştirdiği görülmektedir. İzlenen bu yol sayesinde somut bir savunma mekanizması kurulamasa da Çin için siber güvenlik konusu batıya göre daha güvenli bir hal almıştır. Buradan da anlaşılacağı üzere siber güvenlik kavramının genel çerçevede Çin için

bağımsızlık kriterini ön plana çıkardığı görülmektedir. Siber güvenlik meselesini aynı zamanda ulusal güvenlik ile eş değer tutan Çin, stratejilerini belirlemeden önce siber güvenliğe yönelik tehditleri belirlemektedir. Bu tehditlerden ilki ulusal güvenliğinin risk altına girmesidir. İkinci tehdit algısı ise rejimin istikrarsızlaşmasıdır. Diğer bir tehdit algısı ise; su, enerji, kamu hizmeti, sağlık, eğitim gibi önemli altyapıların ele geçirilme riskidir. Son tehdit algısı ise ABD'den gelebilecek olası tehlikelerdir. Aslında Çin, dışarıdan gelebilecek her türlü siber tehdide önem vermektedir fakat ABD'nin teknoloji alanındaki etkinliği onu farklı bir yere konumlandırmaktadır. Siber uzaydan gelebilecek tüm bu tehditleri bilen Çin; bu tehditleri ortadan kaldırmak veya en aza indirebilmek için siber güvenlik stratejilerini geliştirmekte ve uygulamaktadır. Askerî, teknolojik, sosyal ve diplomatik alanlarda birçok adım atarak siber güvenlik stratejilerini geliştiren ve bu alanda bağımsızlığını korumayı hedefleyen Çin, siber uzaya yönelik uygulamada tedbirler ve planladığı stratejilerle bu alanda dikkatleri üzerine çeken bir ülke olmuştur.

Hauke Johannes Gierow'un Çin'in batılı ülkelerden farklı olan politikası üzerine yaptığı çalışmaya (2015) göre Çin, siber güvenliği sağlamak için bağımsız internet teknolojisine önem vermektedir. Kendi bilişim teknolojisini üreterek sektördeki lider ülkelerin üstünlüğünü ve baskınlığını azaltarak ulusal egemenliğini bu alanda da sağlamlaştırmak isteyen Çin Devleti, ihracat yapan yerli teknoloji firmalarına da büyük oranda destek vermektedir. Bu firmalar, uluslararası alanda kabul görmüş internet yazılımlarına ve teknoloji donanımlarına karşı alternatif yeni üretimler yapmaktadırlar. Çin'de üretilen akıllı telefonlar ve alternatif akıllı telefonlar için uygulama indirme mağazaları bu konu hakkında önemli örneklerdir. Casusluk faaliyetleri, ülke içi ve ülke dışı bilgi sızdırılması gibi tehditler sebebiyle Çin'de dış ülkeler tarafından üretilen ürünler için de bazı sansürler ve kullanım yasakları da uygulanmaktadır. Ayrıca, Çin'de korsan yazılımların kullanım oranı yüksektir ve bu sebeple bu yazılımlar güncellenerek daha güvenli hale getirilememektedir. Dolayısıyla ülkedeki hackerlık ve siber suç girişimleri artmakta ve bu durum siber güvenliğe zarar vermektedir.

Çin'in siber güvenlik stratejilerini geliştirirken göz önünde bulundurduğu ana unsurlar ABD'ye yönelik güvensizlik algısı ve siber uzayın kontrolsüz

olmasıdır. Bu iki risk, Çin için ulusal güvenlik alanında sorunlar doğurma potansiyeline sahiptir. Ulusal güvenlikteki bozulmalar da Çin için ekonominin zarar görmesi, toplumsal güvenin azalması, rejimin güç kaybetmesi, bölgesel ve küresel itibarın kaybolması gibi olumsuz etkileri doğurmaktadır. Çin, diğer ülkelerden farklı olarak *Facebook* yerine *Renren*, *Google* yerine *Baidu* ve *Twitter* yerine *Sina Weibo* isimli internet platformlarını hizmete sunarak hem ABD'nin kontrolündeki hizmetleri engellemiş hem de siber güvenliğini ve siber egemenliğini bir anlamda sağlamıştır. Bu adımlar Çin için sansür kararlarını da istediği gibi yönetme fırsatı sunmuştur. Böylece Çin, vatandaşlarını da bu alanda belirli bir sınırla konumlandırmıştır. Ayrıca Çin, 2020'nin ocak ayından itibaren *Facebook* ve *Twitter* gibi sosyal medya mecralarını da politikacıların kullanımına sunmuştur. Bu konuyla alakalı Çin Dışişleri Bakanlığı Sözcüsü Geng Shuang şu ifadeleri kullanmıştır: “Pekin yönetimi yurt dışındaki insanlarla daha iyi iletişim kurabilmek ve Çin'in politikalarını daha iyi tanıtabilmek amacıyla *Twitter* ve *Facebook* gibi sosyal medya platformlarını politikacıların kullanımına açmıştır.” (Çin'de Halka Yasak Olan Sosyal Medya, Diplomatların Kullanımına Açıldı”, NTV, 2020).

Çin, başlangıçta siber uzayın küresel yönetimi hakkında kısmen savunmacı bir tutum sergilese de Devlet Başkanı Xi Jinping yönetimi ile birlikte daha etkin bir siber diplomasi kabullenmiştir. Bu diplomasinin üç temel amacı ise internet ve bilgi akışından doğabilecek ve iç istikrara, rejimin meşruiyetine zarar verebilecek tehdidi aza indirmek, siber uzayı şekillendirerek Pekin'in siyasi, askerî ve ekonomik etkisini büyütmek, siber uzayda ABD'nin avantajlarına karşılık Çin'in hareket kabiliyetini artırmaktır (Segal, 2017, s.1). Bu anlamda, Çin'in siber güvenlik ve siber uzay ile alakalı stratejilerini iç ve dış politikada risk olarak gördüğü tehditlerin şekillendirdiği anlaşılabilir.

Sosyalist devlet anlayışını sürdürmesi, ekonomik mevcudiyeti ve potansiyeli, rakiplerinin gücü, ülke nüfusu ve etnik-dini grupların fazla oluşu gibi etkenler göz önünde bulundurulduğunda Çin, ülke içinde ve dışında güvenliğin sarsılması ihtimalini değerlendirmektedir ve siber alanın ülke güvenliğinde yarattığı açığı kapatma arayışına girmiştir. Bu bağlamda 2017 yılından itibaren yürürlüğe giren Çin'in Siber Güvenlik Kanunu'nun ilk maddesinden de anlaşılacağı üzere; güvenlik, ekonomi, kişilik hakları ve sosyal alan gibi unsurlar

için siber güvenliğin sağlanması hükûmet tarafından büyük önem arz etmektedir. Bu maddede geçen ifade, “Kanun kapsamında siber güvenliği sağlamak; siber uzay egemenliğini, yasal egemenliği, ulusal güvenliği, sosyal ve kamu menfaatlerini korumak; vatandaşların, tüzel kişilerin ve diğer kuruluşların hukuka uygun haklarını ve menfaatlerini korumak ve ekonominin ve toplumun bilgilendirilmesine teşvik etmek amaçlanmaktadır” şeklindedir (Creemers vd. 2018). Bir devletin herhangi bir kurumuna karşı gerçekleşen bir siber saldırının ulusal güvenliği krize sokma potansiyeli çok yüksektir ki, Çin’in devlet kurumlarının ve finans sektörünün bazı tarihlerde siber saldırılara maruz kaldığı da görülmüştür (Kshetri, 2013, s.14).

Çin’de internet kullanımının başladığı ilk andan itibaren Çinli politikacılar ve analistler için siber uzay; hem ekonomik büyüme ve iyi yönetim için gerekli hem de iç istikrara ve rejim meşruiyetine yönelik bir tehdit olarak görülmüştür (Segal, 2017, s.3). Bu sebeple Çin Komünist Partisi (ÇKP), olası bir siber saldırının Çin toplumunda partiye karşı güvensizlik duygusu oluşturacağından ve bunun da rejimin devamlılığına olumsuz tesir edeceğinden endişe duymaktadır.

Çin’deki siber güvensizlik algısının bir diğer sebebi ise kritik altyapı sistemlerinin tehlikeye girme riskidir. Devletler nezdinde çok kritik altyapıları korumak için geleneksel güvenlik yöntemlerinin yetersiz kaldığını fark ederek gelişen teknolojilerle birlikte siber güvenlik konusunda da atılımlar gerçekleştirilmiş ve farkındalıkları artmıştır (Göçoğlu ve Aydın, 2019, s.237). Çin de Siber Güvenlik Kanunu’nun 3/31. maddesinde; iletişim, bilgi hizmetleri, enerji, trafik, su kaynakları, ekonomi, kamu hizmeti, e-devlet ve diğer tüm kritik bilgilere sahip alt yapıların siber güvenlik sistemleriyle korunduğu belirtilmektedir. Aynı şekilde bu kanunda, altyapılarda yaşanan sıkıntıların veya herhangi bir veri sızıntısının; ulusal güvenliği, kamu yararını, toplumun refahını ve ihtiyaçlarını tehlikeye sokabileceği de belirtilmektedir (Creemers vd., 2018).

Kritik bilgi altyapılarının korunmasına ayrı bir önem veren Çin yönetimi, Kamu Güvenliği Bakanlığı ve Sanayi ve Bilgi Teknolojisi Bakanlığı gibi farklı kurumlara da bu konuyla alakalı görevler vermiştir. Fakat Çin’in kritik bilgi altyapılarını koruma amacına ve bu konudaki çabalarına rağmen zorluklar ile karşılaşma ihtimali vardır çünkü siber alan günden güne gelişmekte ve değişmektedir.

Çin'in siber güvensizlik algısının sebeplerinden birisi ise ABD'ye karşı olan güvensizliktir (Raud, 2016, s.7). Bu bağlamda Çin, siber egemenlik isteğini uluslararası alana taşıyarak siber güvenlik stratejisinde ayrı bir kulvar açmıştır. Dünya üzerinde bulunan 13 ana sunucunun 10 tanesi ABD'dedir ve tüm sunucular ABD'nin merkezinde olan İnternet Tahsisli Sayılar ve İsimler Kurumu'nun kontrolündedir. Çin, internetin Los Angeles merkezli bir kuruluş olan ICANN tarafından yönetilmesinin ABD istihbaratına ve ABD'nin çıkarlarına hizmet ettiğini düşünmektedir (Baezner, 2018, s.3). Bu durum Çin'in yinelediği siber egemenlik fikrinin de güçlenmesine yol açmaktadır (Balke, 2018, s.141). Çin İnternet Veri Merkezi Kurucu ve Başkanı Hu Yanping'in kullandığı "Çin'in internet endüstrisi ABD'nin elinde koşuyor" (CCVT, 2013) ifadesi de Çin'in bu konudaki tavrını ortaya koyan söylemlerden biridir.

4. BÖLÜM

SİBER REKABETTE FARKLI BÖLGE: ORTADOĞU

Ortadoğu bölgesi, sahip olduğu ekonomik, sosyal, kültürel ve siyasi unsurlar sebebiyle tarih boyunca dünya meselelerinde son derece kritik bir önemi haiz olmuş bir bölge olarak karşımıza çıkmaktadır. Dünya hidrokarbon kaynaklarının çok büyük kısmına sahip, kutsal mekânları barındıran, tarih boyunca önemli olmuş ve önemli olmaya devam eden ticaret güzergâhlarının kavşak noktasında bulunan bu bölge, günümüzde de stratejik önemini muhafaza etmektedir. Özellikle son dönemlerde ekonomik, sosyal ve siyasi öncelikler ışığında bölgede yaşanan değişim ve gelişmeler, küresel ve bölgesel aktörlerin tüm dikkat ve gayretini üzerinde toplamıştır.



Şekil 2: Ortadoğu

Kaynak: <https://www.britannica.com/place/Middle-East>

Bölgenin sahip olduğu bu kritik önem, dünyanın başat güçlerinin de tüm gayret ve imkânlarını Ortadoğu'dan maksimum çıkar elde edebilmek için seferber etmelerine sebep olmaktadır. Bu imkânlar zaman zaman askerî, ekonomik, siyasi veya teknolojik olarak bölgeye yansımaktadır. Özellikle teknolojik gelişmeler ve buradan hareketle internet alanının genişlemesi ve küreselleşme, güçlerin rekabetini sıcak çatışmaların yanı sıra siber alana da taşımış durumdadır.

Özellikle son yıllarda ABD ile Çin arasındaki siber çalışmalarda da kendisini göstermiş; bahsi geçen iki ülke küresel etkiler de yaratacak şekilde karşı karşıya gelmiştir. Öte yandan Ortadoğu'nun jeopolitik, jeostratejik ve jeoekonomik önemi göz önünde bulundurulduğunda, bölgede oyun kurucu isteyen ABD ve enerji ihtiyacının yanı sıra bölgedeki ticareti domine etmek isteyen Çin'in siber alandaki mücadelesini buraya da taşımaktadır. ABD ve Çin tarafından siber güvenlik, bölgedeki aktörleri etkilemek için kullanılmaktadır. Bu bağlamda söz konusu rekabeti, son dönem gelişmeler ışığında mücadelenin en fazla görüldüğü ülkeler olan İsrail, İran ve Körfez bölgesi bağlamında ele almak, konunun anlaşılmasına yardımcı olacaktır.

4.1. İsrail ve İran Bağlamında Rekabet

ABD ve İsrail'in ilişkileri birçok alanda iyi olarak değerlendirilmektedir. 1950 sonrası dönemden itibaren İsrail'in Ortadoğu'da ABD'nin en iyi müttefiki olduğu bilinmektedir. Söz konusu iki ülkenin bölgedeki güvenlik çıkarları, bu ülkelerin yakınlaşmasını ve birlikte hareket etmesini beraberinde getirmiştir. ABD-İsrail ilişkileri sadece geleneksel güvenlik noktasında değil farklı alanlarda da ilerleme kaydetmiştir. İkili arasında gelişen istihbarat ilişkileri neticesinde teknoloji alışverişi artmıştır. Bu teknoloji alışverişi ve buradan hareketle siber alan ilişkileri ise bölgede etkisini göstermektedir.

Teknolojinin gelişmesi ile birlikte savaş teorisi ve savaş stratejileri de şekillenmiştir. Ortadoğu'da oyun kurucu olmak isteyen ABD ve ABD'nin hamisi olduğu İsrail, kendi çıkarları doğrultusunda dengeli politikalar izleyerek istihbarat paylaşımında bulunmaktadırlar. Öte yandan ABD'nin iç siyasetinde Yahudi lobisinin yadsınamaz bir etkisi vardır. İsrail açısından da Ortadoğu coğrafyasındaki çıkarlarına ulaşma noktasında ABD'nin desteği büyük bir önem arz etmektedir. Hem teknoloji alanında hem de Ortadoğu'da güçlü olan bu iki ülke bölgede varlıklarını korumak ve çıkarlarını sağlamak amacıyla birlikte hareket etmektedirler.

Kurulduğu tarihten bugüne kadar İsrail, dış politikada adımlarını güvenlik endişeleri çerçevesinde atmaktadır. Bu noktada güvenlik garantörü olan ABD ile aynı düzlemde hareket eden İsrail, teknoloji ve siber güvenlik alanlarında Washington yönetiminin de desteği ile kendini geliştirmekte ve bölgede varlığını

sürdürmektedir. İsrail, bu bağlamda tehdit algısının temel motivasyon olmasının etkisi ile siber güvenlik konusunda attığı adımlar neticesinde kendini koruma gayretinin yanı sıra diğer devletler ile siber güvenlik ticaretini de geliştirerek uluslararası arenada var olmayı hedef olarak benimsemiştir. İsrail Devleti'nin en büyük siber güvenlik firması olan CyberArk'ın İcra Kurulu Başkanı Udi Mokady'nin "İsviçre saatlerini İsviçre'den ve bilgi güvenliğini İsrail'den aldığınızı herkes anlıyor" ifadesi İsrail'in konuya ilişkin iddiasını ortaya koymaktadır (So, 2014).

İsrail'in siber güvenlik endüstrisi, 2020 yılında sektördeki küresel yatırımların %31'ini oluşturmakla birlikte, ülkeyi ABD'den sonra ikinci sırada konumlandırmıştır. Bu bağlamda İsrail, siber güvenliği geliştirmeye adanmış yüzlerce şirket ve düzinelerce araştırma ve geliştirme girişimi neticesinde ABD'den sonra en büyük ikinci siber ürün ve hizmet ihracatçısı olarak karşımıza çıkmaktadır. İsrail İhracat Enstitüsü verilerine göre, İsrail'den yapılan toplam siber güvenlik ihracatının 2021'de 11 milyar dolar olduğu tahmin edilmektedir. 100'den fazla anlaşmada 8,8 milyar dolarlık rekor bir artış sağlayan İsrail 2021 yılı için bir rekora imza atmıştır (Ben-David, 2022). Öte yandan siber istihbarat kapasitesi güçlü olan İsrail, küresel alanda var olan en önemli siber casusluk ürün ihracatçısı ülkelerden biri konumundadır.

Konuya ilişkin İsrailli bir şirketin satışını sağladığı bir siber casusluk yazılımı küresel düzeyde ciddi bir etki yaratmıştır. İsrail'in en bilinen siber casusluk ve teknoloji şirketi NSO Group tarafından geliştirilen ve siber silah pazarına hâkim konumunda olan dijital casusluk programı olan *Pegasus*, hedef alınan kişinin tıklamasıyla veya hiçbir eylem olmaksızın; cep telefonlarının mesaj, konum ya da mikrofon gibi özelliklerini ele geçirmeyi ve bu şekilde takip edilmesi amaçlanan kişinin kişisel hayatına girerek program sahibi için istihbarat toplamayı sağlamaktadır (Kirchgaessner vd., 2021). Dünyanın en güçlü siber silahı olarak tanımlanan (Bergman ve Mazzetti, 2022) yazılımın, abonelik yöntemi ile 45 ülkede kullanımda olduğu araştırmalar sonucunda ortaya koyulmuştur. ABD ile ortak bir düzlemde hareket eden Tel Aviv, söz konusu yazılımı Rusya, Çin ve İran'a satamamaktadır ve hatta bazı çalışmalarda yazılımın, bu ülke sınırlarına girdiği anda andan itibaren kendini imha etme (self-destruction) özelliğine sahip olduğu ifade edilmiştir (Çahmutoğlu, 2021). Benzer şekilde ABD'ye de satılmadığından kendi içinde ABD'nin yazılımı kullanamamasından dolayı NSO

Group, FBI için Pegasus'un farklı bir versiyonunu geliştirmiştir (Kirchgaessner, 2022). ABD için özel olarak geliştirilen ve Çin'e satılamayan bu yazılım, ülkenin siber güvenlik notasında ABD'ye olan bağlılığının bir göstergesi olarak kabul edilebilecektir.

Washington yönetimi, 2021 yılının Kasım ayında Pegasus'u, kullanmaktan vazgeçmesinin de ötesinde NSO'yu ulusal güvenliğe ve ABD'nin dış politika önceliklerine aykırı eylemler nedeniyle kitle imha silahları üretme çabasında olabilecek ülkelere ve diğer kuruluşlara satış yapılmasını engellemek için tasarlanan ancak sonrasında siber silah şirketlerini de içermeye başlayan bir tür kara listeye dâhil etmiştir ("ABD, Pegasus casus yazılımını geliştiren İsrail şirketi NSO Group ile ticareti yasakladı", BBC News Türkçe, 2021). Bu doğrultuda ABD'li şirketlerden bundan sonraki süreçte kritik parçaları temin edemeyecek olan İsrailli şirket, abonelerine hizmet vermeyi sürdürmek noktasında ihtiyaç duyduğu Amerikan teknolojisine erişimi olmadan işleyemez hale gelme tehlikesi ile karşılaşmıştır. Öte yandan şirketin geleceği hususunda kaygılı olan İsrailli yetkililer, NSO'nun iflasının Çin ve Rusya'nın kendi casus yazılımlarını başka ülkelere satarak bu alandaki nüfuzlarını genişletebileceklerine yol açacağı konusunda Washington yönetimini uyarmıştır (Bergman ve Mazzetti, 2022).

Söz konusu iki müttefikin Ortadoğu'daki ortak şekilde hareket ettiğinin bir diğer göstergesi, İran'a yönelik gerçekleştirilen siber saldırılar olmuştur. İsrail'in ABD ile birlikte oluşturduğu iddia edilen "Stuxnet virüsü" aracılığıyla İran'ın nükleer tesislerine saldırmış ve fiziki hasar meydana getirmiştir (Nakashima ve Warrick, 2012). Bu olayla birlikte 2010 yılından itibaren İsrail siber güvenlik stratejisinin gelişmesi de büyük bir önem arz etmiştir. Tel Aviv yönetiminin gerçekleştirdiği bu saldırı sonrası İran'ın nükleer programının büyük bir zarara uğradığı öne sürülmüştür. Aynı zamanda bu saldırı, siber imkânlarla fiziki hasar yaratılabileceğini gösteren ilk siber saldırı olması hasebiyle büyük bir öneme sahiptir (Darıcı, 2021).

İran nükleer santrallerini hedef alan ve 21. yüzyılın en kritik siber saldırısı olarak kabul gören Stuxnet saldırısı bulgulara göre İran'ın Natanz nükleer yakıt zenginleştirme tesislerindeki bilgisayar ağına düzenlenmiştir. Bu saldırının ardından sadece bir ülke değil birçok ülke etkilenmiş ve siber güvenlik ile alakalı küresel çapta bir iş birliği gerekliliği dikkat çekmeye başlamıştır. Siber saldırının

geleneksel silahlarla yapılan saldırılar kadar şiddetli bir fiziki zarar meydana getirebileceğinin anlaşıldığı Stuxnet saldırısından sonra herhangi bir can veya mal kaybı yaşanmamış ancak böylesine bir saldırının meydana getirebileceği etkiler gözler önüne serilmiştir. Saldırının ardından ABD, dahli olduğuna dair resmî beyanda bulunmasa da virüsün yazılımı ve kullanımı ile alakalı rolü olduğunu da yalanlamamıştır. İran Sivil Savunma Kurumu ise bir açıklama yaparak Stuxnet virüsünün nükleer santrallerden aldığı bilgileri nereye rapor ettiğinin peşine düştüğünü ve bu adresin ABD'nin Texas eyaletinde olduğunu tespit ettiklerini belirtmiştir. Aynı zamanda birçok bilişim uzmanı da bu saldırıyı ABD ve İsrail'in birlikte gerçekleştirdiğini iddia etmiştir (Valeriano ve Maness, 2015, s.151). Saldırıda kullanılan virüs, sistemlere her 100 milisaniyede bir komut göndererek çok yüksek hızda frekans değişimi gerçekleştirmiştir. Bu durum incelendiğinde, virüsün sadece uranyum zenginleştirme sürecini veya tesisleri sabote etmek amacıyla değil aynı zamanda tüm çalışmaları sekteye uğratmak amacıyla da geliştirildiği ortaya çıkmıştır (Çelik, 2013, s.148).

İran Araştırmaları Merkezi uzmanları tarafından geçtiğimiz yıl yayımlanan “İran’ın Siber Gücü” raporunda, 2010 yılını bir dönüm noktası olarak kabul eden İran’ın ABD ve İsrail’in siber saldırılarıyla karşılaşması sonucu siber saldırı yeteneklerini artırdığı belirtilmiştir. Raporda, Stuxnet saldırısından sonra İran’ın siber altyapı ve bilgi teknolojileri için çalışmalarını artırdığı, siber saldırı kapasitesini değerlendirmeye başladığı ve siber çalışmalara daha fazla ağırlık verdiği açıklanmıştır. Raporda aynı zamanda ABD yaptırımları sebebiyle İran’ın internet altyapısına katkı sağlayan yabancı şirketlerin tekrar İran ile iş birliği yapmamasından dolayı İran’ın yerel şirketlerle bu boşluğu doldurmaya çalıştığı aktarılmıştır. Öte yandan; Google, WhatsApp gibi uygulama ve internet platformlarının casusluk faaliyetleri için birer tehdit olduğu belirtilerek yerli internet çalışmalarının sebebi olarak uluslararası internet ağının istihbarat servisleri tarafından oluşturulduğu inancı da vurgulanmıştır. Son olarak raporda, İran’ın ABD, İsrail ve Suudi Arabistan’a yoğunlaşan siber saldırılarına da yer verilmiştir. Ayrıca, 2010 yılından bugüne kadar siber kapasitesini güçlendiren İran’ın ülke içinde de muhalif kişi ve gruplara karşı birtakım faaliyetleri olduğu raporda belirtilmiştir (Gürer, 2021).

Ulusal siber güvenliği ve internet ağını geliştirme yönünde çalışmalara ağırlık veren İran, maddi kaynaklarının da el verdiği ölçüde çabalarını sürdürmektedir. Bu bağlamda Tahran, bilgi/iletişim altyapısını geliştirmek amacı ile 2010 yılından beri pek çok kez Huawei ve ZTE gibi Çin'in öne çıkan şirketleri ile iş birliği yapmıştır. Çin'in en büyük ikinci telekomünikasyon ve bilgi teknolojisi şirketi olan ZTE, İran'ın ulusal bilgi altyapısına uzun bir süredir yatırım yapmaktadır. Örneğin, 2012 yılında, İran'ın telekomünikasyon ve internet altyapısını kontrol eden İran Telekomünikasyon Şirketi (Telecommunication Company of Iran-TCI) ile ZTE arasında 130 milyon dolar değerinde bir anlaşma yapılmıştır. Ortaya koyulan belgeler ışığında İran'ın ZTE'den mobil cihazlar üzerinden teknik takip ve gözetim amaçlı sistemler satın aldığı ve İran'a satılan ürün ve yazılımların çoğunluğunun ABD'li şirketlere ait olduğu ifade edilmiştir (Stecklow, 2012).

İran'ın internetin kontrolünü sağlamak üzere uluslararası bir ağdan tamamen ayrıştırılmak suretiyle bir internet ağı oluşturmak için ortaya koyduğu Ulusal Bilgi Ağı Projesi'ne yönelik çalışmalarında Çin'den önemli oranda yardım aldığı ve almaya devam ettiği düşünülmektedir. Somut bir örnek olarak, 2015 yılının Haziran ayında İran Bilgi ve İletişim Teknolojileri Bakanlığı ile Çinli yetkililer arasında söz konusu projenin genişletilmesi ve tamamlanmasına ilişkin iş birliğinde karar kılınmıştır (Islamic Republic of Iran Ministry of I.C.T., 2015). 2020 yılında ise İran'ın Çin ile yaptığı 25 yıllık taslak anlaşma kapsamında İran'ın Ulusal Bilgi Ağı Projesi'ne ilişkin çalışmalarının Çinli şirketlerin katkıları dolayısıyla yürütüleceği belirtilmiştir (Esfandiari, 2020). Buradan hareketle söz konusu iki ülke arasında internet ve bilgi teknolojileri konusunda iş birliğinin hat safhada olduğunu ve ilerleyen dönemlerde daha da gelişme imkânı barındırdığını söylemek yanlış olmayacaktır.

Bölgeyi ilgilendiren bir diğer gelişme yukarı belirtilen İran ve Çin arasında uzun zaman süren müzakereler sonucu imzalanan ticaret, yatırım ve savunma konularını içeren 25 yıllık taslak anlaşmasıdır. Pekin ve Tahran yönetimleri arasında imzalanan söz konusu anlaşma, ABD'nin baskılarına karşı İran'a daha çok hareket etme kabiliyeti sağlamıştır. ABD Başkanı Joe Biden, İran ve Çin arasındaki güçlü iş birliğine ilişkin yıllardır kaygı duyduğunu belirtmiştir. ABD de ortaya koyduğu yaptırımlarla İran ile olan hemen hemen bütün ticareti

engellemişken ekonomisi hızlı bir şekilde yükselişte olan Çin ise dünyada İran petrolünü en çok ithal eden ülke durumundadır.

İran ve Çin arasında farklı birliktelikler farklı konularda da ABD'nin dikkatini çekmektedir. İki ülke aynı zamanda ortak askerî tatbikatlar da yapmaktadır. Hint Okyanusu'nda Rusya ile birlikte yapılan ortak tatbikat bunlardan biridir. Aynı zamanda iki ülke arasında Tahran'ın ABD insansız hava araçları (İHA) ve insani istihbarat ağı ile alakalı Pekin'e önemli bilgiler sağladığı düşünülen bir iş birliği de gündemde yer almaktadır. Buna göre İran kendi sınırları içerisinde düşen ABD menşeli İHA'daki (RQ-170) ileri teknolojiyi kopyalamaktan ve kullanmaktan yoksun olduğundan Çinli yetkililerin aracı inceleme talebinde bulundukları ifade edilmiştir (Wiseman, 2011).

Bu anlaşma ile dünyanın en büyük gücü olma yarışında ABD'ye karşı atılımlar yapan Çin'in dünyada farklı ülkelerde yatırım yapma ve Çin etkisini büyütme amacıyla ortaya koyduğu Kuşak Yol Projesi'ne İran da dahil olmuş olacaktır. Öte yandan bazı medya kuruluşları tarafından bu anlaşma sayesinde Çin'in İran'a 25 yıl içerisinde toplamda 400 milyar dolar değerinde yatırım yapacağını belirtilmiştir (Daragahi, 2021).

Üzerindeki baskılar ve yaptırımlarla birçok sıkıntı yaşayan İran için ciddi bir fırsat niteliğinde olan bu anlaşma kapsamında yapılacak iş birlikleri ile alakalı; tarım, su kaynakları, sulama ve çevreyi koruma çalışmaları öne çıkmaktadır. Aynı zamanda finans, telekomünikasyon, ulaştırma ve altyapı projeleri ile maden, doğal gaz ve petrol gibi sektörler, nükleer enerji santralleri, uzay araştırmaları, teknolojik transferler ve eğitim konuları da anlaşmada göz çarpan alanlardır (Kalaycıoğlu, 2021).

Çin Dışişleri Bakanı Vang Yi ve İran Dışişleri Bakanı Muhammed Cevad Zarif tarafından imzalanan anlaşma kendilerinin açıklamalarına göre 25 yıllık bir stratejik ortaklığı içermektedir. Çin'in Kuşak Yol Projesi'nin de bir parçası olan bu anlaşma ile Çin küresel gücünü artırmayı hedeflemektedir. Bu stratejik ortaklığın Ortadoğu'yu nasıl etkileyeceği de anlaşmadan sonra gündeme gelen konuların başında gelmektedir. Yaptırımlar ile boğuşan ve bu anlaşma ile güç kazandığını düşünen İran ve yine bu anlaşma sayesinde özellikle bahsi geçen proje kapsamında yarar sağlayan Çin'in dışında birçok küçük ve yoksul ülke

başlangıçta avantajlı gördükleri bu anlaşma imzalandıktan sonra bir takım tereddüde de kapılmışlardır. Aslında İran'ın da bu anlaşmada farklı bir konumu bulunmaktadır çünkü Çin ile bir anlaşma yapılması ABD-İran çekişmesini de etkileyecektir.

Nükleer faaliyetlerde bulunan İran'ın bu çalışmalarını sınırlandırmak amacıyla 2015 yılında İran ve BM Güvenlik Konseyi'nin (BMGK) beş daimî üyesi olan ABD, Çin, İngiltere, Rusya ve Fransa ile Almanya arasında nükleer anlaşma yapılmıştır. Anlaşma, İran zenginleştirilmiş uranyum üretimi ve saklama kapasitesine sınır getirmeyi, tesislerinin denetlenmesine izin verilmesini ve tavsiyeler üzerine tesisleri modifiye edilmesi veya tamamen kapatılmasını kapsamaktaydı. Dönemin ABD Başkanı Trump ise 2018 yılının Mayıs ayında, anlaşmanın İran'ın balistik füze programını kapsamayarak cılız kaldığı gerekçesiyle diğer ülkelerin tüm itirazlarına rağmen anlaşmadan çekilmiştir. "Kapsamlı Ortak Eylem Planı (KOEP)" adıyla anılan İran'ın nükleer faaliyetlerini düzenleyen anlaşmaya geri dönüşmesi için müzakereler halen devam etmektedir. İran ile nükleer faaliyetlerinde bulunduğuna yönelik şüphelere sahip bölge ülkeleri arasında son zamanlarda tansiyon yükselmiş durumdadır. Öte yandan, Tel Aviv yönetiminin, olası bir durumda ordunun İran'ın nükleer tesislerine saldırı düzenlemek için hazır bulunması için 1,5 milyar dolar ayırdığı ifade edilmektedir. İran ve Biden yönetimlerince ABD'nin anlaşmaya yeniden katılması istenmekteyse de İsrail, İran'ın nükleer silah sahibi olmasına izin vermeyeceklerini ifade etmektedir ("İran nükleer anlaşması nedir ve tekrar yürürlüğe girer mi?", BBC News Türkçe, 2021). Bu bağlamda İsrail'in Washington üzerinde etkili olup olmadığı sorusu akıllara gelmektedir.

Öte yandan KOEP taraflarından Çin'in Tahran yönetimi ile stratejik ortaklık yaparak petrol satışlarından büyük avantaj elde etmesi, yaptırımlar sebebiyle zarara uğrayan ekonomisi için önemli bir etkidir ancak anlaşmanın İran için bir diğer boyutu da ABD karşısında daha fazla avantaj elde etmesi anlamına gelmektedir. ABD Başkanı Biden da kendinden önceki iki yönetimde de olduğu gibi dış politikanın merkezini Ortadoğu ekseninden kaydırmak istese de bölge, ABD'nin çıkarları doğrultusunda önem verdiği birçok unsuru barındırmaktadır. Bu unsurlardan birinin İran olduğu düşünüldüğünde, ABD'nin bölgeden uzaklaşması pek mümkün görünmemektedir. ABD bölgeden

çekilmemiştir ancak bu minvalde ileriye yönelik de bir adımda bulunmamıştır. Buna karşılık ABD'nin artık güç kaybettiğine inanan Çin ise kendisini dünyanın yeni gücü olarak değerlendirmekte ve dolayısıyla Ortadoğu'yu da göz ardı etmemekle birlikte, bölgenin potansiyelini kendi lehine kullanmaya çalışmaktadır. Buradan hareketle İran ve Çin arasındaki iş birliğinin İran'a kıyasla uzun vadede Çin'e sağlayacağı fayda bakımından önemli olduğu söylenebilecektir.

4.2. Körfez Bölgesi Bağlamında Siber Rekabet

Uzun yıllardır devam eden ABD-Körfez ülkeleri ilişkileri, zaman zaman sorunlar yaşansa da son dönemlerde artan bir ivme ile devam etmektedir. Bölgenin coğrafi konumu, sahip olduğu hidrokarbon kaynakları ve bu kaynakların özellikle Suudi Arabistan, BAE ve Katar'a sağladığı ekonomik üstünlükler bölgeyi ABD için daha da cazip hale getirmektedir. Öte yandan söz konusu ülkeler için monarşik rejim, rantiyer ekonomi sistemleri dolayısıyla enerji gibi unsurların güvenliği en kritik meselelerdir ve ABD Körfez ülkelerinin ihtiyaç duyduğu güvenlik açısından birincil partner olarak karşımıza çıkmaktadır. Bu noktada, özellikle Suudi Arabistan ve BAE'nin gelişmeleri öncelikli olarak ABD ile istişare ettiği görülmektedir. Örneğin, Yemen'deki İran destekli Husilerin 17 Ocak 2022 tarihinde balistik füze ve İHA'lar aracılığı ile başkent Abu Dabi'deki bazı hedeflere yönelik saldırılar düzenlemesi sonucunda BAE Dışişleri Bakanı Abdullah Bin Zayed, ABD Dışişleri Bakanı Anthony Blinken ile telefonda görüşmüş; yakın zamanda terör örgütü listesinden çıkarılan Husilerin tekrar terör örgütü olarak tanınmasını istemiştir (Ravid, 2022).

2010 yılına kadar ABD, istikrarlı bir şekilde Körfez ülkelerinin siyasi istikrar ve toprak bütünlüğü açısından en önemli güvenlik garantörü olarak gözlemlenirken bu tarihten sonra Körfez politikasında farklılaşmaya başlamıştır. Kaya gazı üretimiyle Körfez'deki enerji kaynaklarına bağımlılığı ortadan kaldıran ABD için Körfez bölgesi, önceliğini kaybetmeye başlamıştır (Acar, 2021). Ancak 14 Eylül 2019 tarihinde günlük ham petrol üretiminde dünya lideri olan Suudi Aramco'nun ülkenin doğusunda yer alan Bıkayk ve Hırayıs beldelerindeki petrol işletme tesislerine yönelik olarak gerçekleştirilen saldırılar sonrası, küresel petrol piyasaları adeta sarılmıştır. Küresel petrol üretimin %5'lik kısmını tek başına sağlayan bu bölgede yaşananlar sonrasında ham petrolün fiyatı %20 artmak suretiyle 72 dolar seviyelerine yükselmiştir (Eberhart, 2019). İran'ın suçlandığı

ancak herhangi somut bir delil ortaya konulamayan bu hadise sonrasında ABD'den yüzlerce milyar dolar karşılığında satın alınan güvenlik sistemleri Suudi Arabistan ve diğer İran karşıtı bölge ülkeleri için hayal kırıklığı yaratırken, ABD Suudi Arabistan'daki askerî varlığını artırma kararı almış; Suud Krallığı'na bir Patriot bataryası, dört Sentinel radarı ve yaklaşık 200 ABD destek personelinin konuşlandırılacağını ifade etmiştir. 200 askerle birlikte toplamda yaklaşık 3 bin askerî Krallık'ta konuşlandıran ABD, korumayı güçlendirmek için ek destek olarak da 2 Patriot bataryası ve bir Terminal Yüksek İrtifa Alan Savunma Sistemi'ni göndermeyi onayladıklarını duyurmuştur. ABD'nin "ortaklıklarına bağlılık" göstergesi olarak yaptığı bu destekleri çok geçmeden geri çekme kararı alması, başta Suudi Arabistan olmak üzere diğer ABD ortaklarının da "ortaklıkları çeşitlendirme" politikasına yönelmesinin önemi vurgulamaktadır. Ancak Irak ve Afganistan'dan sonra Körfez'den de çekilme senaryoları gündem de olsa da bölgenin enerji sektöründeki etkinliği, coğrafi avantajları ve İran tehdidi de dikkate alındığında ABD'nin tam anlamıyla bir çekilme sağla(ya)mayacağı ve Rusya, Çin gibi aktörlerin bölge nüfuz oluşturma ihtimallerini engelleme çabasında bulunacağı söylenebilecektir.

Ekonomisini çeşitlendirme politikalarına ağırlık veren rantiyer bölge devletleri arasında ortaklıkların çeşitlendirilmesi politikaları BAE ve Suudi Arabistan'a nazaran en çok Katar'da gündemde yer almaktadır. Özellikle, Suudi Arabistan, BAE ittifakına eklemlenen Mısır ve Bahreyn'in beklenmedik biçimde Katar'ı terörizmi finanse etmekle suçladıkları Katar ile tüm diplomatik ilişkilerini kesmesi ve hava sahalarını başkent Doha'ya kapatmaları ile başlayan ve 3,5 yıl boyunca süren Körfez krizinin, Katar'ın söz konusu politika üzerinde yoğunlaşmasında etki yarattığını söylenebilecektir.

ABD'nin Körfez ülkeleri ile kurduğu/kurmaya çalıştığı ilişkiler güvenlik üzerine iken, Çin ise ilişkilerini ticari ve ekonomik olarak kurmakta/kurmaya çalışmaktadır. Bu bağlamda ABD, bölgede yaşanan gelişmelerde siyasi ve askerî söylem ve eylem bazında aktif bir rol almaktadır. Örneğin, 2017 tarihli Körfez krizinde ABD, taraflar arasındaki gergin ABD'nin krizde bir taraf tutması durumu rakip güçleri kazançlı çıkaracağından ve Katar'da sahip olduğu askerî ayrıcalıkları ve bölgede krize kadar devamlılık arz etmiş iş birliklerinin tehlikeye girmesi ihtimalinden çekinerek arabulucu bir rol üstlenmeye çalışmıştır. Rakiplerini

izole etme politikası ile baskılamaya çalışan ABD, Ortadoğu'daki en büyük ABD askerî üssüne ev sahipliği yapan Katar'ı da dikkate almış ve krize karşı daha dengeli bir politika izlemiştir.

Körfez ülkeleri üzerinde herhangi bir garantörlük iddiası olmayan Çin ise bölgede ilişkilerini tamamen kazan-kazan politikası üzerinden kurmaktadır. Çin, gelişmekte olan ekonomisi dolayısıyla enerji ihtiyacının günden güne artması, küresel bir atılım yaparak ortaya koyduğu Bir Kuşak Bir Yol Projesi'nin sıkıntısız işlemesi doğrultusunda bölge ülkeleri ile yaşanan mücadelelerden bağımsız olarak ilişkiler geliştirmektedir. Özellikle son on yıl içinse Çin bölgeye yönelik faaliyetleri, enerji güvenliğinin sağlanması, ABD ile rekabet edilebilirlik ve bölgede stratejik bir güç olarak konumlanma amacı taşımaktadır. Yine örneklandırmek gerekirse; Çin, en büyük petrol tedarikçisi ve ikinci en büyük doğal gaz tedarikçisi olan Körfez ülkeleri arasında yaşanan Körfez krizinde yaşananları diğer ülkelerin "iş meseleleri" olarak görmek suretiyle krizin çözümü noktasında diyalog ve müzakere yanlısı bir tutum benimsemiştir. Pekin yönetimi, Ortadoğu'daki en büyük ticaret ortağı ve petrol müşterisi olduğu Suudi Arabistan, Çin malları için bölgedeki en büyük Pazar olan BAE, Katar sıvılaştırılmış doğal gaz (LNG) tedarikçisi Katar (Al-Tamimi, 2017) arasında bir tercih yapmaktan kaçınmıştır. Resmî Çin verilerine göre bakıldığında ise Körfez İşbirliği Konseyi (KİK) piyasaları, Pekin'in Ortadoğu'ya yaptığı toplam ihracatın %46'sını oluşturmaktadır. Diğer bir ifadeyle Körfez, Çin için büyük ölçüde ticari ve ekonomik temelli olarak güvende tutmak istediği bir bölgedir ve bahsi geçen ülkeler, Pekin yönetiminin Ortadoğu'daki ekonomi politikalarının olmazsa olmaz bir parçası olmaya devam etmektedir. Mesele Katar bağlamında değerlendirilecek olursa; Çin ile Katar arasında doğrudan doğruya siber güvenlik açısından belirgin bir iş birliği gözlemlenmese de söz konusu ülkelerin ticari ilişkilerinin bu alana da yansımalarının muhtemel olduğu söylenebilecektir.

Katar gibi ortaklıları çeşitlendirme politikası doğrultusunda hareket eden BAE, yakın zamanda Çin menşeli bir gemicilik ve lojistik hizmeti şirketi olan COSCO ülkenin kuzeyindeki el-Halife Limanı'nda 35 yıllık süre için bir konteyner terminali geliştirme ve işletme noktasında anlaşmaya varmıştı. Biden, uydu görüntüleri üzerinden yapılan araştırmalar sonrasında, Çin'i limanda gizli faaliyetlerde bulunarak askerî bir yerleşke kurmaya çalıştığının öne sürerek BAE

Veliaht Prensi Muhammed bin Zayed el-Nahyan ile yoğun şekilde görüşmeler gerçekleştirmiş ve yönetimi konuya ilişkin olarak ikaz etmiştir. Yaklaşık olarak 300 milyon dolarlık bir değere sahip bu anlaşma sonrası başlayan inşaat çalışmaları, ABD'nin tüm baskı ve çabaları neticesinde durdurulmuştur.

Birincil partner ABD, uzun yıllar Körfez bölgesinde müttefiklerinin Pekin yönetimi ile ileri teknoloji ve savunma sanayisi alanlarında iş birliği yapmasına şiddetli biçimde karşı çıkmıştır. Ancak yaşanan gelişmeler ile birlikte gelinen son noktada Washington yönetiminin dış politika adımlarının tahmin edilemez oluşu, kendini güvende hissetmeyen ABD müttefiki ülkeler için alternatif iş birliği kapılarını çalma durumunu gündeme getirmektedir. Çin'in uzunca bir süredir İran füze programına destek verdiği bilinmesine rağmen Riyad yönetimi de Tahran gibi savunma sanayi alanında Pekin'e yönelmek durumunda kalmıştır. Bu durum, ABD'nin Körfez'de sarsılmaz üstünlüğünün ilerleyen dönemlerde riske girme ihtimalini ortaya koymaktadır. Biden yönetiminin kararı ile bölgeden çekilmeye yönelik adımlar, Çin nezdinde ABD'nin çekilmesi ile oluşan boşluğu bir fırsat olarak değerlendirmek şeklinde Körfez'e yansıyabilecektir. Bu bağlamda Çin'in bölge için alternatif partner olduğunu geliştirmekte olduğu siber güvenlik çalışmaları ile desteklemesi mümkündür.

ABD-Çin siber politikalarında bölge ülkelerinden BAE, Suudi Arabistan, Katar gibi ülkeler yararlanmaya çalışmaktadır. Konu teknolojik bir alan olduğundan her ülkenin siber güvenliğini sağlama noktasında bu teknolojiyi sağlayabilen ülkelerden maksimum seviyede faydalanmaya çalışmaktadır. Hızlı dijitalleşme ve artan sayıda internete bağlı cihaz sebebiyle, özellikle Ortadoğulu şirketlerin ve insanların karşı karşıya olduğu siber tehlike artmaktadır. IBM Security'ye göre, Suudi Arabistan ve BAE'de bir veri ihlalinin maliyeti 2020 yılında %9,4 artarak ortalama 6,53 milyon dolara kadar yükselmiştir. Bu bağlamda yatırımlara ağırlık veren BAE, 5G'nin hayata geçirilmesi Çin'in şirketleri iş birliği yolunu seçmiştir. ABD ise BAE'yi, ürünleri aracılığıyla casusluk yapmakla suçladığı Huawei ile bu iş birliğini yapmaması için ikaz etmişse de BAE ortaklıklarını çeşitlendirme bağlamında söz konusu şirket ile Emirliklerin bir siber güvenlik merkezine dönüşmesi doğrultusunda anlaşmaya varmıştır. Şirket yetkilisi Aloysius Cheang bu konuyla ilgili "Emirliklerin kritik altyapı sistemlerini beraber koruyacaklarını ve bu şekilde Dubai başta olmak üzere birçok şehrin

'akıllı şehir' modeline geçmesini sağlayacaklarını ifade ederek iki ülke arasındaki 5G birlikteliğini açıklamış; ABD'de 2020 yılında bilgi işlem şirketi olan SolarWinds'e ait Orion adlı programı üzerinden Maliye ve Hazine bakanlıklarına, 2021 yılında ise Colonial Boru Hattı sistemleri üzerinden akaryakıt transferlerine yönelik saldırıların altını çizerek siber meydan okumaların günden güne karmaşık bir hal aldığını öne sürmüştür (Sharma, 2021). ABD'nin siber güvenlik zafiyetlerinin işaret edilmesini Çin'in, bölgede kendini alternatif siber güvenlik sağlayıcı aktör olarak nitelendirmesi olarak değerlendirilebilecektir.

Huawei'nin de BAE ile siber güvenlik konusunda birtakım anlaşmalar yaptığı belirtilmiştir. 2021 yılının Mayıs ayında Dubai'deki Körfez Bilgi Güvenliği ve Konferansı'nda Huawei, İslam İşbirliği Teşkilâtı'nın "5G Güvenlik Çalışma Grubu Eş Başkanı" olarak konumlanmıştır ("Huawei ve BAE arasında siber güvenlik anlaşması", Savunmatr, 2021).

Çin-ABD siber rekabetin bölgeye önemli bir yansıma bu bağlamda BAE üzerinden gerçekleşmiştir. Abu Dabi yönetimi, Washington yönetimi ile yakın zamanda 23 milyar dolarlık savunma anlaşması imzalamıştı. Söz konusu anlaşma, 10,4 milyar dolar değerinde 50 adet F-35A jetini, 3 milyar dolar değerinde 18 adet MQ-9B (Reaper) İHA'yı içermekteydi. Ancak BAE, anlaşmadan ABD'nin şartlarının çok ağır olması ve Emirliklerin ulusal egemenliğini tehlikeye atması nedeniyle geri çekilmiştir. ABD tarafı, BAE'nin son dönem Çin ile geliştirdiği ilişkilerden dolayı BAE üzerinde Çin'in etkisinin artması endişesi ile anlaşma doğrultusunda Emirliklerin Çin ile güvenlik ilişkilerini gevşek tutmasını önkoşul olarak ortaya koymuştur. Washington, sürekli olarak teknolojik bilgilerin Çin tarafından çalınması tehlikesini gündeme getirmekle birlikte BAE'ye satılacak F-35'lere ait bilgilerin Pekin tarafından çalışma tehlikesini göz önünde bulundurarak anlaşmanın önkoşullarını bu minvalde oluşturmuştur. Ancak BAE, ABD'nin Emirlikler için tercih edilen tedarikçisi olmaya devam edeceğini ve müzakerelerin yeniden gündeme gelebileceğini yenilemiştir ("BAE F-35 Satın Alma Planını Dondurdu", VOA, 2021).

5G meselesine yönelik son gelişmelerden birisi de geçen aylarda BAE ulusal hava yolu şirketinin 5G'ye geçiş nedeniyle ABD'ye yapılan uçuşları askıya almasıdır. Emirates Hava Yolları, internet sitesinden bir yazılı açıklamada bulunarak, ABD'de 5G mobil servisinin aktifleştirilmesi ile ilgili operasyonel

endişeler nedeniyle bu ülkeye yapılacak uçak seferlerinin askıya alındığını belirtmiştir. Uçak üretiminde dünyanın en büyük şirketi olan Boeing ve Airbus bu konuda ABD'yi uyarmış, 21 Aralık 2021 tarihinde Ulaştırma Bakanı Pete Buttigieg'e 5G telefon servisinin havacılık endüstrisine vereceği zararlar ile alakalı bir mektup göndermiş ve bu mektupta ABD'nin 5G teknolojisine geçişinin ertelenmesi talep edilmiştir (Semiz, 2022).

Öte yandan ortaklıları çeşitlendirme doğrultusunda Suudi Arabistan da bugüne kadar Çin'in dâhil olduğu birtakım adımlar atmıştır. Krallık, 2017 yılında 10 milyar dolar değerinde Çin yapımı Wing Loong II isimli 300 adet İHA sipariş etmiştir. Söz konusu sipariş Çin haber ajansı Xinhua tarafından anlaşma, o dönem ülkenin şimdiye kadarki en büyük silah ihracatı olarak nitelendirilmiştir (Chuanren ve Pocock, 2017). 2019 yılında Suudi Arabistan'ın Çin'den yaptığı alımlarla hem füze altyapısını hem de teknolojisini genişlettiğine dair bilgiler elde eden ABD istihbarat teşkilatları (Mattingly vd., 2019), 2021 yılında ise Suudi Arabistan'ın bölgedeki en büyük rakibi olan İran'ın nükleer füze çalışmalarından dolayı Çin ile balistik füze üretimine başladığı incelemeye başladığı öne sürülmüştür. ABD merkezli CNN isimli haber kanalı tarafından elde edilen uydu görüntüleri doğrultusunda Suudi Arabistan'ın silahları en az bir yerde söz konusu füzeleri ürettiği belirtilmiştir (Cohen, 2021).

Öte yandan, daha önce Suudi Arabistan'da CH drone sınıfı için bir üretim tesisi inşa etmek üzere Çin Havacılık ve Uzay Bilimi ve Teknolojisi Şirketi'ne (China Aerospace Science and Technology Corporation) bağlı bir kuruluş olan Çin Havacılık ve Aerodinamik Teknolojileri Akademisi (China Academy of Aerospace Aerodynamics), Kral Abdülaziz Bilim ve Teknoloji Şehri (China Aerospace Science and Technology Corporation) ile bir ortaklık imzalamıştır. Son olarak Suudi menşeli Gelişmiş İletişim ve Elektronik Sistemleri Şirketi (Advanced Communications and Electronics Systems Company) ile Çin Elektronik Teknolojisi Grubu Şirketi (China Electronics Technology Group Corporation) arasında 6-9 Mart 2022 tarihlerinde Suudi Arabistan'ın başkenti Riyad'da gerçekleşen Dünya Savunma Fuarı sırasında iki şirketin bağlantılarını duyurduğu bir anlaşma imzalanmıştır. "Aerial Solutions (Havaya İlişkin Çözümler)" olarak adlandırılan bu girişim kapsamında Çin tarafının bir araştırma ve geliştirme merkezi kurması ve farklı tipte İHA sistemleri üretecek bir ekip oluşturmasını

sağlaması planlanmaktadır. Söz konusu çalışma; iletişim, uçuş kontrol, kamera, radar ve kablosuz algılama sistemlerini içerecektir. Bu girişim ile birlikte ayrıca elektrikle çalışan dikey iniş-kalkışlı dronelar, drone karşıtı çözümler, analitik, helikopter ürünleri ve radar sistemleri geliştirmeye de odaklanılacağı öne sürülmüştür. Riyad yönetimi tarafından “Vizyon 2030” girişimi ile uyumlu olduğu ifade edilen anlaşma neticesinde yerel sanayi büyütmeyi amaçladıkları ifade edilmiştir (Helou, 2022).



SONUÇ

Güvenlik kavramı yaşanan tüm gelişim ve değişimlere rağmen varlığını sürdürmekte ve aktörler için her zaman önemini korumaktadır. Değişik boyutlarda karşılaştığımız bu kavram, Soğuk Savaş dönemi sonrası ve özellikle de 2000'li yıllara gelindiğinde internet ağları, teknolojik gelişmeler ve küreselleşme ile birlikte çeşitlenmiş ve devletlerin kendi güvenliklerini sağlayabilmeleri noktasında farklı politikalar ile ortaya konulmuştur. Bu bağlamda devletlerarası yaşanan mücadele farklı bir alana kaymış ve devletler artık siber uzay, siber savaş, siber tehdit, siber güvenlik gibi pek çok kavram ile ilintili ulusal politikalar geliştirilmeye başlamış ve siber alanda çalışmalara yönelmişlerdir. Siber alandaki çalışmaları yalnızca kendilerine yöneltilebilecek herhangi bir saldırıdan korunmak geliştirmeyen devletler, geliştirilen siber teknolojik ürün ve hizmetlerden kâr elde etmek, ekonomik, siyasi veya askerî bir üstünlük sağlamak gibi pek çok amaç doğrultusunda yatırımlar yapmış ve yapmaya devam etmektedir.

Soğuk Savaş dönemi sonra tek kutup olarak karşımıza çıkan ve bugüne kadarki süreçte gücünü her alanda konsolide etmeye çalışan ve süper güç olarak konumlanan ABD, siber teknolojik çalışmalarıyla rekabetin bu alanında da yer almaktadır. Bu karşın Asya'nın yükselen gücü olarak ortaya çıkan Çin, çok kısa bir sürede küresel sistemin ekonomik düzenine entegre olarak ABD ile ekonomik açıdan aralarında oluşan farkı kapatabilmiştir. Teknolojik gelişmelere ağırlık veren ve askerî alandan daha çok teknolojik alandaki yatırımlarını artıran Çin, bu alanda da ABD'nin rakibi olarak yerini almıştır.

ABD siber güvenlik belgelerinde, yayımladığı ulusal güvenlik strateji raporlarında her fırsatta Çin'den söz etmiş ve son dönem raporlarında ise Çin'i en büyük tehdit olarak lanse etmiştir. Buradan hareketle, yaşanan siber saldırılara ilişkin olarak ABD Çin'i doğrudan suçlamaktadır. Yani söz konusu iki ülkenin rekabet alanına artık siber alan da dâhil olmuştur.

Bu minvalde ABD, Çin'i yalnızca tehlike olarak nitelendirmekle kalmamış; Çin'in iş birliği geliştirmek istediği müttefiklerini de Pekin yönetimine karşı uyarmıştır. Özellikle jeostratejik, jeopolitik ve jeoekonomik açıdan kritik bir öneme sahip olan Ortadoğu ve bölgedeki önemli aktörler yaşanan bu rekabetten fazlasıyla etkilenmektedir. ABD, bölgede öne çıkan İsrail ile Çin'e karşı görece

ortak bir düzlemde hareket ederken, güvenlik garantörü olduđu Körfez’de Çin ile kurulması planlanan iş birliklerini engellemek noktasında çaba sarf etmektedir.

Ulusal güvenlik noktasında ülkeler bazı sistemlere ihtiyaç duymaktadır. ABD’nin Körfez için tarihi bir garantör olması, ebediyen bölge ülkelerinin güvenlik, teknolojik ekipman desteđi, lojistik destek, siyasi güvenlik sağlayıcısı olacağı anlamına gelmemektedir. BAE, Suudi Arabistan ve Katar gibi rantiyer devletler, Çin ile iş birlikleri geliştirmekte ve son dönemde siber güvenlik bağlamında ortaklıklarını çeşitlendirme çabasında bulunmaktadır. Yani bölge ülkeleri, anarşik dünya düzeninin "kendi kendine yardım (self-help)" anlayışı düşünülecek olduğunda yalnızca ABD kanalı üzerinden hareket etmemektedirler. İhtiyaçlarını da büyük ölçüde hangi aktörün verdiğiine bakmaksızın kabul etmektedirler. Ancak yine de ABD’nin bölge için birincil aktör oluşu devamlılık arz eden bir durumdur ve ABD hem silah sağlama hem politik söylem hem de yazılım-teknolojik destek sağlama bazında temel partneridir.

Öte yandan İran ile ABD-İsrail ilişkilerinde yaşanan gerilimler İran’ı Çin’e yönlendirmiştir. Bu açıdan bakıldığında Çin’in alternatif bir partner olması diğer bölge ülkeleri için de bir örnek teşkil etmektedir.

Sonuç olarak, ABD ve Çin’in yaşanan son dönem gelişmeler ışığında, siber güvenlik alanında sahip oldukları üstünlükleri, gelişim ve teknolojileri bölgedeki ülkeleri etkilemek ve iş birliği sağlamak için kullandıklarını söylenebilecektir. Ancak ABD bu üstünlüğü bölgede güvenlik üzerinden kurmak ve tarihi garantörlüğünü sürdürmek için kullanırken, Çin ise ABD’nin iddialarından büyük oranda farklı olarak ticari ve ekonomik olarak kullanmaktadır.

KAYNAKÇA

Kitaplar

- Akyeşilmen, N. (2018). *"Disiplinlerarası Bir Yaklaşımla Siber Politika & Güvenlik"*. Ankara: Orion Kitabevi.
- Arı, T. (2010). *"Uluslararası İlişkiler Teorileri"*, Bursa: MKM Yayıncılık.
- Brauch, H. (2012). *"Güvenliğin Yeniden Kavramsallaştırılması: Barış, Güvenlik, Kalkınma ve Çevre Kavramsal Dörtlüsü"*. M. Aydın, H. Brauch, M. Çelikpala, U. Spring, & N. Polat içinde, *Uluslararası İlişkilerde Çatışmadan Güvenliğe*. Çev. Z. Arkan. s.167-198. İstanbul: İstanbul Bilgi Üniversitesi Yayınları.
- Brenner, S. W. (2009). *"Cyber Threats: The Emerging Fault Lines of the Nation State"*. Oxford; New York: Oxford University Press.
- Clark, D., Berson, T. and Lin, H. S. (2014). *"At the Nexus of Cybersecurity and Public Policy. Computer Science and Telecommunications Board"*. National Research Council, Washington DC: The National Academies Press.
- Clarke, R. A. ve Knake, R. K. (2011). *"Siber Savaş"*. İstanbul: İKÜ Yayınları.
- Dedeoğlu, B. (2008). *"Uluslararası Güvenlik ve Strateji"*. İstanbul: Yenyüzyıl Yayınları.
- Evans, G. ve Newnham, J. (2007). *"Uluslararası İlişkiler Sözlüğü"*. Çev. H. Ahsen Utku. İstanbul: Gökkuşbu Yayınları.
- Janeliūnas, T. ve Tumkevič, A. (2020). *"Avoiding a Cyber World War: Rational Motives for Negative Cooperation among the United States, China and Russia"*. *Emerging Cyber Threats and Cognitive Vulnerabilities*. Ed. V. Benson and J. McAlaney. ss.118-146. Londra: Elsevier Press.
- Johnson, T. A. (2015). *"Cyber-Security Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare"*. New York: CRC Press.
- Kaldor, M. (2012). *"New & Old Wars"*. Cambridge: Polity Press.
- Karedeli, C. (2021). *"Küreselleşme, Bölgesel Bloklar ve Gelecek"*. *Küreselleşen Dünya*. Ed. Nurgül Bekar. s.13-40. Ankara: Nika Yayınevi.
- Koç Aytekin, G. (2021). *"COVID-19 Süresinde Küreselleşme Boyutuyla Küresel Tedarik Zincirleri, Uluslararası Ticaret ve Lojistik Merkez: Türkiye"*. *Küreselleşen Dünya*. Ed. N. Bekar. s.147-177. Ankara: Nika Yayınevi.
- Kshetri, N. (2016). *"The Quest to Cyber Superiority"*. Switzerland: Springer Press.
- Medeiros E. S. (2009). *"China's International Behavior Activism, Opportunism, and Diversification"*, RAND Corporation.

- Sağıroğlu, Ş. (2018). “*Siber güvenlik ve savunma: Önem, tanımlar, unsurlar ve önlemler*”. Ed. Şeref Sağıroğlu ve Mustafa Alkan. Siber Güvenlik ve Savunma: Problemler ve Çözümler. s.21-45. Ankara: Grafiker Yayınları.
- Shirk, L. S. (2007). “*China-Fragile Superpower*”, Oxford University Press, Oxford.
- Valeriano B. ve Maness R. C. (2015). “*Cyber War Versus Cyber Realities: Cyber Conflict in the International System*”. United Kingdom: Oxford University Press.
- Wendt, A. (2003). “*Social Theory of International Politics*”. New York: Cambridge University Press.

Süreli Yayınlar

- Aslay, F. (2017). “Siber Saldırı Yöntemleri ve Türkiye’nin Siber Güvenlik Mevcut Durum Analizi”. *International Journal of Multidisciplinary Studies and Innovative Technologies*, 1(1), 24-28.
- Balke, L. (2018). “China’s New Cybersecurity Law and U.S-China Cybersecurity Issues”. *Santa Clara Law Review*, 58 (1), 137-162.
- Çelik, Ş. (2013). “Stuxnet Saldırısı ve ABD’nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme”, *Dokuz Eylül Hukuk Fakültesi Dergisi*, 15 (1): 137-175.
- Darıcı A. B. (2017). “Demokrat parti hack skandalı bağlamında ABD ve RF’nin siber güvenlik stratejilerinin analizi”. *Uluslararası Çalışmalar Dergisi*, 1(1), 1-24.
- Darıcı, A. B. ve Özdal, B. (2018). “Analysis of the Cyber Security Strategies of People’s Republic of China”. *Güvenlik Stratejileri*, 14 (28), 1-35.
- Doyle, R. B. (2007). “The U.S. National Security Strategy: Policy, Process, Problems”. *Public Administration Review*, Vol. 67, No. 4 (Jul. - Aug., 2007), pp. 624-629.
- Dupont, B. (2013). “The proliferation of cyber security strategies and their implications for privacy”. *Circulation internationale de l’information et sécurité*. 67-80.
- Göçoğlu, V. ve Aydın, M. D. (2019). “Siber Güvenlik Politikası: ABD, Rusya ve Çin Üzerine Karşılaştırmalı Bir Analiz”. *Güvenlik Bilimleri Dergisi*, 8 (2), 229-252.
- Kula, S. & Çakar, B. (2015). “Maslow İhtiyaçlar Hiyerarşisi Bağlamında Toplumda Bireylerin Güvenlik Algısı ve Yaşam Doyumu Arasındaki İlişki”, *Bartın Üni. İ.İ.B.F. Dergisi*, Cilt 6, Sayı 12, 191-210.
- Kurnaz, İ. (2016). “Siber Güvenlik ile İlişkili Kavramsal Çerçeve”. *Cyberpolitik Journal*, 1 (1), 56-77.
- Oğuzlu, H. T. (2007). “Dünya Düzenleri ve Güvenlik: Ulus-Devlet Güvenlik Anlayışı Açılıyor Mu?”. *Güvenlik Stratejileri Dergisi*, (6), 14, s. 7-42.

Sandıklı, Atilla (2009), “Geleceğin Süper Gücü Çin”, Bilge Strateji, Cilt 1, Sayı 1, Güz 2009.

Seemma, P.S.; Sundaresan, N. ve Sowmiya, M. (2018). “Overview of Cybersecurity”. International Journal of Advanced Research in Computer and Communication Engineering, 7 (11), 125-128.

Swaine, M. D. (2013). “Chinese Views on Cybersecurity in Foreign Relations”. China Leadership Monitor, 42, 1-27.

Makaleler

Akyazı, U. (2013). “Uluslararası Siber Güvenlik Strateji ve Doktrinleri Kapsamında Alınabilecek Tedbirler”. 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı.

Allison, G. ve Schmidt, E. (2020). “Is China Beating the U.S. to AI Supremacy?”. Avoiding Great Power War Project. Harward Kennedy School, Belfer Center for Science and International Affairs.

Baezner, M. (2018). “Cybersecurity in Sino-American Relations”. Center for Security Studies, 224. Zürih.

Cavelty, M. D. (2014). “Breaking the Cyber-security Dilemma: Aligning Security Needs and Removing Vulnerabilities”. Science and Engineering Ethics, 20(3), 701-715.

Clemente, D. (2013). “Cyber Security and Global Interdependence: What Is Critical?”. Londra: The Royal Institute of International Affairs.

Darıcı, A. B. (2015). “NATO’nun Siber Güvenlik Stratejisi’nin Analizi. Uluslararası Sistemde Yeni Düzen Arayışları”, 407-417.

Eren, M. (2017). “Avrupa Birliği’nin Siber Güvenlik Stratejisi İçin Kuramsal Çerçeve ve Stratejik Belgesi Öncesi AB’nin Eylemleri”. Siber Politikalar Dergisi, Cilt: 2, No: 3.

Kello, Lucas (2013), “The Meaning of the Cyber Revolution: Perils to Theory and Statecraft”, International Security, 38 (2): 7-40.

Koç, Y. E. (2020). “ABD-Çin Rekabetinde Gerilim Alanları”. Kriter Dergisi, Sayı: 47, Haziran 2020, s.75-77.

Kshetri, N. (2013). “Cybercrime and Cyber-security Issues Associated with China: Some Economic and Institutional Considerations”, Electronic Commerce Research 13 (1): 41-69.

Raud, M. (2016). “China and Cyber: Attitudes, Strategies and Organisation”. Tallinn: The NATO Cooperative Cyber Defence Centre of Excellence.

Segal, A. (2017). “Chinese Cyber Diplomacy in a New Era of Uncertainty”. Aegis Paper Series. No 1703. Stanford: Hoover Institution.

Spade, C. J. M. (2012). "Information As Power: China's Cyber Power and American's National Security". U.S. Army War College.

Raporlar

10 Steps to Cyber Security. (2012). The Information Security Arm of GCHQ.

Hildreth, S. A. (2001), "Cyberwarfare Congressional Research Service Report for Congress", Congressional Research Service & The Library of Congress, No: RL30375.

The US-China Business Council ve Oxford Economics. (2021). "The US-China Economic Relationship: A Crucial Partnership at A Critical Juncture".

Tezler

Demirel, M. (2012). "Asimetrik tehdit kavramı bağlamında 11 Eylül 2001 sonrası dönemde Amerika Birleşik Devletleri'ndeki siber tehdit algılamasının ve geliştirilen güvenlik politikalarının incelenmesi". (Yayımlanmamış Yüksek Lisans Tezi). Kara Harp Okulu/Savunma Bilimleri Enstitüsü, Ankara.

Kara, M. (2013). Siber Saldırılar – Siber Savaşlar ve Etkileri, İstanbul Bilgi Üniversitesi Sosyal Bilimler Enstitüsü.

Patton, D. E. (2016). Evaluating U.S. and Chinese Cyber Security Strategies Within a Cultural Framework. Yüksek Lisans Tezi. Alabama: Air Command and Staff College Air University.

Belgeseller

Tiley M. ve Bower D. (Yapımcı/Yönetmen). (2020). "Çin'in Yükselişi". Netflix.

İnternet Kaynakları

"ABD Huawei'yi neden hedef alıyor?". (2019) Anadolu Ajansı. <https://www.youtube.com/watch?v=t105Wsi9YRS>, (Erişim tarihi: 01.02.2022).

"ABD ve Çin arasında siber gerilim". (2013). BBC News Türkçe. https://www.bbc.com/turkce/haberler/2013/05/130507_abd_cin, (Erişim tarihi: 01.02.2022).

"ABD ve Çin: Rekabetleriyle geleceği şekillendirecek iki süper güç". (2021). BBC News Türkçe. <https://www.bbc.com/turkce/haberler-dunya-55929359>, (Erişim tarihi: 01.02.2022).

"ABD, Pegasus casus yazılımını geliştiren İsrail şirketi NSO Group ile ticareti yasakladı". (2021). BBC News Türkçe. <https://www.bbc.com/turkce/haberler-dunya-59159283>, (Erişim Tarihi: 10.02.2022).

- “BAE F-35 Satın Alma Planını Dondurdu”. (2021). VOA. <https://www.amerikaninsesi.com/a/bae-f35-satin-alma-planini-dondurdu/6354821.html>, (Eriřim Tarihi: 10.02.2021).
- “Biden, Tayvan’ı Çin’e karřı koruyacaklarını aıkladı”. (2021). *Deutsche Welle*. <https://www.dw.com/tr/biden-tayvan%C4%B1-%C3%A7ine-kar%C5%9F%C4%B1-koruyacaklar%C4%B1n%C4%B1-a%C3%A7%C4%B1klad%C4%B1/a-59584609>, (Eriřim tarihi: 01.02.2022).
- “China denies hacking Microsoft, calls allegations 'groundless' and 'irresponsible’”. (2021). *France 24*. <https://www.france24.com/en/asia-pacific/20210720-china-denies-hacking-microsoft-calls-allegations-groundless-and-irresponsible>, (Eriřim Tarihi: 01.02.2021).
- “Çin, siber saldırı iddiasını reddetti”. (2021). *Dünya*. <https://www.dunya.com/dunya/cin-siber-saldiri-iddiasini-reddetti-haberi-628495>, (Eriřim tarihi: 01.02.2022).
- “Çin’de Halka Yasak Olan Sosyal Medya”, Diplomatların Kullanımına Açıldı”. (2020). *NTV*. <https://www.ntv.com.tr/dunya/cinde-halka-yasak-olan-sosyal-medya-diplomatlarin-kullanimina-acildi,IAL-mOzrdU-ySjvnk79S4w>, (Eriřim Tarihi: 05.02.2022).
- “Çin’den 143 řirket Fortune Global 500 listesine girdi”. (2021). *CRI Türk*. <https://www.criturk.com/cinden-143-sirket-fortune-global-500-listesine-girdi/#:~:text=%C4%B0%C5%9Fletme%20gelirlerine%20g%C3%B6re%20d%C3%BCnyan%C4%B1n%20en,%C3%87in%2C%20listedeki%20birin cilik%20konumunu%20korudu>, (Eriřim Tarihi: 11.09.2021).
- “Çin-ABD ilişkilerinde Soğuk Savaş’tan beri en gergin dönem”. (2021). *TRT Haber*. <https://www.youtube.com/watch?v=j3lBeiVVasc>, (Eriřim tarihi: 01.02.2022).
- “Eski Pentagon yetkilisi: ABD Çin’e karřı siber savařı kaybetti”. (2021). *TRT Haber*. <https://www.trthaber.com/haber/dunya/eski-pentagon-yetkilisi-abd-cine-karsi-siber-savasi-kaybetti-616419.html>, (Eriřim tarihi: 01.02.2022).
- “Huawei ve BAE arasında siber güvenlik anlaşması”. (2021). *Savunmatr*. <https://www.savunmatr.com/siber-guvenlik/huawei-ve-bae-arasinda-siber-guvenlik-anlasmasi-h12397.html>, (Eriřim Tarihi: 10.05.2021).
- “İran nükleer anlaşması nedir ve tekrar yürürlüğe girer mi?”. (2021). *BBC News Türke*. <https://www.bbc.com/turkce/haberler-dunya-59433112>, (Eriřim Tarihi: 10.02.2022).
- “Koronavirüs: ABD istihbaratı 'Çin’in siber saldırılarını' soruşturduğunu aıkladı”. (2020). *BBC News Türke*. <https://www.bbc.com/turkce/haberler-dunya-52655953>, (Eriřim Tarihi: 10.02.2022).
- “US blames China for hacks, opening new front in cyber offensive”. (2021). *CNN Politics*. <https://edition.cnn.com/2021/07/19/politics/us-china-cyber-offensive/index.html>, (Eriřim tarihi: 01.02.2022).

- “Uzakdoğu’da hava sahası gerilimi artıyor”, *BBC News Türkçe*, 27 Kasım 2013, http://www.bbc.com/turkce/haberler/2013/11/131127_cin_abd_hava, (Erişim Tarihi: 06.10.2021).
- “Yapay zeka: ‘Çin dünyayı domine edecek, ABD’nin rekabet şansı yok’ diyen Pentagon yetkilisi istifa etti”. (2021). *BBC News Türkçe*. <https://www.bbc.com/turkce/haberler-dunya-58866243>, (Erişim tarihi: 01.02.2022).
- Acar, N. (2021). “Suudi balistik füze programı: Körfez’de ABD-Çin rekabeti”. <https://www.aa.com.tr/tr/analiz/suudi-balistik-fuze-programi-korfezde-abd-cin-rekabeti/2459244>, (Erişim Tarihi: 09.02.2022).
- Al-Tamimi, N. (2017). “China and the Gulf crisis – the stakes are high”. <https://www.arabnews.com/node/1126461/middle-east>, (Erişim Tarihi: 09.02.2022).
- Aslan, A. (2021). “ABD-Çin gerginliği: Yeni bir Soğuk Savaş mı?”. Anadolu Ajansı. <https://www.aa.com.tr/tr/analiz/abd-cin-gerginligi-yeni-bir-sojuk-savas-mi/2194982>, (Erişim Tarihi: 10.02.2022).
- Başa, Ş. (2010). “ABD İç Güvenlik Bakanlığı”. [http://www.safakbasa.com.tr/yuklenen/akademik/calismalar/40-ABD_IC_GUVENLIK_BAKANLIGI_\(SUNUM\).pdf](http://www.safakbasa.com.tr/yuklenen/akademik/calismalar/40-ABD_IC_GUVENLIK_BAKANLIGI_(SUNUM).pdf), (Erişim tarihi: 30.01.2022).
- Ben-David, R. (2022). “Israeli cybersecurity firms raised record \$8.8b in 2021, exports reached \$11b”. <https://www.timesofisrael.com/israel-cybersecurity-firms-raised-record-8-8b-in-2021-exports-reached-11b/#:~:text=According%20to%20Israeli%20Export%20Institute,at%20%2411%20billion%20in%202021.&text=Last%20year%2C%20there%20were%20also,estimated%20worth%20of%20%243.5%20billion>, (Erişim Tarihi: 10.02.2022).
- Bergman R. ve Mazzetti M. (2022). “The Battle for the World’s Most Powerful Cyberweapon”. <https://www.nytimes.com/2022/01/28/magazine/nso-group-israel-spyware.html?referringSource=articleShare>, (Erişim Tarihi: 10.02.2022).
- CENSUS. 2021. “U.S. Trade in Goods with China”. <https://www.census.gov/foreign-trade/balance/c5700.html>, (Erişim Tarihi: 05.02.2022).
- Chuanren, C. ve Pocock, C. 2017. “Saudi Arabia Buying and Building Chinese Armed Drones”. *AINonline*. <https://www.ainonline.com/aviation-news/defense/2017-04-12/saudi-arabia-buying-and-building-chinese-armed-drones>, (Erişim Tarihi: 01.02.2022).
- Clark, C. 2021. “‘One of the largest shifts in global geostrategic power:’ Milley on China’s rise”. *Breaking Defense*. <https://breakingdefense.com/2021/11/one-of-the-largest-shifts-in-global-geostrategic-power-milley-on-chinas-rise/>, (Erişim Tarihi: 12.11.2021).

- Cohen, Z. 2021. "CNN Exclusive: US intel and satellite images show Saudi Arabia is now building its own ballistic missiles with help of China". *CNN Politics*. <https://edition.cnn.com/2021/12/23/politics/saudi-ballistic-missiles-china/index.html>, (Eriřim Tarihi: 03.05.2021).
- Creemers R.; Webster G. ve Triolo P. (2018). "Translation: Cybersecurity Law of the People's Republic of China (Effective June 1, 2017)". <https://digichina.stanford.edu/work/translation-cybersecurity-law-of-the-peoples-republic-of-china-effective-june-1-2017/>, (Eriřim Tarihi: 03.02.2021).
- Çahmutoğlu, E. (2021). "Dünyayı tehdit eden casus yazılım: Pegasus". <https://www.aa.com.tr/tr/analiz/dunyayi-tehdit-eden-casus-yazilim-pegasus/2314321>, (Eriřim Tarihi: 10.02.2022).
- Çopur, H. (2020). "ABD ile Çin birinci faz ticaret anlaşmasını imzaladı". <https://www.aa.com.tr/tr/dunya/abd-ile-cin-birinci-faz-ticaret-anlasmasini-imzaladi/1703875>, (Eriřim Tarihi 05.10.2021).
- Daragahi, B. (2021). "İran ve Çin 25 yıllık anlaşma imzalayarak ABD'ye mesaj gönderdi". <https://www.indyturk.com/node/339736/yazarlar/i%CC%87ran-ve-%C3%A7in-25-y%C4%B1l%C4%B1k-anla%C5%9Fma-imzalayarak-abdye-mesaj-g%C3%B6nderdi>, (Eriřim Tarihi: 10.02.2022).
- Darıcı, A. B. (2021). "İsrail'in siber istihbarat stratejisi". <https://www.yenisafak.com/dusunce-gunlugu/israilin-siber-istihbarat-stratejisi-3702007>, (Eriřim Tarihi: 10.02.2022).
- Eberhart, D. (2019). "Drone Attacks Test Saudi Aramco, Deliver Wake Up Call To Global Markets". <https://www.forbes.com/sites/daneberhart/2019/09/16/drone-attacks-test-saudi-aramco-deliver-wake-up-call-to-global-markets/?sh=4100238a17b9>, (Eriřim Tarihi: 09.02.2022).
- Esfandiari, G. (2020). RFERL. "Iran To Work With China To Create National Internet System". <https://tinyurl.com/5bw4e6ps>, (Eriřim Tarihi: 11.09.2021).
- Gürer, B. (2021). "İRAM raporu: İran 2010'dan sonra operasyonel siber saldırı kapasitesini artırdı". <https://www.aa.com.tr/tr/bilim-teknoloji/iram-raporu-iran-2010dan-sonra-operasyonel-siber-saldiri-kapasitesini-artirdi/2197020>, (Eriřim Tarihi: 10.02.2022).
- Helou, A. 2022. "Chinese and Saudi firms create joint venture to make military drones in the kingdom". *Defense News*. <https://www.defensenews.com/unmanned/2022/03/09/chinese-and-saudi-firms-create-joint-venture-to-make-military-drones-in-the-kingdom/>, (Eriřim Tarihi: 09.03.2022).
- Horn, S., Carmen, M. ve Trebesch, C. (2020). "How Much Money Does the World Owe China?". *Harvard Business Review*. <https://hbr.org/2020/02/how-much-money-does-the-world-owe-china>, (Eriřim Tarihi: 09.09.2021).

- Islamic Republic of Iran Ministry of I.C.T. (2015). "Dr. Vaezi meets Head of Chinese Cyberspace Administration". Ministry of Information and Communications Technology of Iran: <https://tinyurl.com/w24xnb6z>, (Eriřim Tarihi: 10.05.2020).
- Kabakçı, F. (2021). "Microsoft, Çin'i 'ABD'deki kurumların elektronik postalarına siber saldırı düzenlemekle' suçladı". <https://www.aa.com.tr/tr/bilim-teknoloji/microsoft-cini-abddeki-kurumların-elektronik-postalarına-siber-saldiri-duzenlemekle-sucladi/2163172>, (Eriřim tarihi: 01.02.2022).
- Kalaycıoğlu, S. (2021). "Çin ve İran İliřkisi řimdi Önemli". <https://tasam.org/tr-TR/Icerik/64878/cin-ve-iran-iliskisi-simdi-onemli>, (Eriřim Tarihi: 10.02.2022).
- King, R. (2011). "China claims US started global 'Internet war' after Google attack". ZDNet. <https://www.zdnet.com/article/china-claims-us-started-global-internet-war-after-google-attack/>, (Eriřim tarihi: 01.02.2022).
- Kirchgaessner S., Lewis P., Pegg D., Cutler S., Lakhani N. ve Safi M. (2021). "Revealed: leak uncovers global abuse of cyber-surveillance weapon", <https://www.theguardian.com/world/2021/jul/18/revealed-leak-uncovers-global-abuse-of-cyber-surveillance-weapon-nso-group-pegasus>, (Eriřim Tarihi: 10.02.2022).
- Kirchgaessner, S. (2022). "FBI confirms it obtained NSO's Pegasus spyware". <https://www.theguardian.com/news/2022/feb/02/fbi-confirms-it-obtained-nsos-pegasus-spyware>, (Eriřim tarihi: 10.02.2022).
- Klawans. J. (2021). "Pentagon Official Resigns Over Belief China Has Won AI Battle, Heading to Global Dominance". <https://www.newsweek.com/pentagon-official-resigns-over-belief-china-has-won-ai-battle-heading-global-dominance-1637772>, (Eriřim Tarihi: 01.02.2021).
- Korhan, S. (2018). "Siber Uzayda Uluslararası İliřkilerin Deęiřen Parametreleri", Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü.
- Kozanoğlu, H. (2021). "Teknolojide ABD-Çin rekabeti". <https://www.birgun.net/haber/teknolojide-abd-cin-rekabeti-357150>, (Eriřim tarihi: 01.02.2022).
- Kurunç, K. (2021). "Tayvan Savunma Bakanlıęından Çin Tehdidi Raporu". *SavunmaSanayiST*. <https://www.savunmasanayist.com/tayvan-savunma-bakanligindan-cin-tehdidi-raporu/>, (Eriřim Tarihi: 06.12.2021).
- LeBlanc, P. ve Lillis, B. 2022. "FBI urges Olympic athletes to leave personal phones at home ahead of Beijing games". *CNN Politics*. [https://edition.cnn.com/2022/02/01/politics/olympics-china-burner-phones/index.html#:~:text=FBI%20urges%20Olympic%20athletes%20to,home%20ahead%20of%20Beijing%20games&text=Washington%20\(CNN\)%20The%20FBI%20is,for%20%22malicious%20cyber%20activities.%22](https://edition.cnn.com/2022/02/01/politics/olympics-china-burner-phones/index.html#:~:text=FBI%20urges%20Olympic%20athletes%20to,home%20ahead%20of%20Beijing%20games&text=Washington%20(CNN)%20The%20FBI%20is,for%20%22malicious%20cyber%20activities.%22), (Eriřim Tarihi: 29.12.2021).

- Maizland, L. 2020. "China's Modernizing Military". *Council on Foreign Relations*. <https://www.cfr.org/backgrounder/chinas-modernizing-military>, (Eriřim Tarihi: 09.02.2022).
- Mattingly, P. Cohen, Z. ve Herb, J. 2019. "Exclusive: US intel shows Saudi Arabia escalated its missile program with help from China". *CNN Politics*. <https://edition.cnn.com/2019/06/05/politics/us-intelligence-saudi-arabia-ballistic-missile-china/index.html>, (Eriřim tarihi: 01.02.2022).
- Nakashima, E. ve Warrick, J. 2012. "Stuxnet was work of U.S. and Israeli experts, officials say". *Washington Post*. https://www.washingtonpost.com/world/national-security/stuxnet-was-work-of-us-and-israeli-experts-officials-say/2012/06/01/gJQAlnEy6U_story.html, (Eriřim Tarihi: 10.02.2022).
- Neufeld, D. (2021). "Visualizing the \$94 Trillion World Economy in One Chart". *Visual Capitalist*. <https://www.visualcapitalist.com/visualizing-the-94-trillion-world-economy-in-one-chart/>, (Eriřim Tarihi: 27.12.2021).
- OECD. 2021. "China (CHN) Exports, Imports, and Trade Partners". <https://oec.world/en/profile/country/chn#latest-data>, (Eriřim Tarihi: 27.02.2022).
- Pham, S. (2019). "The US-China trade war is back on. That's bad news for Huawei". *CNN Business*. <https://edition.cnn.com/2019/08/02/tech/huawei-us-ban/index.html>, (Eriřim Tarihi: 11.09.2021).
- Protection (CIIP). "9th ISDP-AMS Joint Conference". <https://www.isdp.eu/28368-2/>, (Eriřim Tarihi: 10.11.2020).
- Ravid, B. (2022). "UAE asks U.S. to reinstate Houthi terrorist designation after attack". *Axios*. <https://www.axios.com/emiratis-seek-terrorist-designation-blinken-6ca0bed0-3e17-4f73-ac4c-9d24371e82bd.html>, (Eriřim tarihi: 09.02.2022).
- Segal, A. (2012). "China Moves Forward on Cybersecurity Policy". <https://www.cfr.org/blog/china-moves-forward-cybersecurity-policy> (Eriřim Tarihi: 19.11.2020).
- Semiz, M. (2022). "BAE ulusal havayolu řirketi, 5G'ye geçiř nedeniyle ABD'ye uçuřları askıya aldı". *Anadolu Ajansı*. <https://www.aa.com.tr/tr/dunya/bae-ulusal-havayolu-sirketi-5gye-gecis-nedeniyle-abdy-ucuslari-askiya-aldi/2478858>, (Eriřim Tarihi:10.05.2022).
- Sharma, A. (2021). "Huawei to help establish UAE as cyber security hub". *The National News*. <https://www.thenationalnews.com/business/technology/huawei-to-help-establish-uae-as-cyber-security-hub-1.1235410>, (Eriřim Tarihi: 10.02.2022).
- SIPRI. (2021). "World military spending rises to almost \$2 trillion in 2020". <https://sipri.org/media/press-release/2021/world-military-spending-rises-almost-2-trillion-2020>, (Eriřim Tarihi: 05.07.2021).

- So, D. (2014). "Cyber Security Nation: Why Israel Leads The World In Protecting The Web". <https://nocamels.com/2014/12/cyber-security-nation-israel/>, (Eriřim Tarihi: 10.02.2022).
- Stecklow, (2012). "Special Report: Chinese firm helps Iran spy on citizens". <https://www.reuters.com/article/us-iran-telecoms-idUSBRE82LOB820120322>, (Eriřim Tarihi: 10.02.2022).
- Sutton, H. ve LaGrone, S. 2021. "China Builds Missile Targets Shaped Like U.S. Aircraft Carrier, Destroyers in Remote Desert". *USNI News*. <https://news.usni.org/2021/11/07/china-builds-missile-targets-shaped-like-u-s-aircraft-carrier-destroyers-in-remote-desert>, (Eriřim Tarihi: 19.11.2021).
- The Department of Defense. (2018). "Summary of the 2018 National Defense Strategy of The United States of America, Sharpening the American Military's Competitive Edge". <https://dod.defense.gov/Portals/1/Documents/pubs/2018-National-Defense-Strategy-Summary.pdf>, (Eriřim tarihi: 30.01.2022).
- The Department of Homeland Security. (2018). "U.S. Department of Homeland Security Cybersecurity Strategy". https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf, (Eriřim tarihi: 30.01.2022).
- The White House. (2003). "The National Strategy to Secure Cyberspace". https://www.cisa.gov/uscert/sites/default/files/publications/cyberspace_strategy.pdf, (Eriřim tarihi: 30.01.2022).
- Tomlinson, L. Y. ve Miles, F. 2018. "Pentagon orders stores to ban certain Chinese phones amid spying concerns". *Fox News*. <https://www.foxnews.com/politics/pentagon-orders-stores-to-ban-certain-chinese-phones-amid-spying-concerns>, (Eriřim Tarihi: 06.02.2022).
- USA Historical Office, Office of the Secretary of Defense. "National Security Strategy", <https://history.defense.gov/Historical-Sources/National-Security-Strategy/>, (Eriřim tarihi: 30.01.2022).
- Whalen, J. & Alcantara, C. (2021). "Nine charts that show who's winning the U.S.-China tech race", Washington Post.
- Wiseman, J. (2011). "How Downed U.S. Drone Helps China". <https://thediplomat.com/2011/12/how-downed-u-s-drone-helps-china/>, (Eriřim Tarihi: 10.02.2022).
- Wolf, J. 2012. "U.S. lawmakers seek to block China Huawei, ZTE U.S. inroads". *Reuters*. <https://www.reuters.com/article/us-usa-china-huawei-zte-idUSBRE8960NH20121008>, (Eriřim Tarihi: 06.02.2022).
- Yıldızoğlu, E. (2021). "ABD-Çin ilişkileri: Tehlikeli ve belirsizliklerle dolu bir ortam şekilleniyor". *BBC News Türkçe*. <https://www.bbc.com/turkce/haberler-dunya-59726695>, (Eriřim tarihi: 01.02.2022).

Zengin, D. (2021). “Rapor: ABD ve Çin arasındaki ticaret savaşı 245 bin kişinin işine mal oldu”. Anadolu Ajansı. <https://www.aa.com.tr/tr/dunya/rapor-abd-ve-cin-arasindaki-ticaret-savasi-245-bin-kisinin-isine-mal-oldu/2110566>, (Erişim tarihi: 01.02.2022).



ÖZGEÇMİŞ

Kişisel Bilgiler

Adı Soyadı : Nurbanu KESGİN

Eğitim Durumu

Lisans Öğrenimi : Ufuk Üniversitesi, Siyaset Bilimi ve Uluslararası İlişkiler (%100 Burslu)

Bildiği Yabancı Diller : İngilizce

Bilimsel Faaliyetleri

Görev : Ortadoğu Analiz Dergisi Editör Asistanlığı (Kasım 2019-Devam Ediyor)

Makale : Akcan*, N. "BAE'nin İş Gücünü Millileştirmesi Mümkün Mü?". *Ortadoğu Analiz Dergisi*, Kasım-Aralık 2019 Cilt: 10 Sayı: 90.

Akcan, N. "Suudi Arabistan'ın Son Dönem Ekonomik Hamleleri ve Vizyon 2030". *Ortadoğu Analiz Dergisi*, Ocak-Şubat 2020 Cilt: 11 Sayı: 91.

Akcan, N. ve Yetim, M. "Türkiye-Katar Ortaklığında Sert Güç". *Ortadoğu Analiz Dergisi*, Mart-Nisan 2020 Cilt: 11 Sayı: 92.

Akcan, N. ve Erel, G. "Körfez Ülkelerinin Koronavirüs ile Mücadelesi". *Ortadoğu Analiz Dergisi*, Mayıs-Haziran 2020 Cilt: 11 Sayı: 93.

Akcan, N. ve Altun, T. "BAE'nin Son Dönem Teknolojik Atılımları". *Ortadoğu Analiz Dergisi*, Eylül-Ekim 2020 Cilt: 11 Sayı: 95.

* 2022 yılının Temmuz ayı itibarıyla "Akcan" olan soyadım "Kesgin" olarak değişmiştir.

Akcan, N. ve Doğan, A. “Es-Sabah Sonrasında Kuveyt ve Normalleşme Süreci”. *Ortadoğu Analiz Dergisi*, Kasım-Aralık 2020 Cilt: 11 Sayı: 96.

Akcan, N. ve Yetim, M. “Türkiye–KİK Ülkeleri İlişkilerinde Siyaset-Ticaret Etkileşimi”. *Ortadoğu Araştırmaları Merkezi*, Mayıs 2020, Analiz No:248.

Akcan, N. ve Yetim, M. “Körfez İşbirliği Konseyi Ülkelerinin Temel Politik-Ekonomik Parametreleri”. *Ortadoğu Araştırmaları Merkezi*, Aralık 2020, Bakış No:156.

Kitap Bölümü

: Kesgin, N. ve Yetim, M. “KİK Sosyo-Politik Gelişmelerinde Temel Unsurlar”. *21. Yüzyılda Ortadoğu’nun Ekonomi Politikası*, ed. Recep Yorulmaz. Ankara: Nobel Yayınevi, Nisan 2022’de yayımlanması planlanıyor.

Başarılar

: Ufuk Üniversitesi, Siyaset Bilimi ve Uluslararası İlişkiler Bölümü Birinciliği (2016-2017)
Ufuk Üniversitesi, İktisadi ve İdari Bilimler Fakültesi Birinciliği (2016-2017)

İş Deneyimi

Stajlar

: Türk İşbirliği ve Koordinasyon Ajansı Başkanlığı (TİKA) (Temmuz 2017)
Türkiye Büyük Millet Meclisi (TBMM) (Temmuz 2016)
Siyaset, Ekonomi ve Toplum Araştırmaları Vakfı (SETA) (Mart-Haziran 2018)

Eğitimler

: Dışişleri Bakanlığı Stratejik Araştırmalar Merkezi (SAM) Kış Okulu (Ocak 2016)

Çalıştığı Kurumlar

: Ortadoğu Araştırmaları Merkezi (ORSAM) (Mayıs 2019-Devam Ediyor)

Tarih

: 18.02.2022