

KARADENİZ TEKNİK ÜNİVERSİTESİ * SOSYAL BİLİMLER ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER ANABİLİM DALI

ULUSLARARASI İLİŞKİLER PROGRAMI

ABD VE ÇİN'İN SİBER GÜVENLİK ALANINDA KARŞILAŞTIRMALI ANALİZİ

YÜKSEK LİSANS TEZİ

Dila Nur ÖZHANCI

EYLÜL -2023

TRABZON

KARADENİZ TEKNİK ÜNİVERSİTESİ * SOSYAL BİLİMLER ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER ANABİLİM DALI

ULUSLARARASI İLİŞKİLER PROGRAMI

ABD VE ÇİN'İN SİBER GÜVENLİK ALANINDA KARŞILAŞTIRMALI ANALİZİ

YÜKSEK LİSANS TEZİ

Dila Nur ÖZHANCI

Tez Danışmanı: Doç. Dr. Vahit GÜNTAY

EYLÜL-2023

TRABZON

ONAY

Dila Nur ÖZHANCI tarafından hazırlanan “ABD ve Çin’in Siber Güvenlik Alanında Karşılaştırmalı Analizi” Yüksek Lisans Tezinin Tez Yazım Kılavuzu’na Uygun Hazırlanması: Karadeniz Teknik Üniversitesi Sosyal Bilim Enstitüsü Uygulaması” adlı bu Çalışma 03/11/2023 tarihinde yapılan savunma sınavı sonucunda oybirliği / oyçokluğu ile başarılı bulunarak jürimiz tarafından Uluslararası İlişkiler Anabilim Dalı Tezli Yüksek Lisans Programı’nda **yüksek lisans tezi** olarak kabul edilmiştir.

Jüri Üyesi		Karar		İmza
Unvanı - Adı ve Soyadı	Görevi	Kabul	Ret	
Prof. Dr. Metin AKSOY	Başkan	☐	☐	
Doç. Dr. Vahit GÜNTAY	Üye	☐	☐	
Dr. Öğr. Üyesi Göktuğ KIPRIZLI	Üye	☐	☐	

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduklarını onaylarım.

Prof. Dr. Tülay İLHAN NAS
Enstitü Müdürü

BİLDİRİM

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca KTÜ-Sosyal Bilimler Enstitüsü Tez Yazım Kılavuzu'na uygun olarak hazırlanan bu Çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını aksinin ortaya çıkması durumunda her tür yasal sonucu kabul ettiğimi beyan ediyorum.

Dila Nur ÖZHANCI

29/09/2023

ÖNSÖZ

Siber uzay Uluslararası İlişkiler disiplini içerisinde kendisine yer edinmiş önemli bir çalışma alanıdır. Kendine özgü yapısıyla daha önceki yüzyıllarda deniz ve hava alanlarının ön plana çıktığı gibi bu yeni alan da adından söz ettirmektedir.

“Siber Alanda ABD ve Çin’in Dış Politikaları Nelerdir?”, “Siber alanda hangi aktör daha saldırgan bir politikaya sahiptir?” gibi genele ilişkin soruların cevabı için çok farklı yaklaşımlar söz konusudur. Güncel boyut ele alınarak, tartışma alanını oluşturan siber alanda hangi aktörün dış politika yaklaşımının ön planda olduğu ve alana ait kavramlar, ayrıntılı ele alınmaya çalışılan tez konusunun temel yapı taşını oluşturacaktır.

Bu tezde yardımlarını ve fikirlerini eksik etmeyerek beni yönlendiren danışman hocam Doç. Dr. Vahit GÜNTAY’a en derin teşekkürlerimi sunarım.

Eylül, 2023

Dila Nur ÖZHANCI

İÇİNDEKİLER

ÖNSÖZ.....	IV
İÇİNDEKİLER	V
ÖZET.....	VII
ABSTRACT	VIII
TABLolar LİSTESİ.....	IX
ŞEKİLLER LİSTESİ.....	X
KISALTMALAR LİSTESİ	XI
GİRİŞ	1-2

BİRİNCİ BÖLÜM

1. SİBER GÜVENLİK VE SİBER ALAN, KAVRAMSAL ÇERÇEVE.....	3-26
1.1. Siber Güvenliği Anlamak.....	3
1.1.1. Uluslararası Politikada Güvenlik Kavramı	3
1.1.2. Siber Güvenlik Kavramı	7
1.1.3. Dış Politika ve Siber Güvenlik.....	9
1.2. Siber Alan	10
1.2.1. Siber Uzay (Cyberspace)	11
1.2.2. Siber Alanda Mücadele.....	12
1.2.3. Siber Alan ve Küreselleşme.....	14
1.3. Siber Savaş.....	15
1.3.1. Siber Savaş Kavramı.....	16
1.3.2. Siber Terörizm	18
1.3.3. Siber Saldırı	20
1.3.4. Kritik Altyapılar.....	24
1.3.5. Siber Caydırıcılık.....	26

İKİNCİ BÖLÜM

2. DIŞ POLİTİKADA SİBER ALANI YORUMLAMAK.....	28-45
2.1. Dış Politika.....	27
2.1.1. Dış Politika Kavramı.....	29
2.1.2. Dış Politika Araçları	31

2.1.3. Dış Politikada Karar Verme Süreci.....	32
2.2. Dış Politika – Siber Alan İlişkisi.....	35
2.2.1. Siber Alanın Dış Politikadaki Yeri	35
2.2.2. Dış Politikada Siber Savunma Mümkün Mü?.....	36
2.2.3. Dış Politika Karar Verme Sürecinde Siber Alan.....	39
2.2.4. Siber İstihbarat	40
2.3. Dış Politika – Siber Alan İlişkisinin Tarihsel Seyri	42
2.3.1. Siber Alanın Tarihsel Gelişiminde Dış Politikaya Etkisi.....	42
2.3.1.1. Soğuk Savaş Dönemi Gelişmeleri ve Siber Alan	43
2.3.1.2. Soğuk Savaş Dönemi Sonrası ve Siber Alan	44

ÜÇÜNCÜ BÖLÜM

3. SİBER ALANDA ABD VE ÇİN DIŞ POLİTİKALARI.....	46-94
3.1. ABD Dış Politikası ve Siber Alan.....	46
3.1.1. ABD'nin Siber Savaş Yeteneği.....	51
3.1.2. Siber Alanda ABD ve NATO İş Birliği	53
3.1.3. ABD Kurumlarının Siber Alanda İncelenmesi	57
3.1.3.1. Ulusal Güvenlik Teşkilatı (NSA)	59
3.1.3.2. Federal Araştırma Bürosu (FBI)	61
3.1.3.3. Siber Komutanlık (USCYBERCOM).....	63
3.1.3.4. İç Güvenlik Bakanlığı (DHS)	65
3.2. Çin Dış Politikası ve Siber Alan	67
3.2.1. Çin'in Siber Savaş Yeteneği	69
3.2.2. Çin Kurumlarının Siber Alanda İncelenmesi	72
3.2.2.1. Genelkurmay Daireleri	75
3.2.2.2. Teknik Keşif Büroları	77
3.3. Siber Alanda ABD ve Çin Mücadelesi	79
3.3.1. ABD ve Çin Mücadelesinin Teknolojik Boyutu.....	82
3.3.2. ABD ve Çin'in Siber Alana Yönelttiği Saldırgan Politikaları	85
3.3.3. ABD'nin Uluslararası İş Birlikleri ve Baskınlığı, NATO Örneği.....	87
3.3.4. Çin'in Siber Alanda Gelişen Ekonomisi ve Yatırımlar.....	90
3.3.5. İki Ülkenin Dönüşen Dış Politika Kararlarında Siber Alan.....	93
SONUÇ ve ÖNERİLER.....	95
KAYNAKÇA	99
ÖZGEÇMİŞ.....	120

ÖZET

Bu çalışmanın temel konusu Çin ve ABD arasındaki rekabetin siber alandaki yansımalarını değerlendirmektir. Siber alan değerlendirilirken öncelikli olarak bu yeni alanın kavramsal çerçevesi çizilmeye çalışılmıştır. Bu çerçevenin kendine özgü nitelikleri Uluslararası İlişkiler disiplini içerisindeki eski kavramlar ile karşılaştırılmıştır. Siber alanın dünyanın küreselleşme sürecine olan etkisi incelenirken karşılıklı bağımlılık olgusu üzerinden de konu analiz edilmiştir. Daha sonrasında ise savaş, terör, saldırı ve caydırıcılık gibi birçok kavramın siber alan perspektifinden yeniden ele alınmıştır. Bu noktada siber alan ve siber güvenlik kavramlarından yola çıkılmış olup daha sonra siber alan ve dış politika ilişkisine yoğunlaşmıştır. Çalışmanın son bölümünde ise ana konu olan ABD ve Çin rekabeti ele alınırken bu rekabetin hangi araçlar aracılığıyla tırmandırıldığına değinilmiştir.

Anahtar Kelimeler: ABD-Çin, Siber Güvenlik, Dış Politika, Yeni Tehditler, Rekabet

ABSTRACT

The main subject of this study is to evaluate the reflections of the rivalry between China and the US in the cyber domain. While evaluating cyberspace, first of all, the conceptual framework of this new field has been tried to be drawn. The specific characteristics of this framework are compared with the old concepts within the discipline of International Relations. While examining the impact of cyberspace on the globalization process of the world, the issue was also analyzed through the phenomenon of interdependence. Afterward, many concepts such as war, terrorism, aggression, and deterrence are re-examined from the perspective of cyberspace. At this point, the concepts of cyberspace and cybersecurity were started and then the relationship between cyberspace and foreign policy was focused on. The last part of the study deals with the main topic, the US-China rivalry, and the instruments through which this rivalry has escalated.

Keywords: US-China, Cybersecurity, Foreign Policy, New Threats, Rivalry

TABLÖLER LİSTESİ

Tablo Nr.	Tablo Adı	Sayfa Nr.
1	Güvenliğin Etki Ettiği Sektörler	5
2	Dış Politika İşlevlerinin Geleneksel Hiyerarşisi	6
3	Son 200 Yıl İçerisinde Yaşanan 5 Teknolojik Devrim.....	8
4	Siber Savaş Karşısında Panik Olanlar, Kuşku Duyanlar ve Gerçekçi Yaklaşımlar	18
5	Hükümetin Karar Verme Sürecinde Yaşanan Değişimler	33
6	Küresel Siber Güvenlik Endeksi 2014 ve 2017 Verileri.....	46
7	Clarke ve Robert’a Göre Ülkelerin Siber Güvenlik Puanlamaları.....	47
8	Uluslararası Telekomünikasyon Birliğine Göre Ülkelerin Siber Güvenlik Puanlamaları (ITU 2015, 2017, 2018).....	48
9	Siber Güvenlikte Sekiz Önemli Öncelik.....	50
10	Siber Çatışmanın Aşamaları	52

ŞEKİLLER LİSTESİ

Şekil Nr.	Şekil Adı	Sayfa Nr.
1	Modern Toplum, Yapay Zeka ve Nesnelerin İnterneti (IoT) Arasındaki İlişkinin Gelişim Süreci	12
2	Siber Caydırıcılık Teorisi	13
3	Siber Terörün Yapısını Tanımlayan Unsurlar	20
4	Siber Saldırı Anatomisi.....	23
5	Siber Suç, Siber Savaş ve Siber Saldırı Arasındaki Ayrım	24
6	ABD Kritik Altyapı Risk Yönetimi	25
7	Uluslararası İlişkiler, Dış Politika ve Diplomasi	29
8	Bir Devletin Dış Politikasını Belirlerken Ele Alması Gereken Özellikler.....	30
9	Bir Devletin Dış Politika Katmanlarının Analizi.....	31
10	Dış Politikanın Makroskobik Haritası	34
11	AB'nin Siber Tehditlere Karşı Cevabı.....	37
12	Siber İstihbarata Dayalı Savunma Diyagramı.....	40
13	Siber Güvenlikle İlgili Emir Komuta İlişkisi.....	65

KISALTMALAR LİSTESİ

AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
ADCO	: Abu Dabi Kıyı Petrol Operasyonları Şirketi
ADNOC	: Abu Dabi Ulusal Petrol Şirketi
AFAD	: İçişleri Bakanlığı Afet ve Acil Durum Yönetimi Başkanlığı
AFSA	: Silahlı Kuvvetler Güvenlik Servisi
APT	: Geliştirilmiş Kalıcı Tehditler
ARPANET	: Gelişmiş Araştırma Projeleri Ajansı
ASAT	: Anti Uydu Silahı
BİS	: Bilgi ve İletişim Sistemleri
BM	: Birleşmiş Milletler
BRICS	: Brezilya, Rusya, Hindistan, Çin ve Güney Afrika Cumhuriyeti
C2	: Komuta ve Kontrol Trafikini
CAC	: Çin Siber Uzay İdaresi
CCCI	: Çin Siber Güvenlik ve Bilişim Merkezi Komisyonu
CCD COE	: NATO Mükemmeliyet Merkezi
CCS	: Siber Suç Bölümü
CDMA	: Siber Savunma Yönetim Otoritesi
CERT	: Ülkede Bulunan Bilgisayar Acil Müdahale Ekibi
CIA	: Amerikan Haber Alma Örgütü
CIRT	: Siber Olaylar Müdahale Ekibi
CISO	: Baş Bilgi Güvenliği Görevlisi
CLSGISI	: Devlet Ekonomik Bilgi Yönetimi Öncü Küçük Grubu
CMF	: Siber Görev Gücü
CNCERT	: Ulusal Bilgisayar Ağı Acil Müdahale Teknik Ekip Koordinasyon Merkezi
CNO	: Bilgisayar Ağı Operasyonları
CNSS	: Siber Ulusal Güvenlik Bölümü
COSTIND	: Çin Milli Savunma Bilim, Teknoloji ve Sanayi Komisyonu
CPECC	: Çin Petrol Mühendislik ve İnşaat Anonim Şirketi
CPMIEC	: Çin Hassas Makine İthalat-İhracat Şirketi
CSIRT	: Bilgisayar Güvenliği Müdahale Ekibi
CSIS	: Stratejik ve Uluslararası Çalışmalar Merkezi
CTIIC	: Siber Tehdit İstihbarat Entegrasyon Merkezi

CVE	: Yaygın Güvenlik Açıkları ve Maruziyetler
ÇİN	: Çin Halk Cumhuriyeti
ÇKP	: Çin Komünist Parti
DARPA	: Savunma İleri Araştırma Projeleri Ajansı
DDOS	: Dağınık Servis Engelleme Hizmeti
DHS	: İç Güvenlik Teşkilatı
DIB	: ABD Savunma Sanayi Üssü
DOD	: ABD Savunma Bakanlığı
DOJ	: ABD Adalet Bakanlığı
DPA	: Dış Politika Analizi
DSL	: Çin Veri Güvenliği Kanunu
DTÖ	: Dünya Ticaret Örgütü
Ed	: Editor
ENISA	: Avrupa Ağ ve Bilgi Güvenliği Ajansı
FBI	: Federal Araştırma Bürosu
FYPNI	: Çin 14. Beş Yıllık Ulusal Enformasyon Planı
GGE	: BM Hükümet Uzmanlar Grubu
IDF	: İsrail Savunma Kuvvetleri
IOT	: Nesnelerin İnterneti
IP	: İnternet Adresi
ISO	: Uluslararası Standartlar Birliği
ISS	: İnternet Hizmet Sağlayıcıları
IT	: Bilgi Teknolojisi
ITU	: Uluslararası Telekomünikasyon Birliği
KDHC	: Çin Siber Tehdit İstihbarat Ekibi
KDPA	: Karşılaştırmalı Dış Politika Analizi
KYG	: Kuşak Yok ve Girişim
MASEGK	: Merkez Askeri-Sivil Entegrasyon Geliştirme Komisyonu
MIIT	: Çin Sanayi ve Bilgi Teknolojileri Bakanlığı
MPS	: Çin Kamu Güvenliği Bakanlığı
MSS	: Çin Devlet Güvenlik Bakanlığı
NAS	: Ağa Bağlı Depolama Cihazları
NASA	: Ulusal Havacılık ve Uzay İdaresi
NATO	: Kuzey Atlantik Anlaşma Örgütü
NCCIC	: Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi
NCIJTF	: Ulusal Siber Araştırma Birleşik Gücü
NCIRC	: NATO Bilgisayar Olaylarına Müdahale Yeteneği
NCSA	: NATO İletişim ve Enformasyon Sistemleri
NCSS	: Çin Ulusal Siber Güvenlik Stratejisi

NIATC	: NATO Bilgi Güvenliđi Teknik Merkezi
NIPC	: Ulusal Altyapı Koruma Merkezi
NEEC	: NATO Ağ ile Etkinleştirilmiş Güç Programı
NPC	: Çin Ulusal Kongresi
NPO	: Çin Yeni Politika Görüşü
NSA	: Ulusal Güvenlik Teşkilatı
NSS	: ABD Ulusal Güvenlik Sistemleri
ODNI	: Ulusal İstihbarat Direktörü Ofisi
OEWG	: Müzakereye Açık Çalışma Grubu
PIPL	: Çin Kişisel Bilgilerin Korunması Kanunu
PLA	: Çin Kurtuluş Örgütü
PPD-41	: Siber Olay Koordinasyonu Başkanlık Politikası Direktifi
RRRTs	: Hızlı Tepki Takımları
SAP	: Çin Stratejik Eylem Planı
SASTIND	: Çin Ulusal Savunma Bilim, Teknoloji ve Sanayi Devlet İdaresi
SCIO	: Çin Danıştay Bilgi Ofisi
SILG	: Çin Devlet Bilişim Öncü Grubu
SNISCSG	: Çin Devlet Ağı ve Bilgi Güvenliđi Koordinasyonu Küçük Grubu
SOHO	: Küçük Çaplı Ev/Ofis Ağ Yönlendiricileri
SSCB	: Sovyet Sosyalist Cumhuriyetler Birliđi
SSF	: Çin Stratejik Destek Gücü
STC	: Bilim ve Teknoloji Komitesi
TDK	: Türk Dil Kurumu
TTPs	: Prosedürler
USCYBERCOM	: ABD Siber Komutanlık
USG	: Daha Geniş ABD Hükümeti
USSTRATCOM	: ABD Stratejik Komutanlık
VPS	: Sanal Özel Sunucu
2/PLA	: Çin Genelkurmay Başkanlığı 2. Daire
3/PLA	: Çin Genelkurmay Başkanlığı 3. Daire
4/PLA	: Çin Genelkurmay Başkanlığı 4. Daire

GİRİŞ

Soğuk Savaş döneminin ardından Uluslararası İlişkiler (Uİ) sistemi çok kutuplu bir boyuta evrilmiştir. Özellikle son dönemlerde yaşanan teknolojik gelişmeler uluslararası arenayı etkilemiştir. Bu yeni dönem de siber uzay; kara, deniz ve hava alanlarından sonra literatürdeki yerini almıştır. Devletler arasındaki sınırlar geçerliliğini yitirdiği için klasik güvenlik anlayışı yeni dönemde tehdit ve riskler karşısında yetersiz kalmıştır. Siber alanın mevcudiyeti ise yeni tehdit ve riskleri başka bir boyuta taşımıştır. Klasik yaklaşımların geçerliliği yitirmesinin siber güvenliği ön plana taşımasının yanı sıra güvenlik, dış politika, tehdit, saldırı, savaş ve caydırıcılık gibi birçok kavramın yeniden tanımlanmasına da ihtiyaç duyulmuştur.

Dış politika Uİ sistemi içerisinde her aktör için zorunlu bir araçtır. Uİ disiplini içerisindeki temel aktör sayılan devletlerin iç ve dış güvenliğini birleştiren bu kavram sistem içerisindeki olayları yorumlama da bizlere yeni bir bakış açısı kazandıracaktır. Yeni teknolojik gelişmeler sayesinde dış politika artık farklı ele alınmalıdır. Çalışmanın konusu olan ABD ve Çin'in siber alana yansıyan rekabeti teknolojik gelişmelerin ülkelerin dış politika süreçlerine nasıl etki ettiğini yansıtacaktır. Bu doğrultuda özellikle bu rekabet Çin'in var olan gücünü ABD ile olan mücadelesine aktarmasından ziyade kendi etki alanına yöneltmesinin bir sonucu olarak saldırgan politikaları tercih etmemesi devletler için siber alanın dış politika çalışmalarında nasıl yorumlanacağı konusunda önem kazanmakla beraber uluslararası arenada ön plana çıkan bu iki devletin siber alana yansıyan güç mücadelesi ilgileri üzerlerine çekmiştir.

Siber uzayın literatürdeki yerini alması aynı zamanda birden fazla sayıda durmaksızın ilerleyen her biri farklı bir etki boyutuna sahip uzayların kombinasyonu modern toplumda Uİ sistemindeki tüm aktörleri kapsayacaktır. Bu yeni alan karşımıza mücadele ve iş birliğinin farklı kombinasyonlarını sunacaktır. Soğuk Savaş sonrasında uluslararası arena da etkin olan ABD karşısında hem ekonomik hem de siyasi olarak yükselen Çin potansiyel olarak güçlü bir rakiptir. Yeni alanın sınırlarının belirsiz olması aktörlerin daha rahat hareket etmesine imkan tanımaktadır. Uluslararası hukukun yetersiz kalması da siber saldırılar noktasında caydırıcılığı azaltmaktadır.

Çin ve ABD arasındaki rekabetin siber alandaki yansımasının stratejik belgeler, başkanlık direktifleri, resmi açıklamalar, sosyal medya ve güncel çalışmalar aracılığıyla değerlendirilmiştir. Çalışmanın hipotezi ise dış politika metodolojisinden yola çıkılarak karşılaştırma yöntemi aracılığıyla Çin ve ABD'nin siber alandaki rekabetinin analizinde Çin'in yansıtıldığı kadar saldırgan olmadığıdır. Her ne kadar büyüyen siyasi, ekonomik ve askeri güç kapasitesi açısından

ele alındığında Çin, ABD karşısında güçlü potansiyel bir düşman olsa dahi Çin var olan gücünü daha çok kendi etki kapasitesini arttırmak için kullanmaktadır.

Birinci bölümde değişen güvenlik algısında siber güvenlik kavramına nasıl yer verileceği üzerinde durulmuştur. Uluslararası politika da güvenlik kavramına yer verildikten sonra dış politika ve siber güvenlik arasındaki ilişki analiz edilmiştir. Daha sonrasında siber uzay tanımlanmıştır. Siber uzay kavramına yer verildikten sonra siber alan ile küreselleşme arasındaki ilişki irdelenirken siber savaş, terörizm, saldırı, kritik altyapı ve caydırıcılık kavramlarına yer verilmiştir.

İkinci bölümde dış politikadaki karar alıcı mekanizmalar tarafından siber alanın nasıl yorumlanması gerektiğine dikkat edilmiştir. Klasik güvenlik anlayışının yetersiz kaldığı noktalar vurgulanırken dış politika araçlarında yaşanan değişimlere yer verilmiştir. Soğuk Savaş öncesi ve sonrası dönemlerinin siber alan ile ilişkisine ayrıntılı bir şekilde yer verilmiştir.

Son bölümde ise siber alanda ABD ve Çin arasındaki rekabet ön plana çıkarılmıştır. İlk olarak ABD dış politikası ve siber alan yorumlanmıştır. ABD siber savaş yeteneği, ABD ve NATO arasındaki iş birliği ve siber alanda ön plana çıkan ABD kurumlarına yer verilmiştir. Özellikle bu noktada NSA, FBI, USCYBERCOM ve DHS vurgulanmıştır. İkinci olarak Çin dış politikası ve siber alan ele alınmıştır. Çin'in siber savaş yeteneği analiz edilirken PLA, Çin Genelkurmay Daireleri ve keşif bürolarına değinilmiştir. Son kısımda siber alanda hangi aktörün daha saldırgan politikalara sahip olduğu sorusuna cevap verilmeye çalışılmıştır.

BİRİNCİ BÖLÜM

1. SİBER GÜVENLİK VE SİBER ALAN, KAVRAMSAL ÇERÇEVE

1.1. Siber Güvenliği Anlamak

Siber güvenlik kavramının anlaşılabilmesi için öncelikle uluslararası politika içerisinde güvenliğin ne olduğu tanımlanmalıdır. Güvenliğin tüm taraflarca kabul gören bir tanımı yoktur. Bu kısımda siber güvenlik kavramının daha iyi analiz edebilmesi için ulusal güvenliğin sağlanması için gerekli tüm altyapı mekanizmalarının güvenliği üzerinde durulmuştur.

Güvenliğin etki ettiği sektörler incelendiğinde ulusal güvenliğin daha çok devletlerin sahip oldukları askeri imkan ve kapasitelerine göre şekillendiği görülmektedir. Ancak Uİ disiplini içerisinde meydana gelen gelişmeler sonucunda devletlerin güvenlik anlayışları değişmiştir. Soğuk Savaş döneminin sonlarına doğru siyasi, ekonomik, sosyal ve çevresel konular güvenlik analizlerine dahil edilmiştir. Soğuk Savaş sonrası dönemde ise bireysel, ulusal ya da uluslararası güvenliğin yanı sıra toplumsal güvenlik tartışılmaya başlanmıştır. Dolayısıyla realistlerin ön plana çıkardığı askeri ve siyasi tabanlı güvenlik alanlarına alçak politika içerisine dahil edilen diğer konular eklenmiştir.

Güvenliğin genişleyen tanımları içerisinde siber güvenlik sadece somut olanı ortaya çıkarmamaktadır. Teknolojik gelişmeler aracılığıyla küreselleşen ekonomi ve bilgi işleme süreçlerindeki farklılıklar farklı bir boyuta evrilmiştir. Her türlü veri akışının dijitalleşmesi ve durmaksızın ilerlemesi siber güvenlik kavramının önemini ortaya çıkaracaktır. 1990'lı yıllardan sonra internetin sivil kullanıma açılması ve 2000'li yıllardan sonra telekomünikasyon teknolojisinde yaşanan gelişme sayesinde sadece devletler değil kurumlar, şirketler, siyasi ve ekonomik yapıların yanı sıra bireysel güvenliğin önemi artacaktır.

Realist perspektife göre Uİ disiplini içerisinde yer alan en önemli aktör olan devletler uluslararası sistemdeki güç dengesinin korunması için güvenlik kavramına ayrı bir önem vermiştir. Siber güvenlik devletlerin dış politika çıktıklarına yansıyan yeni bir mücadele biçiminin varlığına etki etmiştir. Ulusal sınırların geçerliliğinin kaybedilmesi ulusal güvenlik gereksinimlerinin yeniden tanımlanmasını zorunlu kılmıştır. Siber güvenlik ulusal güvenliğin ayrılmaz bir parçası haline gelmiştir. Ulusal güvenlik artık devlet sınırlarını baz alan kısıtlı bir tehdit alanına dahil değildir. Bu durum Uİ içerisindeki güç dengelerini etkileyecektir. Güç dengeleri yeniden

kurulurken asimetrik güç dağılımları da ortaya çıkmıştır. Kritik altyapıların güvenliği burada ön plana çıkmaktadır.

1.1.1. Uluslararası Politikada Güvenlik Kavramı

Uİ disiplini içerisinde güvenlik çalışmaları özel bir yere sahiptir. Özellikle güvenliğin kim için ve nasıl sağlanacağı gibi birçok soru güvenlik hakkında fikir elde etmemize yardımcı olacaktır. Elbette bütün güvenlik tanımlarının ortak özelliklerini birleştirmek olası değildir. Fakat güvenlik kavramına yöneltilen her soru aynı zamanda bu kavramda anlam genişlemesinin sebebidir. Temelde güvenlik nesne (özne) ve çevresindekiler arasındaki ilişkiyi ifade etmektedir. Klasik olarak güvenlik kavramı üç şekilde ele alınabilir. İlk olarak güvenlik geleneksel anlamda yorumlanmaktadır. Devletler için temel olarak güvenlik askeri çatışmanın olmamasıdır. Dolayısıyla geleneksel güvenlik askeri güvenlik olarak değerlendirilebilir. Elbette güvenliğin daha geniş bir perspektiften ele alınmalıdır. Uluslararası arenada meydana gelen doğrudan ya da dolaylı olarak devletler arasında cereyan eden olgular ön plana çıkmaktadır. İkinci olarak bir kamu malı olarak güvenlik ele alınabilir. Son olarak ise evrensel anlamda güvenlik bir diğer ifade ile insan güvenliğidir. Burada asıl kastedilen bir birimin, sosyal varlığın güvenliğidir.

Güvenlik kavramını daha iyi anlayabilmek için kavram etimolojik olarak incelenmelidir. Bu noktada iki yaklaşım söz konusudur. İlk yaklaşım güvenlik kavramının Latince securus safe kavramına dayanmasıdır. -se olmadan +cura, care güvende olmayı ya da tehlikeden arınmayı, özür olmayı ifade etmektedir. İkinci yaklaşım ise klasik anlamda güvenliğin securites kavramına dayanmasıdır. Güvenlik bu noktada kaygının yokluğudur (Liotta, 2002: 477).

Güvenlik kavramı üzerine birçok çalışma yapılmış olup bu çalışmalarda güvenlik tanımlanmaya çalışılmıştır. Ancak güvenlik kavramının ele alındığı farklı yaklaşımlar olmasına karşın realistler için bu kavramın tanımı oldukça sadedir. Hans Morgenthau (1960) çalışmasında, “Ulusal güvenliği, ulusal bölgenin ve kurumlarının bütünlüğü olarak tanımlamıştır.” Burada güvenlik kavramına en yakın kavram olarak ulusal güvenlik ele alınmıştır.

Uluslararası politika içerisinde güvenlik olgusunun yorumlanması için öncelikli olarak güvenlik kavramının ne olduğunu ele alınmıştır. Güvenliğin etimolojik olarak incelenmesi politika kavramı içinde yararlıdır. Politikanın kökeni esas olarak polis kavramına aittir. Polis; “site, kent, yöre ve vatandaşların toplandığı şehir” demektir. Burada dikkat edilmesi gereken nokta vatandaşların toplandığı bu şehir yapısının sistemidir. Bu sistem belli bir siyasal rejimi temsil etmektedir. Bu anlamda politika kelimesi tam olarak polise ait unsurları barındırmaktadır (Küçükalp, 2012: 23). Bütün bu unsurlar birleştiğinde politika kavramına olan bakış açımız netlik kazanacaktır. Ulusal ve uluslararası politikaları daha iyi anlamlandırabilmek için politik çerçeve analiz edilmelidir.

Ulus devlet yapılanmasında devletin bekası için öncelikli olan devletin çıkarlarıdır. Bu noktada Kardinal Richelieu'nun ortaya attığı *raison d'état* kavramı yol göstericidir (Kissinger, 2014: 50). Çünkü devletin bekası diğer tüm ihtimallerin üzerindedir. Karar alıcı mekanizma için en önemli husus devletin çıkarları doğrultusunda geliştirilen ulusal politikalar. Uluslararası sistem içerisinde ise hem ulusal hem de uluslararası politikalar oldukça önemlidir.

Uİ disiplini için tartışmaya açık olan bu kavram devletlerin güvenlik algılarında da değişimlere sebep olmuştur. Temelde hem gruplar hem de bireyler için olası tehdit ihtimallerinin ortadan kaldırılması noktasında genel bir kanı oluşmuştur. Ancak güvenliğin kim için sağlanacağı konusu tartışmalıdır. Güvenlik olgusu bireysel, ulusal ya da uluslararası bir perspektiften değerlendirilebilir

Tablo 1: Güvenliğin Etki Ettiği Sektörler

Sektör	Referans Nesnesi
Askeri	Devletler veya diğer siyasi oluşumlar
Siyasi	Egemenlik
Ekonomik	Firmalar
Sosyal	Kolektif kimlikler (uluslar ve dinler)
Çevresel	Çok geniş (insan türünden biyosferin geri kalanına kadar)

Kaynak: Buzan vd., 1998: 5-6.

Tabloda da belirtildiği gibi güvenliğe etki eden alanlar farklılaşmıştır. Ulusal güvenlik daha çok devletlerin sahip oldukları askeri imkân ve kapasitelerine göre şekillenirken son zamanlarda devletlerin güvenlik algısında değişimler gözlemlenecektir. Bu noktada Barry Buzan; güvenlik olgusuna sadece askeri boyuttan yaklaşmamıştır. Siyasi, ekonomik, sosyal ve çevresel konular da güvenlik analizleri kapsamına alınmıştır (Buzan, 1983: 214).

Özellikle yaşanan bu gelişmelerle birlikte Soğuk Savaş sonrasında bireysel, ulusal ya da uluslararası güvenliğin yanı sıra toplumsal güvenlik kavramları da tartışılmaya başlanmıştır (Kaldor, 1999). Güvenlik kavramı birçok parametreyi kapsamadığı için bu kavramın çerçevesi çizilirken bütün tarafların onayladığı genel bir tanım yapmak zordur (Özcan, 2011: 447-448). Elbette burada tehlikenin nasıl değerlendirildiği de oldukça önemlidir. Güvenlikle ilgili yapılan değerlendirmelerde objektif kriterler kadar sübjektif yaklaşımlar da karşımıza çıkmaktadır. Buradaki objektif güvenlik, bir tehlikenin var olmadığını, sübjektif güvenlik ise şüphelenilecek bir tehlikenin olmadığına inanma durumunu ifade etmektedir (Caşın vd, 2007: 64).

Uİ disiplini içerisinde yer alan güvenlik çalışmaları II. Dünya Savaşı sonrasında literatürde yerini almıştır. Elbette bu çalışmalardaki güvenlik yaklaşımının kapsamı sınırlıdır. Realist bir perspektif baz alınarak değerlendirmeler yapıldığı için daha çok askeri alana yoğunlaşmıştır

(Yılmaz, 2007: 70). Realistler, askeri ve siyasi konuları yüksek politika olarak kabul ettiği için ulusal güvenlik politikalarının temeli askeri ve siyasi tabanlı olmalıdır. Ekonomi, sağlık, çevre ve benzeri konular ise alçak politika içerisinde dahil edildiği için ikinci planda değerlendirilmelidir (Oğuzlu, 2007: 14).

Tablo 2: Dış Politika İşlevlerinin Geleneksel Hiyerarşisi

Somut Çıkarlar	Ulusal Güvenlik Ekonomik Çıkarlar Gelişme	Yüksek Politika Konuları
İnsani Değerler	İnsanlık Onuru ve Sağlık	Alçak Politika Konuları

Kaynak: Feldbaum ve Michaud, 2010.

Yukarıda yer alan tablo alçak politika ve yüksek politika konularına dahil olan alanları göstermektedir. Yüksek politika konularına maddi ve somut bileşenler dahil edilirken alçak politika konularına daha çok insani değer ve yargıları dahil edilmektedir. Uİ disiplini içerisinde yer alan idealizm ya da liberalizm güvenlik olgusuna realistlerden farklı yaklaşmaktadır. Liberallere göre uluslararası güvenliği sağlayabilecek koşullar sadece yüksek politika konuları değildir. Realistlerin alçak politika olarak değerlendirdiği ekonomi ve ticaret gibi unsurlar da uluslararası güvenliğin bileşenleri olabilir (Caşın vd, 2007: 229-234).

Teorilerin güvenlik kavramına farklı yaklaşmasının yanı sıra Uİ disiplini için güvenlik kavramında meydana gelen dönüşüm Soğuk Savaş dönemine aittir. Uİ disiplini I. Dünya Savaşı sonrasında bağımsız olarak tarih sahnesinde yerini almıştır (Burchill ve Linklater, 2012: 18). Güvenlik kavramı ise II. Dünya Savaşı sonrasında analiz edilmeye başlanmıştır. Soğuk Savaş dönemine kadarki süreç bizleri askeri kapasite ve maddi imkânlarla yoğunlaştırmıştır. Soğuk Savaş dönemi güvenlik algısı ise güvenlik politikalarını ön plana çıkarmıştır. Güvenlik tehdidinin temeli bizzat devletlerdir. Göz ardı edilmesi mümkün olmayan güvenlik olgusu özgürlük ile iç içedir. Soğuk Savaş sonrası dönem ise devletlerin güvenlik politikalarına olan yaklaşımını kökünden değiştirdiği bir dönem olduğu için eski tehdit algıları geçerliliğini yitirmiştir. Artık tehdit unsurları tek boyutlu değildir. Asimetrik tehdit unsurları önem kazanmıştır. Tehditlerin kaynağı, zamanı ve şeklini önceden tahmin etmek olası değildir. Bu durum özellikle uluslararası güvenlik politikalarını etkilemiştir.

Güvenlik kavramında yaşanan en can alıcı dönüşüm ise tehdidin artık sınır tanımamasıdır. Dolayısıyla sınırlı bir coğrafyayı baz alan tehdit algısı geçerliliğini yitirdiği için tüm ülkeler artık tehdit altındadır (Koçer, 2005: 288).

1.1.2. Siber Güvenlik Kavramı

Gerçek olan artık sadece somut olan değildir. Gerçeklik, bilginin evrilmesiyle günümüz dünyasındaki teknolojik gelişmeler ışığında küreselleşen ekonomi ve bilgiyi işleme süreçlerindeki farklılıkla birlikte başka bir boyuta evrilmiştir. Artık devletler için ulusal güvenlik kadar toplumsal güvenlik de ön plana çıkmıştır. Toplumsal güvenlik artık ön görülemeyen unsurlar ya da kişiler tarafında tehdit edilebilmektedir. Aslında bu değişim artık bir dünya kültürüdür. Wallerstein (2013: 4)’ın “Bizim bugün, dünya genelinde kültürel olarak bulunduğumuz nokta budur. Kendimizi, bilgi kaynak ve kurumlarının denetimi için sürdürülen bir mücadeledeki ithamların çatışması içerisinde buluyoruz” ifadesiyle de anlatmak istediği bu kültürün aslında çatışmaları tetiklediğidir. Elbette buradaki çatışma alanı geçmiş dönemlerde karşımıza çıkan kara, hava, deniz ve uzayda sürdürülen mücadelelerden oldukça farklıdır. Yeni mücadele alanı sayesinde bilişim ve haberleşme teknolojileri, telsiz sensor ağları, uzay teknolojileri, internet, ileri malzemeler, nanoteknoloji, biyoteknoloji, nano-solar enerji pilleri, temiz enerji, yapay zekâ, derin öğrenme, gen mühendisliği, nesnelerin interneti, sezgisel algoritmalar ile ilgili çalışmalar mevcut paradigmaları altüst etmiştir (Çiftçi, 2013: 2).

Aslında bu dönüşümün temel parametresi olan bilginin ve dahası bilgi toplumunun kaynağı analiz edilmelidir. Bilgi, Latince “informato” kökünden türemiştir. “biçim verme”, “biçimlendirme” ve “haber verme” anlamlarında kullanılmaktadır. Düşünsel ürün ya da öğrenilen şey olarak da tanımlanabilmektedir. Esasen bilgi yönetsel bir karar alırken stratejik bir öneme sahiptir (Öğüt, 2003: 9). Modern dünyanın evrildiği bilgi düzeyini tanımlamak için ortak bir paydadan bahsetmek zordur. Ancak bilim ve teknolojinin ön görülemez ilerlemesinin sonucu olan bilgi ve bilgi teknolojilerinin toplumsal ve ekonomik alanları ne kadar etkilediği göz önüne alınırsa Toffler’ın “üçüncü dalga” olarak adlandırdığı seviye “bilgi çağı” dır. Bu noktada bu döneme ait toplumsal yapı da “bilgi toplumu” olarak adlandırılacaktır (Özden, 2002: 15). Bu sürecin literatürdeki karşılığı da Enformatik yüzyıldır. Bilgi artık üretim için esas kaynaktır. Sürekli öğrenme ve bilgilenme aracılığıyla değişim ve gelişme kaçınılmazdır. Artık dünya yeni toplumsal ve ekonomik örgütlenme biçimini kabul etmiştir. Bilgi çağı bütün aktörler için öğrenmeyi mümkün kılmaktadır (Öğüt, 2003: 5). Bu durum Sanayi Devrimi’nden sonra tecrübe edilen en önemli olaydır. Dolayısıyla Enformasyon Devrimi’nin ekonomik, siyasal, toplumsal ve kültürel alanlarda ve ilişkilerde köklü değişimlere yol açacağı düşünülmektedir (Kaplan, 1991: 5).

Tablo 3: Son 200 Yıl İçerisinde Yaşanan 5 Teknolojik Devrim

Çağ	Başlangıç Tarihi	Tanım
Sanayi Devrimi	1771	Cromford Mill'in İngiltere'de Açılması
Buhar ve Demiryolları Çağı	1829	İngiltere'de Liverpool-Manchester Demiryolu'nun Açılmasıyla Başlayan Buharlı Tren Seferleri
Çelik, Elektrik ve Ağır Mühendislik Çağı	1875	Pensilvanya, Pittsburgh'da Carnegie Bessemer Çelik Fabrikasının Açılması
Petrol, Otomobil ve Seri Üretim Çağı	1908	İlk Ford Model T'nin Detroit, Michigan, ABD'de Üretimi
Bilgi ve Telekomünikasyon Çağı (Dijital Çağ)	1971	Intel mikroişlemcinin Santa Clara, Kaliforniya'da İlanı

Kaynak: West ve Dave, 2022.

Yukarıdaki tabloda yer alan gelişmeler Dijital Çağ'ın geçirdiği evreleri yeni çalışma biçimleriyle ortaya koymaktadır. Modelleme Cromford Mill'de dünyanın ilk suyla çalışan iplik fabrikasının açılmasıyla başlamıştır. Bu modelleme 1971 yılında Intel mikroişlemcinin Kaliforniya'da açılmasına kadarki süreci baz almıştır. Bu model karmaşık, sürekli değişen bu yeni dünyaya anlam vermemize yardımcı olacaktır. Özellikle bu noktada önemli olan Dijital Çağ'da hayatta kalabilmenin zorluğudur. Tecrübe edilen dijitalleşme süreci tüm dünyayı etkileyecektir.

Güvenlik algısının toplumu tehdit eden yapısını ele alındığında bu noktada en önemli yer internete aittir. Her türlü veri akışının dijitalleşmesi ve durmaksızın ilerlemesi siber güvenlik kavramının doğmasına sebep olacaktır. 1990'lı yıllardan sonra internet sivil kullanıma açılmıştır. Dolayısıyla artık bireylerin somut alanlarına dijital ve sanal ortamlar da dâhildir. Siber uzay adını verdiğimiz bir diğer kavram ortaya çıkmıştır. 2000'li yıllardan sonra telekomünikasyon teknolojisinin gelişmesiyle beraber sadece kurumların, şirketlerin, siyasi ve ekonomik yapıların değil bireylere ait verilerin de güvenliği ön planda olacaktır.

Günümüzde internet kullanıcılarının sayısı 5,16 milyardır. Bu rakam toplam dünya nüfusunun %64,4'üne denk gelmektedir (Digital Around The World 2023, <https://datareportal.com>). Ancak burada dikkat edilmesi gereken bir nokta vardır. Güvenlik olgusu internetin ortaya çıkmasından sonra tartışılmaya başlanmıştır. Çünkü internetin gelişim göstermesine etki eden temel parametreler kullanım kolaylığı, düşük maliyet ve evrensel olmasıdır. İnterneti kullanma yetkisinin verebileceği potansiyel zararlar üzerinde durulmamıştır. Dolayısıyla internetin etki kapasitesi dikkate alındığında güçlü savunma sistemleri geliştirilmelidir. Acil durum hazırlıkları şarttır. Saldırıları gerçekleştiği ilk anda tespit edilmelidir, sanal ya da fiziksel bariyerler inşa edilmelidir. Ulusal ve bölgesel siber güvenlik politikalarının siber güvenlik kavramını şekillendirdiği boyut artık bir zorunluluktur (Goodman, 2008: 27-31).

1.1.3. Dış Politika ve Siber Güvenlik

Dış politika esasen bir devletin başka bir devlete veya devletlere karşı uluslararası arenada yürüttüğü politikalar (Sondermann, 1961: 8). Devletlerin dış politika eksenini ulusal çıkarlarını yansıtmalıdır. Bu noktada ulusal çıkarları en iyi yansıtan araçlar dış politikaya ait karar alıcı mekanizmalardır. Karar alıcı mekanizmalar karşısında devlet hukuksal statüsüyle karşımıza çıkmaktadır. Modern anlamda devlet, sınırları belirlenmiş bir ülke toprağı üzerinde bulunan, belli bir hükümet ile yönetilen ve hukuksal olarak egemen olan bir yapıdır. Devlet aslında milletin hukuki kişilik kazanmış hali olarak değerlendirilebilir (Arı, 1997). Bu durum da politikaya egemen olan aktörler devletlerdir.

Devletlerin uluslararası sistemdeki etkinlikleri devletlerin siyasal yapısı ve niteliği kadar önemlidir. Çünkü devletin devamlılığı ve gelişimini sürdürmesi sadece iç politika ile sağlanamaz. Devletlerin diğer ülkelere yönelik tutum ve davranışları da dikkate alınmalıdır. Dış politika unsurları geniş bir perspektiften konuya dahil edilmelidir (Sönmezoğlu, 1992).

Dış politika unsurları geniş bir perspektiften ele alındığında bazı faktörler ön plana çıkmaktadır. Hem iç hem de dış faktörlerin çerçevesi çizilmelidir. Özellikle iç faktör olarak kastedilen unsurlar ülkelerin sınırları içerisinde gerçekleşen gelişmelerdir. Ülkenin yönetim şekli, yönetimde hâkim olan ideoloji, toplumun çoğunluğunun sahip olduğu inanç biçimi, ahlaki değerler, liderlerin özellikleri, devlet-toplum yapısı gibi birçok etmen ele alınabilir. Dış faktörler ise dış politikadaki karar alıcı mekanizmaların kontrol edemedikleri, ülke sınırları içerisinde ortaya çıkmayan gelişmelerdir. Devletlerin dahil olduğu bölgelerin ve genel olarak uluslararası yapının özellikleri ön plana çıkmaktadır. Uluslararası sistemdeki güç dengesi ve ülkenin genel güç dağılımındaki konumu ve diğer dış ülkelerde meydana gelen gelişmeler daha belirgindir (Bilgin, 2005: 175-201).

Devletler için iç ve dış faktörler temel olarak devletlerin güvenlik eksenleri üzerinde inşa edilmektedir. Asıl önemli olan güvenlik kültürünün ülkelere nasıl tanımlandığı, aktörlerin etki kapasitesi, tehdit algısının yapısı ve bu tehditlerle mücadelede kullanılan araçlardır. Kimin/neyin güvenliği, neye karşı güvenlik, nasıl güvenlik sorularının cevabı o ülkenin güvenlik kültürüdür (Williams, 2008: 1-12). Literatürde güvenlik kültürüne ait tartışmalar üç farklı başlık altında incelenebilir (Bloomfield, 2012: 437-461). İlk olarak, güvenlik kültürü bağımsız bir değişken olarak ele alınmalıdır. İkinci olarak, asıl üzerinde durulması gereken husus güvenlik kültürünün nasıl oluştuğudur. Tarihsel bir süreç içerisinde güvenlik kültürü aşamalı bir şekilde kendini var edecektir ve inşacı bir perspektiften konuya yaklaşılmaktadır (Wendt, 1999). Son bakış açısında ise güvenlik kültürü ne bağımlı değişken ne de bağımsız değişkendir. Güvenlik kültürü daha çok bir ara değişken olarak karşımıza çıkmaktadır. Sebep – sonuç ilişkisine şekil veren arka plandır (Gray, 1999: 51). Kısacası burada asıl üzerinde durulmak istenen husus güvenlik kavramının önemidir.

Hem iç hem de dış politika üzerinde durulan bu kavram devletin devamlılığının ve gelişim gösterebilmesinin temelidir. Bu sebeple özellikle dış politikadaki karar alıcı mekanizmalar için güvenlik vazgeçilmez bir unsurdur. Farklı tanımlamalara karşın güvenlik dış politikadaki analizlerde birinci sırada yer almaktadır. Hem iç siyaset hem de dış siyasete konu olan güvenlik kavramı göz ardı edilemeyecek kadar önemlidir. Özellikle ulusal çıkarların ulusal güvenliğin ötesinde olduğu yaklaşım tarzının değiştiğini göz önüne alacak olursak artık ulusal güvenlik devletlerin sahip olduğu en önemli ulusal çıkar olacaktır.

Küreselleşme sürecinin etkisiyle birlikte artık ulusal sınırlar farklı bir anlam kazanmaya başlamıştır. Son yıllarda yaşanan teknolojik gelişmeler ışığında ulusal güvenlik gereksinimleri yeniden tanımlanmıştır. Bu aşamada siber güvenlik ulusal güvenliğin en önemli unsuru haline gelmiştir. Çünkü ulusal güvenlik artık devlet sınırlarını baz alan kısıtlı bir tehdit alanına dâhil değildir. Ülkelerin güç dağılımlarında değişiklikler yaşanmıştır. Güç dengeleri yeniden kurulmuştur ve asimetrik güç ilişkileri ortaya çıkmıştır. İnternetin ülke sınırlarını aşması, kritik alt yapıların güvenliğinin gündeme taşınması siber güvenliği ulusal güvenlik perspektifinde merkeze taşımıştır. Bu yeni güvenlik tanımları, güvenlik politikalarında değişikliklere sebep olmasına karşın güvenlik olgusu önemini hala korumaktadır.

1.2. Siber Alan

Siber alan siber uzay ya da siber dünya olarak adlandırılan internetin ve tüm teknolojik gelişmeleri yansıtan sanal bir alandır. Bu kavram ilk olarak 1984'te literatürdeki yerini almıştır. Kavram ilk olarak hayvanlar ve makineler arasındaki ilişkinin irdelendiği bir kitaptan doğmuştur. İlerleyen yıllarda Birleşmiş Milletler (BM), ABD Savunma Bakanlığı, AB gibi birçok kurum ve kuruluş tarafından tanımlanmıştır. Bu tanımların ortak noktası internet, iletişim altyapısı, telekomünikasyon ağları, bilgisayar sistemleri, bilgi teknolojilerine çekilen dikkattir. Siber alan birden fazla sayıda, durmaksızın ilerleyen, her biri farklı bir etki boyutuna sahip uzayların bir araya gelerek oluşturduğu bir platformdur.

Uİ disiplini içerisinde siber alanı değerlendirmek için modern insanın toplum içerisinde internete ve teknolojik gelişmelere bağımlı hale geldiğine dikkat çekilmelidir. Özellikle yapay zeka sayesinde makineler artık insanlara ait eylemleri gerçekleştirebilmektedir. İnsanın makineleri güçlendirdiği boyutta makineler insan ihtiyaçlarına göre tasarlanmaktadır. Bu durum insanın makinelere bağımlı hale gelmesine yol açarken ilerleyen dönemlerde makinelerin insan zihnini kontrol etme fikri siber alandaki mücadelenin önemini ortaya çıkaracaktır. Uİ disiplini içerisinde etkin olmayı arzulayan devletler için bu yeni alan oldukça çekicidir.

1.2.1. Siber Uzay (Cyberspace)

Günümüz dünyası bilişim ve iletişim ağları tarafından şekillendirilen ve yönetilen bir siber alandır. Norbert Wiener'in Sibernetik adlı kitabı sayesinde sibernetik kavramı tanımlanmıştır. Kitaba göre bu kavramın çerçevesi hayvanlar ve makineler arasındaki ilişkidir. Özellikle bu ilişki kontrol ve iletişim unsurlarıyla çerçevelenmiştir (Wiener, 1948). Siber uzay terimi ise 1984 yılında ilk kez dünya sahnesinde yerini almıştır. William Gibson tarafından kaleme alınan "Neuromancer" bilim kurgu kitabında siber uzay kelimesine yer verilmiştir. Etimolojik olarak siber uzay kavramını tartışacak olursak bu terim siber ve uzay kelimelerinin bir araya gelmesiyle türetilmiştir (Fourkas, 2021). Bu noktada bir parantez açmak gerekir. Siber uzay kavramı zaman içerisinde farklı anlamlarda kullanılmaya başlanacaktır. BM Terimler Sözlüğü siber uzayı, net olarak bilinen internete, iletişim altyapısına, online konferans kuruluşlarına, bilgi depolama ve işletme aygıtlarına bağlı küresel bir yapılanma olarak tanımlamaktadır (United Nations, 2021). ABD Savunma Bakanlığı Askeri Terimler Sözlüğü ise, siber uzayı internet, telekomünikasyon ağları, bilgisayar sistemleri, gömülü işlemci ve kontrol sistemleri gibi bilgi teknolojileri altyapılarını kapsayan bilgi ortamı olarak nitelendirmiştir (Department of Defence Dictionary of Military and Associated Terms, 2021). Dolayısıyla siber uzay kavramı ile asıl anlatılmak istenen tek bir uzay tanımının geçerli olmadığıdır. Bu kavram birden fazla sayıda, durmaksızın ilerleyen, her biri farklı bir etki boyutuna sahip uzayların kombinasyonudur. Dolayısıyla siber uzay için tek bir merkez söz konusu değildir.

Siber uzayı Uİ disiplini içerisinde değerlendirmek için modern insanın toplum içerisinde nasıl internete bağımlı hale geldiği göz ardı edilmemelidir. Çünkü özellikle yapay zeka ve Nesnelerin İnterneti (IoT) aracılığıyla makineler artık insanlara ait eylemleri gerçekleştirebilmektedir. Dolayısıyla aslında yaşanan bu süreç insan zekasının makineleri kontrol etmesi, diğer insanların düşünme süreçlerini, faaliyetlerini ve yürütülmesinde kontrol noktası oluşturmaktadır. Bu sürecin nasıl geliştiğinin gözlemlenmesi için aşağıdaki diyagram bizlere yol gösterecektir.

Şekil 1: Modern Toplum, Yapay Zeka ve Nesnelerin İnterneti (IoT) Arasındaki İlişkinin Gelişim Süreci



Kaynak: Halder ve Debarati, 2019.

Yukarıdaki tabloda da belirtildiği gibi bu süreç öncelikle insanların makineleri güçlendirmesiyle başlamıştır. Daha sonrasında insan ihtiyaçlarına uygun makineler tasarlanmıştır. Bunun sonucunda insanlar makinelere bağımlı hale gelmiştir. En son gelinen aşamada ise dramatik bir sonuç olarak makineler insan zihnini kontrol etme noktasındadır.

Uluslararası arenada etkin olmaya çalışan birçok aktör vardır. Temelde realist bir bakış açısını benimseyecek olursak devletler ön plana çıkmaktadır. Bu noktada gerek devletlerin gerekse diğer etkin olmaya çalışan aktörler açısından siber uzay dikkat edilmesi gereken bir kavramdır. Çünkü Soğuk Savaş sonrasında tecrübe edilen değişen düşman algısı ve yeni tehdit unsurlarının ötesinde artık tehdit unsuru olabilecek yeni bir alan doğmuştur. Bu durum siber uzayın ağ biçiminde şekillenen yapısı kontrol edilmesini zorlaştırmaktadır. Ayrıca bu konudaki hukuksal çerçevenin eksikliği de bu alanın kontrol edilebilirliğini güçleştirmektedir. Bir diğer perspektiften konuya yaklaşacak olursak siber uzayın yapısı ve hukuksal çerçevenin eksikliğinin ötesinde suç tanımının ve suçlu aktörlerin tanımlanması da oldukça zordur. UI için siber uzay öncelikli olarak aktörlerin siber uzayı nasıl tanımladıklarına ve bu kavram çerçevesinde kendi çıkarlarını ne kadar ön plana çıkarabildiklerine göre farklı yorumlanabilmektedir. Ulusal sınırların geçerliliğinin söz konusu olmadığı bu alanda her devlet potansiyel olarak kolaylıkla suçlu sayılabileceği gibi olası tehditlere karşı açık hedef haline de gelecektir.

1.2.2. Siber Alanda Mücadele

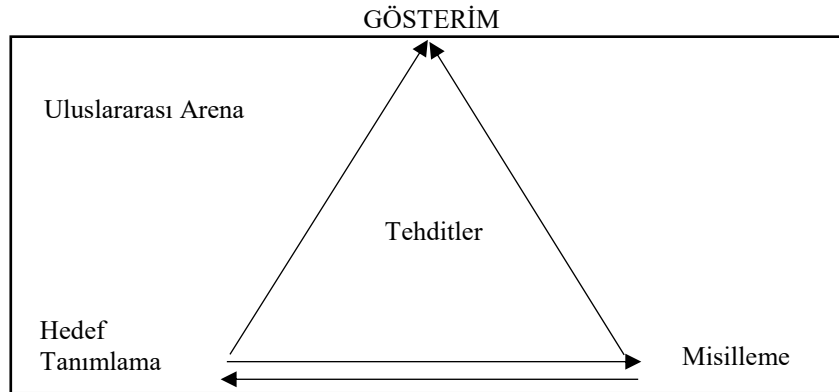
UI temel prensipleri, küreselleşmeyle beraber değişikliğe uğramıştır. Bu değişikliğin bir sonucu olarak güç dengesi ve egemenlik kavramlarının yanı sıra güçlü aktör olabilmek için gereken mücadelenin yöntem ve araçları da değişmiştir. Çünkü siber alan, küreselleşme sürecinin en güzel

örneklerindendir. İnternet sayesinde dünyadaki sınırlar etkisiz hale gelmiştir. Dolayısıyla tehdit unsuru sayılabilecek aktör sayısı çoğalmıştır. Buna bağlı olarak da tehdit araçlarının etki kapasitesi artık daha güçlüdür. Peki, siber alanda mücadele mümkün müdür? Uİ disiplini açısından bu alana yöneldiğimizde güç ve aktör kavramları ön plana çıkacaktır. Bunun sebebi ise mücadelenin temel yapı taşının güç elde etme arzusu olmasıdır. Aktörler ise bu mücadeleyi gerçekleştirecek failer olarak kabul edilmektedir.

Öncelikli olarak cevaplanması gereken soru siber alanın bir mücadele alanı olup olmadığıdır. İkinci soru ise bu mücadelenin aktörlerinin ve yöntemlerinin nasıl tanımlanacağıdır. Siber alanda gerçekleştirilmeye çalışılan mücadele kavramına genel bir perspektif kazandırılmalıdır. Klasik Uİ disiplini içerisinde savaşlar en temel olgudur. Politikalar ise savaşların cephe gerisinde kazanılmasını sağlayan araçlardır. Dolayısıyla klasik bir bakış açısına bağlı kalırsak savunma, mücadele ve tehdit gibi kavramlar net olarak ortaya koyulmaktadır. Ancak günümüzde artık devletlerin sınırları belirsizleşmiştir. Siber alan sayesinde somut sınırlar geçerliliğini yitirmiştir. Muğlaklık sayesinde klasik çerçeve yıkılmıştır. Siber alanın yapısından kaynaklanan bu belirsizlikle beraber bu alanda mücadele oldukça zorlu bir hal almıştır. Mücadelenin şekline nüfuz eden siber alan sadece mücadelenin yapısını değiştirmemiştir. Uİ yapısı artık sınırları belirsiz bir alana taşındığı için meydana gelen olaylar, ilişkiler ve davranışlar çok kutuplu yapıyı ortaya çıkarmıştır.

Siber alanın varlığı Soğuk Savaş Dönemi'nde karşımıza çıkan siyah ve beyaz alanların dışındadır. Bu noktada daha esnek bir bakış açısına sahip olduğumu düşündüğümüz bu gri alan, birçok ülke, kurum ve kuruluşların dikkatini çekmektedir. Özellikle siber uzay aktörler için yeni bir mücadele alanıdır. Dolayısıyla siber alanda etkin olan aktör diğerleri için caydırıcı bir güce sahip olacağı için siber uzay caydırıcılığın yeni boyutunu oluşturacaktır.

Şekil 2 : Siber Caydırıcılık Teorisi



Kaynak: Taddeo ve Mariarosaria, 2018.

Bu alandaki saldırgan aktörün esasen saldırı hedefi açıktır. Ancak saldırıya maruz kalan karşı taraf için siber suçlunun tespiti ve takip edilmesi oldukça zordur. Belirsizlik ve öngörülemezlik temel yapı taşlarıdır. Bu ortamda verilen taşınması (işlenmesi, gönderilmesi ve depolanması) için bütün bilgi sistemleri aktif olarak kullanılmaktadır. Siber ortam insani, teknolojik, sanal ve fiziksel ortamların bir kombinasyonudur.

Siber alan büyük, küçük ya da orta büyüklükteki bütün aktörlerin dâhil olduğu bir sistemdir ve bu sistem artık Uİ disiplini içerisindeki yerini almıştır. Siber alanda gerçekleştirilmek istenen mücadelenin sınırlarının belli olmamasına karşın bu mücadele diğer mücadele alanları kadar etkilidir. Hedeflenen mücadele için gerekli araç ve yöntemler etki eden aktörün konumuna ve gücüne göre değişiklik gösterecektir.

1.2.3. Siber Alan ve Küreselleşme

Siber alan ve küreselleşme arasındaki ilişkiyi tartışmadan önce uluslararası arena açısından küreselleşme sürecinin tam olarak ne ifade ettiği üzerinde durulmalıdır. Genellikle Soğuk Savaş sonrasındaki süreç küreselleşme ile ilişkilendirilmiştir. Sadece Uİ bünyesinde değil tüm sosyal bilimlerde içerisinde ekonomik, siyasal, kültürel, düşünsel ve askeri boyutlarıyla küreselleşme kendisine bir yer edinmiştir. Holton (1998)'a göre küreselleşme çağdaş yaşamı tanımlayan başlıca niteliklerden biridir. Küreselleşme kavramı kendisine bir ün kazanmıştır. Kısacası herhangi bir olgunun, düşüncenin ya da somut olanın küresel olarak nitelenmesi, nitelenen kavrama bir ayrıcalık sağlamaktadır. Hâlihazırdaki bütün problemlerin çözüm aracı küreselleşme olarak görülmektedir. Başka bir örnek verecek olursak Bauman (1997)'a göre küreselleşme “bazı taraflara göre onsuz mutlu olamayacağımız, bazılarına göre ise mutsuzluğumuzun sebebini oluşturacaktır.”

Küreselleşmeyi karşımıza çıkaran süreç Soğuk Savaş'ın sonlandığı dönemdir. Ancak iki kutuplu sistemin geçerliliğini yitirmesine rağmen iki kutuplu sistemin yerine geçebilecek yeni bir sistem doğmamıştır. Bu noktada küreselleşme kendisine “Tarihin Sonu”ndan (Fukuyama, 1992a; Fukuyama, 1992b). “Medeniyetler Çatışması”na (Huntington, 1997a; Huntington, 1997b) kadar tüm taraflarca kabul edilen bir tanım bulamamıştır.

Elbette küreselleşme kavramının çok boyutlu etki alanına sahip olması da tanımlanmasını güçleştirmiştir. Temelde küreselleşme süreci değişimi baz almaktadır. Ancak dünyadaki değişim taraflara göre farklı yorumlanmaktadır. Örnek verecek olursak post-modern teorisyenlere göre bu dönüşüm, Soğuk Savaş sonrası teorisyenler için geçiş, küreselleşme teorisyenleri için de süreçtir (Shaw, 2000).

Siber alan ve küreselleşme arasında bir bağlantı kurabilmek için öncelikli olarak küreselleşme kavramının nasıl kullanıldığı ele alınmalıdır. Kavramın ortaya çıkış şekli siber alan ile bağlantıyı

anlamımıza yardımcı olacaktır. Tarafların ortak bir payda da bir araya gelemediği iki konu vardır. Birincisi küreselleşmenin nasıl tanımlanması gerektiğidir. İkincisi ise küreselleşme kavramının ilk olarak ne zaman ortaya çıktığıdır. Kavramın literatüre nasıl kazandırıldığı ile ilgili üç farklı yaklaşım söz konusudur. İddialardan ilki, 1963 yılında Kanadalı sosyoloji profesörü Marshall McLuhan (1963) “Gutenberg Galaxy” isimli kitabında yeni dünya düzeni için “Global Köy” betimlemesini yapmıştır. Bu sayede küreselleşme ilk kez literatüre dâhil edilmiştir. McLuhan, eserinde en azından dünyanın bir bölümünün özellikle iletişim teknolojilerindeki gelişmeler sayesinde “küresel köy” haline gelmesinden yola çıkarak küreselleşmeyi betimlemiştir. İkinci iddia, küreselleşme kavramının Amerikalı bilim adamı Zbigniew Brezinski’nin ve bazı ekonomistler sayesinde yeniden biçimlendirildiğidir (Ziegler, 2004). Son iddia ise London School of Economics’ten Anthony Giddens’e aittir. Giddens (1990)’a göre, küreselleşme terimi 1980 yılların sonu ile 1990 yılların başlarında ilk kez kullanılmıştır. Küreselleşme esasen, bir ülkede meydana gelen olayların başka yerlerdeki olaylar üzerinde etkiye sahip olması ya da ulusal sınırlar dışında meydana gelen olaylardan etkilenme kapasitesini yansıtmaktadır. Sosyal ilişkiler dünya genelinde yoğunlaşmıştır.

Aslında Giddens’in bakış açısı siber alan ve küreselleşme arasındaki bağlantıyı açıklayacaktır. Artık ulusal sınırlar geçerliliğini yitirmiştir. Herhangi bir ülkede meydana gelen bir olay fiziksel olarak çok uzak olan coğrafyalara etki edebilmektedir. Bunun en güzel örneği ise artık siber alandır. Mekâna bağlı kalmaksızın herhangi bir ülke, grup ya da kişi dünyanın öbür ucundaki bir diğer ülke için tehdit oluşturabilmektedir. Küreselleşmenin çok boyutlu yapısı, siber alanın etki kapasitesini yansıtmaktadır.

1.3. Siber Savaş

Savaş kavramı Uİ disiplini için önemli bir kavramdır. İnsanlık tarihi kadar eski olan savaş kavramı uluslararası sistemde şiddet kullanımı ya da kuvvet kullanma kapasitelerine göre devletler ve devlet dışı siyasal aktörler arasında meydana gelen, büyük ölçekte fiziksel çatışma olarak tanımlanabilir. Klasik savaş kavramında diplomasinin yetersiz kaldığı alanlarda organize olmuş grupların şiddet içeren eylemlerini yürütebilmesi için başvurduğu silah kullanma yetkisi daha çok zayıf ve güçlü devlet ayrımını ortaya çıkarmaktadır. Askeri kapasitenin gücü savaşta kimin galip geleceği noktasında önemlidir.

Siber savaş kavramı klasik savaş kavramının çok ötesindedir. 1980’li yıllarda kamu içerisinde siber savaş kavramına ait bilinç oluşmasına karşın bu kavram 2000’li yıllardan sonra literatürde tartışılmaya başlanmıştır. Siber savaşın belirli eylemlerinin, aktörlerinin, etkilerinin, coğrafyasının olmaması ve hedeflerinin farklı olması ortak tanımlanmasını zorlaştırdığı için tüm taraflarca kabul gören bir siber savaş kavramı yoktur. Ancak siber savaş kavramı üç farklı perspektiften incelenebilir. İlk bakış açısı siber savaşı kabul edip proaktif önlemler almayı uygun gören

yaklaşımıdır. Bu yaklaşıma göre ABD ve müttefikleri için siber savaş kavramı acil bir tehlikedir. İkinci perspektife göre siber savaş kavramı hem kavramsal hem de gerçeklik olarak tartışmalı olduğu için bu kavramın varlığı nasıl tanımlanacağına bağlıdır. Dolayısıyla siber savaş kavramı net değildir. Son bakış açısına göre ise siber uzay bir çatışma alanıdır. Bu çatışma mevcut uluslararası yasal yapılar ve devlet normları sayesinde yorumlanabilir.

Siber savaş kavramının yanı sıra terör, saldırı ve caydırıcılık gibi kavramlar yeniden ele alınırken kritik altyapıların güvenliği ön plana çıkarılmıştır. Siber terör kavramı ilk defa 1980’li yıllarda literatürdeki yerini almıştır. Siber alanda yapılan her saldırının siber terör adı altında ele alınması doğru değildir. Bunun için küçük altyapıların tehdit edildiği durumlar bu alana dahil değildir. Bilgi operasyonlarının bir alt başlığı olarak incelenebilen elektronik savaş, bilgisayar ağı, askeri hile, özel destek ile koordine edilen güvenlik operasyonları ve ilgili yeteneklere nüfus edilmesi, durdurulması, yok edilmesi ya da düşüncelerin gasp edilmesi ve ulusal kurumların karar alma süreçlerinin manipüle edildiği bütün saldırı çeşitleri siber saldırı olarak nitelendirilebilir. Siber alandaki çok sayıda saldırı çeşidinin mevcudiyeti bu saldırılar karşısında önlem almayı oldukça zorlaştırmaktadır. Tüm bu tehditler karşısında istenilen sonuca ulaşmak için potansiyel bir saldırganın kendisine misilleme yapılacağı noktasında rakibin tehdit kapasitesini inandırıcı olması gerekmektedir. Caydırıcılık olarak karşımıza çıkan bu kavram Uİ disiplini içerisindeki devletler için ön plandadır. Siber saldırıların etki kapasitesi belirlenemediği için caydırıcılık ön plana çıkmaktadır.

1.3.1. Siber Savaş Kavramı

Uİ açısından siber savaş olgusunu ele almak için öncelikli olarak savaş kavramının çerçevesi üzerinde durulmalıdır. Savaş olgusunun genel perspektifi çizildikten sonra siber savaş kavramının genel savaş kavramından farkı ortaya çıkacaktır.

Savaş, uluslararası sistemde şiddet kullanımı ya da kuvvet kullanma kapasitelerine göre devletler ve devlet dışı siyasal aktörler arasında meydana gelen, büyük ölçekte fiziksel şiddet barındıran çatışma olarak ifade edilebilir. Uİ disiplini esasen iki temel nokta üzerinde durmaktadır: diplomasi ve savaş. Diplomasi daha çok askeri kapasitenin kullanılmasını engelleyebilmek için devletler arasındaki diyalogun kurumsallaşmasını temek almaktadır (Barston, 2006). Bu noktada savaş, diplomasinin yetersiz kaldığı durumlarda en az iki taraf arasında gerçekleşen, organize olmuş grupların şiddet içeren eylemleri yürütmek için silah kullanma yetkisine başvurusudur.

Savaş Uİ disiplininin en önemli kavramlarından biridir. Savaş kavramına ait tartışmalar Tukidides’e kadar dayanmaktadır. Realizmin ilk eseri olarak kabul edilen Peleponnez Savaşları kitabı, savaş ve savaş stratejilerine ait önemli bilgileri barındırmaktadır. Sun Tzu (2018), “Savaş Sanatı” adlı eserinde savaş eseri savaş stratejilerinin önemini vurgulamaktadır. Niccola Machiavelli

(2004), ise “Prens” adlı etkin liderliğin savaş üzerindeki etkisi üzerinde durmuştur. Son olarak Carl Von Clausewitz (1976: 55), “Savaş Üzerine” adlı kitabında savaşı devletler arasındaki ilişkinin devamını sağlayan araç olarak nitelendirmektedir. Taraflardan güçlü olan savaş sayesinde karşı tarafa şiddet kullanarak isteklerini zorla kabul ettirebilecektir.

Savaş kavramı Uİ disiplini için vazgeçilmez olduğu kadar insanlık tarihinin de gelişim sürecini yansıtmaktadır. İnsanlığın varoluş mücadelesi savaş olgusunun tetikleyicisidir. Ancak günümüzde artık savaş olgusu, güçlü ve zayıf devlet ayrımı, savaş türleri gibi birçok kavram değişikliğe uğramıştır. Teknolojik gelişmeler sayesinde dijital dünya da sadece geleneksel savaş kavramı değil aynı zamanda ülkeler arasındaki mücadele yöntemleri de değişmiştir. Geleneksel savaş kavramında değişen en önemli unsurlardan biri de zayıf ve güçlü devlet ayrımı olacaktır. Çünkü artık askeri kapasite savaş üzerindeki etkisini yitirmiştir.

Siber savaş kavramı klasik savaş olgusunun çok ötesindedir. Michael Warner (2012)’ın “Siber Güvenlik Öncesi Tarih” adlı eserinde 1980 yılında siber savaş kavramının kamu bilincinde yer edindiğinin dikkatini çekmiştir. Ancak Oona Hathaway (2011: 76)’ın “Siber Atak Hukuku” adlı eserinde belirttiği üzere tüm taraflarca kabul gören bir siber savaş tanımı yoktur. Bu konu üzerinde hükümetler, ordu, akademisyenler çokça yoğunlaşmış olsa dahi ortak tanım elde edilememiştir. Başlangıçta kavramın erken tanımlanmasında popüler kültür etkili olmuştur. Özellikle medyanın bu noktada katkısı büyüktür. Örnek verecek olursak siber savaş tanımlama çalışmalarında 1983 yılında yayınlanan Savaş Oyunları sayesinde medyanın etkisi ön plana çıkmıştır. Daha sonrasında John Arquilla ve David Ronfeldt (1993: 141-165) yılında yayınladıkları “Siber Savaş Geliyor” adlı makalede, dikkatleri siber savaş kavramı üzerine çekmiştir. Bu makalede üzerinde durulan konu siber savaşın yakın bir tehdit unsuru olduğudur. Özellikle alarm verilmesi gereken tanım sınıflarının oluşturulmasının yanında ABD ve müttefiklerinin tehdit altında olduğunun önemi vurgulanmıştır. Siber savaş tehdidine karşı güçlü bir savunma sistemi ön görülmüştür. Bu sayede siber uzay ABD’nin hakimiyet elde edebileceği yeni bir alan olarak yorumlanmıştır.

Tablo 4: Siber Savaş Karşısında Panik Olanlar, Kuşku Duyanlar ve Gerçekçi Yaklaşımlar

Değişkenler	Tanım	Panik Olan /Endişe Duyan Taraflar	Kuşku Duyanlar	Gerçekçiler
Olaylar	Siber Uzayda Düşmanca Eylemlerin Doğası	Ucuz ve Yaygın	Pahalı ve Karmaşık	İkisi de
Aktörler	Siber Savaşta "Meşru" Aktörler	Hiç kimse/ hiçbir şey sorumluluk alamaz. Nihai sorumluluk devletlerdedir.	Devletler	Hiç kimse/Hiçbir şey
Etkiler	Siber Savaşın Olası Etkileri	Büyük Ölçekli Kesinti veya Yıkım, Askeri Kapasitenin Dekapasyonu	Küçük Ölçekli: Yerel Bozulma, Fikir ve Kavramlar	Uluslararası devlet sistemi için yasal sonuçlar.
Coğrafya	Siber Savaşın Gerçekleştiği Yer/Mekân	Siber alan ayırdır, ancak fiziksel alanla kesişebilir.	Siber uzay yalnızca fiziksel alanın yansımasıdır. (Vekil)	Siber alan ve fiziksel alan yasal ve pratik olarak birbirinden ayrılamaz.
Hedefler	Siber Savaşın Hedefi	Kritik Devlet, Askeri veya Özel Altyapı/Bilgi	Kritik Altyapı, Bilgi, İnsan	Askeri Hedefler, Bireyler, Şirketler, Devletler

Kaynak: Ashraf, 2021: 274-294.

Tüm taraflarca kabul gören ortak bir siber savaş tanımının olmaması; siber savaşın belirli eylemlerinin, aktörlerinin, etkilerin, coğrafyasının ve hedeflerinin farklı vurgulanmasına sebep olmuştur. Elbette siber savaş kavramı için tüm tarafların kabul ettiği bir çerçeve çizmek zordur. Ancak siber savaşın çerçevesini oluştururken olaylar, aktörler, etkiler, coğrafya ve hedefler Tablo 4’te görüldüğü gibi değerlendirilebilir. Siber savaş üç perspektiften değerlendirilebilir. Birinci kısım, alarm veren taraftır. Bu bakış açısına göre siber savaş ABD ve müttefikleri için acil bir tehlikedir. İkinci kısım Şüpheli taraftarlardır. Şüphelilere göre siber savaş hem kavramsal olarak ve gerçeklik olarak tartışmalıdır. Dolayısıyla siber savaş kavramı net değildir. Bu noktada siber savaşın varlığı bu kavramın nasıl tanımlanacağına bağlıdır. Üçüncü olarak Gerçekçiler ele alınabilir. Gerçekçilere göre siber uzayda çatışma vardır. Bu çatışma mevcut uluslararası yasal yapılar ve devlet davranış normları sayesinde anlaşılabilir (Ashraf, 2021: 274-294).

1.3.2. Siber Terörizm

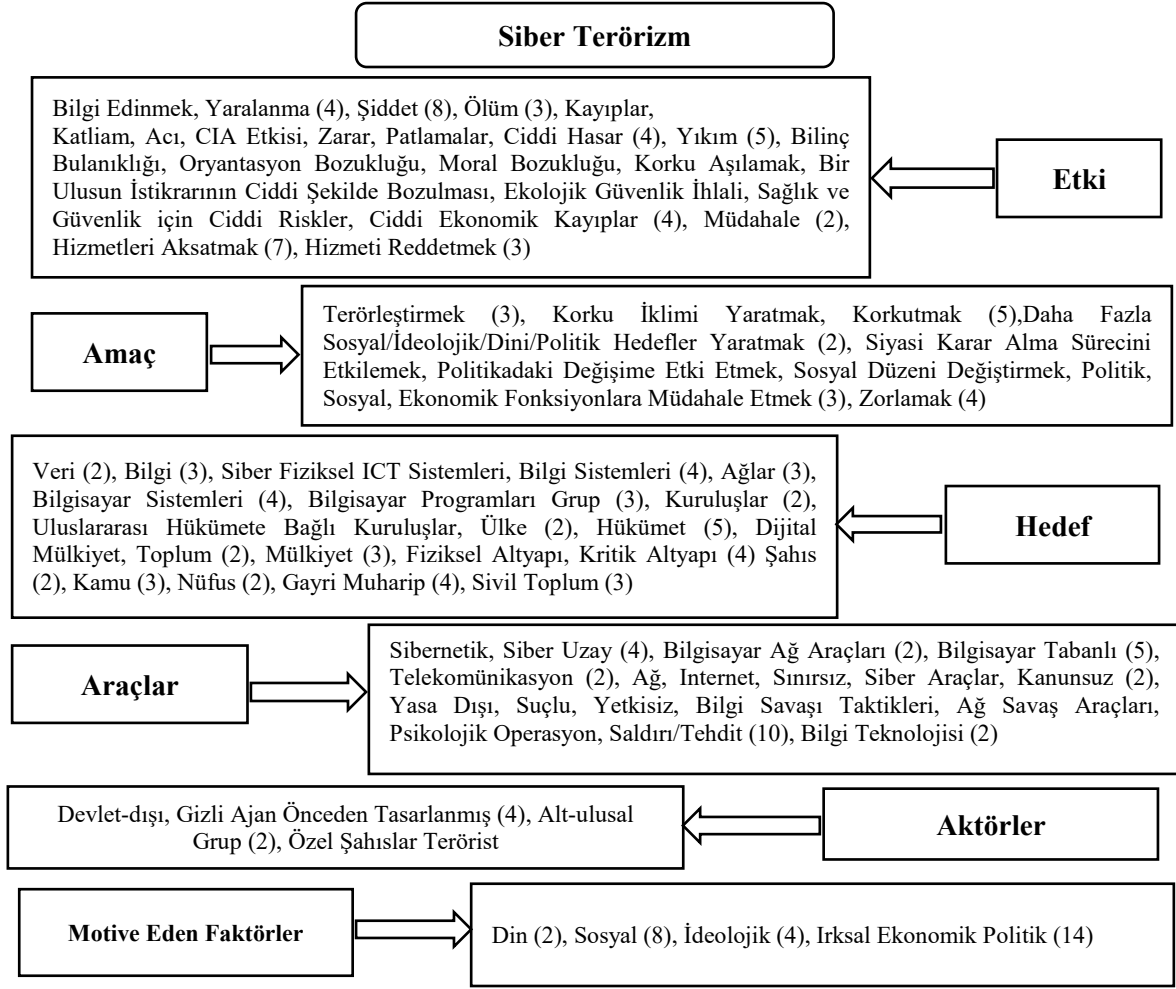
Etimolojik olarak terör kelimesi Latince korkutmak, ürkütmek ve sindirmek anlamlarına gelen “terrere” kelimesinden gelmektedir (Örgün, 2001). Terörizm insanlık tarihi kadar eski ve karmaşık bir kavramdır. Dolayısıyla net bir tanım yapılması oldukça zordur. Ancak terör ve şiddet birbirlerini tamamlayan iki yakın unsurlar olduğu için siyasal bir düzlemde terör ve şiddet kavramlarının yorumlanması oldukça önemlidir. Batı için terör kelimesi 1789–1794 Fransız Devrimi esnasında, devrimcilerin iç düşmanlara karşı gerçekleştirdikleri eylemler ve hükümet tarafından yürütülen baskı ve doğrudan gerçekleştirilen infazlar sonucunda meydana gelen “Terör Dönemi”yle ilgilidir. Bu dönemde binlerce kişi hayatını kaybetmiştir (Charles, 2004: 8). Özellikle

1789 Fransız Devrimi sonrasında 1793 yılında Jakoben iktidarınca uygulanan sistematik şiddet politikaları “terörizm” kavramının doğmasına sebep olmuştur (Çitlioğlu, 2006). Terör kavramının ortaya çıkışından günümüze kadar geçen süre içerisinde bu kavram birçok değişikliğe uğramıştır. Ancak asıl önemli olan siber terör kavramının nasıl yorumlanması gerektiğidir. Çünkü günümüzde siber terör kavramı farklı yorumları beraberinde getirmiştir. Terörizm özellikleri göz önüne alındığında siber eylemlerin terörizmin bir türü olup olmadığı ve siber terörizm olarak adlandırılması noktasında ortak bir tanım yoktur.

Siber terörizm kavramı ilk ortaya çıktığında basit bir hackleme ya da internet üzerinden bazı şirketlere ait özel bilgilerin ifşa edilmesi gibi olaylar üzerinden tanımlanmıştır. 1980’li yıllarda ise siber terörizm ilk defa Kaliforniya’da Güvenlik ve İstihbarat Enstitüsü’nde üst araştırmacı olarak çalışan Barry Collin tarafından isimlendirilmiştir (Collin, 1996: 16-17). Burada dikkat edilmesi gereken husus bir saldırının siber terörizm olarak adlandırılması için taşınması gereken niteliktir. Çünkü siber terörizm için gerçekleşen saldırının insanlarda korkuya sebep olacak kadar hasar vermesi gerekmektedir. Önemli bir etkiye sahip olmayan küçük alt yapıların tehdit edildiği durumlar siber terörizmin alanına dahil değildir. Ayrıca bir saldırının siber terör alanına girmesi için doğrudan şiddet içermesine de gerek yoktur. Psikolojik olarak insan zihninde tahribata sebep olan eylemlerin de siber terör alanına dahil olduğu göz ardı edilmemelidir (Denning, 2003: 27).

Genel olarak bilgisayar ağlarını bozmaya yönelik bilinçli ve geniş kapsamlı eylemler dahil olmak üzere, terör eylemlerinde internet ve internete bağlı kişisel bilgisayarların araç olarak kullanılması siber terörizmdir. İlk başta insanların can ve mal güvenliklerini tehdit eden bu durum geniş bir perspektiften ele alındığında can ve mal güvenliğinin tehdit edilmesinin yanı sıra sosyolojik, dini, ideolojik, politik veya başka niyetlerle gerçekleştirilen saldırılar da siber terörizm alanına dahildir (Çiftçi, 2013: 6).

Şekil 3: Siber Terörün Yapısını Tanımlayan Unsurlar



Kaynak: Plotnek ve Jordan, 2019.

Şekil 3'te görüldüğü üzere siber terör kavramını ortaya çıkaran hedef, aktör, motivasyon unsurları, saldırının amacı, etki kapasitesi ve saldırıda kullanılan araçlar büyük önem taşımaktadır. Esasen bu altı unsurun tanımlanması sadece siber terörün anlaşılması noktasında önem taşımamaktadır. Eski altyapı sorunlarının çözülmesi için dünyanın dört bir yanına dağılan geniş elektrik şebekeleri modern teknolojinin hayatımıza girmesiyle birlikte bu sorunların ortadan kalkacağı kanısı artık geçerli değildir. Bu yeni teknoloji düşmanlar tarafından kullanılacak yeni karmaşık ve güvenlik açıklarını beraberinde getirecektir. Siber teröre dair altı unsur yeni güvenlik açıklarının da yorumlanmasında yardımcı olacaktır.

1.3.3. Siber Saldırı

Uİ içerisinde kendine bir yer edinen siber alan artık hayatımızın her alanında karşımıza çıkmaktadır. Devletler arası ilişkilerde olduğu kadar günlük hayatımızın da her alanına dahil olan teknoloji sayesinde aslında hepimiz tehdit altındayız. Bizi tehdit eden siber saldırıların

tanımlanması oldukça zorlu bir süreçtir. Siber uzayda çok sayıda saldırı çeşidi karşımıza çıkmaktadır. Saldırı türlerindeki bu çeşitlilik saldırılar karşısında da önlem almayı oldukça zorlaştırmaktadır.

Stephen Hart (2020)'ın "Risk: Siber Güvenlik Farkındalığı ve Eğitim" adlı makalesinde belirttiği gibi siber saldırılar geleneksel olarak bilgi operasyonlarının ötesindedir. Siber saldırıların daha geniş bir perspektiften ele alınması gerekmektedir. Bilgi operasyonları; elektronik savaş, psikoloji, bilgisayar ağı, askeri hile, özel destek ile koordine edilen güvenlik operasyonları ve ilgili yeteneklere nüfus etmek, durdurmak, yok etmektir ya da fikirleri gasp etmek ve ulusal kurumların karar alma süreçlerine etki etmektir.

Zararlı yazılımlar, trojanlar, mantık bombaları, virüsler, solucanlar aracılığıyla gerçekleştirilen DDoS (Dağılık Servis Engelleme Saldırıları) atakları, oltalama ve yemleme (phishing) ve daha birçok saldırı türü siber saldırı olarak karşımıza çıkmaktadır. Siber saldırılar sayesinde internet aracılığıyla saldırının gerçekleştirildiği sistem hizmeti aksatılmaktadır. Tahribata uğratılan sistem içerisindeki bilgiler ele geçirilebileceği gibi sadece sistemin zarara uğratılması da hedeflenebilmektedir.

Bilgisayar Korsanlığı: Hack eylemi olarak adlandırılan siber saldırı çeşididir. Bir bilişim sistemine yasa dışı yollar aracılığıyla gerçekleştirilen ataklardır. Buradaki en temel parametre bu faaliyetin sadeliği ve uzmanlık gerektirmesidir. Hack eylemi bir kişi veya grup tarafından gerçekleştirilebilir (Hekim ve Başbüyük, 2014: 142).

Botnet (Bot Networks): Birden fazla botun bir araya gelerek oluşturduğu özel ağ sistemidir. botnet gibi zararlı yazılımlar aracılığıyla sistem üzerinden kullanıcıya e-posta gönderilmektedir. Buna ilaveten gönderilen mesaj içeriğinde yer alan linklere tıklandığında açılan internet sayfaları üzerinden sisteme sızılabilmesi gibi Truva atı (trojan) olarak adlandırdığımız zararlı yazılımlar vasıtasıyla da sisteme erişilebilmektedir. Sisteme sızılmasını sağlayan botnet aracılığıyla sistemin normal kullanıcısı tarafından talep edilen işlevlerin yanı sıra arka planda bilinmeyen ve program kullanıcı tarafından istenmeyen işlevler de sisteme yüklenebilmektedir. Bu tür gizli işlev içeren yazılımlar şirketler ve ülkeler tarafından casusluk faaliyetleri için kullanılmaktadır. Bu tür yazılımlar APT (Advanced Persistent Threat-Geliştirilmiş Kalıcı Tehditleri) olarak isimlendirilmektedir (Hekim ve Başbüyük, 2014: 142).

Virüsler: Özel olarak tasarlanmış programlardır. Bilgisayar virüsleri aktifleştirildiği takdirde kendisini sistem dosyalarından veya programlardan biri olarak değiştirebilmektedir. Bu sayede kendilerini diğer programlara bulaştırabilir ve çoğalabilirler (Akarslan, 2015). Mantık bombaları da bir çeşit bilgisayar virüsüdür.

Truva Atı (Trojan): Truva atı legal bir program içindeki illegal talimatlar ya da bir işi yapıyormuş gibi görünüp arka planda kullanıcıdan habersiz gizli işlemler yapan zararlı programlardır (Akarslan, 2015).

Kök Kullanıcı Takımı (Rootkit): Bir bilişim sisteminde sisteme bulaşması ile mevcut işlemin arkasında saklanabilen, kötü niyetli kişilere sisteme uzaktan tam erişim ve kontrol sağladığı gibi çok zor tespit edilebilen bilgisayar programlarıdır. Bu tür yazılımların iki temel özelliği vardır. Etkiledikleri sistemde üst düzey erişim yetkilerini gerektiren komutları çalıştırabilmekte olup kendilerini diğer üst düzey erişim yetkilere sahip sistem yöneticilerinden gizleyebilirler (Akarslan, 2015).

Gizli - Arka Kapılar (Back Doors): Bilgisayar sistemine yönelik normal kimlik doğrulama yöntemlerini devre dışı bırakarak başka yöntemler aracılığıyla sisteme giriş yapılmasına izin veren yazılımlardır (Akarslan, 2015).

Spyware (Casus) Yazılımlar ve Adware (Reklam) Yazılımlar: Casus yazılımlar aracılığıyla kullanıcıya ait önemli bilgiler ve yaptığı işlemler kullanıcının bilgisi haricinde ele geçirilmektedir. Casus yazılımları virüs ve solucanlardan ayıran en temel nokta bulaştıkları sistemde yayılma ihtiyacı duymadan sistemin gizliliğini ihlal ederek verileri ele geçirebilmeleridir (USOM, 2014).

Yemleme (Phishing): Yasa dışı yollar aracılığıyla sisteme erişim için kullanıcının isim, şifre, kimlik ve hesap bilgileri gibi verilerin ele geçirilmesi yoluyla gerçekleştirilen saldırılardır (USOM, 2014).

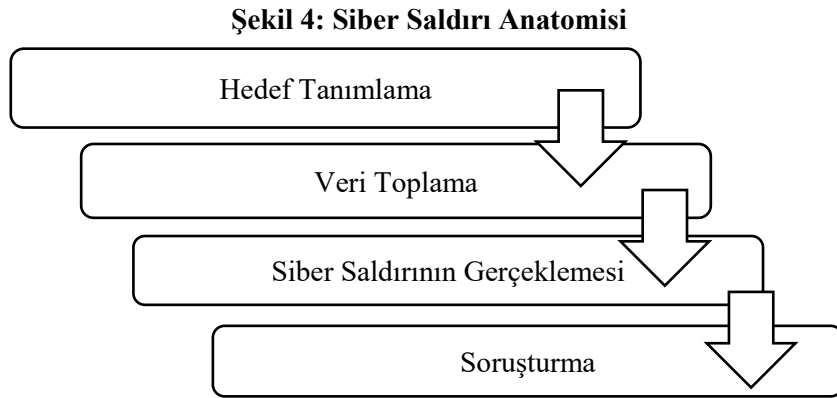
Zararlı Yazılımlar: Bilgisayar sistemlerinin kötüye kullanım amacıyla sistem bilgilerine erişimi amaçlayan veya bilgisayar sistemlerine ciddi zararlar verebilen kötü amaçlı yazılımlardır. Virüsler, Truva atları, casus yazılımlar ve rootkitler gibi birçok saldırı yöntemi zararlı yazılım olarak değerlendirilebilir. Buradaki temel nokta kritik ve önemli bilgileri elde etmek için sisteme yetkisiz olarak erişilebilmesidir (USOM, 2014).

Solucanlar: Solucanlar virüsler gibi kendilerini bir bilgisayardan başka bir bilgisayara kopyalayabilirler. Ancak virüslerden ayrıldıkları temel nokta yayılma işleminin ağ üzerinden otomatik olarak kendilerinin gerçekleştirebilmeleridir. Dolayısıyla bilgisayar ağlarının yavaşlamasına, internetteki sayfaların donmasına ve geç açılmalarına sebep olabilirler (USOM, 2014).

APT yazılımı hedef alınan sisteme sızmayı ve hedef alınan sisteme veri / bilgi aktarımını amaçlamaktadır. En bilindik örneği İran nükleer sistemlerini kontrol eden bilgisayar sistemine karşı gerçekleştirilen Stuxnet'tir (TNETWORKS 2021, <http://www.tnetworks.com.tr>).

Scanning (Tarama) Yöntemi ve Şifre Kırıcılar, Servis Dışı Bırakma Saldırıları- (Denial-of-Service), Sahte (Fake)-İstem dışı alınan (Spam) Elektronik Postalar, Klavye Kaydediciler (Keylogger), İp Aldatması (IP Spoofing), SQL İnjeksiyon Yöntemi; Sosyal Mühendislik Saldırıları (Social Engineering), Defacement (Web sitesinde tahrifat oluşturan ya da web sayfasının görüntüsünü değiştiren saldırılar) ve siber casusluk ve istihbarat saldırıları gibi daha birçok siber saldırı çeşidi vardır. Dolayısıyla siber saldırı türlerinin çeşitliliği bu saldırılara karşı önlem alınmasını zorlaştırmaktadır.

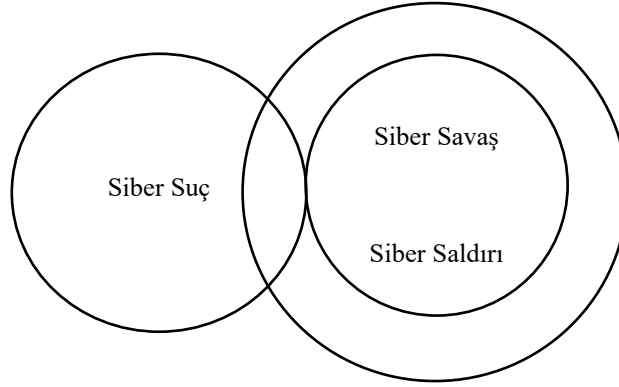
Şekil 4'te görüldüğü gibi siber saldırının gerçekleşmesi için ilk olarak hedefin tanımlanması gerekmektedir. Daha sonrasında veri toplama aşaması gelmektedir. Bu aşama saldırı öncesi en önemli aşamadır. Hedef belirlendikten ve gerekli veriler elde edildikten sonra siber saldırı gerçekleşmektedir. Siber saldırı sonrası ise soruşturma olarak adlandırılan aşama gelmektedir. Bu aşama da ise önemli olan saldırının kaynağının tespittir.



Kaynak: Li ve Liu, 2021: 8176-8186.

Siber suç, siber savaş ve siber saldırı arasındaki anlamsal farklılıklar oldukça önemlidir. Siber eylemlerin doğası ve özellikleri dikkate alındığında siber uzay olarak adlandırdığımız yapı siber suç, saldırı ve savaş içerisinde barındırır da anlamsal farklılıklar ön plana çıkmaktadır. Öncelikle siber suç kavramıyla siber savaş ve siber saldırı kavramları farklıdır. Siber suç, yalnızca hükümet dışı saldırganlar tarafından gerçekleştirilen siber eylemlerdir ve yalnızca ceza hukukunun ihlali söz konusudur. Şekil 5'te de görüldüğü üzere siber suç kavramı, siber savaş ve siber saldırıdan farklıdır. Siber savaş ve saldırı aynı düzlemde yer alırken siber suçlar farklı bir düzlemde yer almaktadır.

Şekil 5: Siber Suç, Siber Savaş ve Siber Saldırı Arasındaki Ayrım



Kaynak: Li ve Liu, 2021: 8176-8186.

1.3.4. Kritik Altyapılar

“Kritik altyapı” kavramı bir ülkede ekonomik ve sosyal hayatın aksamadan işlemesi için hayati öneme sahip olan fiziksel ve sayısal sistemlerin tamamıdır (Kara ve Çelikkol, 2011: 25-26). Çağdaş dünya da toplumun can damarını meydana getiren bu altyapı sistemlerinin korunması ve güvenilirliklerinin sağlanması ulusal güvenlik ve ekonominin devamlılığı için esastır (Ten vd., 2010). Kritik altyapı kavramı ilk kez 1996 yılında ortaya atılmıştır. ABD’de imzalanan kanun hükmünde kararname de kritik altyapı kavramına yer verilmiştir. Kritik altyapıların korunmasıyla alakalı olarak oluşturulan komisyonun ABD’nin sahip olduğu kritik altyapı sistemleriyle ilgili olarak inceleme ve önerilerini içeren bir rapor hazırlanması talep edilmiştir. Bu raporun talep edilmesinde iki önemli temel parametre vardır. Bu parametreler ulusal savunma ile ilgili gerekli kararların alınması ve ekonomik güvenirliliğin sağlanmasıdır (Karanacak, 2011: 24-25; US PCCIP, 1997: 6) Ayrıca 1997 yılında kritik altyapı aşağıdaki gibi tanımlanmıştır.

Telekomünikasyon. (II) Elektrik güç kaynakları, gaz ve petrol depolama ve üretim üniteleri. (III) Bankacılık ve finans kurumları. (IV) Ulaştırma birim ve unsurları. (V) Suyun tedarik edildiği birimler. (VI) Acil tıbbi müdahale birimleri, genel kolluk, yangın ve arama kurtarma ünitelerini içine alan acil hizmet birimleri. (VII) Devlet hizmet ve kurumlarıdır (US PCCIP, 1997: A-1/B-1).

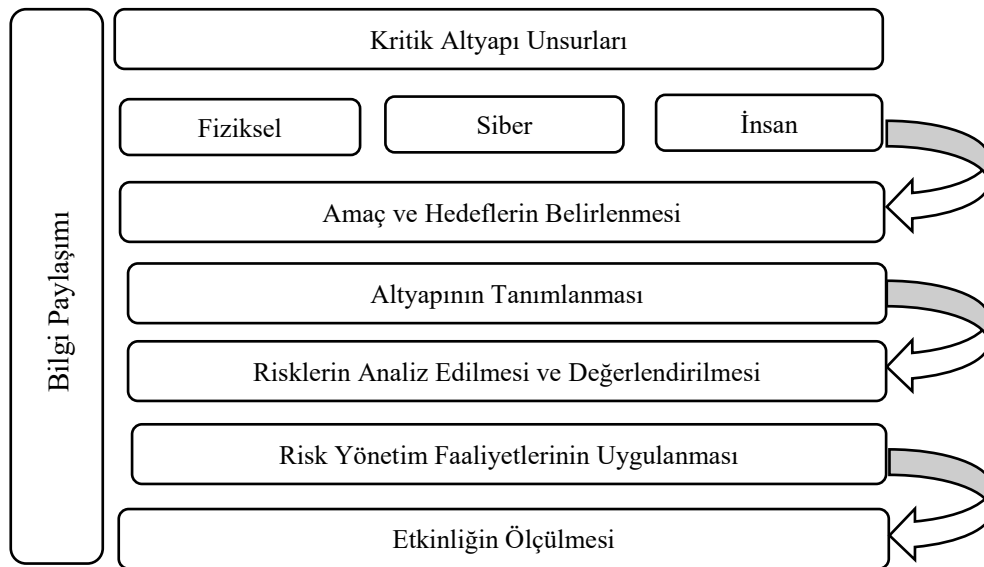
“Kritik altyapı” kavramı, tanım olarak Türkiye’de Afet ve Acil Durum Yönetimi Başkanlığı (AFAD) tarafından hazırlanan “2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi” nde *“İşlevini kısmen veya tamamen yerine getiremediğinde çevrenin, toplumsal düzenin ve kamu hizmetlerinin yürütülmesinin olumsuz etkilenmesi neticesinde, vatandaşların sağlık, güvenlik ve ekonomisi üzerinde ciddi etkiler oluşturacak ağ, varlık, sistem ve yapıların bütünüdür”* şeklinde tanımlanmıştır (AFAD, 2014a: 4). Avrupa Birliği (AB), kritik altyapılar kavramını ise *“Bozulduğunda veya tahrip edildiğinde üyesi devletlerin vatandaşlarının sağlığı, emniyeti, güvenliği ve ekonomik refahı veya hükümetlerin etkin işleyişi üzerinde ciddi bir etkisi olacak olan fiziksel ve bilgi teknoloji tesisleri, ağları, hizmetleri ve varlıkları”* olarak tanımlamaktadır.

Buna ilaveten AB, 2004 yılında ilk kez bu tanımlamaya uyan dokuz sektör belirlemiştir. Belirlenen bu sektörler:

(I) Enerji kuruluşları ve ağları. (Elektrik enerjisi, petrol ve gaz üretimi, depolama tesisleri ve rafineriler, iletim ve dağıtım sistemleri) (II) İletişim ve bilgi teknolojilerinin kendisi ve altyapıları. (İnternet dâhil telekomünikasyon, yayın sistemleri, yazılım, donanım ve ağlar) (III) Finansman hizmetleri. (Bankacılık, menkul kıymetler ve yatırım) (IV) Sağlık hizmetlerinin kendisi ve yapıları. (Hastaneler, sağlık ve kan sağlama tesisleri, laboratuvarlar ve eczacılık ürünleri, arama kurtarma, acil durum hizmetleri) (V) Gıdanın kendisi, yapıları ve ağları. (Gıda güvenliği, üretim araçları, toptan dağıtım ve gıda endüstrisi) (VI) Suyla ilgili altyapılar. (Barajlar, depolama, arıtma ve ağlar) (VII) Ulaşım araçları ve ağları. (Havaalanları, limanlar, demiryolu ve toplu taşıma ağları, trafik kontrol sistemleri) (VIII) Kimyasal, biyolojik, radyolojik ve nükleer maddeler gibi tehlikeli malların üretimi, depolanması ve taşınması. (IX) Hükümete ait değerli varlıklar ve işlevlerdir (EU COM702(F1), 2004: 3-4).

Kritik alt yapıların güvenliğinin sağlanması devletin ulusal çıkarlarının devamı için gereklidir. Çünkü devlet yapılanmasındaki her birimin güvenliği sağlanmalıdır. Siber saldırı karşısında önlem alınması gereken kritik altyapıların varlığı bu noktada ön plana çıkmaktadır. Kritik altyapıların korunması Şekil 6'da görüldüğü gibi öncelikli olarak amaç ve hedeflerin belirlenmesiyle başlayacaktır. Amaç ve hedeflerin önceliği bizleri altyapı birimlerinin tanımlanmasına götürecektir. Altyapı birimlerinin tanımlanması risk faktörlerinin analiz ve değerlendirilmesi noktasında kolaylık sağlayacaktır. Bütün bu süreç esas olarak risk yönetimini oluşturacaktır. Geline en son noktada etkinliğinin boyutu ortaya çıkacaktır. Elbette tüm birimler arasında sağlanan bilgi akışı da ön plana çıkarılmalıdır. Kritik altyapı sürecinin temel bileşenlerinin hem psikolojik hem siber hem de insanı boyutta ilerleme kaydettiği de göz ardı edilmemelidir.

Şekil 6: ABD Kritik Altyapı Risk Yönetimi



Kaynak: Amerika Birleşik Devletleri İç Güvenlik Bakanlığı, 2019.

ABD'nin, Türkiye'nin ve AB'nin kritik alt yapı tanımlamalarını incelediğimizde yapı sistemlerinin varlığının garanti altına alınması zorunludur. Çünkü siber tehditler aracılığıyla bu sistemlerin güvenliği baskı altına alınmıştır. Herhangi bir ülke, kişi ya da grubun gerçekleştireceği siber saldırı karşısında toplumsal güvenlik ve ülke ekonomisi tahribata uğrayacaktır. Dolayısıyla etki kapasitesini henüz anlayamadığımız siber alanın varlığı karşısında en çok göz önüne alınması gereken kritik alt yapıların güvenliğidir.

1.3.5. Siber Caydırıcılık

TDK tarafından caydırıcılık “bir saldırganlığı önlemek ve engellemek için önlem alma işi” şeklinde tanımlanmaktadır (TDK, 2021). Kalevi Jaakko Holsti (1995) ise caydırıcılığı “bir devletin diğer bir devleti askeri güçle etkileme girişiminin engellenmesi” biçiminde tanımlamıştır. Dolayısıyla caydırıcılık kavramı ile asıl anlatılmak istenen savunmadır. Siber caydırıcılık kavramının ana çerçevesi tam bu noktada şekillenmektedir. Siber caydırıcılık, siber alanda meydana gelebilecek saldırılara karşı aktörlerin bu saldırıları gerçekleştirmeden önce durdurması ya da engelleyebilme kapasitesidir.

Caydırıcılık kavramı iki dünya savaşı arası dönemde, Soğuk Savaş boyunca ve 9/11 süreçlerinde farklı yorumlanmıştır. Genel olarak caydırıcılık politikasının istenilen sonuca ulaşması için potansiyel bir saldırganın kendisine misilleme yapılacağı konusunda rakibin tehdit kapasitesini inandırıcı bulması gerekmektedir (Danilovic, 2001: 341).

Ayrıca taraflar arasında bir caydırıcılık sürecinden bahsedebilmek için ‘caydırıcı’ ve ‘caydırılan’ olmak üzere bu iki tarafın ilişki içerisinde olduklarını kabul etmeleri gerekmektedir (Dorman vd., 2005). Caydırıcılık politikasının başarısı sadece tarafların koşulları kabul etmesine bağlı değildir. Aynı zamanda caydırıcılığın başarısı, tehditlerin potansiyel saldırganlara inandırıcı gelmesiyle de bağlantılıdır. Bu bağlamda tehditlerin inandırıcılığı “askeri kapasite”, “sinyalizasyon ve pazarlık gücü”, “itibar” ve “tehlikedeki çıkarlar” olmak üzere dört faktörün varlığından etkilenebilir (Huth, 1999: 25-48). İlk olarak askeri kapasiteyi ele alacak olursak, saldırgan tarafın karşı tarafa askeri gücünü kullanmakta kararlı olduğunu iletmesi gerekir. Bu mesaj biçimi “maliyetli sinyallere” duyulan ihtiyacın somut bir göstergesidir (Lieberman, 2013: 236). İkinci olarak, manipüle edilebilen ve inandırıcı olmayan “sinyaller” ile inandırıcılık kapasitesi yüksek ve manipüle edilmesi zor “sinyaller” arasındaki ayrım net bir şekilde ortaya konulmalıdır (Kydd, 2015: 149-151). Üçüncü olarak, “itibar” kavramı ön plana çıkmaktadır. Caydırıcılık politikalarında aktörlerin geçmişteki davranışlarının gelecekteki davranışlarına etki edip edemeyeceği konusunda ortak bir tanım söz konusu değildir (Miller, 2003: 40-78) Son olarak çıkarlar konusunda ise anlatılmak istenen anlaşmazlık noktasında yüksek çıkar sahibi aktörün güç kullanma noktasındaki arzudur. Güçlü olan çıkarlarını askeri kapasitesini kullanarak garanti altına almayı isteyecektir.

Ancak hayati önem taşımayan çıkarlar söz konusu olduğunda ise askeri güç kullanma arzusu azalacaktır.

Siber caydırıcılık kavramını yorumlayabilmek için klasik caydırma politikalarının çerçevesinden yararlanılabilir. Ancak siber alan içerisinde klasik çerçeve değişmek zorundadır. İlk olarak aktörlerin askeri kapasite kullanma arzusu, sinyaller ve itibar kavramları değişiklik gösterebilir. Siber tehditlerin etki kapasitesi henüz tam olarak belirlenmemiştir. Ancak çıkarlar siber alanda da diğer alanlarda olduğu gibi ön plana çıkacaktır. Bu alana egemen olmak isteyen devlet için kendi çıkarlarını ön planda tutması kaçınılmazdır.

İKİNCİ BÖLÜM

2. DIŞ POLİTİKADA SİBER ALANI YORUMLAMAK

2.1. Dış Politika

Dış politika bir devletin karar alıcı mekanizmaları tarafından, diğer devletler ve uluslararası sisteme yönelik geliştirilen ulusal çıkarların hayata geçirilmesi için planlanan davranış ve stratejilerin bütünü olarak ele alınabilir. Bir devletin dış politikasını belirlemesi için cevaplaması gereken bazı sorular vardır. Uİ sisteminin özellikleri, uluslararası arenada devletin yeri, devletin ulusal çıkarları ve bu çıkarların gerçekleşmesi için gerekli araçların mevcudiyeti, hükümetin yönetim sistemi, ülke içerisindeki güç dağılım şekli, ülkeye hakim olan politik hava ve dış politikada karar verme noktasında etkin olanın ortaya koyulması gerekmektedir. Genel anlamıyla dış politika devletlerin uluslararası arenada diğer devletler karşısında ürettiği çıktılardır. Özellikle II. Dünya Savaşı sonrasında ABD uluslararası arenada diğer devletler hakkında daha detaylı bilgi elde edebilmek için bölgesel çalışmalarda etkin rol oynayabilecek enstitü ve merkezleri desteklemiştir.

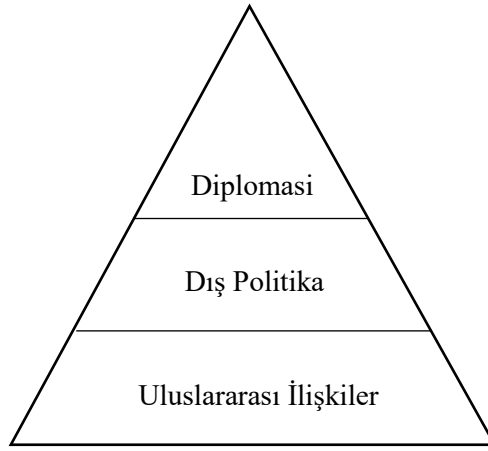
Dış politika analizleri için en temelde uluslararası sistem var olmak üzere dış politikanın yerel kaynakları, karar verme süreci ve devlet ya da diğer kolektif aktörlerden elde edilen dış politika çıktıları 1950’li yıllarda Uİ disiplininin bir alt dalı olan dış politikanın temellerini oluşturmuştur. Süreç içerisinde dış politika olgusunun yalnızca bir etki – tepki olmadığı anlaşılmıştır. Kurumsal anlamdaki dış politika olgusu ulus devletin ortaya çıkışıyla bağlantılıdır.

Dış politika araçlarının etkinliği dış politika kavramını doğrudan etkilemektedir. Dış politika araçları geleneksel ve modern dönem olarak ele alınabilir. Devletler karşılaştıkları durumlar karşısında farklı dış politika araçlarına ihtiyaç duymaktadır. Özellikle siber alan dış politika içerisinde değerlendirilmelidir. Çünkü askeri hareket sayesinde savaş politikasının önüne geçme fikri artık geçerli değildir. Askeri güç kullanımı kadar diplomasiye ihtiyaç duyulan politik düzlemde artık yeni tehdit türleri meydana gelmiştir. II. Dünya Savaşı sonrasında uluslararası hukuk, uluslararası iş birliği gibi kavramlar ön plana çıkmıştır. Soğuk Savaş döneminde ise taraflar askeri çatışmadan kaçındığı için yeni dış politika araçlarına yönelmiştir. Siyaset, kültür, ekonomi, spor ve daha birçok alanda devletler arasındaki rekabet artmıştır. Karşı tarafa üstünlük sağlayabilmek için önceki dönemlerde kullanılmayan dış politika alanlarına ihtiyaç duyulmuştur.

2.1.1. Dış Politika Kavramı

Dış politika kavramı detaylıca ele alınması gereken bir kavramdır. Özellikle Realistler için dış politika, bir devletin karar alıcıları tarafından geliştirilen, diğer devletlere ve uluslararası sisteme yönelik olarak, ulusal çıkarları hayata geçirmek amacıyla planlanan davranış ve stratejilerin kombinasyonudur (Efegil, 2012). Esasen dış politika olgusu, bir devletin dış dünya ile siyasi, ekonomik, hukuki ve diğer alanlardaki ilişkisini baz almaktadır. Bu ilişkiler yumağı çoğunlukla diplomasinin çerçevesine dâhil edilmektir (Sönmezoğlu, 2005).

Şekil 7: Uluslararası İlişkiler, Dış Politika ve Diplomasi



Kaynak: Ester ve Nispen, 2013: 12.

Şekil 7’de görüldüğü üzere Uİ disiplini içerisinde diplomasi ve dış politika birbirini tamamlayan kavramlardır. Temel olarak bu ilişkinin tabanı Uİ disiplininden beslenmektedir. Dış politika devletin devamlılığını sağlarken diplomasi kavramı, dış politika olgusunu kapsamaktadır. Çünkü diplomasi, bir devletin dış dünya ile olan tüm bağlantısının dilidir.

Dış politika iç politika gibi devleti ön plana çıkarmaktadır. Bundan dolayı dış politika, uluslararası arena ile uyum sağlamalıdır. Christopher Hill (2003)’e göre bağımsız aktörler (çoğunlukla devletler) tarafından resmi dış politikalar belirlenmektedir ve uluslararası arenaya yansıyan resmi ilişkilerin tamamı dış politikayı oluşturmaktadır. Bu noktada dış politika, politika ve tutarlılık kavramları üzerine inşa edilmektedir. Aynı zamanda dış politika ve iç politika birbirleriyle bağlantılıdır. Bu yüzden Hill, dış politika kavramı yerine uluslar-içi ifadesini tercih etmiştir. Bir diğer önemli isim George Modelski (1962) ise dış politikayı “toplumların diğer devletlerin davranışlarını değiştirmek ve kendi eylemlerini uluslararası ortama uygun hale getirmek için geliştirdikleri faaliyetler sistemi” olarak tanımlamıştır. Dış politikayı tanımlamak için uluslararası alanda faaliyet gösteren aktörlere, bu aktörlerin amaçlarına, gerçekleştirilen eylemlere ve bu eylemleri gerçekleştirmek için kullanılan yöntemlere ihtiyaç duyulmaktadır.

Şekil 8: Bir Devletin Dış Politikasını Belirlerken Ele Alması Gereken Özellikler

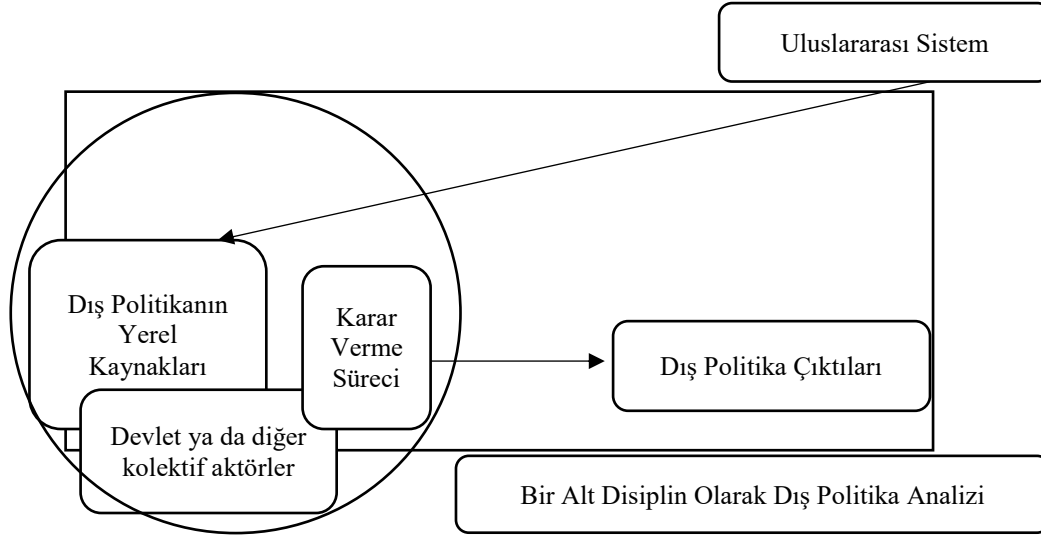
Nasıl bir Uİ sistemi mevcuttur?
Uİ sisteminde devletin yeri nedir?
Bir devletin ulusal çıkarları nelerdir?
Bir devlet ulusal çıkarlarını gerçekleştirmek için hangi araçları kullanır?
Hükümet sistemi nedir?
Ülkedeki güç dağılımı nasıldır ve nasıl bir politik ortam vardır?
Dış politika karar verme sürecinde anahtar kimdir ve özellikleri nelerdir?

Kaynak: Kakauridze ve Gvantsa, 2019.

Şekil 8’de görüldüğü gibi bir devletin dış politika yörüngesini belirmesinde birçok aşama etkilidir. Uİ sisteminin özellikleri, sistem içerisinde devletin konumu, ulusal çıkar tanımları, ulusal çıkarların gerçekleştirilmesi için gereken araçlar, ülkedeki güç dağılımı, mevcut siyasi atmosfer ve karar alma sürecindeki kilit aktörler gibi birçok soruya cevap verilmelidir. Genel anlamıyla dış politika devletlerin uluslararası arena da diğer devletlere yönelik ürettiği politikalarıdır. Bu politikalar oldukça geniş bir perspektiften ele alınmalıdır. Bu aşamada dış politika kavramının tanımları kadar bu kavramın ne zaman ortaya çıktığı da önemlidir. Özellikle II. Dünya Savaşı sonrasında ABD uluslararası arenada etkin bir konum elde etmiştir. Bu süreçte ABD, diğer ülkeler hakkında daha fazla bilgi elde edebilmek amacıyla Uİ çalışmalarını bölgesel çalışmalarda etkin rol oynayan enstitü ve merkezleri desteklemiştir.

Dünya savaşlarının nedenlerinin analiz edilebilmesi ve engellenmesi amacıyla Dış Politika Analizi (DPA) faaliyetleri ön plana çıkarılmıştır (Özcan, 2014). 1950 ve 1960 yılları arasında DPA sayesinde dış politikaları oluşturan faktörler sınıflandırılmış ve alınacak kararların dış politika çıktıları üzerinde nasıl bir etkiye sahip oldukları saptanmıştır. DPA, karar alıcı mekanizmalar tarafından ortaya koyulan dış politikaların dışsal bir uyarıya karşı kendiliğinden oluşmadığını göstermiştir. Geliştirilen dış politikalar ve bu politikaları tanımlayan mekanizmalar tanımlanabilmektedir (Aydın, 1996).

Şekil 9: Bir Devletin Dış Politika Katmanlarının Analizi



Kaynak: Maffra, 2021: 3.

Uİ disiplininin bir alt dalı olan dış politikanın temelleri 1950’li yıllarda ABD’de atılmıştır. Kavramın ilk ortaya çıktığı andaki yoğunlaştığı konular devletlerin dış politika analizleri olmuştur. Daha sonraları bu süreç uluslararası siyaset alanına evrilecektir. DPA, dış politika kavramının ortaya çıkmasında temel etkindir. Karar alıcı mekanizmaların ileri sürdüğü dış politika olgusunun sadece bir etki - tepki süreci olmadığını anlaşılması çok önemlidir. Dışa yansıyan bu politikalar aslında kurumsallaşmanın da temellerini atacaktır.

2.1.2. Dış Politika Araçları

Uİ disiplini içerisindeki en önemli aktörlerden sayılan devletler için dış politika olgusu hayati önem taşımaktadır. Dış politika kavramı yalnızca bir devletin uluslararası arenada sahip olmak istediği potansiyel konumu ortaya çıkarmamaktadır. Aynı zamanda devletlerin varlığını sürdürebilmeleri de dış politikadaki başarılarına bağlıdır. Karar alıcı mekanizmalar için dış politika olgusu her dönem aynı anlamı ifade etmemektedir. İmparatorluk ve krallık dönemlerinde, devletler arası ilişkilerin temeli savaş olgusuna dayanmaktadır. Devletler diğer devleti ganimet elde etmek, topraklarını genişletmek ya da karşı devletin kendisine yönelttiği tehdidi ortadan kaldırmak amacıyla savaşı bir araç olarak kullanmışlardır. Bugünkü anlamıyla dış politika faaliyetlerinin başlangıcı 1648 Westphalia Antlaşması’ndan sonraki döneme aittir. Kurumsal anlamda bir dış politika olgusunun varlığı ulus devletlerin ortaya çıkış dönemine aittir. Kurumsallaşmanın temelleri ortaya atılmıştır (Arı, 2003). Dış politika araçlarının detaylıca analiz edilmesi gerekmektedir. Bu noktada iki farklı dönemden bahsedilebilir. Ancak dış politika araçlarını geleneksel ve modern olmak üzere iki başlıkta birleştirmek doğru değildir. Çünkü devletler karşılaştığı durumlar karşısında farklı dış politika araçlarına yönelmektedirler. Geleneksel dış politika araçları olarak

savaş ve diplomasi ele alınabilir. Modern anlamda ulus devletin ortaya çıkışından itibaren ise dış politika araçları oldukça farklılaşmıştır.

Politik amaç askerî harekât sayesinde sağlanacaksa savaş politikanın önüne geçmektedir. Ancak devletler arasındaki uyumsuzluk diğer alanlardaki ilişkiler göz önüne alınırsa, politik amaç diğer alanların ilerisine geçecektir ve uygun koşullarda kader tayin edecek kadar önemli bir rolü üstlenecektir. Bir diğer önemli politika aracı diplomasidir. Diploması, Uİ oluşturan antlaşmaların tamamını, yabancı bir ülkede ve uluslararası toplantılarda ülkelerin temsil edilme görevi ve sanatı için çalışan kişilerin mesleği olarak tanımlanabilir (Sönmezoğlu vd., 1992). Aynı zamanda diploması, politikaları gerçekleştiren araçlardır. Dış politika ile bağlantılıdır. Devletler arasındaki diyalogun müzakereler aracılığıyla yönetilmesidir. Özellikle 19. yüzyıldan sonra dış politika aracı olarak kullanılmaya başlanmıştır. Diplomasinin dış politika aracı olarak kullanılması oldukça önemlidir. Çünkü eğer diplomatik diyaloglar başarılı olmaz ise ilk yöntem devletleri anlaşmalara zorlamak olacaktır. Böylece yaptırımlar gündeme gelecektir. Bu yaptırımlar diplomatik ve ekonomik yollar ile sağlanabileceği gibi diplomatik ilişkilerin kesilmesi, ekonomik bariyerler ve ambargolar aracılığıyla sağlanabilir (Arı, 2003).

Dış politika araçları her devlet için aynı anlamı ifade etmemektedir. Hatta devletler daha önce uyguladığı dış politika araçlarını tekrardan tercih etmek zorunda da değildir. Dolayısıyla dış politika araçları hakkında bir tasnif yapmak zordur. Ancak dış politika araçlarının gelişim süreçlerini incelenebilir. 19. yüzyılda ulus devlet sistemini temel alan uluslararası sistemde reel politika söylemleri ön planda tutulmuştur. Devletler salt kendi çıkarları etrafında dış politika araçlarına yönelmişlerdir. I. Dünya Savaşı bu sürecin sonucudur (Polanyi, 2005). I. Dünya Savaşı sonrası 19.yüzyıla ait dış politika araçları yerine uluslararası iş birliği, sürdürülebilir barış savları ileri sürülmüştür. Özellikle II. Dünya Savaşı sonrasında ise uluslararası hukuk ve uluslararası iş birliği, karşılıklı dayanışma gibi kavramlar uluslararası sistemde genel kabul gören iddialar olmuştur (Kazgan, 2004). Soğuk Savaş döneminde ise taraflar askeri çatışmadan kaçındığı için yeni dış politika araçları gündeme gelmiştir. Devletler siyaset, ekonomi, kültür, spor ve daha birçok alanda rekabetçi tavrı benimsemiştir. Karşı tarafa karşı üstünlük sağlamak isteyen devletler önceki dönemlerde kullanılmayan dış politika araçlarına yönelmişlerdir (Kazgan, 2004). Yeni araçların siyaset alanına dâhil edilmesi insanların doğrudan ya da dolaylı olarak bilinçaltına yöneltilmiş politikaları ön plana taşımıştır (Arıboğan, 1998).

2.1.3. Dış Politikada Karar Verme Süreci

Devletlerin uluslararası arenayı etkileme kapasitesi dış politikada karar verme süreçlerine etki etmektedir. Burada etki düzeyinin analiz edilmesinden önce analiz düzeyi ele alınmalıdır. Analizin nasıl temellendirileceği ve sürdürülebileceği konusu da göz ardı edilmemelidir.

Tablo 5: Hükümetin Karar Verme Sürecinde Yaşanan Değişimler

Ana Değişim Birimleri	Hükümet Kararını Değiştiren Boyut	Dış Politikadaki Değişimin Boyutu
Lider Odaklı Bürokratik Taraftarlar Yurtiçi Yeniden Yapılanma Dış Baskı	Karar Verme Süreci	Program Değişikliği Hedef/Problem Değişikliği Uluslararası Yön Değişikliği

Kaynak: Al-Fadhat, 2019.

Tablo 5’te görüldüğü üzere hükümetin yönetim anlayışının sahip olduğu belli kriterleri halihazırda mevcuttur. Bu kriterlere etki eden bazı temsil grupları oluşturulabilir. Lider odaklı yaklaşım, bürokrasi taraftarları, yurtiçi yapılanmaya odaklananlar ve dış baskı olmak üzere dört temel değişkenden bahsedilebilir. Bütün bu grupların ana hedefi karar verme sürecinde etkili olmaktır. Elbette dış politikada tecrübe edilen değişimleri de ele alınmalıdır. Karar verme sürecinde yaşanan değişikliklerin sonucunda hükümet programı, hükümetin sahip olduğu hedef ve ele aldığı meseleler ya da uluslararası arenaya yansıyan eğilimde değişiklikler meydana gelebilir. Bu değişimleri yorumlayabilmek için DPA’ya ihtiyaç duyulmaktadır. Synder, Bruck ve Sapin’in çalışmalarında ise DPA’nın bir analiz şekli olarak karar alıcı mekanizmalar tarafından dikkate alındığını gözlemleyebiliriz (Snyder vd., 1969). Bu çalışmaların temel argümanı devlet davranışlarının, o devletin resmi karar alıcı mekanizmaların davranışı olduğudur. Dolayısıyla dış politika analizlerinde bireyler, bireyleri bünyesinde barındıran guruplar ve bu grupların etki ettiği örgütsel süreçlere vurgu yapılmalıdır. Dış politika analizlerindeki en önemli varsayım, karar alıcı mekanizmalar tarafından belirlenen dış politikanın aslında etki - tepki çerçevesinde gelişmediğidir. Dış politika davranışları tanımlanabilir ve ortaya çıkış şekilleri temellendirilebilmektedir (Aydın, 1996).

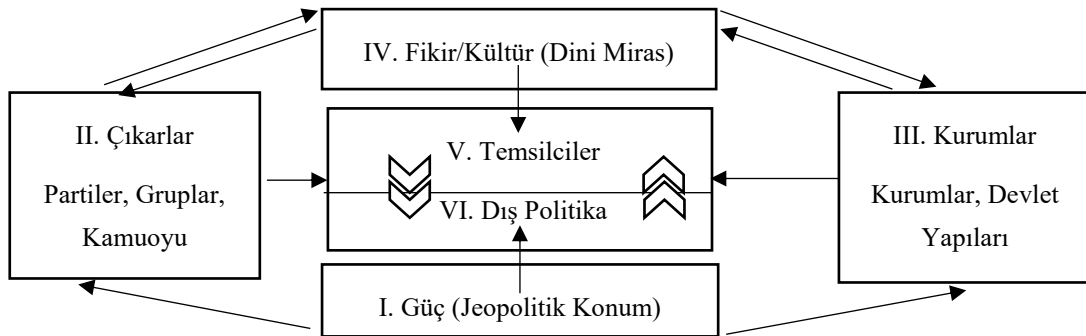
Analiz düzeylerinin tanımlanmasından önce Uİ disiplini içerisinde bir analiz düzeyi sorununun varlığı kabul edilmelidir. Bu sorun ilk defa Kenneth Waltz tarafından 1950 yılında ortaya atılmıştır (Waltz, 1959). Waltz savaşın nedenleri üzerine ortaya koyduğu çalışmada mikro alandan makro alana doğru analiz düzeylerini oluşturmuştur. Birey, toplum, devlet ve uluslararası sistemi doğru evirilen analiz düzeyleri ele alınmıştır. Genel hatlarıyla geçerliliğini koruyan bu analiz düzeyi kısıtlı kalmaktadır. Ulusal - ulus altı gruplar (politik partiler, basın, çıkar grupları vb.), ulus devletler, uluslar-üstü veya ulus ötesi gruplar da (çok uluslu şirketler, hükümet dışı örgütler) analiz düzeylerine dâhil edilmelidir (Aydın, 1996). David Singer (1961) “The Level of Analysis Problem in International Relations” adlı eserinde analiz düzeyi sorununu ilk defa uluslararası politika disiplini bünyesine dâhil etmiştir. David Singer, bu çalışmada “uluslararası sistem” ve “ulus devlet” olmak üzere iki temel analiz düzeyi belirlemiştir. Elbette analiz düzeylerine yönelik yaklaşım birkaç isimden ibaret değildir. James Norah Rosenau, Ronald Joseph Yalem, Louis Cantori ve Steven Spiegel “ulusal”, “bölgesel” ve “küresel” olmak üzere üç temel

analiz düzeyini ele almıştır. Sönmezoğlu ise, uluslararası politika alanını için beş analiz düzeyini ele almıştır. Bu analiz düzeyleri:

“Birey/grup”, “devlet”, “uluslararası kuruluşlar”, “alt sistem” ve “küresel sistemdir”. Fakat 5 analiz düzeyi genel olarak temel iki başlık altında toplanmaktadır. Aktör düzeyi; birey / grup, devlet, uluslararası kuruluşlar iken sistem düzeyi olarak alt sistem ve küresel sistemler ele alınmıştır (Sönmezoğlu, 2012).

Kalevi Jaakko Holsti ve Joseph Frankel ise DPA için “birey”, “devlet” ve “sistem” olmak üzere üç analiz düzeyine yoğunlaşmıştır (Holsti, 1968; Frankel, 1968). Dış politika alanının analiz edilmeye başlaması II. Dünya Savaşı sonrasına denk gelmektedir. Dış politika alanının temelleri ise 1950 – 60’lı yıllarda atılmıştır. Önemli olan uluslararası arenada hâkim olan aktörlerin davranış biçimleridir. Bunun için bilimsel modellere ihtiyaç duyulmuştur (Özcan, 2011).

Şekil 10: Dış Politikanın Makroskobik Haritası



Kaynak: Warner ve Walker, 2011: 113-135.

Dış politikada davranış biçimlerinin incelendiği bu dönemde klasik çalışmalar karşımıza çıkmaktadır. 1954 yılında Richard Christopher Snyder, Henry Bruck ve Burton Sapin'in "Decision-Making as an Approach to the Study of International Politics" adlı çalışmada karar verme sürecindeki davranış biçimi örgütsel olarak tanımlanmıştır (Snyder vd., 2002). İkinci çalışma ise James N. Rosenau'nun 1966'da yazdığı "Pre-theories and Theories of Foreign Policy" isimli çalışmasıdır. Bu makalede daha çok dış politika davranışlarının sebeplerini çözümleyebilmek için farklı düzeylere dikkat çekmiştir.

Dış politika analizleri için bazı modellemelere ihtiyaç vardır. “Rasyonel Aktör Modeli” yaklaşım biçiminde devlet liderlerinin kararları temel olarak kabul edilmektedir. Dolayısıyla liderler ülkesi için uzun vadede ulusal çıkarlar ile hareket etmektedir. Ulusal çıkarlar anlık değişmediği için, liderlerin kararlarında değişiklik çok sık yaşanmaktadır (Neack, 2008). İkinci olarak “Örgütsel Model” yaklaşım modelinde her örgüt kendi kurumsal özelliklerinden ötürü bazı ilkeler geliştirmiştir. Geliştirilen bu ilkeler standart davranış biçimlerini ortaya koymaktadır. Örgütsel davranışlar da bu süreç içerisinde prosedür ve bir dizi teamüller sonucunda ortaya

çıkılmaktadır (Mintz ve Derouen, 2010). Üçüncü model olarak “Bürokratik Modeli” ele alabiliriz. Dış politikada alınan kararlar devlet kurumlarının farklılaşan karışık çıkarlarının bir sonucudur (Goldstein ve Pevehouse, 2014). Karar vericiler, devlet adına hareket eden bürokratik birimlerdir. Her bürokratik birim kendi kurum çıkarlarını ön plana çıkaracağı için dış politikaya hâkim olma arzusu etkindir. Alınan kararlar rasyonel aktör modelinin aksine en iyi seçenek değildir. Her kurumun uzlaştığı optimal seçenektir (Efegil, 2012). Bir diğer model olarak ise “Bireysel Karar Alıcı Mekanizmaları” ele alınabilir. İlk olarak karar verici mekanizmalar kararın alınmasına etki eden bilgi kümesini azaltmalı ve filtrelemelidir. Dikkat edilmesi gereken temel nokta bu filtreleme sürecinde ön yargılı davranılmaması gerektiğidir. İkinci olarak duygusal ön yargı olmadan hareket edilmelidir. Son olarak “Bilişsel Ön Yargılar” modeli incelenebilir. Bilişsel ön yargılar duygusal hislerle ele alınmamalıdır. Rasyonel hesaplamaların sistematik çarpıklıklarına yer verilmemelidir (Goldstein ve Pevehouse, 2014).

2.2. Dış Politika – Siber Alan İlişkisi

Devletlerin dış politika kararlarını temellendirirken siber alanın Uİ disiplini içerisinde nasıl ele alınması gerektiği tartışmalıdır. 1950 ve 1960’lı yıllarda dış politika kavramı daha çok devletlerin birbirleriyle olan ilişkisiyle ilgilidir. İlerleyen dönemlerde devletlerin dış politika süreçlerini etkileme kapasitesinden daha çok karar alıcı mekanizmaların işlevselliği ön plana çıkmıştır.

Dış politika analizlerinin ilk ortaya çıktığı klasik dönem ile Soğuk Savaş Dönemi dış politika analizleri birbirinden oldukça farklıdır. Soğuk Savaş döneminde dış politika kavramı ele alınırken özellikle “dış” olarak kastedilenin tanımlanması önemlidir. Bir ülke için dış sadece kendi ülkesel alanlarına dahil edemediği toprakları değildir. Karşılıklı bağımlılığın da etkisiyle beraber iç ve dış arasındaki ayrım da gündeme gelmiştir.

Soğuk Savaş sonrasında meydana gelen yeni tehdit türleri dış olanın tanımlanmasını zorlaştırırken teknolojik gelişmeler sayesinde siber alan başka bir boyuta evrilmiştir. Siber saldırılar karşısında caydırıcılık sağlayabilmek adına siber savunma gündeme taşınmıştır. Dolayısıyla devletin güvenliği için yeni dış politika araçlarına ihtiyaç duyulmaktadır.

2.2.1. Siber Alanın Dış Politikadaki Yeri

1950 ve 1960’lı yıllarda daha çok devletlerin birbirleriyle olan ilişkileri ön plana çıkarılmıştır. Temel nokta, uluslararası arenada etkin olan aktör ya da aktörlerin davranış biçimlerinin analizidir. Gelecek için varsayımda bulunabilmek için çeşitli modellemeler kullanılmıştır (Özcan, 2011). 1950 ve 1960’lı yıllardaki çalışmalar için Laura Neack ve

meslektaşları “Birinci Kuşak” tanımlamasını yapmışlardır ve bu dönemi “Karşılaştırmalı Dış Politika Analizi (KDPA)” olarak adlandırmışlardır. Bilimsel bir teori oluşturabilmek için nicel verilerden yararlanılmıştır (Neack vd., 1995). 1960’lı yıllar kalıcı mekanizmaların nasıl işlevlik kazandığından ziyade etkin aktörlerin dış politikada nasıl karar verdiklerine odaklanıldığı bir dönemdir. İlk dönemden günümüze kadarki süreçte devletlerin dış politikayı algılama biçimleri oldukça farklılaşmıştır.

Dış politika algısındaki bu değişimlerin temelinde farklı sebepler vardır. Dış politika analizlerinin ilk ortaya çıktığı dönem ile Soğuk Savaş dönemi dış politika analizleri birbirlerinden oldukça farklıdır. Soğuk Savaş sonrası dönemde ise dış politika analizleri farklı bir boyuta evrilecektir. Uİ için dış politika iki kavramdan oluşmaktadır. “Dış” sıfatıyla kastedilen genellikle bir ülkenin kendi sınırlarına dâhil edilmeyen alanlardır. Ancak bu noktada daha fazla bilgiye ihtiyaç vardır. Dış ile kastedilen alanın tam olarak nerede başladığı, hangi ülkeleri içermesi gerektiği gibi soruların cevabı belirsizdir. Ayrıca karşılıklı bağımlılığın etkisini arttırdığı bu dönemde dış ve iç arasındaki ayrımın önemi ortaya çıkmıştır (White, 1989: 16). Politika kavramı ise tanımlı tartışmalı bir kavramdır. Daha çok iktidar mücadelesi, sınıf mücadelesi, çatışma, iş birliği gibi farklı birçok anlama gelmektedir (Arı, 2008:36). Dış politika olgusuna gelince, bazı taraflar “dış” üzerine yoğunlaşırken bazı taraflar ise “politika” alanına yönelmiştir (Gözen, 2001: 3). Kalevi Jaakko Holsti (1992: 9)’ye göre ise dış politika bir devletin ihtiyaç, arzu ve kapasitesine göre karar alma sürecinde belirlenen ve bu amaçları gerçekleştirmek için dış çevresine yönelttiği siyasal temelli tutum ve davranışların bir bütünüdür. Siber alanın dış politika alanına nasıl entegre edilebileceği de belirsizdir. Ancak etki kapasitesi henüz belirlenemeyen bu alan her devlet için tehdit potansiyeline sahiptir. Bu sebeple gelecek dönemlerde karar alıcı mekanizmalar için siber alan göz ardı edilemeyecektir.

2.2.2. Dış Politikada Siber Savunma

Uİ disiplini için devletlerin dış politika kararlarını temellendirirken siber savunmanın bu alan içerisine dâhil edilip edilemeyeceği tartışmalı bir konudur. Siber savunmanın karar alıcı mekanizmalar tarafından nasıl yorumlanması gerektiği konusu net değildir. Siber tehditler, siber savunma olgusunu ön plana çıkarmıştır. Devletler için güvenlik olgusunun ne kadar önemli olduğu düşünülürse modern dönemin en büyük tehdit unsuru siber saldırılar olarak nitelendirilebilir. Bilgi ve iletişim alanında yaşanan gelişmeler tehdit boyutunun etki kapasitesini gözler önüne sermektedir. Siber tehditler yalnızca devletlerin değil aynı zamanda uluslararası sistemde yer alan uluslararası örgütlerin de dikkatini çekmektedir.

Kuzey Atlantik Anlaşması Örgütü (North Atlantic Treaty Organization / NATO) veya AB gibi ulus – üstü yapılanmalar örnek verilebilir. Siber güvenliğin temel alınması noktasında NATO ve AB kıyaslayacak olursak, NATO’nun ele aldığı politikaların daha kapsamlı olduğu fark

edilecektir (Darıcı, 2019). Dış politika her devlet için özel bir anlam ifade etmektedir. Karar alıcı mekanizmaların itici gücü her devlet için aynı özelliklere sahip değildir. Her devlet için siber güvenlik politikalarının ele alınma biçimi farklılık gösterecektir. Ayrıca siber savunma olgusu için henüz devletleri bir araya getiren ortak bir platform yoktur. Ancak AB'nin siber güvenlik kaygısıyla ortak hareket etme düşüncesi siber savunma olgusuna ışık tutacaktır. Siber savunma, siber uzay adı verilen yeni, karmaşık, çok boyutlu ve henüz keşfedilmemiş alandaki tehditlere karşı alınabilecek önlemlerin bütünüdür. Bu noktada somut bir tanım yoktur (Craig vd., 2014). AB'nin siber savunma kavramına ilişkin bakış açısını anlayabilmek için siber güvenlik olgusunu nasıl yorumladığı ön plana çıkarılmalıdır. AB siber güvenlik kavramına kolektif olarak yaklaşmaktadır. 7 Şubat 2013 yılında Komisyon tarafından yayınlanan yayımlanan “AB'nin Siber Güvenlik Strateji (Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace) belgesi, bu belgenin 2017 yılında yeniden güncellenmiş versiyonu olan belge (Resilience, Deterrence and Defence: Building Strong Cybersecurity for the EU) ve 11 Mart 2019 tarihinde Avrupa Parlamentosu tarafından onaylanan, 27 Haziran 2019 tarihinde yürürlüğe giren Siber Güvenlik Yasası'nda (Cyber Security Act) siber güvenlik kavramına yer verilmemiştir. Ancak AB'ye bağlı, ağ ve bilgi güvenliğinden sorumlu olan Avrupa Ağ ve Bilgi Güvenliği Ajansı, (European Network and Information Security Agency-ENISA) siber güvenliği tanımlamıştır.

Şekil 11: AB'nin Siber Tehditlere Karşı Cevabı

Mevcut Durum: Çoğu AB ülkesi için eş-güdümlü hareket edilmesi beklenmektedir.
Özellikle İspanya ve Portekiz için “Sessiz Diplomasi” ön plana çıkarken İspanya ile “Karşılıklı İmtiyaz Ticareti” mevcuttur.
Arka plandaki görüşmelerde çoğu zaman Fransa ön plandadır. Bu noktada siber konular Fransa ve Almanya için bölümlere ayrılmıştır.
İngiltere, Hollanda ve bazen Fransa tarafından siber tehditler kamuoyuna duyurulmaktadır ancak siber sorunlar bölümlere ayrılmamıştır. Bu yaklaşım farklılıkları genel olarak ilişkilerin kötüye gitmesine sebep olmuştur.
AB için teoride siber saldırılar karşısında ekonomik yaptırımları vurgulamaktadır. Siber uzayda hackleme ve savunma-taarruz gibi konular İngiltere, Hollanda ve Fransa tarafından ele alınmaktadır. AB'ne ait iddialar, ABD tarafında takip edilmektedir.

Kaynak: Gressel ve Gustav, 2019.

Şekil 11'de görüldüğü gibi dış politikada siber tehditlere karşı ortak önlem alınması kolay değildir. AB gibi ulus - üstü bir yapılanma içerisindeki devletlerin dahi konuya bakış açısı farklıdır. Dış politikada ortak siber savunma anlayışını tartışabilmek için AB üzerine yoğunlaşıldığında aslında ortak savunma anlayışını benimsemenin zorluğu ortaya çıkmaktadır. AB içerisindeki devletlerin siber tehditler karşısında koordineli bir şekilde hareket etmesi beklenmektedir. Devletler

arasındaki çıkar ilişkileri ortak değildir. Zaman zaman siber saldırılar karşısında Fransa ön plana çıksa dahi İngiltere ve Hollanda'nın siber tehditleri değerlendikleri hususlarda önemlidir. Siber tehditler karşısında ortak bir savunma görüşü kolay değildir ancak AB siber alandaki ortak bir görüş için çabaları göz ardı edilmemelidir. Bu ortak anlayış biçimi ilerde devletlerin dış politika eksenlerine etki edebilir.

NATO ise özellikle 2000 yılı ve sonrasında siber tehditlere yoğunlaşmıştır. 1999 yılında Sırbistan müdahalesi sonrası Çin ve Rusya kaynaklı saldırılar, NATO'nun bu alanda güçlü olmadığını kanıtlamıştır. 2002 Prag Zirvesi'nde Siber Savunma Programı kabul edilmiştir. Bilgisayar Olaylarına Müdahale Gücü Teknik Merkezi, Prag Yetenekler Taahhüdü, Kapsamlı Siyasi Yönerge gibi araçlar sayesinde siber savunma politikalarının temelleri atılmaya çalışılmıştır. Daha sonrasında Estonya'ya yapılan saldırının bir sonucu olarak NATO, siber güvenlik meselesini birincil risk alanı olarak tanımlamıştır. Çünkü Estonya maruz kaldığı saldırı sonucunda haftalarca yönetilemez duruma getirilmiştir (Seren, 2006: 16-17). Siber saldırıların ana hedefi başta ulus devletler olmasına rağmen uluslararası alandaki her aktör tehdit altındadır. Sadece yönetim mekanizmaları değil uluslararası toplumda bu saldırılardan etkilenmektedir.

İlk siber saldırı 1982 yılında Sibirya'daki doğalgaz boru hatlarını hedef almıştır. Bu saldırı sonucunda meydana gelen patlamanın aktörleri ABD ve SSCB'dir. Ambargo altındaki SSCB Kanada'daki bir şirketin doğalgaz boru hatlarını kontrol eden sistemlerine erişim sağlamıştır. CIA (ABD Haber Alma Örgütü) bu durumu fark edip yazılımın içerisine "Logic Bomb" adlı bir saatli bomba yerleştirmiştir. Bir diğer siber saldırı örneği Ay Işığı Labirenti (Moonlight Moze)'dir. ABD'nin NASA, ABD Enerji Bakanlığı, Pentagon ve üniversitelerini hedef alan bu saldırının amacı askeri tesislere ait bilgiler ve araştırma – geliştirme projelerinin bilgilerini ele geçirmektir (Tandoğan, 2010: 1).

1990'lı yıllarda NATO'nun Yugoslavya'nın sonuna getiren çatışmalara etki eden müdahaleleri ve özellikle 1999 yılındaki hava saldırılarıyla birlikte gerçekleştirdiği eylemler bazı hacker grupları tarafından eleştirilmiştir (Yener, 2014: 1). 2008 yılına gelindiğinde ise Gürcistan'a yöneltilen siber saldırıların arkasında Rusya Federasyonu'nun olduğu iddia edilmiştir. SSCB'nin çökmesinin ardından Güney Osetya ve Abhazya de facto olarak özerk bir bölge statüsü elde etmişti. Ancak artan milliyetçilik söylemleri ile Gürcistan ordusu Güney Osetya bölgesine askeri harekatta bulunmuştur. Rusya Federasyonu bu askeri hareketin ardından Güney Osetya'ya müdahale edince taraflar arasında gerginlik hâkim olmuştur (Darıcılı, 2014: 7). Bir başka örnek ise Wikileaks Belgeleri'dir. Irak'ta görev almış ABD ordusuna mensup Bradley Manning, ABD Dış İşleri Bakanlığı'nın 1996-2010 yılları arasındaki gizli yazışmaları, ordu veri tabanına ait bilgileri 2010 yılında Wikileaks aracılığıyla dünyaya sızdırmıştır (Kara, 2013: 17). Özetle dış politikadaki karar alıcı mekanizmalar için artık siber alan göz ardı edilemeyecek bir etkiye sahiptir. Başta sadece devletleri tehdit eden bu saldırılar tüm uluslararası alanı etki altına almıştır. Henüz siber

savunma kavramının dış politikaya nasıl entegre edileceği konusu netlik kazanmamıştır. Devletin ulusal çıkarları farklı olduğu için siber alana bakış açısı da farklılık gösterecektir.

2.2.3. Dış Politika Karar Verme Sürecinde Siber Alan

Dış politikadaki karar alıcı mekanizmalar için siber alan artık yeni bir anlam ifade etmektedir. Uluslararası İlişkiler disiplini içerisinde güvenlik birçok kavramın temelini oluşturmaktadır. Bu noktada siber güvenlik karar verme süreçlerine etki edilen boyutu ortaya çıkarmaktadır. Siber güvenlik öncesini oluşturan siber uzay ise esasen Soğuk Savaş'ın ürünü olarak kabul edilmektedir. Daha çok siber uzay denildiğinde askeri güvenlik ve güç mücadelesi ön plana çıkmaktadır. Gelişmiş Araştırma Projeleri Ajansı Ağı (ARPANET) sayesinde internetin temellerinin atıldığı süreç bilgi akışını çok farklı bir aşamaya taşımıştır. 1960'lı yıllardaki Doğu ve Batı arasındaki çatışmada internetin gelişmesine katkı sağlamıştır. Bu dönemden sonra dış politikadaki karar alıcı mekanizmalar siber alana yönelmiştir. Güvenlik birey, toplum ve uluslararası arena için vazgeçilmezdir. Bu aşamada siber uzayın tek bir merkezden yönetilememesi her devletin karar alıcı mekanizmaları için siber alanı ön plana çıkarmıştır.

Karar alıcı mekanizmalar için siber güvenlik kavramı tek başına yeterli değildir. Bir başka açıdan ise savaş olgusunda meydana gelen değişimler dikkat çekicidir. Siber alandan önce savaş; kara, deniz, hava ve uzayın dâhil edildiği alanlarda meydana gelen çatışmalardı. Siber alan beşinci boyut olarak karşımıza çıktığında siber uzayın sadece teknolojik gelişmelerin başka bir boyutu olmadığı anlaşılmıştır. Hibrit savaş sayesinde geleneksel savaş yöntemleri geçerliliğini yitirmiştir. Siber savaş; bir devletin başka bir devletin siber uzaydaki varlığını tehdit etmek amacıyla ya da siber alandaki varlıklarını kendi lehine kullanma amacını güttüğü saldırıların tümü olarak kabul edebiliriz (Keleştemur, 2018: 77). Devletlerin dış politikadaki karar alıcı mekanizmaları artık siber alanı dış politika analizlerine dâhil edecektir. Siber savaş, siber tehdit, siber saldırı gibi birçok kavram esasen güvenlik kavramları ile ilişkilidir. Siber güvenlik özellikle 9/11 ve sonrasındaki Madrid ve Londra gibi metropol şehirlerde meydana gelen terör saldırılarıyla gündeme gelmiştir. Bu saldırılar bize siber alanda gerçekleştirilen herhangi bir saldırının konvansiyonel terör eylemlerinin yıkım kapasitesinin sebep olabileceği etkiye sahip olduğunu kanıtlamıştır (Dupont, 2013: 67-80). Dış politikadaki karar alıcı mekanizmaların siber alanı göz ardı etmesi mümkün değildir.

Karar alıcı mekanizmalar için siber alan artık göz ardı edilemeyecek bir etki boyutuna sahiptir. Uluslararası sistemdeki her devlet siber alanda güvenlik anlayışlarını değiştirmelidir. Bu değişim esasen bir tercihten çok zorunluluktur. Sadece devletler değil aynı zamanda bireyler ya da bireylerin oluşturduğu gruplar da siber alanda tehdit potansiyeline sahip aktör haline gelebilirler. Dahası bu tehditlerin etki boyutları henüz belirlenememiştir. Her devletin karar alıcı mekanizmaları dış politikadaki eksenlerini belirlerken siber alanı da bu eksen içerisine dahil etmelidir.

yeteneklerle saldırı gerçekleştirilebilir. Beşinci adım, erişim kapasitesinin geliştirilmesidir. Saldırının hedefi olan yapı içerisindeki özel yetkili kişiden alınacak bilgiler, bilginin tedarik edildiği zincir sistemi, SQL gibi veri tabanına dayalı uygulamalar için kullanılan atak tekniği ve yemleme kancası adı verilen yöntemler sayesinde erişim kapasitesi arttırılmaktadır. Altıncı adım, eylemlerin uygulanma aşamasıdır. Bu aşamada saldırının hedefi kontrol altına alınabilir, ağ sisteminde hareket edilebilir, veri çalınabilir, zarar görebilir veya manipüle edilebilir ve saldırının izleri gizlenebilir. Yedinci adım; değer biçme aşamasıdır. Saldırı başarılı mıdır?, Saldırı etkili midir?, Saldırı hedeflenene ne kadar etki etmiştir? gibi birçok soru sorulmaktadır. Son aşama ise yeniden bir saldırı ihtimalinin değerlendirilmesidir. Siber istihbarat kavramı; siber saldırı engelleme, caydırma ve bu saldırıları yok etme noktasında oldukça önemlidir.

Siber istihbarat kavramı Soğuk Savaş döneminde ilerleme göstermiştir. İki kutuplu bu düzende ulusal güç askeri güç ile özdeşleştirilmiş olup istihbarat daha çok düşmanın etki kapasitesini keşfetmeye odaklanmıştır. Askeri güce birincil önem atfedilmiştir (Caşın, 2002). 1990'lı yılların başında ise Soğuk Savaş döneminin sona ermesiyle birlikte dünyadaki güvenlik ve tehdit algılamalarında önemli değişimler gerçekleşmiştir (Sandıklı ve Emeklier, 2012).

Bilgi teknolojilerinde yaşanan gelişimler sonucunda geleneksel/klasik istihbarat yöntemlerinin yerini özel bir istihbarat alanına bırakmıştır. Teknik istihbarat, sinyal istihbarat, ölçüm ve iz istihbaratı gibi spesifik istihbarat alanları literatüre girmiştir (Roberts vd., 2011). Klasik istihbaratın aksine bu yeni alanda daha az personel ve malzemeye ihtiyaç duyulmasının yanı sıra bilgiye erişim noktasında azalan maliyetle beraber mevcut kaynaklarda yaşanan artışla birlikte bilgilerin depolanması ve analiz edilmesinde bilgisayarlar siber istihbaratın vazgeçilmez unsurlarıdır. İnternete duyulan bağımlılık artmıştır. İstihbarat servisleri artık sadece internetten değil aynı zamanda ağa bağlı bilgisayar sistemlerine erişim sağlayarak gizli bilgilere erişme olanağını elde etmiştir (Lewis, 2022).

Siber istihbarat yöntemleri devletten devlete farklılık göstermektedir. Bu noktada Kemal Girgin (2003)'e göre, siber istihbaratın iki temel özelliği vardır. İlk olarak internet aracılığıyla kısa sürede elde edilen bilgilerin yayılmasıdır. İkincisi de aktif durumdaki bilgisayarlardan teknik hileler aracılığıyla bilginin alınmasıdır. Siber istihbarat yöntemlerine biraz daha yoğunlaşmak için siber elektronik istihbarat kavramını ele alalım. Bu noktada hükümetler, iç işlemleri için kendi iç ağlarına özel yazılımlar geliştirmektedir. Dışarıdaki kuruluşlar ile iletişime geçilmesi durumunda güvenilirliği kanıtlanmış yazılımlar baz alınsa dahi istihbarat servisleri çok özel yazılımlar sayesinde bu iç ağlara erişebilmektedir. Bir diğer yöntem olarak açık kaynaklı gerçekleştirilen siber istihbarat faaliyetleri ele alınabilir. İnternetin yaygınlaşması, uydu yayınlarının artması ve özel kanalların çoğalması gibi birçok kaynak alan oluşmuştur. Medyanın gösterdiği gelişim ele alınırsa istihbarat servislerinin medya kanallarına neden yoğunlaştığı anlaşılacaktır. Dünyadaki gelişmeler ile ilgili önemli bilgiler açık kaynaklar aracılığıyla kolayca elde edilebilmektedir.

İnternetin hayatımızda edindiği konumu ele alacak olursak klasik medya bağlantılarının takip edilme süreci yeni bir boyuta ulaşmıştır. Bu süreç sosyal mühendisliği gündeme getirmiştir. Sosyal mühendislik perspektifi için bilgi güvenliği sistemlerindeki en zayıf unsur insandır. İyi bir analiz düzeyi ile insanların eğilimleri göz önüne alınarak gizli bilgilere erişilebilmektedir. Siber istihbarat için sosyal ağlara dayalı istihbarat faaliyetleri burada ön plana çıkmaktadır. Siber istihbarat diğer istihbarat alanlarına bakılmaksızın kendine özgü özelliklere sahip farklı bir istihbarat alanını oluşturacaktır.

2.3. Dış Politika – Siber Alan İlişkisinin Tarihsel Seyri

2.3.1. Siber Alanın Tarihsel Gelişiminde Dış Politikaya Etkisi

Uİ disiplini içerisinde dış politika çalışmalarının detaylıca ele alınması gerekmektedir. Burada ele alınan konu dış politika ve siber alan ilişkisi olduğu için güvenlik olgusu ön plana çıkmaktadır. Kopenhag Okulu öğretileri güvenlik çalışmalarında dikkat çekicidir. Bu noktada güvenlikleştirme teorisiyle güvenlik çalışmalarına atıfta bulunulabilir. Her problem güvenlik sorunu olarak algılanmamalıdır. Zaman içerisinde bir sorunun güvenlik problemine dönüşme ihtimali de göz ardı edilmemelidir (Birdişli, 2014). Kopenhag Okulu öğretilerine göre güvenlik beş bölümden oluşmaktadır. Bu alanlar çevre, ekonomi, askeri, siyasi ve ideolojiktir (Çıtak, 2017).

İnternetin hayatımıza girmesiyle birlikte coğrafi sınırlar etkinliğini yitirmiştir. Siber güvenlik disiplin içerisinde yerini almaya başlamıştır. Güvenlik teorilerindeki temel taşlar yeniden şekillenecektir. Devlet sınırlarını aşan yeni sistemde, siber güvenlik için iş birliği artık bir zorunluluktur (Bıçakçı, 2013). Siber güvenlik kavramı uluslararası sisteme siberin ortaya çıkışıyla kazandırılmıştır. Tüm bilişim sistemlerini içeren bu kavram güvenliğin tanımlanması açısından oldukça önemlidir. Çoğu zaman bilgi güvenliğiyle karıştırılmaktadır. Ancak siber güvenlik bilgi güvenliğini kapsamaktadır (Altınkaynak, 2017). ARPANET döneminde gerekli altyapı hizmetleri belirli ve güvenilir araştırmacılar tarafından kullanıldığı için ilk dönemlerde güvenlik ihtiyaç haline gelmemiştir. Zamanla siber güvenlik kavramı sadece birey, toplum için değil aynı zamanda devletler için önemli bir konuma gelmiştir. Siber güvenlik, kullanıcıların, kurum ve kuruluşların siber alandaki varlıklarını siber tehditlere karşı korumayı hedeflemektedir (Çiftçi, 2017).

Aynı zamanda siber güvenliğin bir başka amacı da Bilgi ve İletişim Sistemleri bünyesinde yer alan güvenlik açıklarını en az seviyeye indirmektir (Ünal, 2015). Siber güvenlik, siber tehditlerin karşısında yer alan bir kavramdır. Bu kavramın önemi siber tehditlerin devletin temel güvenliğini etkileme kapasitesinden kaynaklanmaktadır. Bilimsel ve teknik olarak ortaya çıkan bu yeni alan devletlerin dış politika algılarını da değiştirmektedir. Yeni olgular ışığında toplumsal inanç, kurumsal ve siyasal sistemlerde köklü değişiklikler yaşanmıştır. Yeni güvenlik anlayışı, yeni

kavram ve önlemler ortaya çıkacaktır (Dedeoğlu, 2014). Bu yeni alan devletlerin sahip oldukları dış politika mekanizmalarına da etki edecektir.

2.3.1.1. Soğuk Savaş Dönemi Gelişmeleri ve Siber Alan

Soğuk Savaş dönemi Uİ disiplini içerisinde uzun yıllar üzerinde çalışan özel bir alandır. Bu bölümde siber alanın Soğuk Savaş döneminde gösterdiği gelişmeler üzerinde durulacaktır. Dünyada en büyük yıkıma neden olan ilk kez Japonya'ya atılan iki atom bombası (Hiroşima ve Nagazaki) II. Dünya Savaşı'nı sonlandırmıştır. Bu süreçten sonra savaş başka bir boyuta evrilmiştir (King, 1991: 3-8). Soğuk Savaş dönemini ele aldığımızda daha çok Batı ve Komünist Doğu Blok arasındaki güç mücadelesi karşımıza çıkacaktır. Fakat temel olarak asıl odaklanmamız gereken konu güvenlik çalışmalarıdır. Özellikle Arnold Wolfes (1952)'in ilk kez ulusal güvenlik kavramıyla birlikte ulusal çıkarlar ön plana çıkarılmıştır.

ABD ve SSCB arasındaki güç mücadelesinde ulusal çıkar fikrinin güçlenmesiyle birlikte güvenlik ikilimi de önem kazanacaktır. ABD'nin atom bombasını kullanmasının ardından SSCB'de kısa bir süre sonra 1949 yılında atom bombası üretmeye başladığında güvenlik ikilimi tırmanma noktasına geçmiştir (Douglass, 1999: 1).

SSCB ve ABD arasındaki bu mücadele SSCB'nin 4 Ekim 1957 tarihinde ilk uyduyu uzaya fırlatmasıyla (Wall, 2017) farklı bir boyuta evrilmiştir. SSCB'nin öncülük ettiği bu uzay çağı Soğuk Savaş döneminde siber uzay için dönüm noktası olmuştur (Bulduk, 2006: 63). ABD, SSCB karşısında hızlı bir reaksiyon almak istediye de 6 Eylül 1957 tarihindeki ilk denemesi başarılı olmayacaktır. Devletlerin hızlı bir şekilde aldığı tepkiler ele alındığında silahlanma ön plana çıkmaktadır. Karşı tarafın refleks olarak vereceği cevap belirsizliğe sebep olacaktır (Szalai, 2009: 107). Ancak Soğuk Savaş dönemi için bu geçerli değildir. İlk uydu yarışlarından sonra yeni silahlanma süreci oldukça açıktır. ABD Başkanı Eisenhower, Ulusal Havacılık ve Uzay İdaresi (NASA)'nin kuruluş talimatını 1 Ekim 1958'de vermiştir (A Brief History of NASA, 2019). NASA, Sputnik atmosferine verilen cevaptır. Uzay yarışında amaç teknolojik üstünlüğü elde etmek olacaktır (Dick, 2019). Aynı dönemde ABD Hükümeti, Gelişmiş Araştırma Projeleri Ajansı (ARPA)'nı kurmuştur (ARPA is born, 2019; Techopedia, 2019; DARPA, 2019).

1972 yılında ARPA'nın ismi değiştirilerek Savunma İleri Araştırma Projeleri Ajansı (DARPA) olmuştur (ARPA Becomes DARPA, 2019). Bu ajans yapılanması daha sonraki süreçte özel kuruluşlar ve üniversiteleri de bünyesine alarak ARPANET'e dönüşmüştür (Akyeşilmen, 2018: 26). ARPANET (ARPANET, 2019; Techopedia, 2019) çağdaş dünyamızın her alanına nüfuz eden internetin temelini oluşturacaktır. Dünya genelinde farklı coğrafyalardaki bilgisayarlar için, ARPANET olarak geliştirilen bu yeni ağ sayesinde güvenilir bir yol hedeflenmiştir (Radiantlunatic, 2019).

Uzay çalışmaları ile başlayan bu süreç Soğuk Savaş dönemini çok farklı bir boyuta taşımıştır. ABD ve SSCB arasındaki mücadele uzay teknolojisi üzerinden yürütüldüğü için siber uzay kavramının gelişmesine de katkıda bulunulmuştur. Bu mücadelede karşımıza çıkan güvenlik ikilimi sayesinde taraflar yeni bir alanın gelişmesine katkı sağlamışlardır. ARPANET bu gelişmelerin en önemlilerinden biridir. Soğuk Savaş dönemindeki ilk reaksiyon ARPANET aracılığıyla gerçekleşmiştir. ARPANET sayesinde SSCB'den gelecek saldırı ve tehditlerin kontrol edilmesi amaçlanmıştır (Lukasik, 2011: 7).

1960 yılların ortalarına gelindiğinde Soğuk Savaş'ın zirve döneminde ABD Savunma Bakanlığı nükleer silah saldırı ihtilallerine karşı zorlu bir mücadele içerisindeydi. Çünkü ABD'ye karşı nükleer bir saldırı gerçekleşirse ordunun nasıl yönetileceği belirsizdi. Bu noktada o yıllarda yürürlükte olan iletişim merkezleri, telefon santralleri, radyo ve TV yayın istasyonları saldırı ihtimaline karşı savunmasızdı. Pentagon'un telefon hatlarına olan ilgisi yoğundu. 1960 ve 1970'li yıllarda teknolojinin ilerlemesiyle beraber tüm bilgisayar ağlarının ana merkezi internet ortaya çıkmıştır. Özellikle Clinton yönetimi telefon ve TV şirketlerini kontrol etmek için girişimlerde bulunmuştur. 1980'lerin ortasında Ulusal Birim Vakfı (SINAM) kurulmuştur. ABD'nin omurgası internet olarak kabul edilmiştir. Yüksek hızla ve uzun mesafeleri kapsayan veri hatları inşa edilmiştir (Elmer-Dewitt, 1993: 62-64). Siber alan Soğuk Savaş döneminde doğmuştur. ABD ve SSCB arasındaki rekabetin uzaya taşınması ve teknolojik gelişmelerle birlikte siber alan başka bir boyuta evrilecektir.

2.3.1.2. Soğuk Savaş Dönemi Sonrası ve Siber Alan

Soğuk Savaş sonrası dönemi ele aldığımızda özellikle 9/11 saldırılarından sonra uluslararası arenada belirsizlik hâkim olmuştur. Ulusal güvenlik algısı değişmiş olup devletler artık ulusal güvenliğin sadece fiziki ya da askeri unsurlar aracılığıyla sağlanamadığını fark etmiştir. Bu yeni algı sayesinde ulusal güvenlik kavramının alanına siber saldırılar, terör, salgın hastalıklar ve ekonomik müdahaleler de dâhil edilmiştir. Buna ilaveten devletlerin önemli verilerinin korunması konusu önem kazanmış olup her devlet için önemli olan enerji, ulaşım, sağlık gibi kritik alt yapıların güvenliği siber suç ve tehditlere karşı ön plana çıkarılmıştır (Göçöglü ve Aydın, 2019: 234).

Helen Nissenbaum (2005)'a göre 1990'lı yılların başından itibaren siber güvenlik kavramı, bilgisayar bilimcileri tarafından ağa bağlı bilgisayarlarla ilgili birçok problemin kaynağına dikkat çekmek için kullanılmıştır. Ancak yeni teknolojik gelişmeler ve değişebilen jeopolitik konumların kombinasyonu sonucu siber güvenlik, ağ güvenliği ve bireysel güvenliğin ötesine geçmiştir. Dijital tehditler artık salt bilgisayar güvenliğini geride bırakmıştır. 1990'lı yıllarda ortaya çıkan bu tehditler Amerikalı politikacılar, özel şirketler ve medya tarafından özellikle "Elektronik Pearl Harbor" ve "Kitlesele Yıkım Silahları"nın gündeme taşınmıştır. Batı dünyası alarına geçmiştir (Bendrath 2003: 50–53; Nissenbaum, 2005: 67). Robert Latham (2003: 1)'a göre, 9/11 saldırıları;

bilgisayarlara, bilgi teknolojisine ve güvenliğine özellikle dijital altyapının korunmasına, terörist eylemlerin durdurulmasına, devletler arasında ve devletlere karşı iletişimde internetin önemini arttırmıştır.

1990 sonrasında internetin yaygın kullanımı devlet, toplum ve bireyleri birbirlerine bağımlı kılmıştır. 1991 Körfez Savaşı'nın internet ve medya üzerinden takip edilmesi Soğuk Savaş sonrasında başlayan yeni dönemin habercisidir. Körfez Savaşı bir çeşit iletişim savaşı olarak yorumlanabilir (Mattelart, 1994: 117). Mary Kaldor (1998: 3)'un "Yeni Savaş" kavramı Körfez Savaşı sonrası dönemde iletişim teknolojisinin genişlemesiyle birlikte değişen ve olduğundan daha farklı bir forma dönüşen geleneksel savaş kavramı karşımıza çıkmaktadır. İletişim araçlarının yaygınlaşması dünyanın küçülmesine sebep olmuştur. Önemli olan siber alan ve iletişim teknolojilerinin ayrı bir savaş birimi olarak değerlendirilmesidir.

Yeni tehditlerin muhatabı devlet, toplum, birey gibi çok taraflıdır. Dolayısıyla bu tehditler karşısında harekete geçen tek aktör devlet değildir. NATO gibi uluslararası örgütlerde yeni alanda etkili olmak istemektedir. SSCB'nin yıkılmasının ardından Doğu blokunun varlığı sonlanması NATO'yu hedef alan düşman algısı da yıkılmıştır. Dolayısıyla NATO'nun meşruiyeti sorgulanmaya açık hale gelmiştir. Bu sebeple 1990 yılında Londra Konferansı'nda yeni bir stratejinin varlığına ihtiyaç duyulmuştur. 1991 Roma Zirvesi'nde ise yeni stratejik konseptlerin geliştirilmesi kararlaştırılmıştır (Bayraktar, 2015: 37).

Soğuk Savaş sonrası dönemde ortaya çıkan yeni tehdit unsurlarının bir diğer sonucu da asimetrik güvenlik kavramıdır. (Paul, 1994). Soğuk Savaş sonrasında internetin sivil alana olan etkisi göz önüne alındığında siber uzay, asimetrik mücadeleyi tetikleyecektir. Saldırının herhangi bir ağa erişim sağlanması sonucunda gerçekleşmesi güvenlik kavramının derinden tartışılmasına sebep olacaktır.

ÜÇÜNCÜ BÖLÜM

3. SİBER ALANDA ABD VE ÇİN DIŞ POLİTİKALARI

3.1. ABD Dış Politikası ve Siber Alan

Uİ disiplini için küreselleşme kavramının gelişim süreci ile siber alan arasında bağlantı kurulabilir. Bu ilişki ülkelerin dış politika algılarında değişikliklere yol açmıştır. Dış politika süreçlerinde ulusal güvenlik tanımlamaları da değişmiştir. Küreselleşme sayesinde ülkelerin güç dağılımları yeniden şekillendirilmiş olup asimetrik güç ilişkileri ortaya çıkmıştır. Ulusal güvenlik gereksinimleri artık daha kapsamlı ve farklı biçimlerle ifade edilmiştir (Kay, 2004: 9). Süper güç olarak kabul gören devletlerin dış politikalarında siber alana olan yaklaşımları dikkat çekicidir. Siber güvenlik kavramının yorumlanması noktasında birçok analiz sistemi geliştirilmiş olup birçok farklı parametreye dikkat edilmiştir. BM Bilgi ve İletişim Teknolojileri Özel Ajansı Uluslararası Telekomünikasyon Birliği (International Telecommunication Union – ITU)’nin 2017 yılının Kasım ayında yayınladığı Küresel Siber Güvenlik Endeksi Raporu ele alınabilir. Bu raporun önceliği siber güveniktir. Aynı zamanda bu rapor 25 göstergeyi tek bir kıyaslama ölçütüne göre birleştirmesi açısından da önemlidir. Buna ilaveten Küresel Siber Güvenlik Endeksi (2017)’ne göre özellikle beş sütun önemlidir. Bunlar; kanuna uygun hareket edilmesi, teknik, örgütsellik, kapasitenin geliştirilmesi ve iş birliğidir.

Tablo 6: Küresel Siber Güvenlik Endeksi 2014 ve 2017 Verileri

Ülke	İndeks (2014)	Küresel Sıralama	Ülke	İndeks (2017)	Küresel Sıralama
ABD	0.824	1	Singapur	0.92	1
Kanada	0.794	2	ABD	0.91	2
Avustralya	0.765	3	Malezya	0.89	3
Malezya	0.765	3	Umman	0.87	4
Umman	0.765	3	Estonya	0.84	5
Yeni Zelanda	0.735	4	Marityus	0.82	6
Norveç	0.735	4	Avustralya	0.82	7
Brezilya	0.706	5	Gürcistan	0.81	8
Estonya	0.706	5	Fransa	0.81	8
Almanya	0.706	5	Kanada	0.81	9
Hindistan	0.706	5	Rusya Federasyonu	0.78	10
Japonya	0.706	5			
Kore Cumhuriyeti	0.706	5			
Birleşik Krallık	0.706	5			

Kaynak: GCI, 2017.

Tablo 6’da görüldüğü gibi ITU’nun ikinci kez yayınladığı Küresel Siber Güvenlik Endeksi devletlerin siber saldırılar karşısında savunma kabiliyetlerini baz almaktadır. Bu rapor sayesinde siber saldırılar karşısında alınan önlemler ve devletlerin savunma güçleri analiz edilmiştir. Bu raporda dikkat çekici husus bu alana hakim olmanın zorluğudur. 2014 yılında ABD’nin öncü rolü 2017 yılında Singapur’a devredilmiştir. Klasik anlamda başat güç kavramını ele alırsak bu alanda var olmak çok daha önemlidir.

Siber güvenlik konusunda bir diğer çalışma ise Richard Alan Clarke ve Knake Robert (2010)’ın süper güç olarak kabul edilen devletlerin siber tehditlere karşı dayanıklılığı ölçmek için geliştirdikleri puanlama yöntemidir. Bu yöntem, tüm ülke bağlantısını bir anda kesebilmek, internet ağının yayılımı, siber bağımlılık, sunucuların gücü gibi kriterleri baz almaktadır. Clarke ve Robert (2010)’ın hazırlamış olduğu rapor aşağıdaki tabloda sunulmuştur.

Tablo 7: Clarke ve Robert’a Göre Ülkelerin Siber Güvenlik Puanlamaları

Unsurlar	ABD	RUSYA	ÇİN
Siber Saldırı	8	7	5
Siber Bağımlılık	2	5	4
Siber Savunma	1	4	6
Toplam	11	16	15

Kaynak: Richard ve Clarke, 2010.

Yukarıdaki tablodaki puanlama ABD, Rusya ve Çin’in siber güvenlik kavramını nasıl ele aldıklarını göstermektedir. Özellikle siber saldırı, savunma ve bağımlılık gibi unsurlarının ele alınması aslında bu ülkelerin siber güvenlik ve güç ilişkisini ortaya koymaktadır. Tabloya göre toplam puanlama baz alınırsa Rusya ön plandadır. Ancak siber saldırı ve savunma karşısında yüksek puanlamalar karşısında Rusya siber bağımlılık noktasında en yüksek puanı almıştır. Bu durum bize siber güvenlik ve güç ilişkisini değerlendirirken ele alınan her kavramın güce etki etme noktasında doğrusal bir etkiye sahip olmadığını gösterecektir.

Devletlerin dış politika algısında siber güvenlik kavramını ele aldığı bir başka kanıt ise Uluslararası Telekomünikasyon Birliği tarafından hazırlanan rapordur (ITU, 2015, 2017, 2018). Bu rapor ülkelerin siber güvenlik durumlarını değerlendirirken aşağıda yer alan kriterler baz alınmaktadır:

- Ülkede yürürlüğe konulan siber suç mevzuatı,
- Ülkede bulunan Bilgisayar Acil Müdahale Ekibi (Computer Emergency Response Team/CERT),
- Siber Olaylar Müdahale Ekibi (Computer Incident Response Team/CIRT)
- Bilgisayar Güvenliği Müdahale Ekibi (Computer Security Incident Response Team/CSIRT),

- Belirlenen ulusal siber güvenlik stratejileri ve ölçütlerinin mevcudiyeti,
- Siber güvenliğe dair farkındalık kampanyalarının mevcudiyeti,
- Siber güvenliğe dair mesleki eğitim,
- Siber güvenlik ile ilgili uluslararası forumlara katılım,
- Siber güvenlik ile ilgili kamu-özel sektör iş birliğidir.

Yukarıda yer alan kriterler baz alınarak hazırlanan anketler ülkelerin ilgili kurumlarına iletilmektedir. Verilerin doğrulanması için belge analizi, ülkelerin resmi internet sitelerinden alınan veriler gibi ikincil veri toplama yöntemleri tercih edilmektedir. Bu veriler sonucunda elde edilen bulgular aşağıda yer almaktadır.

Tablo 8: Uluslararası Telekomünikasyon Birliğine Göre Ülkelerin Siber Güvenlik Puanlamaları (ITU 2015, 2017, 2018)

Ülke	Skor 2015	Dünya Sıralaması 2015	Skor 2017	Dünya Sıralaması 2017	Skor 2018	Dünya Sıralaması 2018
ABD	0.824	1	0.925	2	0.926	2
Rusya	0.500	12	0.788	10	0.836	26
Çin	0.441	14	0.624	32	0.828	27

Kaynak: Uluslararası Telekomünikasyon Birliğine Göre Ülkelerin Siber Güvenlik Puanlamaları, ITU, 2015, 2017, 2018.

Tablo 7 ve 8 arasında farklar mevcuttur. Tablo 7 kantitatif verilerden ziyade dönem içerisindeki olayların yorumlarını baz alınarak oluşturulmuştur. Ancak Tablo 8 daha belirgin kriterler baz alınarak oluşturulmuştur. ITU tarafından yayımlanan Tablo 8’de alıntı yapılan raporun 2015, 2017 ve 2018 yıllarına ait ülkelerin siber güvenlik algılamalarını yansıtan versiyonları da mevcuttur.

Tablo 7 incelendiğinde ABD siber saldırı ve siber savunma kavramlarını baz alan Richard Alan Clarke ve Knake Robert (2010)’ın puanlamasında diğer iki ülkeden daha geridedir. Ancak ABD’nin Rusya ve Çin karşısında en geride kaldığı bu durum Tablo 8 ile kıyaslandığında geçerli değildir. 2015, 2017 ve 2018 yıllarını kapsayan ITU’ye göre ülkelerin Siber Güvenlik Puanlamaları baz alındığında ABD, Çin ve Rusya karşısında öndedir. Buna ilaveten Rusya ve Çin arasındaki puanlamalar birbirine yakındır. Ancak önemli bir sonuç olarak ABD dışında, Rusya ve Çin’in önünde ismi geçmeyen birçok ülke vardır. Bu araştırmaya göre “süper güç” olarak ele alınan ABD, Rusya ve Çin’in siber güvenlik yaklaşımları aynı değildir. Buradaki farklılıkta değerlendirme karşısındaki ülkelerin uyum yetenekleri de etkilidir.

ABD dış politikası tek başına incelenmesi gereken kapsamlı bir alandır. Ancak bizim burada asıl belirtmek istediğimiz siber alanın ABD dış politikasındaki yeri ve önemidir. ABD dış

politikasında siber alan öncelikli olarak siber güvenlik kavramıyla yükselişe geçmiştir. ABD siber güvenlik politikasını anlamak için ise bu politikanın hangi bileşen ve aktörlerden meydana geldiği anlaşılmalıdır. ABD siber güvenlik kavramı ulusal güvenlik politikası, diğer strateji belgeleri, kanunlar, direktifler, öneriler düzenlemeler, siber güvenlik ile ilgili kurumlar (9/11 komisyonu da dahil olmak üzere) ve think - tank olarak adlandırdığımız üretim kuruluşları baz alınarak geliştirilmektedir (Tirrell, 2012: 7).

ABD için siber güvenlik ile ilgili ilk kapsamlı belge 2003 yılında yayınlanan Güvenli Siber Uzay Belgesi'dir (WH, 2003). Bu belgede siber güvenlik kavramına üç kez yer verilmiştir. Siber güvenlik kavramı yerine siber uzay kavramı tercih edilmiştir. Siber uzay kavramı ile de "kritik altyapıların işleyişini sağlayan ve birbirine bağlı yüzbinlerce bilgisayarın, sunucunun (server), modemlerin, anahtarların, fiber optik kabloların oluşturduğu alan" olarak ifade edilmiştir (WH, 2003: 7). Bu belgeden hareketle siber uzayın korunması gerekliliği ön plana çıkarılmış olup ulusal güvenliğin bütünlüğü için Ulusal Güvenliğin Sağlanmasına Yönelik Ulusal Strateji (National Strategy for Homeland Security) ile Kritik Altyapıların ve Değerli Varlıkların Fizikî Olarak Korunmasına Yönelik Ulusal Strateji (National Strategy for the Physical Protection of Critical Infrastructures and Key Assets) Belgeleri'nin uygulama bölümleri hazırlanmıştır.

Belge, siber güvenlik ile alakalı olan ulusal ve federal kurumların direktiflerini oluşturmaktadır. Bununla birlikte devlet ve yerel yönetim kurumları, özel sektör firmaları, sivil toplum kuruluşları ve vatandaşların kolektif siber güvenlik için iş birliği üzerinde durulmuştur.

Güvenli Siber Uzay Belgesi'nde ABD ulusal güvenliği için beş adet öncelik belirlenmiştir. Bu öncelikler:

Ulusal bir siber uzay güvenliği karşılık sistemi, ulusal bir siber uzay güvenliği tehdit ve güvenlik açığı savunma programı, ulusal bir siber uzay güvenliği farkındalık ve geliştirme programı, hükümetin siber uzayını güvenlik altında tutma, ulusal güvenlik ve uluslararası siber uzay güvenliği iş birliğidir. Güvenli Siber Uzay Belgesi'nin uygulama alanı olarak ise Siber Uzay Güvenliği Ulusal Strateji Belgesi yayımlanmıştır. Ulusal siber güvenliğin sağlanmasının ardından sekiz eylem planı hazırlanmıştır (WH, 2003: 10).

Bu eylem planları aşağıdaki tabloda gösterilmiştir:

Tablo 9: Siber Güvenlikte Sekiz Önemli Öncelik

Tehditlere Karşı Eylem	Tehditlere Karşı Önlem
Kamu-Özel İş Birliği	Gerekli Hukuki Düzenlemeler
Taktiksel ve Stratejik Analizler	Güvenlik Açıkları ve Sonuç Analizi
Sinoptik bir bakış açısı geliştirmek üzere özel sektör kapasite artırımı	İnternet Mekanizmalarının Güvenliği
Siber Uyarı ve Bilgilendirme Ağının Genişletilmesi	Güvenilir Dijital Kontrol ve Veri Güvenliği Sistemlerinin Yaygınlaştırılması
Ulusal Olaylar Yönetiminin Geliştirilmesi	Yazılım Açıklarının Önlenmesi
Ulusal Boyuttaki Kamu-Özel İş Birliğine Gönüllü Katılım	Siber Ağlar ve İletişim Sistemlerinin Fiziksel Güvenliği
Federal siber güvenlik planlarının yürütülmesi	Federal Siber Güvenlik Ar-Ge Kurumlarının Önceliği
Kamu-Özel Sektör Arasındaki Bilgi Akışı ve Paylaşımın Geliştirilmesi	Aciliyet Sistemlerinin Güvenliği

Kaynak: WH, 2003.

2003 yılının ardından ABD siber güvenlik politikası ile ilgili diğer belgeler 2011, 2013 ve 2015 yıllarında yayımlanmıştır. 2011 yılında yayınlanan Siber Güvenlik Strateji Belgesi beş öncelikten oluşmaktadır. Bu öncelikler “Savunma departmanının organizasyonel olarak geliştirilmesi, yeni savunma içeriklerinin edinilmesi, kamu- özel iş birliği, diğer ülkelerle bu konuda güçlü ilişkiler kurulması ve yaratıcılığın artırılmasıdır (DOD, 2011).”

Daha sonraki süreçte DOD, 2013 yılında, “Savunma Departmanının Ağları, Sistemleri ve Bilgiyi Savunma Stratejisi” (DOD Strategy for Defending Networks, Systems, and Data) belgesini yayınlamıştır. Belgede 2011 yılında yayınlanan belgedeki hedeflere ek olarak savunmada esneklik, asimetrik güvenlik tehditlerine karşı savunma ve bu amaca yönelik yeni savunma mekanizmalarının kurulması gibi yeni hedefler eklenmiştir (DOD, 2013).

Beyaz Saray Basın Ofisi, 2014 yılında ABD ile AB arasında siber güvenlik ile ilgili bir görüşme gerçekleştirmiştir. Özellikle iş birliğinin önemine dair yazılı açıklamalar yapılmıştır. Uluslararası siber uzayın gelişmeleri, çevrim içi olarak insan haklarının tanıtımı ve korunması, uluslararası hukukun uygulanması, siber güvenliğin geliştirilmesi ve üçüncü taraf ülkeleri kapsayacak biçimde siber güvenlik kapasitesindeki etkin gelişim üzerinde durulmuştur (WHOPS, 2014). Burada uluslararası hukukun başta yapay zeka olmak üzere gelişen askeri unsurlar ve diğer alanlar ile olan ilişkisi ele alındığında ne kadar düzenleyici bir yapıya sahip olduğu tartışılmalıdır. Çünkü bireylerden devletlere kadar uluslararası sistem içerisinde kendi arayışını takip eden yapay zekanın askerileşmesi gibi konularda uluslararası hukukun yaptırım gücü ve hangi düzenlemeleri yapabileceği sorusu önemlidir. Uluslararası özel hukuk açısından belirli bir ülkenin yargı yetkisine ihtiyaç duyulup duyulmayacağı ya da hangi mahkemelerin yetkili olacağı, yasaların hangi olayda devreye gireceği, gerekli görülen yaptırımların ne olacağı gibi sorulara cevaplar aranmalıdır (Güntay, 2020: 1). DOD’un son yayınladığı belge 2015 yılında yayımlanmıştır. Siber Strateji

Belgesi ile eylem planlarının somutlaştırılması üzerinde durulmuştur. Eylem planlarının somutlaştırılması için 3 temel yaklaşım vurgulanmaktadır. İlk olarak ABD'nin çıkarları baz alınarak DOD ağlarına ve bilgi sistemlerine karşı saldırıları; ikinci olarak Obama'nın Birleşmiş Milletler (BM) ile ortak olarak hareket ederek oluşturduğu savunma planını ve son olarak ise Siber Görev Güçleri'nin (Cyber Mission Force/CMF) kurulması ele alınmıştır. Siber Görev Güçleri sayesinde DOD kurumu adına sivil ve askeri personeller yeni stratejileri uygulayacaklardır (DOD, 2015).

ABD dış politikası ve siber alan ilişkisi son zamanlarda birlikte yükselmektedir. Özellikle ABD'nin yayınladığı belgeler baz alındığında oluşturulan siber altyapı kuruluşlarının milli olması ABD'ye öncü rolü tanımaktadır. Ancak burada dikkat edilmesi gereken bir nokta vardır. Siber altyapıların milli özelliği taşıması siber bağımlılığı belli bir noktada sabitlerken kritik altyapıların çoğunluğunun siber altyapılara bağlı olması ABD savunmasını zayıflatmaktadır. Richard Alan Clarke ve Knake Robert (2010)'ın ABD için siber güvenlik güç puanlamasında görülmektedir.

3.1.1. ABD'nin Siber Savaş Yeteneği

ABD'nin siber savaş yeteneğini inceleyebilmek için öncelikle bu kavram ile kastedilenin anlaşılması gerekmektedir. Çünkü siber alanda yer alan araçlar ve kavramlar birbirleri ile karşılıklı bağımlıdır. Her alan için farklı hakimiyet teorileri vardır. Siber uzay alanının büyük oranda fiziksel alanın dışında olmasından yola çıkarsak bu alana hâkim olmak kolay olmayacaktır. Fiziksel olanın ötesindeki bu alan için fiziksel araçlar geçersizdir. Martin Libicki (2009)'nin "Siber Caydırıcılık ve Siber Savaş" adlı eserinde siber uzay dört bileşenden meydana gelmektedir. Siber uzayı oluşturan bu dört alanın her bir katmanına egemen olmak için gerekli olan araçlar vardır. İlk katman fiziksel kablolardan ve anahtarlardan oluşmaktadır. Dolayısıyla ilk katman tahrip edici fiziksel güçler tarafından domine edilebilir. İkinci katman bu sistemlerin kontrolünü elinde bulundurmaya baz almaktadır. Sistemlerin kontrol edilebilirliği hakimiyeti sağlayacaktır. Üçüncü katman ise veriler ile ilgilidir. Sansür aracılığıyla hakimiyet kurmak ya da bilgi erişimi kontrol altına alınmak istenmektedir. Son olarak ise dördüncü katmanı ele aldığımızda ise bilişsel ya da pragmatik hakimiyet ön plana çıkmaktadır (Schmidt, 2016). Bu dört katmanın kontrolü siber savaş yeteneğine katkı sağladığı için oldukça önemlidir.

Siber savaş yeteneğine yoğunlaşırken siber saldırı kavramına dikkat edilmelidir. Siber saldırı, sömürü ve casusluk kapasitelerini arttırmak isteyen devletler uluslararası arenaya "silahlanma yarışını" taşıyacaktır. Siber uzay kavramı NATO tarafından kara, deniz, hava ve uzay alanlarından sonra muharebenin beşinci boyutu olarak karşımıza çıkmaktadır. Siber savaş söz konusu olduğunda uluslararası arenada ABD, Çin, Rusya, İngiltere ve İsrail gibi birçok devlet ön plana çıkmaktadır.

Devletlerin kapasitelerini arttırmaya yönelik eylemlerinin sonuçları dikkate alınmalıdır. Çünkü devletler siber yeteneklerini arttırmak için takip ettikleri politikalar sonucunda siber saldırılara maruz kalma risklerini de arttırmışlardır. Bu sebepten ötürü ABD siber alanda davranışlarını kısıtlamak ihtiyacını hissetmiştir.

ABD'nin teknolojik alt yapısı güçlendikçe siber saldırılara karşı daha fazla savunmasız hale gelmiştir. Özellikle Rusya ve Çin gibi büyük rakipleri karşısında sivil ve askeri altyapısının büyük oranda siber alana entegre edildiği gerçeğini göz önüne alırsak ABD bu alanda hem savunma hem de saldırgan aktör rollerini üstlenecektir. Eski NSA çalışanı Edward Snowden ABD'nin "İstihbaratın Beş Gözü" olarak adlandırdıkları yapının kurulduğunu açıklamıştır. Devletler arasında siber istihbarat ve veri paylaşımında bulunmak için sisteme entegre olan ülkeler ABD, İngiltere, Kanada, Yeni Zelanda ve Avusturya'dır. Elde edilen bilgiler ekonomik, askeri ve istihbarat alanlarında stratejilere dönüştürülecektir (Marmon, 2011).

ABD, siber alanda hegemon olma arzusunu yansıtan en önemli aktörlerdendir ve bu alana hakim olmak için daha çok maliyet arttırıcı yöntemleri tercih etmektedir. Devletler siber alana etki edebilmek için hem saldırgan hem de savunma politikalarını geliştirilmelidir. Ancak ABD uluslararası arena için yeni mücadele alanı olarak adlandırdığımız siber alanda etkin olmak istersen bir yandan da sisteme fazla entegre olduğu için kendini savunmasız bir duruma düşürecektir.

Tablo 10: Siber Çatışmanın Aşamaları

Aşamalar	Gerçekleşme	Başlangıç	Askerileştirme
Zaman Aralığı	1980	1998-2003	2003-Günümüz
Dinamikler	Saldıranlar savunulara göre daha avantajlıdır.	Saldıranlar savunulara göre daha avantajlıdır.	Saldıranlar savunulara göre daha avantajlıdır.
Kapasiteye Sahip Aktör/ler	ABD ve birkaç diğer güç	ABD ve Rusya ile birçok küçük aktör	ABD, Rusya, ÇİN ve önemli yeteneklere sahip birçok aktör
Düşmanlar	Hackerlar	Hackivistler, Vatansever Korsanlar, Virüsler ve Solucanlar	Neo-Hackivistler, Casuslar, Kötü Amaçlı Yazılımlar, Ulusal Ordular, Casuslar ve Vekilleri, Hackivistler
Büyük Olaylar	Cuckoos Egg (1986) Morris Worm (1988) Dutch Hackers (1991) Rome Labs (1994) Citibank (1994)	Eligible Receiver, Solar Sunrise, Moonlight Maze, Allied Force, Chinese Patriot, Hackers	Titan Rain Estonya Gürcistan Buckshot Yankee Stuxnet
ABD Doktrini	Bilgi Savaşı	Bilgi İşlemleri	Siber Savaş

Kaynak: Haizler, 2017: 31-45.

Siber savaşın gelişim aşamaları değerlendirildiğinde ABD'nin siber savaş yeteneklerinin yorumlanması daha kolay olacaktır. Tablo 10'da görüldüğü gibi esasen siber çatışma söz konusu

olduğunda saldırganlar savunan taraf karşısında daha avantajlıdır. ABD'nin siber savaş kapasitesi ise bilgi savaşları ve bilgi işlemlerinin siber savaşa evrilmesidir. Düşmanlar hackerlar, vatansever korsanlar, virüsler, solucanlar, hacktivistler, neo-hacktivistler vb. çok taraflıdır. ABD'nin siber alana yönelik politikaları ele alındığında siber savaş kapasitesi ön plana çıkmaktadır. ABD, siber alana yön vermek isteyen aktörler arasında sıvrılmaktadır.

Siber savaş kavramına ilişkin birçok bilgi vardır. 2008'de Rusların Gürcistan'ı işgali esnasında hükümetin web sitelerine, medya kuruluşlarına ve diğer Tiflis yanlısı gruplarını hedef alması, Estonya Hükümetine ait halka açık web sitelerinin DDoS saldırıları aracılığıyla internet erişimlerinin engellenmesi, ABD-İsrail'in Stuxnet operasyonu, Çin'in ABD ağlarını ihlal etmesi esasen siber savaşa örnek olarak gösterilebilir (Gözükeleş, 2014). Estonya Başbakanı, Rus saldırılarını donanma ablukasına benzetmiştir. Siber silahlar dünyanın herhangi bir yerinden bir rakibin kritik altyapısına saldırıya imkan sağlamaktadır. Ayrıca bir siber silah kendi kendini yok etmeye programlanabileceği gibi diğer programlama teknikleri sayesinde programlayıcısına karşı kullanılmayacak şekilde de tasarlanabilir. Programlama koşullarının çeşitliliği savunmayı zorlaştıracaktır. Burada siber savaşı tanımlamak için dört başlık ele alınabilir. İlk olarak sabit bir coğrafya yoktur. Herhangi bir aktör Pakistan ve Suriye'nin hava savunmasını ortadan kaldırabilir. Cidde'deki bir bilgisayar korsanı Tel Aviv'deki İsrail borsasını çökertebilir. İran, ABD bankalarına yönelik siber saldırılarını devam ettirirken Çinli hackerlar ABD'nin silah tasarımlarını çalmayı başarmıştır. İkinci olarak siber alan sürekli büyüyen, doğası gereği yapay ve küresel olduğu için herkes tarafından paylaşılmaktadır. Dolayısıyla siber alanın sürdürülmesi ve korunması noktasında net bir otorite mevcut değildir. Devletler daha çok kendi ulusal ağlarının güvenliğine odaklanmaktadır. Üçüncü olarak, Thomas Rid (2013)'in belirttiği gibi siber alan doğası gereği gizli bir silahtır. Dördüncü olarak siber saldırılar, biyolojik silahlar gibidir. Virüsler, canlı bir yapı gibi hareket etmektedir. Tespit edilmemek ve etkili olmak için sürekli kendisini geliştirmelidir (Atzili ve Boaz, 2014: 43-47).

Mevcut ABD doktrini, siber savaş eylemini geleneksel bir askeri saldırı gibi ele almaktadır. Yüksek düzeyde fiziksel tahribat söz konusu olduğu için bu yaklaşım yanlış değildir. Bu noktada siber saldırılar bir sabotaj eylemi gibi ele alınabilir. Yukarıdaki tanımlamalar göz önüne alındığında ABD'nin yaklaşımının muğlak kaldığı görülmektedir.

3.1.2. Siber Alanda ABD ve NATO İş Birliği

Yeni hibrit tehdit kavramı ilk olarak Hizbullah'ın II. Lübnan Savaşı esnasında Lübnan'da bulunan İsrail Savunma Kuvvetleri (IDF) karşısında somut bir başarı elde etmesiyle kabul görmüştür. İlk hibrit tehdit kavramı devlet dışı bir aktörün askeri yetenekler sayesinde devlet aktörleriyle ilişkisini baz almaktadır. Zamanda hibrit tehditler farklı tanımlanacaktır. NATO 2010 Stratejik Komuta Konsepti'nde hibrit tehditler; hedeflerin gerçekleştirilmesi için aynı anda hem

konvansiyonel hem de konvansiyonel olmayan araçları kullanma kapasitesinin kullanılması sonucunda ortaya çıkan tehditler olarak tanımlamıştır. Hibrit tehdit kavramı Soğuk Savaş öncesinde ve sonrasında farklı ele alınacaktır. Soğuk Savaş döneminde Ukrayna'daki çatışmalar, Irak ve Suriye'de gerçekleştirilen terör eylemleri hibrit tehditlere örnektir. Soğuk Savaş sonrasında ise yeni teknolojik gelişmeler sayesinde hibrit tehditler siber uzayı ön plana taşıyacaktır. Siber çatışma ve siber savaşlar tartışılmaya başlanacaktır. Estonya'nın Talinn merkezini hedef alan 2. Rus askeri operasyonları püskürtme çabası, Gürcistan'a yönelik siber operasyonlar ve parti web sitelerine olan müdahalesinin amacı siber savaş tehdidini ortadan kaldırmaktır (Bachmann, 2015).

Soğuk Savaş sonrasında SSCB'nin yıkılması, küreselleşme süreci, teknolojik gelişmeler, dijital bilgi teknolojilerindeki gelişim, Çin ve Hindistan'ın yükselişi, ekonomik krizler, Arap Baharı, siyasi devrimler ve aşırı İslamcı bir çerçevede uluslararası arenaya hakim olmuştur. Bu gelişmeler tecrübe edilirken uluslararası konjonktür ABD önderliğini ön plana çıkarmıştır. Hatta Soğuk Savaş esnasında karşı karşıya gelen ABD ve Rusya bu yeni dönemde "Karşılıklı Bağımlılık" ilkesinden hareketle aralarındaki iş birliğini geliştirmek zorunda kalmıştır. NATO kilit rol oynayacaktır. NATO ve ABD arasındaki ilişkiler siyasi, diplomatik, askeri, ekonomik ve diğer birçok önemli boyutta birbirine bağımlı hale gelecektir (Van Epps, 2013).

ABD ve NATO arasındaki iş birliği siber alan sayesinde birbirine daha fazla entegre olmuştur. İnsanlığın her aşamasına nüfus eden teknolojik gelişmeler uluslararası toplumdaki her aktörü etkilemektedir. Burada NATO'nun bu yeni tehditler karşısındaki yaklaşımı ön plana çıkmaktadır. NATO'nun sahip olduğu ve işlettiği ağlardaki tüm şüpheli olaylar kaydedilmeye ve izlenmeye başlanmıştır. Buna ilaveten müttefik ülkelerdeki hükümet ve kritik altyapı ağlarına yapılan izinsiz girişler de analiz edilmeye başlanmıştır. Siber savunma, siber güvenlik ve siber caydırıcılık NATO için artık acil konudur. Bilim ve Teknoloji Komitesi (STC)'nin yılda iki kez gerçekleştirdiği toplantılar bizim için yol gösterici olacaktır. Siber tehditlere odaklanıldığında müttefik devletlerin toprak bütünlüğü, siyasi bağımsızlığı ve ulusal güvenliği tehdit eden saldırılar müttefik devletler içerisinde herhangi birine yöneltildiğinde bu saldırının diğer tüm devletlere yönelik olarak değerlendirildiği Washington Antlaşması'nın 5. Maddesi gündeme taşınmıştır. Ancak yapılan toplantılarda müttefik devletlerin karşı karşıya kaldığı tüm saldırı çeşitlerinin ele alınması mümkün değildir (Davis, 2019).

Klasik anlamda savaşın kara, deniz, hava ve uzay olmak üzere dört şekli vardır. Bu noktada bazı taraflara göre savaşın bu dört boyutunun yanı sıra beşinci boyut olarak nitelendirilen siber uzay diğer tüm savaş alanlarına müdahaleyi kolaylaştırmaktadır (Libicki, 2009: 12-13). Bu durum siber alanı ön plana çıkarırken aktörler için kendi güvenlik eksenlerini yeniden gündeme getirecektir. Teknolojinin ön görülemez ilerlemesi baz alındığında güvenliği tehdit eden unsurlarında başka şekillerde yorumlanması gerekmektedir. Klasik güvenlik tedbirleri etki gücünü

yitirmiştir. İnternetin hayatımıza girmesiyle birlikte ise bu değişim etki kapasitesini arttırarak ilerlemeye devam etmiştir.

Değişen güvenlik algıları farklı güvenlik tanımlarını ortaya koyacaktır. Bu noktada siber alan ile güvenliğin birleştiği siber güvenlik kavramı da karşımıza çıkmaktadır. Siber güvenlik tüm devletlerin ilgi odağı olacaktır. Uluslararası arenaya yansıyan siber tehditler ve saldırıların ön planda tutulduğunu baz alındığında ise devletler için iş birliği artık kaçınılmazdır.

Siber alanın varlığından, siber güvenlik algısından ve bu alandaki iş birliğinin gerekliliğinden yola çıktığımızda özellikle ABD için bu kavramların nasıl şekillendirildiğine de değinilmelidir. Küresel internetin ilkel hali olan ARPANET 1962 yılında tasarlanmıştır. Dolayısıyla artık siber uzay literatürde kendisine yer edinmiştir. Özellikle ARPANET sayesinde DDoS'un karşısında yer alabilecek kadar güçlü bir yapılanma hedeflenmiştir (Yılmaz ve Salcan, 2008: 35). 1980'li yıllara gelindiğinde bilgisayar kullanımında gözle görülür bir artış yaşanmıştır. Bu artış güvenliğin önemini de ortaya koyacaktır. ARPANET'e bağlı sunucu sayısındaki artış sistemdeki kullanıcı sayısının artmasına da sebep olmuştur. Sistemin daha hızlı ilerleyebilmesi için farklı yazılımlar üzerinde çalışılmaya başlanmış olup bu çalışmalar sonucunda 1980'li yıllarda ARPANET'in ticari versiyonu olan internet hayatımızdaki yerini almıştır. Artık 1988'lere gelindiğinde ise 60.000 bilgisayara internet hizmeti sunulmuştur. İnternet kullanımının yaygınlaşmasının ilk dönemlerinde siber saldırılar tecrübe edilmeye başlanmıştır. Kullanıcıların %10'unda Morris olarak adlandırılan bir solucan sayesinde sistemde aksaklıklar meydana gelmiştir (Pierce, 2018: 63-65). ARPANET'e yönelik tehditlerin artması üzerine ABD Savunma Bakanlığı bu ağların korunmasına yönelik politikalar geliştirmeye başlamıştır. 1990'lı yıllarda ABD Savunma Bakanlığı tarafınca ARPANET'in askeri faaliyetlerde kritik rol oynadığı kabul edilmiştir. Devletlerin güvenlik eksenlerinde artık ağ güvenliği kavramına yer verilmiştir. Bütün yazılımlar, donanım ve iletişim faaliyetlerini kapsayan bu noktada birbirleri ile bağlantılı ya da bağlantısız sistemlerin yansıması siber uzay uluslararası arenadaki yerini alacaktır. Ancak esasen siber uzayın taraflarca kabul edilen ortak bir tanımı yoktur. Bu kavram ile kastedilen birbirleriyle bağlantılı belli bir zaman dilimindeki bilgi sistemlerinin diğer sistemlerle kullanıcılar aracılığıyla aktif hale geldiğini kabul edebiliriz.

ABD'nin siber uzaya ilişkin düşüncelerinin gelişiminde NATO'nun önemli bir yeri vardır. 1999 yılı NATO'nun kuruluşunun 50.yılıdır. Washington Zirvesi'nde NATO, İttifak üyelerinin güvenliğinin askeri olan ya da olmayan birçok tehdit ile mücadele etmesinin önemi vurgulanmıştır (Pulat, 2002: 38). Bu noktada bilgi sistemlerinin gücü üzerinde durulmuştur. NATO için etkili bilgi sistemleri ittifak için savunmayı arttıracaktır (NATO, 1999a). Ayrıca zirvede "Yeni Stratejik Konsept" ilan edilmiştir. Bu konseptte göre teknolojinin ön görülemez ilerlemesi sonucunda diğer devletler ve devlet dışı aktörlerin özellikle silah üretim bilgilerine müdahale algısı dikkatleri çekerken NATO hibrit savaş kavramını da benimseyecektir.

İttifakın bilgi sistemlerinin güvenliğinin önemi üzerinde durulmuştur. 1999 Zirvesi'nin ardından devlet ve hükümet başkanlarının aracılığıyla Washington'da 21. yüzyılda İttifak adlı toplantı gerçekleştirilmiştir. Bilgi sistemlerindeki etkinliğin üzerinde yeniden durulmuş olup bilgi sistemlerindeki etkin olmanın ittifakın savunma kapasitesini arttıracığına da yer verilmiştir (NATO, 1999). 9/11 sonrasında NATO ittifakın güvenliğini tekrardan gündeminde revize etmiştir. Özellikle NATO'yu ya da müttefiklerini hedef alan Dijital 9/11 sendromu algısı oluşmuştur (Bıçakçı, 2014: 119).

İkinci olarak DDoS saldırısı NATO Halkla İlişkiler Departmanını hedef almasına rağmen bilgi sistemlerinin korunmasına ilişkin ilk resmi beyan 2002 Prag Zirvesi'nde gerçekleşmiştir. Bilhassa siber tehditler karşısında yer alan Yükselen Güvenlik Tehditleri Bölümü'nde siber güvenlik; terörizmi de içeren bel önemli tehdit bünyesinde sayılmıştır. Prag Yetenek Taahhütleri kısmında ise NATO'nun siber tehditler karşısında kendi kapasite arttırımını baz almıştır. Kısacası Prag Zirvesi NATO'nun kapasitesinin askeri ve sivil tüm araçlarıyla birlikte bilgi sistem alt yapısının güçlendirilmesi için NATO Ağ ile Etkinleştirilmiş Güç Programı (Network-Enabled Capability-NEC)'ni kurmuştur (NATO, 2003). Ayrıca NATO zararlı yazılımlar karşısında durabilmek için de NATO Muhabere ve Bilgi Sistemleri Ajansının bir birimi olan Bilgisayar NATO Bilgisayar Olaylarına Müdahale Yeteneği (NATO Computer Incident Response Capability-NCIRC) birimi de oluşturulmuştur. Bu birim sayesinde NATO'nun bilgi işlem ağları siber saldırılar karşısında 7/24 izlenmektedir (NATO, 2011).

Yeni güvenlik tehdit unsurlarından biri olan siber saldırılar karşısında NATO ön plana çıkan Microsoft, Google ve IBM, Uluslararası Standartlar Birliği (International Standards Organization - ISO) ve Internet Mühendisliği Görev Kuvveti (Internet Engineering Task Force/IETF) gibi aktörler ile iş birliğini vurgulamıştır (Huges, 2009: 4). 2004 yılına gelindiğinde ise NATO İletişim ve Enformasyon Sistemleri Servisi Ajansı (NATO Communication and Information Systems Services Agency/NCSA)'ni kurmuştur. NCSA sayesinde kritik alt yapılar için alınan önlem olarak herhangi bir siber saldırı da ilk müdahale gerçekleştirilebilecektir. NCSA bünyesindeki ön plana çıkan merkezlerden biri ise NATO Bilgi Güvenliği Teknik Merkezidir (NATO Information Assurance Technical Centre/NIATC)'dir. NIATC sayesinde bilgi güvenliği ve ittifak arasındaki koordinasyon sağlanacaktır (NATO, 2019).

NATO'nun siber alana yönelik bakış açısını şekillendiren en önemli olay 01 Ağustos - 01 Eylül 2008 tarihlerinde meydana gelen Estonya'nın bilişim sistemlerini hedef alan saldırılardır. Bu noktada NATO iki önemli karar almıştır. İlk olarak bu tarz bir saldırının bir daha meydana gelmemesi için Brüksel'de Siber Savunma Yönetimi Otoritesi (Cyber Defence Management Authority/CDMA)'ni kurmuştur. Böylece siber alanda ortak savunma stratejileri geliştirilecektir. İkinci olarak ise Estonya/Tallinn'de bir NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (Cooperative Cyber Defence Centre of Excellence/NATO CCD COE) kurulmuştur (NATO, 2019).

NATO Müşterek Siber Savunma Merkezi sayesinde siber alanda ittifak kurmak, doktrin ve kavramların üretilmesini ön plana çıkarmıştır (NATO CCDCOE, 2019). CCDCOE ile 3 önemli gelişme uluslararası arenada karşımıza çıkmaktadır. İlk olarak hukuki bir yaklaşımın ön plana çıkarılmasıdır. 2009 ve 2012 yılları arasında siber alandaki gelişmeler ışığında siber dünya ve savaş hukukunun nasıl entegre edileceğini inceleyen Tallinn El Kılavuzu'dur. İkinci olarak NATO üyeleri aracılığıyla kurulan Siber İhtilaf Konferansları (Conference on Cyber Conflict/CyCon)'dır. Son olarak ise NATO bünyesinde gerçekleştirilen tatbikatlardır. CCD COE sayesinde üye ülkelerinin hepsini kapsayacak bir şekilde bilişim uzmanları, askeri personel ve karar vericilerin bir araya gelmesidir. Bu tatbikatlar sayesinde üye devletlerin ulusal bilgi teknolojisi (BT) sistemlerinin güvenliği ön plana çıkarılmıştır (NATO CCD COE, 2019).

2012 yılında Chicago Zirvesi'nde tekrardan güvenlik tehditleri, siber saldırılar, terörizm gibi konuların yanı sıra karmaşık boyutu artan siber tehditler noktasında etkili iş birliği vurgulanmıştır (Chicago Summit Declaration, 2012). 2014 Galler Zirvesi'nde yeniden siber saldırıların ön görülemez kapasitesi tekrardan gündeme getirilmiştir. 2016 Varşova Paktı'nda siber uzay; kara, deniz, hava ve uzay boyutlarından sonra NATO'nun 5. Savaş Konsepti olarak kabul edilmiştir. 2018 Brüksel Zirvesi'nde Mons/Belçika'da siber güvenlik baz alınarak NATO müttefikleri arasında daha güçlü ilişkilerin geliştirilmesi için Siber Operasyonlar Merkezi'nin kurulması kararlaştırılmıştır. 3 - 4 Aralık 2019 tarihlerinde ise Londra Zirvesi gerçekleştirilmiştir. Diğer zirvelerde olduğu gibi siber saldırılara engel olmak temel hedeftir (NATO, 2019).

Siber alanda NATO etkili bir aktördür. Özellikle ABD'nin bu konuya olan ilgisini baz alınırsa NATO öncülüğünde resmi adımlar atılmaktadır. İlerleyen yıllarda alınan kararların değerlendirilmesinde Zirveler, doktrinler, devlet politikaların yanı sıra NATO bünyesinde alınan kararların da gözden geçirilmesi gerekmektedir.

3.1.3. ABD Kurumlarının Siber Alanda İncelenmesi

Politikacılar için siber güvenlik kavramı artık diğer kavramların ötesindedir. 2020 yılından günümüze kadar Covid-19 nasıl uluslararası arenadaki tüm aktörleri etkilediyse siber alan da buna benzer bir etkileme kapasitesine sahiptir. Rusya - Ukrayna arasındaki çatışma bize yol göstericidir. Bu çatışmanın maliyeti 2022 yılında 155,83 milyar dolar olmasına karşın bu rakamın 2029 yılında 376,32 milyar doları aşması beklenmektedir. Bu süre içerisinde yıllık bileşik büyüme oranının %13,4 olmasından hareketle ilerleyen yıllarda siber güvenlik alanında %15-16 oranında bir artış yaşanabilir. Bu noktada siber güvenlik stratejilerine genel yatırım artmaktadır. Bu yatırımlar AB ve ABD'deki hükümetler tarafından desteklenmektedir. ABD Dışişleri Bakanlığı Siber Diplomasi Bürosu (The Bureau of Cyberspace and Digital Policy/CDP)'nin kurulması siber alana artan ilginin göstergesi olacaktır (Kjaersgaard, 2022). Siber tehditler sadece devletler nezdinde değerlendirilmemelidir. Harvard İç Güvenlik Uzmanı Juliette Kayyem siber savaş kavramına sıcak

bakmamaktadır. Çünkü devlet odaklı bir bakış açısı hükümeti tek çözüm yolu olarak gösterebilir. Askeri kapasitenin yanı sıra ABD sivil, federal, eyalet ve yerel yönetimlerin de bu alana dahil olduğu göz ardı edilmemelidir. Sistemin korunması noktasında saldırıların engellenmesi ve savunma için var olan kapasite maksimum seviyede kullanılmalıdır (Neal, 2021).

SSCB'nin çökmesinin ardından uluslararası arenada öncü rolünü üstlenen ABD'nin siber alanda en fazla faaliyet gösteren ülke olması siber tehditler karşısında yürütmeye çalıştığı politikalar ön plana çıkaracaktır. Burada 2 temel nokta vardır. Birincisi ABD, yeni tehditleri belirlemede baskın aktördür. İkincisi de ABD, Bilgi Teknolojileri (IT)'nde baskın rolünü üstlendiği için diğer devletlere bu alanda sorunların belirlenmesi ve çözümlenmesinde kaynak olacaktır (Dunn Cavelti, 2007). Dolayısıyla Uİ disiplini içerisinde önemli aktörlerden olan ABD bazı taraflarca hegemon güç olarak adlandırılmaktadır ve bu devlet uluslararası arenaya yön veren politikalarda etkili olabilmektedir. Ancak özellikle bu kısımda ABD Kurumlarının siber alandaki varlığından söz edilecektir. İlk olarak Ulusal Güvenlik Teşkilatı (NSA), Federal Araştırma Bürosu (FBI), Siber Komutanlık (USCYBERCOM) ve son olarak da İç Güvenlik Bakanlığı (DHS) üzerinde durulacaktır.

ABD'nin siber alana olan yaklaşımını anlayabilmek için ABD siber güvenlik stratejileri üzerinde durulmalıdır. ABD güvenlik stratejilerinin oluşması 1930'dan sonradır. ENIGMA olarak adlandırılan Alman donanmasının isimlendirilmesinden yola çıkılarak SIGIBA üretilmiştir. Hedeflenen amaç II. Dünya Savaşı esnasında gizli yazışmalarının çözümlenmesi olup savaş esnasında karşı devletlerin gizli bilgilerinin ele geçirilmesi olmuştur. Ek olarak 1958 yıllarından sonra kurulan ARPA, ABD kurumlarının siber alandaki konumunun anlaşılmasında oldukça önemlidir. Özellikle SSCB ile sürdürülmek istenen rekabetin siber alanın alt yapısını oluşturun boyutlarda da karşımıza çıkmaktadır. İlerleyen süreçlerde İleri Araştırma Projesi ARPANET adını alacaktır. Elbette bu süreç daha sonrasında İngiliz ve Fransız ağlarının bir araya gelmesiyle birlikte ilk kez uluslararası bir boyuta dönüşecektir.

İlerleyen dönemde ARPANET artık TELENET olarak anılacaktır. Bu teknolojik ilerleme devletler açısından hem avantajları hem de dezavantajları beraberinde getirecektir. Bir örnek verecek olursak virüslere karşı ABD Savunma Bakanlığınca Militarynet (MILNET) kurulmuştur (Darıcılı, 2017: 3-5). Ayrıca siber tehditlerin başlangıç noktasından konuya yaklaşıldığında ilk siber saldırı olayından bahsetmek gerekir. 1982'de Rusya, Kanada'nın doğal gaz boru hatlarının yazılımını ele geçirmek istemiştir. ABD bu duruma yazılım içerisine Truva Atı virüsünü eklemesiyle birlikte bu girişime müdahale edilmiştir. Boru hatlarındaki akışın seviyesinde meydana gelen değişim sonucunda patlama gerçekleşmiştir. Bu durum siber saldırıların sonuçlarının göz ardı edilemeyeceğini göstermiştir (Sertçelik, 2015: 31). ABD ve Rusya o zamanki bilinen adı ile SSCB arasındaki rekabet sürdürülmeye devam etmiştir. Özellikle ABD dış politikası 9/11 olaylarından sonra ise başka bir boyuta evrilecektir. Soğuk Savaş'ın sonlanmasıyla beraber uluslararası arenada

yeni güvenlik tehditler ortaya çıkmıştır. Siber güvenlik bu yeni tehdit unsurlarından olacaktır. Siber politikaların şekillenmesinde başkan direktifleri, stratejik politikalar ve resmî belgeler öncü bir rol oynayacaktır. Siber güvenlik ile ilgili ilk resmî belge bir başkanlık direktifi olarak 1995 yılında ilan edilmiştir.

Daha sonra 1997 yılında ise ilk resmi belgede bilhassa kritik altyapıların önemine vurgu yapılmıştır. Burada kritik alt yapılardan kastedilen iletişim, ulaşım, kamu sağlığı, enformasyon, acil müdahale alt yapısı, bankacılık ve finans kuruluşları olarak nitelendirilmiştir (Darıcı, 2017: 6).

Başkan direktifleri, resmî açıklamalar, doktrinler ve yayınlanan resmî belgelerin yanı sıra siber alandaki güvenlik politikalarına yön verirken kurumsallaşma çabaları da oldukça önemlidir. Örnek verecek olursak 1998 yılında Ulusal Altyapı Koruma Merkezi (NIPC) kurulmuştur. Ulusal Altyapı Koruma Merkezi'nin amacı ABD'ye yönelik olan siber tehdit ve riskli durumların engellenmesidir. NIPC, başta FBI'ya bağlı bir birimdir. Daha sonra 2002 yılına gelindiğinde NIPC FBI'nı bünyesinden bağımsız olarak DHS'ye bağlanmıştır (Demirel, 2012: 91-92).

ABD'nin siber güvenlik politikalarını şekillendirirken etkili olan kurumlar FBI ve DHS ve Savunma Bakanlığı ele alınabilir. Siber tehditler karşısında yer alan bu resmi yapılanma ABD siber güvenlik politikalarının temelini oluşturmaktadır (Darıcı, 2017: 7). Bu noktada ABD Savunma Bakanlığının askeri boyutu ön plana çıkardığı unutulmamalıdır. Ayrıca bu kurumlar içerisinde yer alan 1952 yılında kurulan NSA'da siber alanda oldukça etkilidir. NSA bilhassa şifrelerin kırılması, çözümlenmesi, veri analizi ve istihbarat alanlarında yetkilidir (Darıcı, 2017: 8). ABD siber politikalarını oluşturan kurumların bir diğeri ise DHS'dir. DHS, özellikle terörle mücadelede tam yetkilidir. 2002 yılında yayınlanan Kamu Güvenliği Yasası ile DHS kritik altyapıları koruma ve bu kaynakların direncinin artırılmasında, siber güvenliği sağlayarak ABD'nin bu hedefleri koordinasyon yeteneğini sürdürmesinde de yetkilendirilmiştir (Baş, 33).

ABD güvenlik politikalarının temel yapı taşlarını oluşturan bu kurumlar sadece siber alandaki ABD'nin bakış açısını yansıttığı için önemli değildir. Aynı zamanda bu kurumların varlığı sayesinde ABD'nin Rusya ve Çin'in karşısındaki konumu da netleşecektir. Zira devletler arasındaki bu yeni rekabet alanı hem birbirlerini elimine edebilecekleri hem de uluslararası arenada etkili olabilecekleri etkili bir araçtır.

3.1.3.1. Ulusal Güvenlik Teşkilatı (NSA)

NSA, ABD istihbarat hizmetleri için oldukça önemli bir kurumdur. Bu kurumun ana uzmanlık dalı Kriptoloji bilimidir. Özellikle SSCB ve ABD arasındaki rekabeti yansıtan Soğuk Savaş döneminde NSA'nın yürütmüş olduğu faaliyetler oldukça önemlidir. Ana hedef ABD'yi

diğer devletler arasında öncü yapmaktır. NSA, aynı zaman ABD'nin korumak istediğı öncü devlet olma anlayışını siber alanda da yansıtan kurumdur.

NSA'nın temelleri 20 Mayıs 1949 tarihinde atılmıştır. NSA'nın ilk faaliyet gösterdiği isim AFSA (Silahlı Kuvvetler Güvenlik Servisi)'dir. AFSA temel olarak ABD Genelkurmay bünyesine bağlı bir kurum olarak yapılandırılmış olup ABD Savunma Bakanlığı içerisinde faaliyet göstermiştir. Elbette AFSA için temel hedef yalnızca askeri faaliyetler değildir. Militarizasyonun yanı sıra elektronik bağlantıların önemi üzerinde durulmuştur. Elektronik ortama bağlı iletişim araçlarına da yoğunlaşmıştır. Bir nevi iletişim istihbaratı faaliyetlerini gerçekleştiren AFSA Dışişleri Bakanlığı, CIA ve FBI gibi kurumlarla gerekli bağlantıları istenilen düzeyde sağlayamamıştır (Burns,1990). 1951 yılına gelindiğinde ABD Başkanı, Harry S. Truman AFSA'nın istenilen düzeyde başarıyı sağlayamadığını beyan ederek aksaklıkların giderilmesi talebinde bulunmuştur. Brownell Raporu AFSA'nın eleştirildiğı resmi belgedir. Bu raporun ardından AFSA, NSA'ya dönüştürülmüştür.

NSA, II. Dünya Savaşı'ndan sonra ABD'nin diğer ülkelerin iletişim kapasitelerini analiz eden çok ciddi bir yapılanmadır. İletişim ve bilgi teknolojilerinde yaşanan gelişmeler sonucu NSA'nın görev tanımlaması değişmiştir. NSA'nın ilgi alanı kriptografik uzmanlık, sinyal istihbaratı, güvenlik açığı analizi, savunma sistemlerine yönelik tehditlerin ortadan kaldırılması ve siber güvenlik misyonu gibi birçok alana genişlemiştir. ABD'nin en hassas bilgilerini korurken artık dikkat edilmesi gereken birçok parametre vardır. Özellikle ağ güvenliği ön plana çıkmaktadır. Bu durum yeni sorumluluklar ve operasyonel yetkileri de beraberinde getirecektir. Ulusal Güvenlik Sistemleri (National Security Systems/NSS), ABD Savunma Bakanlığı (The Department of Defense/DOD) ve Savunma Sanayi Üssü (The Defense Industrial Basa/DIB) bahsetmek gerekir. NSS; ABD askeri ve istihbarat faaliyetleri için kritik öneme sahip ağırları baz almaktadır. Bu sayede ABD'nin askeri kapasitesi operasyonel olarak aktif hale getirirken hem ABD'ye ait en hassas bilgilerin güvenliğini sağlamaktadır. DOD; ABD askeri hizmetleri ve muharip komutanlıkların yanı sıra ABD devlet kurumları ve ulusal güvenlikle ilgili departmanlar arasındaki ilişkiyi sağlamaktadır. DIB; ABD Savunma Bakanlığı'nın ulusu korumak için kritik altyapı sistemlerini, platformlarını ve teknolojilerini tasarlayan, geliştiren, işleten ve bakımıyla ilgilenen şirketlerini kapsamaktadır. Eğer bu ağlar herhangi bir tehdit altındaysa ABD'de de risk altındadır (NSA, 2022). NSA'nın etkili olmak istediğı alanlarda ABD ulusal güvenliği ön planda tutulmaktadır. Siber uzayda etkin olma çabasının altında ulusal güvenlik vardır. Güvenlik kavramı daha çok siyasi süreçlerle ilgilidir. Önemli olan siber güvenliğin farklı tehdit temsillerine olan etkisidir. Odak noktası yalnızca ön plandaki aktörlerin söylemsel uygulamaları değil, aynı zamanda hükümetin içinde ve dışında yer alan arka plandaki aktörlerin de nasıl etkilendiğidir (Dunn Cavelty, 2013).

NSA, ABD küresel algısı, şifreleme, verinin elde edilmesi, elde edilen verinin analiz edilmesi, karşı istihbarat faaliyetleri, sinyal izleme yöntemleri gibi birçok farklı alana yönelmiştir.

Dolayısıyla NSA, ABD iletişim ve enformasyon düzeninde yetkili birimdir. Bilhassa ABD Silahlı Birlikleri ve FBI gibi diğer istihbarat birimleri için kriptoloji alanında da iş birliğine açıktır (NSA, 2018). Siber güvenlik ekseninde şüphesiz en önemli kavram siber saldırılardır. Özellikle de etki kapasitesi henüz belirlenmemiş bu alanda siber tehditleri tespit edip savunma aşamasında ekarte etmek hayati önem taşımaktadır. NSA, siber saldırıları önceden tespit edebilmek için istihbarat faaliyetlerinde ön plana çıkmaktadır. ABD siber güvenlik politikaları noktasında tek etkili kurum NSA değildir. ABD Savunma Bakanlığı'nın ortaya koyduğu siber güvenlik stratejileri de dikkate alınmalıdır. Ortaya koyulan siber güvenlik stratejilerinin en önemlisi 2010 yılında USCYBERCOM olacaktır. USCYBERCOM sayesinde ABD'nin sahip olduğu siber kapasitesinin sınırları, bu kapasite ile geliştirilebilecek politikaları ve karşılaşılabilecek olan riskler için planlamalar somut olarak ele alınmıştır (Darıcı, 2017: 88-90). USCYBERCOM birimi aracılığıyla ABD siber alanda kurumsallaşmasının temellerini atmıştır (Tirrell, 2012).

ABD için siber alan da güvenliğin sağlanması ön plandadır. Güç kavramının artık yeniden yorumlanması gerekmektedir. Kritik altyapıların giderek dijitalleşmesi her aktörü riske atmaktadır. Bu noktada siber saldırılar sayesinde uluslararası arenadaki güce etki etmek isteyen aktörlerden de toplumlara kadar herkes siber saldırılara karşı savunmasızdır. Rusya gibi ülkeler diğer ülkelerin vatandaşlarına hizmet sunma ve nüfusları etki altına almak için bu alanda etkin olmaya çalışmaktadır. Siber direncin iyileştirilmesi ve saldırılara hızlıca yanıt verilebilmesi çok önemlidir. Yıkıcı siber saldırılar karşısında kolluk kuvvetleri arasındaki iş birliğinin genişletilmesi gereklidir. ABD, siber tehditleri azaltmada ve siber uzayda istikrarı arttırmak için normlar oluşturmaya çalışarak etkinliğini korumaya çalışmaktadır. ABD'nin amacı devlet ve devlet dışı aktörlerden kaynaklanan siber saldırıları caydırmaktır. Toplumu etkileyen ulusal işlevleri ve kritik altyapıyı bozan veya bozmaya çalışan tüm tehditlere karşı ulusal gücün tüm kapasitesi kullanılmalıdır. Son olarak ABD, siber güvenliği sağlamak için uluslararası hukukun çevrimdışı olduğu bu ortamda BM Genel Kurulu tarafından onaylanan siber uzayda sorumlu devlet davranışı çerçevesinde hareket etmeye devam edecektir. Günümüz dünyasında teknolojik gelişmeler aracılığıyla jeopolitik rekabet farklı bir boyuta ulaşmıştır. ABD ve müttefiklerinin teknoloji alanındaki liderliği ekonomik refahın ve askeri gücün temelini oluşturmaktadır. İlerleyen dönemlerde kritik altyapılar ve teknolojinin gelişmesi sayesinde ekonomi modellerinin yeniden tasarlanmasına, orduların dönüştürülmesine ve dünyanın yeniden şekillenmesinde etkili olacaktır (NSS, 2022).

3.1.3.2. Federal Araştırma Bürosu (FBI)

2006 yılında ABD Savunma Bakanlığı Müşterek Kurmay Başkanlığı, büyük ölçüde etkinleştirilmiş ve operasyonel olarak entegre olmayı yansıtan siber uzay operasyonları için ulusal askeri stratejisini geliştirmiştir. Bu stratejiye göre siber uzay “ağ bağlantılı bilgi sistemleri ve fiziksel altyapılar aracılığıyla bilgi depolanması, değiştirilmesi için elektronik ve elektromanyetik spektrum sayesinde karakterize edilen bir alan” olarak tanımlanmıştır (The National Military

Strategy for Cyberspace Operations, 2006). Artık çatışma ve savaş konseptlerinin değiştiği gözlemlenmektedir. 2012 yılında David Sanger, ABD ve İsrail ile İran'ın Natanz'daki nükleer reaktör sistemine virüs bulaştığını bildirmiştir. Stuxnet sayesinde İran'ın kritik altyapısına zarar vermek, İranlı bilim adamları ve mühendisleri zora sokmuştur. İran'ın nükleer kapasitesine başarılı bir şekilde müdahale edilmiştir. Michael Hayden'e göre bu durum fiziksel yıkımı etkilemek için siber saldırının kullanıldığı ilk saldırdır. Savaş konseptine yaşanan bu dönüşüm 1945'te Hiroşima'ya atılan atom bombası etkisine benzetilebilir (Finkelstein ve Govern, 2015).

Siber alanda meydana gelen değişimlerden başlıca etkilenen aktörler arasında devletler gelmektedir. Bu noktada dünya siyasetini etkileyen devletlerin amacı etkin güç konumunu elde etmektir. ABD ekonomik, siyasal, askeri ve diğer birçok alanda etkili olmak istemektedir. Ayrıca ABD için sadece etkili bir güç olmak yeterli değildir. Aynı zamanda bu gücünü sürdürebilmek temel hedeftir. İşte bu noktada küresel dünyaya egemen olmak için hava, kara, deniz ve uzay alanlarından sonra devletler arasındaki rekabet kendisini siber alana taşımıştır. Ön görülemez teknolojik gelişmeler sayesinde siber uzayda yaşanan gelişmeler devletlerin kapasitelerini ve casusluk faaliyetlerini geliştirmek istedikleri bir alana dönüşmüştür. ABD, uluslararası arenada etkili olabilmek için tüm kapasitesini siber alanda caydırıcı bir güç olmak için kullanacaktır. Özellikle internetin hayatımıza girmesiyle birlikte devlet dışı ve ticari alanlar da dahil olmak üzere ABD için siber uzay kendi ekonomisi ve politikalarını yansıtabileceği bir alan olmuştur. 1990'lı yılların başından itibaren ABD siber uzay kavramına siber güvenlik ekseninden hareket ederek yaklaşmıştır. ABD için Rusya ve Çin karşısında bir güç olabilmek oldukça önemlidir. Hem uluslararası arenaya etki edebilmek hem de diğer rakiplerini eleyebilmek için ABD farklı yöntemleri tercih etmiştir.

Bu yöntemler başkanlık direktifleri, stratejik belgeler ve siber güvenlik ile ilgili kurumlardır. FBI, CIA, DHS, CYBERCOM ve NSA gibi örgütlenmeler sayesinde ABD'nin siber kapasitesi etkin bir şekilde kurumsallaştırılmak istenmiştir.

FBI, ABD'nin resmi siber faaliyetlerini yürüten temel birimlerden biridir. Aslında ABD siber kurumları ABD Savunma Bakanlığı, DHS ve ABD gizli istihbarat birimlerinden oluşmaktadır. ABD gizli istihbarat servisleri ise FBI ve CIA olarak nitelendirilebilir. Esasen bu birimler arasındaki koordinasyonu anlamak çok kolay değildir. Dağınık bir yapılanma olmasına karşın her birim kendi içerisinde oldukça faaldır.

FBI, ilk olarak 1908'de BOI (Bureau of Investigation) ismiyle kurulmuştur. Daha sonra 1935 yılında BOI ismi FBI olarak kabul edilmiştir. Ana merkez Washington DC'dir. FBI, ABD Adalet Bakanlığı bünyesinde çalışmalarına devam etmektedir. Bu birimin temel hedefi ulusal güvenliğin en üst noktaya taşınmasıdır. Özellikle ABD toplumunun güvenliği ön plana çıkarılmaktadır. Burada FBI ve CIA arasında bir fark vardır. Merkezi İstihbarat Teşkilatı (CIA) ABD'nin diğer

güçlere karşı güvenlik tehditlerini ön plana çıkarırken FBI daha çok iç/toplumsal güvenliğe yoğunlaşmıştır. FBI, ABD iç istihbarat ve espionaj faaliyetlerini ele almaktadır.

ABD teknolojisinin siber alanda etkin bir şekilde kullanılması için profesyonel istihbarat çalışmalarını gerçekleştirmektedir. FBI, siber güvenlik stratejisinin faal olarak işleyebilmesi için kilit bir birimdir. Siber risk, tehdit, suçlar ve terörist ataklarının engellenmesi için bazı birimler oluşturulmuştur. Siber Ulusal Güvenlik Bölümü (Cyber National Security Section/CNSS) ve Siber Suç Bölümü (Cyber Criminal Section/CCS) sayesinde profesyonel bir çalışma sistemi benimsenmiştir. Bu noktada bilhassa CNSS terörist kaynaklı siber tehditlere yoğunlaşırken CCS genel olarak nitelendirilen siber suçlar ile ilgilenmektedir. (Tirrell, 2012). CNSS ve CCS birimlerine ek olarak Ulusal Siber Araştırma Birleşik Görev Gücü (National Cyber Investigative Joint Task Force /NCIJTF) sayesinde ise ABD diğer hükümete bağlı resmî kurumlar arasındaki koordinasyon sağlanmaktadır. NCIJTF'nin yönetimi CNSS'e bağlıdır. Çünkü CNSS başkanı eş zamanlı olarak NCIJTF'nin de başkanıdır ve FBI direktör yardımcısının emirlerine uymak zorundadır (FBI, 2017).

3.1.3.3. Siber Komutanlık (USCYBERCOM)

Daha öncesinde ABD siber güvenlik politikalarını oluştururken birçok aktörün etkili olduğundan bahsetmiştik. Başkanlık direktifleri, ulusal stratejik belgeleri ve siber güvenlikle mücadele eden kurumlar ön plana çıkarılmıştır. ABD Adalet ve Savunma Bakanlıkları önemli sorumluluklar üstlenmiştir. ABD Adalet Bakanlığı'na bağlı olan FBI siber suçlar, güvenlik tehditleri, terörist aktivasyonlar gibi ABD iç güvenliğini bozacak riskleri ortadan kaldırmayı amaçlamaktadır.

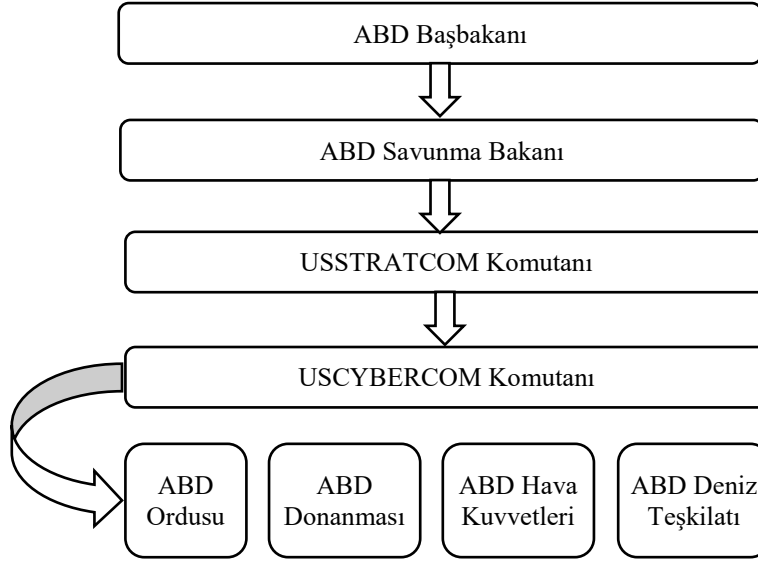
FBI sayesinde ABD'nin siber alanda meydana gelebilecek tüm tehdit ve risklere karşı korunması ön plana çıkarılmıştır (FBI, 2017a). Özellikle FBI Siber Suçlar Merkezi sayesinde amaçlanan hedefleri gerçekleştirmektedir. 2008 yılında kurulan NCIJTF, ABD Emniyet Teşkilatı, İstihbarat Kurumları ve Savunma Bakanlığı gibi kurumlar ile 20'den fazla ortak kuruluşta iş birliğini sağlamıştır (FBI, 2017b).

ABD Adalet Bakanlığı'nın yanı sıra Savunma Bakanlığı'nın da siber güvenlik politikalarına etkisi göz ardı edilemez. Bu noktada Savunma Bakanlığı'na bağlı olarak geliştirilen ABD Stratejik Komutanlığı ve Siber Komutanlığı dikkatleri çekmektedir. Bu iki birim eş güdümlü olarak yetkilendirilmiştir. Özellikle 2012 yılında Savunma Bakanlığı Siber Operasyonlar Planına göre oluşturulan komutanlıklar içerisinde Müşterek Siber Merkezleri'ne de yer verilmiştir. Bu sayede siber tehditler karşısında daha etkili faaliyetler yürütülebilecektir (Tirell, 2012: 56) Buna ilaveten Savunma Bakanlığı bünyesinde USCYBERCOM kurulmuştur. ABD, USCYBERCOM sayesinde siber tehditler karşısında etkin bir sistemin kurulması amaçlanmıştır (DOD, 2017).

Aynı zamanda ABD Savaş Bakanlığı, siber güvenlik ekseninde siber savaş kavramını da ön plana çıkaracaktır. Çünkü ABD, siber savaş kavramı üzerinden hareket ettiğinde önemli düzenlemeleri gerçekleştirmiştir. Bu düzenlemeler özellikle operasyonel faaliyetleri aktifleştirmiştir. Bu konuda atılan en kritik adım 1 Haziran 1992 yılında ABD Stratejik Komutanlık (USSTRATCOM) biriminin oluşturulmasıdır. ABD USSTRATCOM aracılığıyla stratejik üstünlük, karşı tarafa galip gelmek, entegre füze sistemleri, kontrol, iletişim, gözlem ve analize dayalı faaliyetler ön plana çıkarılmıştır. 2009 yılına gelindiğinde ise USSTRATCOM birimine bağlı olarak USCYBERCOM'un kurulmasıyla birlikte siber alanda profesyonelleşmenin adımları atılmıştır. ABD siber güvenlik kapasitesinin geliştirilmesine önem verilmiştir. Hedeflenen amaçlar sadece ABD'nin siber alanda korunmasını içermemektedir. Aynı zamanda siber saldırılar karşısında caydırıcı bir güç olmak, tehditleri ortadan kaldırmak için etkin bir şekilde siber uzay ile ilgili operasyonları gerçekleştirmektir. Proaktif bir yaklaşım tarzı benimsenmiştir. Proaktif yaklaşımının en güzel örneği 2012 yılında 6,200 askeri ve sivil personelden oluşan Siber Koruma, Savaş Görev ve Ulusal Görev Ekiplerinden meydana gelen 133 Siber Görev Gücü (CMF)'nin aktifleştirilmesidir (USCYBERCOM, 2009).

23 Temmuz 2009 yılında Pentagon'un, USSTRATCOM altında ABD Siber Komutanlığı'nı kurmasındaki amaç siber alanda faaliyet gösteren departmanın farklı organizasyon ve unsurlarını bir araya getirmektir. Ancak USCYBERCOM sayesinde tüm ulusu kapsayan kapsamlı bir strateji oluşturulamamıştır. USCYBERCOM; organizasyon, komuta ve kontrol, bilgisayar ağı operasyonları (CNO), senkronizasyon ve kaynak sağlama gibi 5 alt başlık altında incelenebilir. 1990'lı yıllarda DOD'un askeri stratejisinin devamı büyük oranda siber uzaya bağımlı hale gelmeye başlamıştır. Fakat bu süreçte siber güvenlik konularına yeteri kadar önem verilememiştir. 1998 yılında yayınlanan bir başkanlık komisyonu sayesinde siber uzaya dikkat çekilmeye çalışılmıştır. 2003 yılına gelindiğinde Başkan Bush Ulusal Güvenli Siber Uzay Stratejisi (NSSC)'ni yayınlamıştır. Ulusal güvenliğin 5 ana hat üzerinde belirlendiği bu belge de güvenlik İç Güvenlik Bakanlığı (DHS)'ye yüklenmiştir. Bu süreç DOD'un 2006 yılında Ulusal Askeri Stratejisi'ni yayınlamasıyla devam etmiştir. USSTRATCOM, Müşterek Kurmay Başkanlığı'yla birlikte siber uzay operasyonlarının uygulanması noktasında görevlendirilmiştir. Özellikle 2007 ve 2009 yılları arasında Estonya, Gürcistan ve Kuzey Kore'ye ait siber saldırı olaylarına dikkat çekilmiştir. Buna ilaveten 2008'de Stratejik ve Uluslararası Çalışmalar Merkezi (CSIS) Siber Alanı Güvenceye Alma Raporu'nu yayımlanmıştır. Aynı yıl ABD Hava Kuvvetleri, ABD askeri ağlarını savunma görevini tek bir hizmet veya teşkilattan ziyade ABD Stratejik Komutanlığı'na ait olduğunu beyan etmiştir. 2009 yılında Savunma Bakanı Gates, USCYBERCOM'u kurulması emrini vermiştir. Kısacası USCYBERCOM; kendisini kuran düzen USSTRATCOM'un güçlendirilmesiyle ortaya çıkmıştır. USSTRATCOM askeri siber uzay yetki ve sorumluluklarını birleşik bir komuta merkezi USCYBERCOM'a devretmiştir (Jackson, 2011: 10-13).

Şekil 13: Siber Güvenlikle İlgili Emir Komuta İlişkisi



Kaynak: Pajurek ve Monika 2017: 163.

Şekil 13'e göre, ABD Başkanı siber güvenlikle ilgili bir emir verilmesinde yetkilidir. ABD Başkanı'nın emrinden sonra ABD Savunma Bakanı emri USSTRATCOM Komutanı'na iletecektir. USSTRATCOM, USCYBERCOM'un bünyesinde yer aldığı için süreci USCYBERCOM ele aldıktan sonra ilgili askeri birime yönlendirecektir.

USCYBERCOM gibi yapılanmalar siber uzayda güvenliği sağlama noktasında oldukça önemlidir. Çünkü 1990 yıllardan 2015-2016 yılına kadarki süreç bizlere siber uzaydaki tehdit riskinin nasıl arttığını gösterecektir. İlk başlarda risk boyutu DDoS ve web sitelerine gerçekleştirilen saldırıları baz alan küçük ölçekli eylemler ile 2015-2016 yılına gelindiğinde ABD ve birçok Avrupa ülkesinde seçimleri ve Ukrayna örneğinde olduğu gibi ülkenin elektrik altyapısını hedef alan büyük ölçekli saldırılara dönüşmüştür (Deppa, 2017: 12).

3.1.3.4. İç Güvenlik Bakanlığı (DHS)

Uİ disiplinin de Soğuk Savaş sonrasında belirsizlik hakimdir. Özellikle asimetrik güç dengesi ve değişen tehdit unsurları göz önüne alındığında karar alıcı mekanizmalar için politika uygulamaları çetin bir hal almıştır. Bilhassa 9/11 saldırılarından sonrasında bu belirsizlik ortamı ulusal güvenlik kavramının önemini bir kez daha göstermiştir.

Ulusal güvenliğin sağlanabilmesi artık sadece fiziki ve militarizm unsurlarına bağlı değildir. Dolayısıyla ulusal güvenliği tehdit eden yeni tehdit unsurları söz konusudur. Bu tehditlere siber saldırılar, terör, salgın hastalıklar ve dahası örnek verilebilir. Ayrıca bu yeni tehdit unsurlarının yani sıra devletlerin sahip oldukları enformasyon kapasitelerinin korunması da ulusal güvenlik

konularına dahil edilmiştir. Çünkü devletler için hayati önem taşıyan enerji, ulaşım, sağlık gibi kritik alt yapıların siber saldırı ve tehditler karşısında korunması gerekmektedir (Göçoğlu ve Aydın, 2019: 234). Çalışmamızın bu bölümünde daha çok siber kavramıyla ilgili ortaya çıkan kavramlara yoğunlaşan yeni kurumlar üzerinde durulacaktır. Çünkü siber uzay, siber tehdit, siber güç ve siber güvenlik kavramları ABD'nin yeni ulusal güvenlik anlayışında ön plana çıkmaktadır.

Değişen ulusal güvenlik anlayışı sayesinde ABD'nin siber güvenlik konusundaki kurumsallaşma süreci başlamıştır. Siber güvenlik politikalarının temeli başkanlık direktifleri, stratejik belge ve belgeler aracılığıyla atılmıştır. Siber güvenliği kapsayan ilk resmi belge olan başkanlık direktifi 1995 yılında yayımlanmıştır. 1997 yılında yayımlanan resmî belgede ise kritik alt yapıların tanımı üzerinde durulmuştur. Bu belgelerin ardından yayımlanan diğer stratejik belgelerde de iletişim, ulaşım sektörleri, kamu sağlığı, enformasyon, bankacılık ve finans, enerji ABD kritik alt yapıları olarak karşımıza çıkmaktadır (Darıcı, 2017: 6).

Stratejik belgeler sayesinde ulusal güvenlik kavramı yeniden şekillendirilmeye çalışılırken bu süreç aynı zamanda ABD'nin siber alandaki kurumsallaşmasının temellerini atmıştır. 1998 yılında siber tehditlere karşı koyabilmek ve kritik alt yapıların korunmasında etkin olabilmek için NIPC oluşturulmuştur. NIPC, FBI'ya bağlı bir birimdir. NIPC sayesinde ABD siber tehditler karşısında gerekli önlemlerin alınmasının önemi belirtilmiştir. 9/11 saldırılarından sonra ise siber güvenliğin ulusal güvenlik kapsamında değerlendirilmesinin gerekliliği kabul edilmiş olup asimetric durumların saldırı ve tehdit kapasiteleri artık ön plandadır. Bilhassa bu asimetric tehditlerin varlığı sayesinde 2002 yılında NIPC, FBI'dan ayrılarak DHS'ye dönüştürülmüştür (Demirel, 2012: 91-92). FBI, DHS ve ABD Savunma Bakanlığı, ABD'nin siber güvenlik politikalarının önemli bir kısmını oluşturmaktadır.

ABD siber alana yönelik politikalarında DHS ön plandadır. 26 Temmuz 2016'da ABD Başkanı Obama, ABD Siber Olay Koordinasyonu Başkanlık Politikası Direktifi (PPD) 41'i imzalamıştır. PPD-41, ABD'nin herhangi bir siber olaya müdahale ilkeleri belirlenmiştir. Bu sayede ABD'nin siber saldırılarla mücadelesinde birçok federal kurum kritik rol oynarken siber saldırılar karşısında 3 farklı müdahale alanı belirlenmiştir. İlki siber olaylardan etkilenen kurum ve kuruluşlara teknik yardımın sağlanmasıdır. Ulusal Siber Güvenlik ve İletişim Entegrasyon Merkezi (NCCIC) aracılığıyla DHS ön plana çıkmaktadır. İkinci olarak tehdit kapasitesi ile mücadeledir. Burada FBI ve NCIJTF sayesinde Adalet Bakanlığı (DOJ) siber saldırılara müdahale edebilmektedir. Son olarak istihbarat desteği ele alınmıştır. Bu noktada siber tehditler karşısında durum tespiti oldukça önemlidir. Siber Tehdit İstihbarat Entegrasyon Merkezi (CTIIC) aracılığıyla Ulusal İstihbarat Direktörü Ofisi (ODNI), önemli siber olaylara yönelik istihbarat desteğini sağlayan lider federal kurum olacaktır. DHS'nin İstihbarat ve Analiz Ofisi'nin de siber olaylarla müdahalesinde istihbarat faaliyetlerine destek olmaktadır. Buna ek olarak PPD-41'e göre, 5 temel prensip belirlenmiştir. Bu prensipler; ortak sorumluluk, risk bazlı müdahale, siber saldırıdan

etkilenen varlığa saygı gösterme, hükümet çabalarının birliği, saldırı öncesi sistemin geri yüklenmesi ve kurtarılmasıdır (DHS, 2016).

DHS kurulduğu günden itibaren ana vatanı, ABD değerlerini ve yaşam tarzını korumayı hedeflemektedir. Bu noktada küresel tehditler karşısında DHS'nin temel misyonu esasen aynı kalmıştır. Ancak günümüzde büyük güç rekabetinin değişmesi sonucu Çin, ABD karşısında önemli bir tehdit potansiyeli oluşturmaktadır. Bu tehdit durumuna 2017 yılında ABD Ulusal Güvenlik Stratejisi (NSS)'nde ve 2020 yılında Çin Stratejik Yaklaşımı'nda ve daha geniş ABD Hükümeti (USG)'nde dikkat çekilmiştir. Artık Çin'e karşı sürekli devam eden bir rekabet vardır. Amerikan halkı USG'nin Çin'e karşı rekabetinde DHS'nin aldığı rolü desteklemektedir. DHS'nin Çin Stratejik Eylem Planı (SAP)'nı ele alacak olursak ABD'nin Çin'e yönelik dört ana hedefi vardır. Bu hedefler; ABD halkını, vatanını ve Amerikan yaşam tarzını korumak, ABD refahını arttırmak, güç yoluyla barışı sağlamak ve ABD çıkarlarını muhafaza edip ilerletmektir (DHS Stratejik Eylem Planı, 2020).

3.2. Çin Dış Politikası ve Siber Alan

Soğuk Savaş döneminin son ermesi Uİ disiplininde farklı tehdit türlerini gündeme taşımıştır. Gri alan dediğimiz alan artık yerini daha fazla belirsiz ve güvenli olmayan bir döneme bırakmıştır. Özellikle bu dönemin ardından ABD, diğer aktörlere nazaran daha fazla ön planda kalmıştır. ABD, 16 Mayıs 2011'de Siber Uzay Stratejisi'ni yayınlamıştır. Bu strateji ABD'nin siber alanda hangi rolü üstlenmesi gerektiğini ve siber uzayda sorumlu devlet normlarının geliştirilmesini baz almıştır. ABD'de karşısında Çin ise siber alanda soğukkanlılığını koruma eğilimi içerisindedir. Çin için siber alan el üstünde tutulması gereken bir alandır. Siber silahlar kullanılmamalı ve özellikle siviller hedef alınmamalıdır. Çin Ulusal Bilgisayar Ağı Acil Müdahale Teknik Ekip Koordinasyon Merkezi (CNCERT veya CNCERT/CC)'nin yayınladığı yıllık rapora göre Çin, kamu ağlarının ve kritik altyapısının güvenliği ciddi şekilde tehdit altındadır. Çin, 2012 yılından beri çoğunlukla ABD, Japonya ve Güney Kore ve yurtdışından başlatılan siber saldırıların ülkeyi hedef aldığını belirtmiştir. Bu saldırıların yanı sıra Çin BM Bilgi ve Siber Uzay Güvenliği 66. Genel Kurul 1. Komitesi'nde Büyükelçi Wang Qun'un söylemleri ve Hukuk Sekreteri Huang Huikang'ın Budapeşte Siber Uzay Konferansı'nda siber alan ve güvenlik ile ilgili uygulanabilir yasal kuralların geliştirilmesinde aktif katkıda bulunmaya gönüllü olduğu açıkça belirtmiştir ve Çin siber alana yönelik bazı ilkeler yayınlamıştır. Bu ilkeler; siber uzayda hak ve özgürlüklere tam saygı, denge, siber uzayın barışçıl kullanımı ve adil kalkınma ilkesidir (Zhang, 2012: 806-807).

Uİ disiplini içerisinde Çin bazı taraflara göre saldırgan olarak anılırken bazı taraflara göre ABD ve Batılı Devletler karşısında kendi çıkarlarını korumak için gücü abartılan bir devlettir. Ancak bu noktada bilhassa siber savaş kavramı ön plandadır. Çünkü Çin için siber alan uluslararası arenada yükselmek için etkili bir araçtır. Bu yükselme temelde üç ana unsura bağlıdır. Bu unsurlar

kritik altyapıya sızma yoluyla caydırıcılık, askeri bilgi edinmek için teknolojik casusluk ve ekonomik avantaj elde etmek için endüstriyel casusluktur. Dolayısıyla Çin'in siber alana olan ilgisi artarak devam devam edecektir (Hjortdal, 2011: 3).

Çin siber alanda siber güvenlik kavramını iki şekilde ele almaktadır. Birincisi, bilgi teknolojisinin uluslararası güvenliğe etkisidir. İkincisi ise Çin yükselen bir güç olarak gösterdiği siyasi ve ekonomik gelişimidir. İlk başlıkla bilgisayar suçları, sinyal istihbarat, elektronik savaş gibi birçok parametre vardır. İkinci başlık ise ABD ve Çin arasındaki rekabeti etkilemektedir. Siyasi istihbarat, askeri ve kurumsal tehditler baz alındığında Çin'in sebep olduğu tehditler abartılmaktadır. Aynı zamanda Çin'e yönelik tehditler aynı oranda ele alınmamaktadır. Çin ve ABD arasındaki gerginliğin giderek arttığını kabul etmek gerekir. Çin potansiyel olarak ABD karşısında yükselen bir güç konumundadır. Siber güvenliğin siyasi boyuta etki ettiği kısmında Çin ve ABD arasında derin bir ekonomik karşılıklık bağımlılığın yanı sıra güvensizlik üzerine yükselen rekabet yerini korumaktadır. ABD ve Çin arasında sınırlı bir savaşın gerçekleşmesi olası değildir. Fakat Japonya ve Tayvan'ın dahil olduğu bir kriz ortamında ön görülemeyen sonuçlar gerçekleşebilir (Lindsay, 2014: 40).

Çin'in siber alana verdiği önem kurumsallaşma süreçlerinde de karşımıza çıkmaktadır. Bu noktada kurumlar, aktörler, kanunlar ve yönetmelikler önemlidir. Çin 1992 yılında bilgi ekonomisinin gelişimi üzerinde durmuştur. 1990'lı yılların ortalarında Microsoft'tan Bill Gates ile ÇKP Genel Sekreteri ve Çin Devlet Başkanı Jiang Zemin arasında görüşmeler başlamıştır (Austin, 2014). 2000'de Çin'in bir bilgi toplumuna dönüştürülmesine karar verilmiştir. Çin yürütmenin en üst organı olan Devlet Konseyi 2006 yılında 15 yıllık Ulusal Bilişim Geliştirme Stratejisi yayınlamıştır. Xi Jinping, Çin yeni lideri olarak siber güvenlik güvenliği enformatikleşme ile eşit statüde bir politika geliştirmek için ele almıştır. 2014 yılında Xi Jinping Çin bürokrasisi, akademisi ve ordusundan ileri gelenleri bir araya getiren Siber Güvenlik ve Bilişim Merkezi Komisyonu (CCCCI)'nu kurmuştur. CCCI'nın yürütme ofisi Çin Siber Uzay İdaresi (CAC)'dır. 2016 yılında CAC Ulusal Siber Güvenlik Stratejisi (NCSS)'ni yayınlamıştır. NCSS sayesinde iç ve dış tehditler ele alınarak siber güvenlik sosyal-teknik boyutlarıyla ele alınmıştır (Austin, 2018). 2021 yılına gelindiğine Xi Jinping Komünist Parti Yönetim Kurulu (Politbüro)'nda Çin'in dijital ekonomi konusunda uluslararası iş birliğinde etkin olması gerektiğinin üzerinde durmuştur. 2021-22 ise Çin Veri Güvenliği Kanunu (DSL), Kişisel Bilgilerin Korunması Kanunu (PIPL) ve siber uzaydaki ticarete ilişkin çeşitli yönetmelikleri kabul etmiştir. Buna ilaveten 2021 yılının son haftasında CCCI, 14. Beş Yıllık Ulusal Enformasyon Planı (FYPNI) başta olmak üzere siber uzaya ilişkin düzenlemeler ilan etmiştir. FYPNI'ya göre 2025 yılına kadar tüm yerel departmanlarda bilişim çalışmaları için stratejik rehberlik kabul edilmiştir. Altyapı inşa aşamasında veri üretken olarak kullanılacak ve devlet hizmetleri dijitalleşmeye devam edecektir (John, 2022: 13-14). Çin'in siber uzay yönetim bakış açısı önceden belirlenmiş bir vizyona göre şekillenmemiştir. Gelişim aşamasına bağlı olarak uzun, dağınık ve kendisini yineleyen bir evrimleşme süreci karşımıza çıkmaktadır.

Çin, siber alanda uluslararası arenada sadece Batı'nın olmadığını bize gösterecektir. Batı için stabil ilişkilerin varlığından söz etmek mümkün değilken Doğu Batı'ya nazaran daha istikrarlıdır. Özellikle Çin, Asya-Pasifik bölgesinde Batı bloğu ve diğer devletlere kıyasla daha istikrarlıdır. Örneğin Dünya Bankası verilerine göre, Soğuk Savaşın sonra ermesinden 2015 yılına kadarki süreçte dünya ekonomisi 2 kat, ABD ekonomisi 1,8 kat büyürken Çin'in büyüme oranı neredeyse 10 kattır. Yine aynı dönemde AB üye devletlerinin büyüme oranı ise 1,5 kattır. Kuzey ABD'nin 1,8 büyüme oranı ise Asya-Pasifik bölgelerindeki devletlerin 2,6 büyüme oranı karşısında geride kalacaktır. Kısacası verilerden de anlaşılacağı gibi Çin, Asya-Pasifik bölgesinde 10 kat büyüme oranına sahip olarak ön plana çıkmıştır (World Bank, 2019). Bu noktada siber alanın gelişme kapasitesinin teknolojik gelişmelerin varlığına bağımlı olduğu gerçeğinden hareket edersek bu alanda ABD karşısında Asya-Pasifik bölgesinin dinamosu Çin olacaktır. Siber alanda Çin, ABD karşısında hem etkin hem de güçlü bir karşıt güçtür. Dünya Ticaret Örgütü (DTÖ)'ne Çin 2001 yılında üye olduğunda çok etkin bir aktör değildir. Ancak 15 yıl içerisinde GSMH'sını sekiz kat arttırıp, kendisini 21'inci yy küresel bir güç olarak uluslararası arena da yerini almıştır.

Çin'in ekonomik gücü artık altıncı sıradan ikinci sıraya yükselerek ABD'nin altında yerini almıştır. 2014 yılına gelindiğinde Dünya Bankası verilerine göre Çin'in küresel GSMH'nin %16,6'sını karşılamaktadır. Her geçen gün dünya ekonomisi Çin için kendisini gösterdiği bir alandır (Le Corre ve Pollack, 2016: 1; The European Parliament Report, 2017).

3.2.1. Çin'in Siber Savaş Yeteneği

Uİ disiplini için küresel aktör olmak için artık kara, deniz ve hava kuvvetleri yeterli değildir. Askeri, siyasi ve ekonomik bütün gelişmeler artık teknolojik gelişmelere bağımlı bir hale gelmiştir. Özellikle yükselen siber alan artık ABD, Rusya, Çin gibi aktörlerin küresel güç olmasındaki yeni rekabet alanıdır. Esasen bu alan içerisinde Hindistan, Japonya, Kuzey Kore, Güney Kore, İran ve Türkiye'nin de ilgisi büyüktür. Buradaki temel çelişki minör bir aktörün majör aktörün etki kapasitesine sahip olabilmesidir. Dolayısıyla bütün aktörler için siber alan artık vazgeçilmezdir.

Siber alanda Çin kapasitesini anlayabilmek için özellikle ABD ile arasındaki rekabet incelenmelidir. Ancak bu analizi gerçekleştirmek kolay değildir. Çünkü ABD ve Çin arasındaki rekabet taraflar açısından farklı yorumlanmaktadır. Çin, ABD'nin kendisine yönelttiği bilhassa askeri boyutta gerçekleşen suçlamalar ve çoğunlukla ticari bilgisayar sistemlerine yönelik saldırılarının gerekçeden yoksun olduğunu iddia etmektedir. Dolayısıyla Çin, ABD'nin bu alanda kendisine yönelttiği suçlamaları temelsiz olarak nitelendirmektedir. Çinli kaynaklara göre bu saldırılar anonimdir. Çünkü ABD saldırısının gerçekleştirildiği IP adreslerine sızma kapasitesine sahiptir (Swaine, 2013: 15).

ABD ve Çin arasındaki rekabet ülkelerin askeri kapasitelerinin yeniden gözden geçirilmesine neden olacaktır. ABD Savunma Bakanlığı (DOD) ve Çin Halk Kurtuluş Ordusu (PLA) siber alanı yeni çatışma alanı olarak değerlendirmektedir. Bu noktada Çin için özellikle bilgi teknolojisi oldukça önemlidir. Ulusal düzeyde bilgi teknolojiye eğilim 1986 yılında Devlet Ekonomik Bilgi Yönetimi Öncü Küçük Grubu (CLSGISI)'nın kurulmasıyla başlamıştır. Bu sürecin gelişimi 1999 yılına kadar devam etmiş olup 2001 yılında Devlet Bilişim Öncü Grubu (SILG)'nin kurulmasıyla beraber yeniden bir yapılanma sürecine girmiştir. 2003'te SILG altında Devlet Ağı ve Bilgi Güvenliği Koordinasyonu Küçük Grubu (SNISCSG) adıyla bir alt grup oluşturulmuştur. Bu üç grubun amacı yerli bilgi teknolojilerini geliştirmek ve bunları ulusal güvenlik bağlamında harmanlamaktır. 2003'te SILG tarafından Belge 27 yayımlanmıştır. Bu belge ile kritik altyapının korunması, kriz yönetimi, e-devlet planları dahil olmak üzere siber güvenlikle ilgili önlem politikaları ve ulusal stratejilerin nasıl uygulanacağı üzerinde durulmuştur. 2012 yılında Danıştay Bilgi Ofisi (SCIO) bilgi güvenliğinin sağlanması noktasında Yeni Politika Görüşü (NPO)'nü yayınlamıştır. Bilgi teknolojilerine olan hassasiyet Çin askeri kapasitesi için de geçerlidir. Ordunun stratejik çerçevesi teknoloji ve bilgi teknolojisiyle çerçevelenmiştir. Bu noktada Genel Kurmay Başkanlığı'nın 3. ve 4. Daireleri'ne bağlı olan PLA ve onun siber istihbarat faaliyetleri karşımıza çıkmaktadır. Elbette siber alanda etkili olmak için tek aktör PLA değildir. PLA haricinde birçok bakanlık bu alanda etkili olmaya çalışmaktadır. 2008 yılında Sanayi ve Bilgi Teknolojileri Bakanlığı (MIIT) bilgi teknoloji gelişiminin merkezindedir.

Siber saldırılara yanıt vermede birincil görev 2002'de kurulmuş olan Çin Ulusal Bilgisayar Ağı Acil Durum Müdahale Teknik Ekibi/Koordinasyon Merkezi (CNCERT)'ne aittir, MIIT CNCERT'in çalışmalarına yardım etmektedir. Buna ilaveten MIIT ulusal savunma için yasa ve yönetmelikleri hazırlayan Ulusal Savunma Bilim, Teknoloji ve Sanayi Devlet İdaresini (SASTIND)'de bünyesinde barındırmaktadır. MIIT'den önce ise Milli Savunma Bilim, Teknoloji ve Sanayi Komisyonu (COSTIND) benzer görevleri üstlenmekteydi. Bir diğer bakanlık Kamu Güvenliği Bakanlığı (MPS) kritik altyapıların korumasıyla ilgilenmektedir. Devlet Güvenlik Bakanlığı (MSS) karşı casusluk, iç-dış istihbarat yürütme organı olarak işlev görmektedir. Tüm bakanlıkların yanı sıra bazen teknik departman olarak anılan 3. Departman (3/PLA) MSS'nin sivil alanda yürüttüğü istihbarat sorumluluklarını üstlenmektedir. Genelkurmay Başkanlığı 2. Daire (2/PLA)'si ise daha çok geleneksel istihbarat görevleri ile ilgilenirken açık kaynaklı bilgilerin toplanması ve analiz edilmesinde de görevlidir. 4. Departman (4/PLA) diğer 3/PLA'ya nazaran daha az ön plandadır. 2013 yılında mevcut ağ saldırı güçlerinin açığa çıkması sebebiyle 4/PLA, yerini Stratejik Destek Gücü (SSF)'ye bırakacaktır (Raud, 2016).

ABD'ye göre Çin uzayda en fazla kendisi için tehdit ve risk oluşturan devlettir. Bunun birçok sebebi vardır ancak en fazla ön plana çıkan sebepler; hemen hemen eşit güç kapasitesine sahip olmaları, Çin'in ekonomik ve teknolojik gücüdür. 2007 yılında Çin kara bağlantısıyla uzaya gönderdiği bir balistik füze sayesinde kendi meteoroloji uydusunu vurmuştur. Bu olay bize Çin'in

artık uzayda ABD'nin askeri operasyonlarını sekteye uğratabileceğini hatta yok edebileceğini kanıtlamıştır. Anti Uydu Silah (ASAT) sistemleri aracılığıyla da uzaya tam egemen olmak istenmektedir. “Beyaz Kitap: Çin'in Uzay Hırsları” kitabına göre dış uzayın araştırılması hayati önem taşımaktadır. 2020-22 insanlı uzay istasyonu hedeflenmiş olup Mars'a yapılması planlanan yolculuklarla Bedio-2 Navigasyon sistemleri kullanılarak Bir Kuşak Bir Yol projesine dahil olan ülkeler ile iletişim sağlanması hedeflenmektedir. Ayrıca 2050 yılına kadar uzay temelli güneş istasyonunun inşa edilmesi de planlanmaktadır (Goswami, 2018: 76). Bunlara ilaveten Kara Delikleri Araştırma Programı, Astro Fizik obje programları, Güneş sisteminde Dünya ile benzer eko sistemleri araştırma bu amaçla Jüpiter gezegeni projesi, Güneş ile ilgili bilgi toplama, Elektromanyetik güneş radyasyonun ve yüksek enerji partiküllülerinin nasıl hava değişimine neden olduğunu araştırma, mikro uydu projeleri, Mars araştırma projesi, Enerji, su, bio kimyasal döngüleri araştırma projeleri ile uzay alanındaki bilimsel çalışmalara katkı sağlamayı hedeflemektedirler (Wu, 2017: 10-30).

ABD İstihbarat Birliği, 2018 yılında bir rapor yayınlamıştır. Bu rapora göre Çin ve Rusya'nın anti uydu silah kapasiteleri ABD'nin uzaydaki askeri uydularını 2-3 yıl içerisinde geçecektir. ABD istihbarat, iletişim ve küresel koordinasyon yer bulma sistemleri bütünüyle etkisiz hale gelecektir (Cooper, 2018: 10).

Yine 2018 yılında ABD Savunma Bakanlığı tarafından yayınlanan bir raporda ise Çin'in askeri ve güvenlik çalışmaları mercek altına alınmıştır. İncelemeler sonucunda Çin Kurtuluş Ordusu'nun Stratejik Destek Gücü olarak aralıksız uzay çalışmalarına ağırlık verdiği saptanmış olup Çin'in artık siber alanla hava ve uzay güçlerini tek bir güç olarak kullanma kapasitesi tehdit olarak görülmüştür (USA Department of Defense Annual Report, 2018: 39-40).

Çin'in siber alanda yükselen önemli bir aktör olduğundan bahsetmiştik. Bu noktada siber alan hegemonik davranışların temel kaynağını oluşturabilecek kapasiteye sahip yeni bir alandır. Elbette bu alan devletler arasındaki rekabeti zorunlu kıldığı gibi iş birliğini de ön plana çıkarmıştır. Çünkü güvenlik her devletin temel ihtiyacıdır ve bu nokta da siber güvenlik bizler için vazgeçilmezdir. Siber güvenlik genel itibarıyla siber alana ait üç kavramın birleşenidir. İlk kavram mahremiyet, ikinci kavram bütünlük ve son kavram ise ulaşılabilirliktir (Güvenlik Terimleri Sözlüğü, 2017: 621). Siber güvenlik, sadece devletleri tehdit eden risk ve saldırıları konu almamaktadır. Bu noktada siber saldırılar karşısında toplumun da olumsuz etkilendiğini atlamamak gerekir. Özellikle de her sistemin kendisine has bir güvenlik açığına sahip olduğu gerçeğinden yola çıkarsak tüm dünyanın siber saldırılar karşısında gerekli önlemleri alması önemlidir.

Siber alanda yükselen bir güç olan Çin'in iş birlikçi düşüncesini anlamak için Kuşak Yol ve Girişim (KYG) analiz edilmelidir. İlk başta ekonomik temeller üzerinde yürütülen bu proje 2013 yılında Çin Halk Cumhuriyeti Başkanı Xi Jinping tarafından ilan edilmiştir. KYG Çin'den

başlayarak Orta Asya, Orta Doğu, Afrika ve Avrupa'ya kadarki ulaşım hattını kuşak olarak tanımlanmaktadır. Buna ilaveten Çin sahilleri Pasifik Okyanusu, Hint Okyanusu, Akdeniz ve Avrupa'ya uzanan sahil hattı ise yol olarak ifade edilmektedir. Ekonomik iş birliğini ön planda tutulmaktadır (Deepak, 2018). 2013 yılından bu yana Çin başkanı Xi Jinping tarafından ilan edilen KYG Kuzey Kutbuna, Sibirya'ya ve daha da önemlisi siber uzaya doğru genişlemiştir (Hillman, 2018). Ancak bizim burada asıl üzerinde durmak istediğimiz konu Çin'in siber alandaki politikalarıdır. Bu noktada 2015 yılına gelindiğinde Dijital İpek Yolu uluslararası gündemdeki yerini almıştır. Dijital İpek Yolu projesi ile fiber optik kablolar, 5G ağları, uydular ve bu sistemlere entegre olan bütün cihazları kapsayan (Xu ve Chen, 2019) RWR Advisory Group'a göre ise 2018 yılında dünya çapında tahmini olarak 79 milyar dolarlık 13 projeden oluşmaktadır (Prasso, 2019).

Bazı taraflara göre Çin'in dış politikası, mevcut dünya karşısında değerlendirildiğinde özellikle II. Dünya Savaşı sonrasındaki ulusal özerklik, egemen eşitlik, evrensel insan hakları ve demokrasi normlarının karşısındadır. Çin makine öğrenimi, yapay zeka, 5G teknolojisi ve daha fazla alanda ön plandadır. Dolayısıyla bu yeni alanda Çin kuralları belirleyecektir. Tianxia olarak adlandırılan dünya düzeni ele alındığında tüm dünya kastedilmektedir. Pekin'in Çin olmadan, sürekli ve kaçınılmaz olarak hoşnutsuzluk ve güvensizliğin dünyaya hakim olacağı algısı Batı'nın karşısındadır. 2017 yılında Xi Jinping, yeni yıl mesajında Çin halkının her zaman tek bir aile olarak tüm dünya ile uyum içerisinde olmayı istemesidir. Bu ifade ile Mao'nun dünya haklarının büyük dayanışmasına yaptığı vurguya paraleldir. Xi Jinping'in bu ifadesi esasen Vestfalya Sistemi'ne bir meydan okumadır. Bu noktada 2 görüş söz konusudur. İlk görüş; Valeriano, Jensen ve Maness gibi isimlerin de ifade ettiği gibi Çin'in politikalarının zararsız olduğudur. Pekin'in eylemleri dijital alanlarda öngörülebilir ve ölçülebilir. Diğer görüşü savunan Mearsheimer, Allison ve Cheng gibi isimler ise Çin'in dijital alandaki eylemleri sistemi istikrarsızlaştırmaktadır. Çin'i görmek dijital dünyada ejderhayı görmeye benzetilebilir. Çünkü Çin'in eylemleri karşı tarafı karamsarlığa itmektedir. ABD ve Çin arasındaki rekabet olumsuz değildir. Rekabetçi ancak istikrarlı bir güç ilişkisinden bahsedilmektedir. Yan (Xuetong, 2017)'a göre gücün yeniden dağıtılması uluslararası sistemde dönüşüme yol açacaktır. Bu dönüşüm aynı normdan 2 farklı norma sahip aktörler arasında daha sık meydana gelmektedir. Uluslararası düzenin zirvesindeki yeni bir büyük güç zirvedeki konumunu sürdürebilmek için normları değiştirecektir. Çin yükselişi duraksamadığı müddetçe doktrinsel yasal savaş stratejisi aracılığıyla uluslararası hukukun normlarını değiştirebilir. Dahası Çin'in bunu ilk uygulama alanlarının uzay, siber uzay ve diğer alanlar olması olasıdır (White, 2020).

3.2.2. Çin Kurumlarının Siber Alanda İncelenmesi

Siber Güvenlik ve Altyapı Ajansı (CISA)'nın Çin'in kötü niyetli siber faaliyetlerine ilişkin değerlendirmeleri mevcuttur. Buna ilaveten DOD, FBI ve NSA gibi yapılanmalar da Çin'in siber

alandaki faaliyetlerini inceleyerek CISA'nın değerlendirmelerine paralel analizleri mevcuttur. CISA'ya göre Çin sebep olduğu siber saldırı örnekleri aşağıda belirtilmiştir:

- 2017'de en az 12 şirket Çin tarafından hedef alınmıştır.
- 2018 yılında 2016'dan itibaren ABD kritik altyapı sistemlerinin hedef alındığı vurgulanmıştır. Bu sistemler; enerji, sağlık, halk sağlığı ve iletişimdir.
- 2019'da Cloud Hopper (En büyük küresel siber casusluk kampanyası) operasyonu.
- 2020'de CISA ve FBI Covid-19'a karşı Çin tarafından sağlık çalışanları, ilaç ve araştırma sektörlerini baz alan saldırılar üzerinde durmuştur. CISA, Çin Hükümeti aktörlerinin ağ istismları ve Çin MSS'ye bağlı siber tehdit aktörlerinin ABD devlet kurumlarını hedef aldığı belirtmiştir. Buna ilaveten CISA ABD ve Çin arasında artan gerilimi baz alarak Çin bağlı siber aktörlerin kullandığı taktik, taktik ve prosedürleri içeren bir uyarı yayınlamıştır.
- CISA, 19 Temmuz 2021 Beyaz Saray Açıklaması'nda Microsoft Exchange Server ürünlerindeki güvenlik açıkları üzerinde durup uyarı açıklamalarında bulunmuştur. Siber casusluk ve veri hırsızlığı risklerini azaltmak için CISA, FBI ve NSA liderleri bir araya gelmiştir. Bunun sonucunda CISA, bir ön görüş bildirimi yayınlamıştır. Buna ilaveten yine aynı yıl CISA, NSA ve FBI siber tehditlerle ilgili ABD Hükümeti'ni korumaya yardımcı olmak için bir Dayanışma Belgesi yayınlamıştır. Özellikle CISA ve FBI, 19 Temmuz 2021 Adalet Bakanlığı açıklamasında ağ sistemlerine izinsiz girişler üzerinde durmuştur. Son olarak CISA ve FBI 2011-2013 yılları arasında Çinli aktörler tarafından yürütülen ABD petrol ve doğal gaz (ONG) boru hattı şirketleri hedef alan saldırılar karşısında farkındalık oluşturmayı amaçlamıştır.
- 2022 yılına gelindiğinde, CISA, NSA ve FBI Çin destekli siber aktörlerin güvenliği ihlal etmek için geniş bir altyapı sistemi kurmayı hedefleyen güvenlik açıklarından yararlandıkları yöntemleri açıklayan Danışma Belgesi'ni yayınlamıştır. Buna ilaveten yine aynı yıl yayınlanan bir başka Danışma Belgesi'nde Çin tarafından 2020 yılından beri kullanılan en yaygın güvenlik açıkları ve etkilerine yer verilmiştir (Cybersecurity & Infrastructure Security Agency, 2021).

Çin kurumlarının siber alanda ön plana çıktığı nokta siber casusluk faaliyetleri olarak değerlendirilebilir. ABD-Çin Ekonomik ve Güvenlik İnceleme Komisyonu'nun Kongre'ye sunduğu 2022 Yıllık Raporu'nda, Pekin'in siber savaş ve casusluk yetenekleri başta olmak üzere ABD ekonomisine ve ulusal güvenliğine yönelik tehditlerden bahsedilmiştir. Bilhassa Georgetown Üniversitesi Güvenlik ve Gelişen Teknoloji Merkezi tarafından geçen ay yayınlanan bir rapora göre 2015-2021 yılları arasında 49 eyalette en az 1.681 yerel yönetim ABD'nin yasakladığı Çin'e ait beş şirketten bilgi ve iletişim teknoloji hizmetlerini satın almıştır (Graham, 2022).

Uluslararası arenada Çin'in sebep olduğu birçok kötü niyetli siber saldırının gerçekleştiği iddiaları çok yaygındır. Ancak siber casusluk amacı taşıyan saldırıların silahlı çatışmaya dönüşmesi olası değildir. 1990'dan sonra bilgi savaşları Çin için dikkatleri çekmiştir. Özellikle ABD ordusunun 1991 Körfez Savaşı'nda ve ardından Kosova, Afganistan ve Irak'ta kullandığı yüksek teknoloji Çin'i etkilemiştir. 1993'te Çin, Askeri Stratejik Kılavuzu (PMS)'nu yeniden düzenlemiştir. Modern teknoloji, özellikle yüksek teknoloji sayesinde yerel savaşları kazanmak amaçlanmıştır. Dahası 2004'te Irak Savaşı'ndan bir yıl sonra orduya ait PMS, bilgilendirme koşulları altında yerel savaşların kazanılması olarak değiştirilmiştir. Bilgilendirme faaliyetlerinin silahlı kuvvetlerin gücünü arttıran kilit faktör olduğu kabul edilmiştir. Bu düzenlemelerin yanı sıra Çin ilk defa siber savaşın bütüncül olarak ele alındığı çalışma Askeri Bilimler Akademisi tarafından yayınlanan Askeri Strateji Bilimi'nin 2013 versiyonudur. Benzer yaklaşım tarzı 2015 Milli Savunma Bakanlığı'nın Çin'in Askeri Stratejisi adlı makalesinde de karşımıza çıkmaktadır. Siber alanda Çin kapasitesi için iki temel husustan bahsedilebilir. Birincisi Çin'in siber yetenekleri boşlukla gelişim göstermemiştir. ABD ve Rusya'nın siber savaş karşısındaki değişken uygulamalardan yararlanılmıştır. İkinci olarak ise Çin'in siber savaş yaklaşımları ulusal güvenlik ortamına, iç durumuna ve yabancı orduların faaliyetlerine göre değişen askeri stratejilerle uyum içerisinde (Jinghua, 2019).

Siber güvenlik kavramı Çin için göz ardı edilemeyecek kadar önemlidir. Çünkü uluslararası arenada yer alan diğer devletler gibi siber tehdit ve saldırılar karşısında ülkenin kritik altyapı özelliklerinin hasar görmesi, tecrübe edilen çağın bilgi çağı olması, internetin erişim kapasitesinin gücü, toplumsal gelişim, ekonomik süreçlerden askeri kapasiteye kadar birçok alan siber alanın kontrol alanına dahildir (Swaine, 2013: 3). Çin'in siber tehdit ve saldırılar karşısında uyguladığı politikalar Batı bloğunun ön planda tuttuğu politikalardan farklıdır. Çünkü Çin'in siber güvenlik kavramına olan bakış açısı ulusal ve uluslararası platformlara tam anlamıyla açık değildir. Hauke Johannes Gierow (2015: 1-10)'un yaptığı çalışmaya göre Çin bilişim teknolojilerine yön veren öncü devletlerin sistemlerin uzak durmaktadır.

Çin, 1986 yılında ekonomik bilgilerin yönetimine yönelik bir grup oluşturmuştur. 2003 yılında ise siber güvenlik ile ilgili Belge 27 yayımlanmıştır. Belge 27 özellikle kritik altyapıların korunması noktasında aktif bir savunma sisteminin varlığını ön görmektedir (Raud, 2016: 11) Buna ilaveten Çokuluslu dört büyük şirketten (Big Four) biri olan KMPG'nin yayınladığı raporda siber güvenlik alanında kurumsal ve hukuksal düzenlemelere yer verilirken Kamu Güvenliği Bakanlığı (Ministry of Public Security) internet ve virüslere karşı savunma sistemlerinin önemi üzerinde durmuştur. 2014 yılına gelindiğinde ise Çin devlet başkanı Xi Jinping siber güvenlik grubunun tanıtımını yapmıştır. 2015 yılında ise Çin'in Ulusal Kongresi olan NPC'de (Standing Committee of the National People's Congress) Siber Güvenlik Kanun tasarısını sunulmuştur. Bu tasarı 2016 yılında bir kez görüşülmesi için NPC'de sunulmuştur.

1 Ocak 2017 yılında taslak kanun olarak kabul edilmiştir. Kanun (COV, 2017) 7 bölüm ve 79 maddeden meydana gelmektedir. 1. ve 2. bölümde genel prensipler ve hükümetin genel siber güvenlik stratejisi hakkında bilgi verilmektedir. 3. bölümde servis sağlayıcı ve ilgili kuruluşlarının sağlaması gereken siber güvenlik standartları Çok Boyutlu Ağ Güvenliği Koruması Şematiği altında verilmiştir. 4. bölümde bilgi güvenliği konuları; özel hayatın gizliliği, siber suçlar, zararlı yazılımlar, kanunsuz bilgi yayılımı gibi odak noktalar üzerinden ele alınmıştır. 5. bölümde ağların izlenmesi ve acil durumlarda tehlikelere karşı yapılacak hamleler açıklanmıştır. 6. bölümde ağ güvenliği kurallarının ihlal edilmesi durumunda uygulanacak yaptırımlar belirtilirken, son bölümde tanımlar ve diğer ek bilgiler yer almıştır. Çin için siber güvenlik kavramı, geliştirilmesi gereken ulusal güvenlik politikalarını oluşturmuştur.

Hedeflenen güvenlik kapasitesi için milli gücün önemi ön plana çıkarılmıştır. Bu nokta da bir parantez açmak gerekir. Çin'in bu tutumu bazı taraflarca saldırgan olarak nitelendirilmektedir. Bilhassa ABD, Tayvan ve Almanya gibi ülkeler için Çin siber alanda tehdittir. Çin kaynaklı siber saldırılardan etkilenen ülke sayısı 2009 yılına gelindiğinde 103 olacaktır (Spade, 2012: 3-4). Buna ilaveten Çin için siber politikaların şekillenmesinde Genel Kurmay Daireleri'nin ve Teknik Keşif Büroları'nın da payı büyüktür.

3.2.2.1. Genelkurmay Daireleri

Çin Genelkurmay Daireleri'nde tecrübe edilen değişimlerde PLA'nın konumu oldukça önemlidir. Bu noktada Deng Xiaoping'in 1978 yılından sonra PLA'ya olan katkıları da göz ardı edilmemelidir. Daha sonra PLA'nın gelişim süreci 21. Yüzyıl başlarında sanayi, bilim ve teknolojik gelişmelerle ilerleyecektir.

ABD'nin siber komuta birimini oluşturmasından 1 yıl sonra 2010 yılında Çin, PLA'nın siber savaş tehditleriyle mücadele edebilmesi ve bilgi güvenliğini korumak için ilk departman olan Bilgi Güvenliği Üssü (PLA Daily)'nü ilan etmiştir. Bu departman doğrudan Genelkurmay Karargahı'na bağlıdır. Çin için bu üs siber savaş için saldırı karargahı olmayıp Çin'in bilgi güvenliği için bir savunma birimidir. Bu üs aracılığıyla çevrimiçi bilgi toplama faaliyetleri gerçekleşirken gizli askeri bilgileri koruyan duvarlar inşa edilecektir. PLA için bu yapılanma oldukça önemlidir. Çünkü PLA artık farklı kuvvetlerdeki bilgi teknoloji merkezlerini yönetebileceği birleşik ve merkezi bir yönetim sistemine sahiptir. Pekin Posta ve Telekomünikasyon Üniversitesi Başkanı Profesör Fang Binxing'in de belirttiği gibi ABD'nin siber tabanlı saldırı ve savunmada en önde gelen güç olduğu iddiasından yola çıkarsak Çin siber alandaki yeteneklerini geliştirmek zorundadır (Branigan, 2010).

ABD Savunma İstihbarat Ajansı (DIA) 15 Ocak 2019 Çin Askeri Güç Raporu'nun son baskını yayınlamıştır. Bu raporda Çin'in 21. yüzyıl bilgi teknolojisi üzerine yeniden inşa ettiği komuta ve kontrol birimlerinin yanı sıra PLA'nın Stratejik Destek Gücü bünyesinde siber savaş

yeteneklerinin yeniden nasıl düzenlendiğine yer verilmiştir. Çin'in siber uzaya daire kongre ifade ve resmi belgeleri DIA'nın raporunun içeriğine paraleldir. Çin için siber uzay ekonomik ve sosyal kalkınmanın yanı sıra ulusal güvenliğin yeni alanıdır. Bu noktada Çin siber altyapısına yönelik ciddi risk tehditlerini ele alırsak bu tehditlerin önlenmesi, ulusal ağ ve bilgi güvenliğinin sağlanması için siber kuvvetler geliştirilmeli, siber uzaya ait farkındalık arttırılmalıdır (Martelle, 2019).

Çin siber savaş programı analiz edildiğinde Genelkurmay Karargahı'na bağlı departmanlar ön plandadır. Çin bilgisayar ağı operasyonları ve bilgi savaşlarının kilit görevleri PLA Genelkurmay Karargahı'ndaki bu farklı departmanlara bağlıdır. Bu departmanlar 3. ve 4. Departmanlar olup bu noktada farklı askeri bölgelerde özel askeri bürolarda merkezler mevcuttu. İkinci paragrafta bahsedildiği gibi Çin ilk Siber Bilgi Güvenliği Üssü'nü kurulduktan sonra PLA artık siber komuta merkezine sahip olmuştur (PLA Daily, 2010; China Times, 2010; Global Times, 2010). Konuyu başka bir perspektiften ele alacak olursak PLA, 2003 yılından bu yana geliştirmekte olduğu Bilgi Savaşı (IW) birimlerini tamamlamıştır. PLA'nın IW stratejisinin büyük bir kısmı ise elektronik savaş departmanı olarak adlandırılan 4. Departman tarafından yürütülecek olup bu görevi dönemin Tümgeneral Dai Qingmin yürütecektir (Wall Street Journal, 2009). Kısacası Çin Genelkurmay Daireleri Çin'in siber alandaki dönüşüm aşamalarını sağlayan kurumlardır. (Jamestown Foundation, 2010).

Çin'in demografik özellikleri de dikkate alındığında sahip olunan insan kapasitesi askeri açıdan bir avantaj olarak nitelendirilebilir. Özellikle 2015 yılından sonra Çin askeri kapasitesini arttırmayı hedeflemiştir. Bu noktada eğitime, askeri tatbikatlara ve savunma eylem planlarına dikkat edilmiştir. 22 Ocak 2017 yılına gelindiğinde askeri kapasite ile sivil kapasitenin entegre süreci başlayacaktır. Bu süreç Çin Komünist Partisi (ÇKP) Merkez Politbüro Yürütme Komitesi tarafından Merkez Askeri-Sivil Entegrasyon Geliştirme Komisyonu (MASEGK)'nin oluşturulmasıyla aktif hale getirilecektir. MASEGK direk olarak emirleri ÇKP Merkez Politbüro Yürütme Komitesi'nden almakta olup MASEGK'in Başkanı ÇKP Genel Sekreteri ve Çin Devlet Başkanı Xi Jinping'dir. (ÇKP Merkez Politbüro Yürütme Komitesi). Ayrıca ÇHKO yönetim birimlerinde köklü değişikliklere de gidilmiştir. 18 Nisan 2017 ÇKP Merkez Askeri Komisyon Başkanı unvanıyla Xi Jinping, 84 ileri düzey askeri kurum ve kuruluşlarına yeni görevler atamıştır. Tüm ordunun birinci sınıf askeri kurum ve askeri birimleri 84 olarak yeniden yapılandırıldı ve Xi Jinping talimatlar vermiştir.

Çin için 1990-2000 yılları arasında PLA yapılanmasının modernleşmesi ve teknolojik gelişmeler karşısındaki konumu aktif bir şekilde ele alınmıştır (ABD Savunma İstihbarat Ajansı, 2019). 2015 yılına gelindiğinde Başkan Xi Jinping, PLA için ön önemli reformları ilan etmiştir. Bu reformlar Çin'in ABD karşısında profesyonelleşmesini hedeflemiştir. PLA'nın sistematik yapısı yeniden şekillendirilirken yeni Ortak Personel Dairesi aktifleştirilmiştir. Buna ilaveten PLA Roket

Gücü de kurularak Çin'in askeri kapasitesi arttırılmıştır (Wuthnow ve Saunders, 2017). 2017 yılının ekim ayına gelindiğinde ise 19. Parti Kongre Raporu incelenmelidir. Çin başkanı Xi Jinping PLA'yı askeri alanda rekabet edebilmek için tüm stratejik yönleriyle ön plana çıkması gerektiğinin altını çizmiştir. Ayrıca 2020 yılına kadar olan süreçte PLA'nın askeri kapasitesinin önemi vurgulanmış olup gerekli adımların atılmasının altı çizilmiştir. 2035 yılına kadar PLA'nın sahip olduğu tüm askeri kapasitenin teknolojiye adapte edilmesi hedeflenmiştir (Xinhua, 2017). Son zamanlarda PLA'nın faaliyetleri incelendiğinde ise uluslararası arena da konvensiyonel gücün uygulayıcısıdır. Çünkü PLA, Çin'in nükleer ve siber alanda da ön plana çıkmasına aracılık etmektedir. Çin'in karşısında yer alan rakipler için PLA'nın çalışma alanı dikkate alınmalıdır. Pekin'in 2018 yılındaki askeri harcamalar için ayırdığı bütçesi 170 milyar doların üzerinde iken (Liff ve Erickson 2013) Pentagon'un harcamaları 200 milyar doları aşmaktadır (Asan Forumu, 2014).

Çin askeri yeteneklerini siber alana entegre etmeye çalışırken Çin'in askeri yetenekleri uluslararası arena da dijital saldırılardan sorumlu tutulmaktadır. PLA'nın 61398 nolu birimi Şangay'da yer almaktadır. 12 katlı bu beyaz bina Çin PLA'nın üssüdür. ABD'li istihbarat yetkilileri tarafından ileri sunulan kanıtlar ABD kurumlarına yönelik siber saldırılarının bu çevre etrafından gerçekleştirildiği yönündedir. ABD'li kurbanların maruz kaldığı saldırıların çoğunda en iyi Çinli hackerlerin izi sürüldüğünde ilk kez izler askeri birlik ile ilişkilendirilmiştir. ABD bir bilgisayar güvenlik firması Mandiant'ın kurucusu ve CEO'su Mandia'ya göre ise ya saldırılar 61398 Birimi'nden kaynaklanmaktadır ya da dünyanın en kontrollü en çok takip edilen internet ağlarını yöneten binlerce insan bu alandan saldırıların gerçekleştirildiğini bilmiyorlar (Sanger vd., 2013).

3.2.2.2. Teknik Keşif Büroları

NSA, CISA ve FBI bir araya gelerek Siber Güvenlik Danışmanlığı'nı ilan etmişlerdir. Bu rapor daha önceki NSA, CISA ve FBI raporlarında yer alan eyalet, yerel ve bölgesel hükümetleri, Savunma Sanayi Üssü (DIB) dahil kritik altyapı ve özel sektör kuruluşları taktik, teknik ve prosedürler (TTPs) hakkında bilgilendiren raporlara dayanmaktadır. Bu rapora göre kurumlar kullanım ömrünü tamamlamış altyapıyı değiştirerek merkezi bir yama yöntemi kullanarak güvenlik açıklarını azaltabilirler. Özellikle Siber Güvenlik Danışma Raporu'nda, Çin'in desteklediği siber aktörlerin, tehlikedeki altyapı sistemlerinin oluşturduğu geniş bir ağ kurarak güvenlik açıklarından yararlanmayı amaçladıkları iddia edilmektedir. Küçük çaplı ev/ofis (SOHO) yönlendiricileri ve Ağa Bağlı Depolama (NAS) cihazları gibi ağ cihazları, komuta ve kontrol (C2) trafiğini yönlendirmek için ek erişim noktalarına ulaşılmaktadır. 2020'den bu yana Çin destekli siber aktörler ortak güvenlik açıkları ve maruziyetler (CVE) olarak bilinen kamuya açık olan güvenlik açıklarından hızlı bir şekilde yararlanabilmek için faaliyetler yürütmüşlerdir. Aynı zamanda bu Çin destekli siber aktörler izinsiz girişlerini, Çin internet hizmet sağlayıcılarında (ISS) çözümlenen çok

sayıda Çin merkezli internet protokolü (IP) adı verilen tehlikeye atılmış sunuculara erişerek gerçekleştirilmektedirler (CISA, 2022).

İlk paragrafta FBI, NSA ve CISA'nın bir araya gelerek yayınladıkları Siber Güvenlik Danışma Raporu'ndan bahsedilmiştir. Bu raporun önemi ABD'nin siyasi, ekonomik, eğitim ve CI personeli ve kuruluşlarını hedef alan Çin destekli siber faaliyetleri göstermenin yanı sıra proaktif ve geriye dönük analizler sayesinde Çin'in desteklediği kötü niyetli siber operasyonlardaki eğilimi ön plana çıkarılmıştır. İlk eğilim Çin destekli siber aktörlerin çevik ve hızlı davrandığıdır. Bilgi topluluğu uygulamalarını kavrayan bu aktörler bir dizi özel sunucu (VPS) ve açık kaynak veya ticari sızma araçları sayesinde faaliyetlerini gizlemeye çalışmaktadır. İkinci nokta ise; Çin destekli siber aktörler, güvenlik açıklarının kamuoyuna açıklanmasının ardından hedef ağları sürekli olarak kritik ve yüksek güvenlik açıkları için taramaya devam etmektedir. Çoğunlukla Pulse Secure, Apache, F5 Big-IP ve Microsoft ürünleri gibi büyük uygulamalardaki güvenlik açıklarından yararlanmaya çalışmaktadırlar (CISA, 2021).

Çin için siber uzayda istihbarat faaliyetleri ön plandadır. Özellikle Tayvan'daki hükümet, ordu ve diğer hedeflerden istihbarat toplama çalışmaları ön plandadır. Siber alanda etkin istihbarat toplama veya ağ sistemlerinin keşfedilmesi, gelecekteki potansiyel ağ saldırı ve savunma operasyonlarını hızlandırmak amacıyla özel bilgi edinmek için tahribatsız ağ istismarı SMS 2013 olarak adlandırılmaktadır. Ağ keşfi, ağa sızma, sırların çalınması ve casusluk, 3.taraf satıcılar ve diğer araçların yardımıyla fiziksel bilgi depolama cihazlarının ele geçirilmesi yoluyla düşmanın elektromanyetik ve silah kontrol sistemlerinin ele geçirilmesi hedeflenmektedir. SMS 2017 ve SMS 2020 aracılığıyla ise düşmanın ağ sistemleri, bilgi yetenekleri, kritik düğümler, güvenlik açıkları, stratejik planlar, kuvvetler, yöntemler ve potansiyel hareket biçimleri hakkında bilgi ihtiyacı belirtilerek elde edinmek istenen istihbarat ile ilgili ek bilgiler hedeflenmektedir. Dolayısıyla ağ keşfi sayesinde düşmanın sistemleri teknik olarak analiz edilirken hem de ağ saldırısının ötesinde casusluk faaliyetleri de yürütülmektedir. Kısacası hem teknik hem de casusluk bir aradadır. SMS 2013'ün hedefi farklı olsa da ağ saldırı ve savunma yöntemleri teknik düzeyde ağ keşif yöntemleriyle aynıdır. Ağ keşif aşamasında şifre kırma, bilgi ele geçirme ve yerel depolanan bilgileri elde etmek için casus yazılımlar kullanılırken SMS 17 ve SMS 2020'de ağ keşif aşaması virüsler, truva atları ve hacker yazılımlarıyla gerçekleşmektedir. 2020 yılında AMS Harp Araştırma Enstitüsü ve PLA'nın 31003 Birimi'ne bağlı çalışanlar tarafından yazılan makale de 20'den fazla yaygın ağ saldırı modelinden bahsedilmiştir. Bu listede yer alan bazı yöntemler; tam metin ve hesap şifreleri de dahil olmak üzere ağ koklayıcıları; konum, güvenlik açıkları ve hizmetler de dahil olmak üzere ağ tarayıcıları; bilgi hizmetlerinden yararlanmak (Parmak okuyucu ve LDAP hizmetleri); sosyal mühendislik, çeşitli yöntemlerle ağa müdahale; IP ve DNS aldatmacaları; ARP saldırı ve e-posta kimlik avı dahil olmak üzere ağ müdahale yöntemleridir (Insikt Group, 2022).

Çin'in siber uzaydaki etki alanını analiz edebilmek için keşif bürolarını incelerken bir noktaya değinmek gerekir. ABD ve Çin siber alana bakış açısı aynı olmadığı için bu alanın yorumlanması noktasında da farklılıklar mevcuttur. 2011 yılında Beyaz Saray Uluslararası Siber Uzay Stratejisi'nde, ABD siber uzayın meşru kullanımına dikkat çekmiştir. Bu stratejiye göre siber uzay açık, birlikte çalışabilir, güvenli ve güvenilir bilgi ve iletişim altyapısını ön plana çıkarmaktadır. Ancak Pekin için siber alan daha çok bir egemenlik alanıdır. Devletler kendi siber alanlarını tıpkı diğer alan ya da bölgeler de olduğu gibi kontrol etme hakkına sahiptir. Dolayısıyla bu bakış açısı siber alana etki eden araçların da farklı yorumlanmasına sebep olacaktır (Segal, 2017).

Siber güvenlik siyasi, istihbarat, askeri ve kurumsal tehdit riskleri göz önüne alındığında zorunlu bir politika alanı olarak karşımıza çıkmaktadır. Bu noktada Çin'in etki ettiği tehdit kapasitesinin abartıldığına dikkat edilmelidir. Özellikle siber casusluk, ağa sızma gibi faaliyetlerde Çin etkili olsa dahi Çin'e yönelik siber tehditlerden aynı sıklıkla bahsedilememektedir. Bir başka husus ise ABD ve Çin'in siber alana yansıttıkları bakış açılarındaki farklılıklardır. Çin, siber savunmayı teknik olarak ele almak yerine siyasi bilgi kontrolüne öncülük vermektedir. Bu aşamada bilinçsiz olarak kendi ağ ekonomik etkinliğini de azaltmaktadır. Bu durum yabancıların Çin sistemine sızmasını kolaylaştıracaktır. Ayrıca Çin'in bilgi kontrolüne verdiği önem askeri alana da yansıyacaktır. Enformatikleşme olarak adlandırılan bu aşama da deneyimli yabancı siber operatörlerin saldırılabileceği güvenlik açıkları oluşsa dahi agresif bir politika karşımıza çıkmamaktadır. Elbette bu değerlendirmeler yapılırken Çin ve ABD arasındaki güç farkını yorumlanın kolay olmayacağı vurgulanmalıdır. Çünkü her iki aktörün de siber kabiliyet ve operasyon bilgilerinin tamamı şeffaf değildir (Lindsay, 2014: 44).

3.3. Siber Alanda ABD ve Çin Mücadelesi

ABD ve Çin arasında kurulan stabil kapsamlı diplomatik ilişkilerin temelleri Nixon ve Mao döneminde atılmıştır. 1972-1979 yıllarında oluşturulan bu ilişki özellikle Deng'in uluslararası arena da yansıttığı diğer devletler ile barışçıl ilişkiler ve ekonomik büyüme etkisinde gelişmiştir. ABD ve Çin arasındaki ilişkide ABD merkez konumdadır. Ancak kurulan bu ilişkilerin yanı sıra Çin ve ABD arasındaki askeri, siyasi, ekonomik, teknolojik ve kültürel rekabet artmıştır. Özellikle Obama başkanlık görevini yerine getirirken 2012 ABD Savunma Stratejisi'nde bu mücadeleden bahsedilmiştir. 2012 ABD Savunma Stratejisi Raporu'na göre güç merkezinin Ortadoğu ekseninden Asya-Pasifiğe doğru kaydığının üzerinde durulmuştur. Çin karşısında Hindistan ve Japonya dengeleyici aktör olarak değerlendirilmiştir. ABD Savunma stratejisi için Çin belirgin bir hedef haline gelmiştir. Bilhassa ABD karşısında Çin'in siber alandaki faaliyetlerine dikkat çekilmiştir. İlk kez siber alan ve ağların ciddi bir rekabet alanını yansıttığına yer verilirken siber güvenlik kavramı ön plana çıkarılmıştır (Örmeci, 2013: 7).

ABD ve Çin'in siber alandaki mücadelesinin özel bir anlamı vardır. Uluslararası arenada bu iki aktör başka bir alanda bu kadar hızlı bir şekilde karşı karşıya gelmemiştir. Siber uzay öncesinde sınırlı sayıda üniversite laboratuvarlarındaki bilgisayar ağları arasındaki yeni oluşan bağlantıların ötesinde bir durum mevcut değildi. Ancak günümüzde siber uzayın küresel yaşam modelinin merkezini anlamak imkansızdır. İnternete bağlanan yaklaşık 50 milyar cihazın arkasında neredeyse 4 milyar insan vardır. Dolayısıyla ABD-Çin'in ilişkileri nasıl yönettikleri yalnızca kendi siyasal ve ekonomik geleceklerini etkilemeyecek olup aynı zamanda bu alanda izledikleri politikalar küresel istikrar ve refahın temel yapı taşları olacaktır (Lieberthal ve Singer, 2012: 11).

ABD ve Çin arasındaki siber alandaki rekabetinin uluslararası arenada nasıl gerilimi arttırdığı da analiz edilmelidir. İlk olarak, düşük yoğunluklu, sık ve kötü niyetli siber eylemler uluslararası arena da şüpheleri, güvensizlikleri ve güvenlik ikilemlerini arttırabilir. CI sistemlerini hedef alan siber saldırıların maliyetinin düşük olmasının yanı sıra kaynağının saptanması da oldukça güçtür. İkinci olarak, siber uzay operasyonları, diğer ülkelerin çıkarlarına zarar veren stratejik hedeflere ulaşarak ülkeler arasındaki gerilimi arttırabilir. Bu noktada ekonomi, iletişim ve ulaşım gibi CI sistemlerini hedef alan siber saldırılar füzelerden daha ölümcül sonuçlara sebep olabilir. Son olarak ise siber uzaydaki askeri operasyonlar gerçek dünyadaki savaşları tetikleme riskini arttırır. Askeri olarak siber uzay operasyonlarının en büyük avantajı ise yabancı topraklarda fiziksel bir mevcudiyet oluşturmaya gerek kalmadan güç planlama yeteneğidir (Xu ve Lu, 2021).

1990'lı yılların başında ABD Başkanı Bill Clinton Bilgi Otoyolu programını ilan ettiğinde internet küresel olarak yayılmıştır. George W. Bush yönetimi ise ABD Siber Uzay Stratejisi'ni ilan ederek kritik altyapı sistemlerinin güvenliğini ön plana çıkarırken siber güvenlik kavramına eğilmiştir. 1994-2008 yılları arasındaki süreçte ise Çin'deki internet kullanıcıların sayısı ilk kez ABD'yi geçerek birinci olmuştur (CNNIC, 2008). Obama yönetimi sırasında ise, ABD-Çin ilişkilerinde siber alanla ilgili sorunlar artmaya başladı. 2012 yılında yayınlanan Mandiant Raporu'na göre PLA, ABD şirketlerini, hükümeti ve CI sistemlerini doğrudan hedef alan saldırıların kaynağıdır. Bu rapor Çin'in hedef alan ilk siber casusluk raporudur (Finkle, 2013). Mandiant Raporu'na göre Çin tarafından gerçekleştirilen farklı APTs belirlemiştir. APT1 PLA 61398 nolu birim ile ilişkilendirilmiştir. Bu raporda 2006 yılından 2013'e kadarki 141'den fazla şirketin yüzlerce terabayt değerinde bilginin ele geçirilmesinin yanı sıra saldırıya uğrayan şirketlerden 115'inin ABD'de bulunduğu tespit edilmiştir. Bu düzeyde bir siber casusluk 2015 yılında ABD-Çin Siber Güvenlik Anlaşması'na aykırıdır. Önemli olan bu tarz eylemlerin normalleşmemesidir. ABD-Çin, siber egemenliklerini ihlal eden eylemleriyle kınanırken bu durum siber güvenlik kavramına entegre edilememiştir. Eğer ortak bir tanım yapılabilirse siber casusluğun yayılması için ortak bir uluslararası anlaşmaya varılabilir (Julian, 2021). 2014 yılına gelindiğinde ABD-Çin arasındaki siber casusluk tırmanmaya başlamıştır. 2015 yılına gelindiğinde FireEye, Çin'i Güneydoğu Asya ülkeleri ve Hindistan'daki hükümet ve şirketler hakkında casuslukla suçladığında taraflar arasındaki gerilim kötüye gitmiştir (FireEye Labs, 2015). 2018'de Trump

döneminde ise ABD Ticaret Bakanlığı, Çin teknoloji ve ürünlerine, internet şirketlerine, sivil ve askeri amaçlarla ürün üreten teknoloji şirketlerine karşı ulusal gerekçeler aracılığıyla ekonomik yaptırımları kabul etmiştir. Biden yönetimine gelindiğinde ise siber güvenlik ulusal güvenliğin ayrılmaz bir parçası olarak kabul edilmiş olup eski Başkan Trump'ın siber politikalarından radikal bir sapma olmayacağı kabul edilmiştir (Chen ve Lu, 2021: 1).

Bu rekabette Çin'in ön plana çıkmasındaki uluslararası arena da yaşanan değişiklikler de önemlidir. Özellikle SSCB'nin dağılmasından sonra yaşanan paradigma değişimi ile dünya artık siyah ve beyaz olmaktan uzaklaşmıştır. Soğuk Savaşın ardından ABD uluslararası arenada rakipsiz olarak değerlendirilebilir. Küreselleşme döneminde ise Çin'in ekonomik büyümesi göz önüne alındığında Çin analiz edilmesi gereken bir aktör konumundadır. 1,3 milyar nüfusa sahip Çin dünyanın en büyük ordusuna sahip olmanın yanı sıra nükleer silah kapasitesi ve BM Güvenlik Konseyi'nin üyesi olması da Çin'in analiz edilmesi gereken bir aktör olduğunu kanıtlamaktadır. Çünkü Çin sadece ekonomik ve askeri değil aynı zamanda stratejik olarak ön plana çıkmaktadır. Buna ilaveten Çin'in Şanghay İş Birliği Örgütü (ŞİÖ), Güneydoğu Asya Uluslararası Birliği (ASEAN) gibi yapılanmalarda oynadığı roller sayesinde bölgenin etkin bir aktörüdür (TASAM, 2005: 13). Bütün bu gelişmelere dikkat edildiğinde Çin'in ABD karşısında yükselen bir güç olduğu aşikardır. Bu noktada ABD ve Çin hem bölgesel çıkarlarda hem de uluslararası arena da karşı karşıya gelmektedir. Konuya başka bir açıdan yaklaşacak olursak 2015 yılında Çin'in büyüme hızı 6,9'dur. Bir başka örnek de ayın yüzeyine gönderilen araçlardır. ABD ve SSCB'nin ardından ÇİN 2013 yılında aya araç gönderen 3 ülke olmuştur. Stockholm Uluslararası Barış Araştırmaları Enstitüsü (SIPRI) Askeri Harcamalar veri tabanı göre ise 2015 yılında ABD'nin askeri harcama oranı 595 milyar dolarken Çin'in 215 milyar dolardır. Bu noktada Çin'in askeri harcama oranının %7,4'lük artmıştır (Deutsche Welle, 2016). Buna ilaveten Çin'in BRICS (Brezilya, Rusya, Hindistan, Çin ve Güney Afrika Cumhuriyeti) ülkeleri için etkisi göz ardı edilmemelidir. Zira Çin konumu sayesinde hem kendi bölgesinde hem de dünya siyaseti için önemli bir aktör konumuna yükselmiştir. Dolayısıyla ABD ve Çin arasındaki rekabet artık belirgin bir şekilde ortaya çıkmaktadır.

ABD ve Çin arasında siber alana yansıyan rekabet BM Siber Yönetim Yapısı'na da yansıyacaktır. 2004'ten beri Çin, BM'nin siber uzayda sorumlu devlet davranışlarını geliştirmeye yönelik Hükümet Uzmanlar Grubu (GGE)'nda yer almıştır. Ancak grup içerisinde Rusya ile kurulan yakın koordinasyon süreci dikkatleri çekmiştir. İlerleyen yıllarda ABD 2013 ve 2015'te 2 uzlaşma raporunun imzacısı olmuştur (UN Group of Governmental Experts/A/70/174, 2015). 2013 Raporu uluslararası hukukun ve BM Şartı'nın siber uzay ile temel ilişkisini açıklarken 2015 Raporu'nda devlet sorumluluğu, yardım etme yükümlülüğü, barış zamanında devletlerin CI sistemlerine kasıtlı olarak zarar verme ya da bozmanın engellenmesi ve başka bir devletin bilgisayar acil müdahale ekiplerini hedef almamayı baz alan ABD'nin tercih ettiği normlara yer verilmiştir (UN Group of Governmental Experts/A/68/98, 2013). Çin ve Rusya bu iki uzlaşma

raporunda ABD'nin pozisyonlarını destelemesine karşın 2015 GGE toplantısında ABD'nin BM Şartı 51. Maddesi'ndeki meşru müdafaa hükmüne atıfta bulunmasına karşı çıkmıştır (Segal, 2022). 2017 yılında GGE'nin bir diğer toplantısında uzlaşa sağlanamaması sonucu Çin, GGE'ye paralel olarak siber normların geliştirilmesi adına Müzakereye Açık Çalışma Grubu (OEWG) olarak adlandırılan yeni çalışma grubunu oluşturmuştur. Bu durumda Rusya, Çin'in destekleyicidir. GGE ve OEWG 2021 yılında benzer içeriklere sahip raporlar yayınlamışlardır. Ancak OEWG'nin raporunda silahlı çatışma durumunda sivilleri koruyan uluslararası insancıl hukuk terimine yer verilmemiştir (Efrony, 2021; Ponta, 2021). İnsancıl hukuka ait atıfların olmaması siber saldırıların meşrulaştırılması yorumunu gündeme taşımıştır.

3.3.1. ABD ve Çin Mücadelesinin Teknolojik Boyutu

ABD ve Çin arasındaki rekabetin teknolojik alana nasıl yansıdığı esasen aktörlerin ekonomik güçleri ile doğru orantılıdır. Mao Zedong döneminde Çin ekonomisi şu anki durumuna nazaran daha zayıf bir etkisiz bir durumdaydı. Bu durumun sebebi şüphesiz o dönemli Çin siyasetine dayanmaktadır. Çünkü Çin, Mao Zedong döneminde bilhassa ABD hegemonyasına ve politikalarının karşısındaydı. Çin 1970'li yılların sonlarına doğru uluslararası sisteme yavaş yavaş entegre olmuştur. Özellikle bu dönemde Çin'de gerçekleşen Kültür Devrimi'nin etkileri büyüktür. 1972 yılına gelindiğinde ABD Başkanı Richard Nixon'un Pekin'e olan ziyareti ise bu iki güç arasındaki diplomatik ilişkileri başlatan mihenk taşı olmuştur. Çin, bu ziyaret sonrasında ABD'den ticaret alanında destek almıştır. 1978 yılından sonra ise reform faaliyetlerine başlanmıştır. Deng Şiao Ping, sosyalist politikaları kapitalist önlemlerle ayakta tutmaya çalışmıştır. Bilhassa kapitalizme adapte olma süreci de başlamıştır (Van, 2018) Kapitalizme entegre olma sürecinden 2018 yılına kadarki kısımda Çin ekonomisi neredeyse %10 oranında artmıştır. Bu gelişim sosyal ve ekonomik açıdan ülkenin gelişimine olumlu katkıya sebep olmuştur. Çin'in ekonomik büyümesinin bir başka kanıtı ise Çin'in dünya ihracatındaki oranıdır. 1978 yılında bu oran %1 iken 2015 yılına gelindiğinde dünyadaki ihracatın %14,7'si Çin aracılığıyla gerçekleşmektedir. Bu noktada Çin'in Almanya ve Japonya gibi aktörleri de geride bıraktığı göz ardı edilmemelidir. 2009 yılından itibaren Çin, dünyanın en fazla ihracat faaliyetlerini gerçekleştiren aktörüdür (Athukorala, 2017).

Teknolojik gelişmeler ekonomi ekseninde gerçekleşmektedir. Çin, katma değerli ürün imalat sektörüne ve ihracatına önem vermiştir. Slikon vadisi olarak adlandırılan Şenzen şehrinde Alibaba, Baidu, Tencent ve Huawei vb dünyaca ünlü teknoloji firmalarına yer verilmiştir. Force'a ABD'nin 575 halka açık şirketi varken Çin ve Hong Kong'un 309 halka açık şirketi vardır. Çin, ABD'nin ardından hemen ikinci sırada kendisine yer edinmiştir. İkinci olarak yine dünyanın halka açık en büyük teknolojik şirketlerinin bulunduğu listede ise Çin 20 firma aracılığıyla yine 65 firmaya sahip ABD'nin ardından ikinci sıradaki yerini almıştır. 2019 yılına gelindiğinde Forbes dergisinin dünyanın halka açık en büyük şirketleri incelemesinde Çin'e ait ICBC bankası ilk sırada olup ilk 10 bankanın dört ismi yine Çin'e aittir (Force, 2013).

Çin'in %10'luk büyüme payı ülkeyi dünyanın ikinci en büyük ekonomik gücü haline getirmiştir. Ancak Çin ekonomisinin sahip olduğu bazı dezavantajlar vardı Orta gelir düzeyinin Çin için sorun olmasının yanı sıra ülkenin gelir adaletsizliği de hala devam etmektedir. Ayrıca hammaddeye erişim kapasitesi, üretim faaliyetleri sonucunda meydana gelen çevre sorunları etkin bir biçimde çözülmemiştir.

Çin ve ABD arasındaki rekabetin teknolojik boyutu siber tehditlere mücadele stratejilerini yansıtmaktadır. Çin tarafından ABD'ye yöneltilen siber tehditlerle mücadele edebilmek için öncelikle bu siber saldırıların tetikleyicisinin bulunması gerekmektedir. KDHC olarak adlandırılan siber tehdit istihbarat ekibi Same Cloak, More Dagger adlı bir çalışma yayınlamıştır. Bu çalışma sayesinde Çin'in siber saldırıları nasıl yönlendirildiği saptanmaya çalışılmıştır. Çin'in siber saldırılarını öngörmek ve yorumlamak, tehdit analistleri ve ana bilgi güvenliği görevlileri (CISO) için öngörüler ve uygulanabilir tavsiyeler, tehdit aktörleri ve taktiklerine ilişkin bir katalog ve son olarak Çin siber saldırılarının kuruluşları hedef alması veya etkileme kapasitesini arttıran faktörlere dikkat çekilmiştir. Amaçlanan husus ABD CI kuruluşlarının güvenlikleri ve dayanıklılığın arttırılmasıdır (China's Cyberattack Strategy, <https://www.boozallen.com>).

ABD'deki çeşitli enstitüler ve devlete bağlı kuruluşlar Çin'in ABD ve diğer ülkelerdeki siber casusluk faaliyetlerini ifşa etmiştir. Mandiant Raporu, ifşa edilen bilgiler arasında oldukça popülerdir. CISA'nın da Çin'in kötü amaçlı siber faaliyetleri hakkında çeşitli raporlar yayınlamıştır. Çin ise bu suçlamaları kendisini kötülemeye yönelik girişimler olarak görmektedir. Örneğin Çin destekli Global Times, ABD'nin Çin'i kötüleme girişimlerine dikkat çekmiştir. Ayrıca Çin Uluslararası Çalışmalar Enstitüsü (CIIS) 2020 yılında yayınladığı makalede, Qihoo 360 Raporu'nun ardından ABD'yi siber güvenlikte ikiye bölme ile suçlamıştır. Çin ABD'nin suçlamaları karşısında sessiz kalmaktadır. Ancak 2020'de Çin Dışişleri Bakanlığı'nın ABD'yi bir hacker imparatorluğu olarak tanımlamasının ardından bu durum değişmeye başlayacaktır. Çin'in Qihoo 360 Raporu, Ulusal Bilgisayar Ağı Acil Müdahale Teknik Ekip (CNCERT) Raporu ve Qi An Pangu Lab Raporu'nun yayınlaması, esasen ABD'ye karşı değişen stratejisidir. Ayrıca Pangu Lab Raporu aracılığıyla NSA'nın Hindistan, İngiltere, Avustralya, Japonya ve diğer birçok ülkeye sızdığı belirtilmiş olup ABD'nin müttefiklerine karşı kötü niyetli siber saldırılara maruz bıraktığı ön plana çıkarılmıştır (Pardhi, 2022).

Washington ve Pekin arasındaki suçlamaların harareti giderek artacaktır. Pekin, Washington'un kendisini ABD işletmeleri ve devlet kurumlarına karşı siber saldırı düzenlemesini reddedecektir. Ulusal Bilgisayar Virüsü Acil Müdahale Merkezi (CVERC)'nin yayınladığı bir raporda NSA Çin'deki ağ hedeflerine binlerce saldırıyla suçlarken bu raporda özellikle NSA'nın Özel Erişim Operasyonları Ofisi (TAO)'nin Xi'an kentindeki Kuzeybatı Politeknik Üniversitesi'ndeki bilgileri ele geçirmeyi hedeflediğine yer verilmiştir. Washington ise Pekin'i Microsoft'un e-posta yazılımına yönelik, yerel yönetimler de dahil olmak üzere en az 30.000 ABD

kuruluşunu ve diğer ülkelerdeki müşterileri etkileyen saldırılar için suçlamaya devam etmiştir (China Accuses US of 'Tens Of Thousands' of Cyberattacks, 2022).

Çin ve ABD arasındaki rekabetin yansıdığı bir başka boyut ise askeri kapasitelerle ilişkilendirilebilir. Çin Komünist Partisi (ÇKP)'nin 2035 yılı Ulusal Ekonomik ve Sosyal Kalkınma ve Uzun Vadeli Hedefler için 14. Beş Yıllık Planı'nda siber güce dönüşme arzusunu ifade etmiştir. Bu noktada PLA ön plana çıkmaktadır (CSET, 2021). 2015 PLA yeni siber çağa uygun reformlar için önemli bir yıldır. Xi Jinping, 2015-2016'da ordunun ÇKP'ye bağlı kalması için birtakım reformlara yer vermiştir. 2015 yılında Çin Askeri Strateji Beyaz Kitabı aracılığıyla siber alanda ÇKP'nin bir güç unsuru olacağından bahsedilmiştir. 2015 ve 2016 yılındaki bu reformların bir sonucu olarak Stratejik Destek Gücü (SFF) oluşturulmuştur. SSF'nin öncelikli hedefi enformatize savaş doktrinini desteklemek için bilgiye erişim ve çatışmanın başında düşmanı alt etmek için düşmandan yararlanmaktır. Bu süreç Xi Jinping'in 2019'daki enformatize savaştan akıllı savaşa geçişi yansıtacaktır. 2017 Çin Siber Güvenlik Yasası, ÇKP'nin siber egemenlik vizyonunu düzenlemesini somutlaştıracaktır. Bu noktada Çin telekomünikasyon ve teknoloji şirketleri de hükümete bilgi vermelidir. 2021 yılına gelindiğinde ise Çin süper güç olabilmek için Siber Güvenlik Merkezi (NCC) merkezi Wuhan olan enstitünün açılmasını emretmiştir. ABD'nin Çin karşısında stratejik gücü kendisine avantaj sağlayabilir. Ancak ABD yerel özel ve kamu sektörlerinin iş birliği yapması ve ülkenin CI sistemlerini dijital sisteme entegre ederken siber güvenlik ekseninden ayrılırsa Çin, ABD karşısında sadece bir rakip olarak kalmayabilir (Evaluating China's Road to Cyber Super Power (t.y.), <https://nsiteam.com>).

Çin askeri birimleri iç ve dış istihbarat teşkilatı Devlet Güvenlik Bakanlığı personeli tarafından desteklenmektedir. Bu personeller PLA'nın 3. Departman olan Teknoloji Keşif Departmanı ve 4. Departman olan Elektronik Karşı Önlemler ve Radar Departmanı'nı oluşturan siber uzmanlardır (The U.S.-China Economic and Security Review Commission, 2019). Çin'in askeri kabiliyetleri, ABD hükümet sistemleri dahil olmak üzere dünya çapında çok sayıda bilgisayar sistemini hedef alabilir. Bu erişim kapasitesinin büyüklüğü stratejik ve askeri fayda sağlayan verinin dışarıya sızmasını kolaylaştıracaktır. Buna ilaveten Çin siber ajanları ABD'nin elektrik şebekesi, su ve kanalizasyon hizmetleri, finans ve hava trafik kontrol gibi ağa bağlı CI sistemlerini mantık bombaları olarak anılan kötü niyetli kodlamalar aracılığıyla tehdit etmektedir (Gorman, 2009). Clarke, Richard Alan'a göre Çin'in siber kabiliyetindeki hızlı gelişmesine rağmen siber saldırı alanında ABD'nin rakibi olarak görülemez. Çünkü Washington siber alanda uzun zamandır saldırı üstünlüğünü muhafaza etmektedir. DARPA, Pentagon'un ABD saldırı üstünlüğünü koruması için siber silahların test edilmesine imkan sağlamak amacıyla Cyber Range'i işletmeye başlamıştır. Ancak burada Çin ve ABD'nin siber yetenekleri savunma noktasında denk sayılabilir. Çünkü ABD'nin siber savunma sistemi diğer ülkelere kıyasla daha zayıftır (Clarke ve Robert, 2014; Manson, 2011).

3.3.2. ABD ve Çin'in Siber Alana Yönelttiği Saldırgan Politikaları

Kimin daha saldırgan olduğunu anlayabilmek için ABD ve Çin'in askeri kapasiteleri analiz edilmelidir. Çin için PLA siber savaş durumunda bilgi üretme, toplama, iletme, analiz etme ve kullanma da en etkili araçtır. Aynı zamanda PLA, Hindistan'a yönelik siber operasyonları yürüten kurumdur. Dikkat edilmesi gereken nokta Batı'dan farklı olarak siber ağ ve operasyonlar açısından PLA dijital savaş kavramını önemsemektedir. Temel hedef savaş gücü ve caydırıcılık için AI aktif bir şekilde yararlanmaktır. PLA 2015 yılında SSF birimini siber casusluk ve sinyal istihbarattan sorumlu keşif büroları (TRBs) ve CI sistemleri dahil olmak üzere düşman sistemini bozmak veya hasar görmesi amacıyla oluşturmuştur. 4/PLA aracılığıyla Çin'in daha önce birbirinden farklı siber, elektronik, uzay ve psikolojik savaş birimleri SSF sayesinde birleşik bir komuta yapısı altında birleştirilmiştir. SSF aracılığıyla PLA, merkezileştirilmiş olup elektronik harp siber uzay ve psikolojik savaşa entegre edilmeye çalışılmıştır (Mallick, 2022). Konuyu bir başka açıdan ele alacak olursak Uluslararası Stratejik Araştırmalar Enstitüsü (IISS) Siber Güvenlik adlı bir rapor yayınlamıştır. 2020 yılında yayınlanan bu rapora göre ülkelerin siber alandaki kapasiteleri ve ulusal gücü tartışılmıştır. Raporda ilk 15 ülke incelendiğinde ABD birinciyi sırayı alırken Çin ABD'den sonra 2. sıradadır. İngiltere, Rusya, Hollanda, Fransa, Almanya, Kanada, Japonya, Avustralya, Kuzey Kore, İsrail ve Hindistan diğer ön plana çıkan ülkelerdir. Yurtdışında büyük çapta siber operasyonların (casusluk ve siyasi nüfus kurmak gibi) yürütülmesi, dünyanın en kapsamlı siber gözetleme ve izleme sansür sistemi, dijital teknolojiye endüstriyel kapasitesi dikkate alındığında Çin, IISS'ye göre ABD'yi geride bırakmıştır. Ancak temel siber savunma sistemlerinde ABD'ye nazaran Çin daha zayıftır (Voo vd., 2020).

ABD ve Çin arasındaki rekabette dikkat edilmesi gereken 3 husus vardır. Öncelikle ABD, Çin karşısında 5G telekomünikasyon ekipmanları gibi önemli teknolojilerde öndedir. Bu sebeple Çin karşısında daha fazla kısıtlayıcı önlemlere ihtiyaç duyulsa da ABD kendi teknoloji alanlarını daha fazla bölgesel olarak genişletmemelidir. İkinci olarak Washington küresel teknoloji ticaretine yön vermek isterken vizyonu net değildir. Çin tekno-otoriterliğinin karşısında durmalıdır. Çin'e karşı askeri üstünlük sağlanması, Çin destekli sabotaj ve nüfus operasyonlarını önlemek için gerçekçi hedefler belirlemelidir. Son olarak ise saldırgan olarak nitelendirebileceğimiz siber alanda etkili olma faaliyetleri için ABD teknoloji liderliğini, rekabet gücü ve dayanıklılığını devam ettirmek için uzun vadeli bir potansiyele sahiptir. Ancak ABD askeri güçlerinin siber alana entegre sürecinin yavaş olmasının yanı sıra ulusal siber güvenlik ve veri gizliliği standartlarını koruyan merkezci bilgi ekosistemi de siyasi iraden de yoksun bırakılmıştır. ABD'nin güvenliği ve ferahı için Çin'in yükselişi siyasi açıdan koz olarak kullanılabilir (Bateman, 2022).

ABD ve Çin arasındaki rekabette kimin daha saldırgan olduğunu analiz etmek kolay değildir. Ancak kamuoyuna yansıtılan siber saldırılar noktasında Çin, ABD'ye kıyasla daha fazla ön plandadır. Örnek verecek olursak Mandiant Raporu'nda Çin destekli hacker grubu ABD'de deki en

az 6 eyalette siber saldırılar gerçekleştirmiştir. Bu konudaki tüm suçlamalar Çin APT41'e yöneltilmiştir (Kharpal, 2022). Elbette son zamanlarda Çin, ABD tarafından kendisine yöneltilen suçlamalar karşısında daha etkin bir biçimde duracaktır. Çin, Internet Security Company 360 Raporu'ndan edindiği bilgiye göre NSA'nın 47 ülkeyi hedef alan siber saldırıları 10 yılı aşkın bir süredir faali olduğu üzerinde durmuştur. Bu noktada özellikle Çin devlet daireleri, yüksek teknoloji şirketleri, ordu, finans, bilimsel araştırma enstitüleri, iletişim operatörleri hedef alınmaktadır. NSA belgelerinde yer alan sahte sunucu FOXCID kod adlarına göre siber saldırılar İngiltere, Almanya, Fransa, Güney Kore, Polonya ve İran olmak üzere dünya çapında bahsi geçen 47 ülkeden 403 hedef tespit edilmiştir. Ayrıca 2004 yılında kurulan QUANTUM saldırı sisteminin NSA'nın en güçlü saldırı aracı olduğu unutulmamalıdır. QUANTUM sayesinde küresel ağ iletişim ve internet sisteminden ele geçirilen veriler işlenebilmektedir (Lingzhi, 2022).

Çin ve ABD arasındaki rekabetin ülkelerin gelişim kapasitelerine olan katkısına rağmen bu durumun potansiyel saldırıyı da tetiklediği unutulmamalıdır. ABD içerisinde bilhassa saldırgan realizm taraftarlarına göre ABD ve Çin'in çatışmama ihtimali yoktur. John Mearsheimer'e göre, zaman içerisinde Çin, ABD karşısında yerini alan en güçlü rakip olacaktır. ABD Savunma Bakanlığı'nın yayınladığı raporlarda bu durum açıkça ifade edilmektedir (Huisken, 2009). Soğuk Savaşın sona ermesinden bu yana ABD'nin karşısında yer alabilecek tehdit unsurlarının tespiti ABD güvenliği için oldukça önemlidir. Çünkü bu küresel düşmanın ortaya çıkışı hegemon devlet anlayışını ve dünya siyasetini etkileyecektir.

ABD karşısında yükselen bir güç olarak karşımıza çıkan Çin, iç politika konularında Batı'dan ayrılmaktadır. Bu durum ABD'nin Asya'daki çıkarlarının hedef alınabileceğini gösterecektir. Çünkü Çin ve ABD'nin rekabet yöntemleri farklıdır. ABD Kongresi'nde sunulan raporda Çin ve Rusya'nın ortak payda da buluşmalarının oluşturacağı tehditler üzerinde durulmuştur. Olası bir politik birleşme ABD'nin sahip olduğu hegemon güç algısını direk hedef alacaktır. Yine aynı raporda ABD'nin Rusya ve Çin'in demokrasi ve insan hakları gibi bazı kavramlara riayet etmediklerinin üzerinde durulurken mevcut ekonomik düzenin işleyişinin de tehdit edilmesi ön plana çıkarılmıştır. Özellikle bu iki aktörün aktif askeri faaliyetlerine yer vermelerinin yanı sıra ABD karşıtı otoritelerin desteklenmesi noktasında BM Güvenlik Konseyi'ndeki oylamalara dikkat çekilmiştir (Report to Congress of the U.S.-China Economic And Security Review Commission).

ABD için Çin'in Batı'ya ait değerler olan demokrasi ve insan hakları vb kavramlarının karşısında yer aldığı düşüncesi hakimdir. Çin'in devlet rejiminin diğer devletlerin yönetim biçimlerine göre daha otoriter olduğu açıktır. ABD için bu otoriter tavır kesinlikle bir tehdit ve risk unsurudur. Çin'in yönetim biçimi otoriter olarak değerlendirildiği için demokrasi ilkelerinden uzak, çoğulcu anlayıştan yoksun ve sınırlandırılmış özgürlüğü savunan bir devletin ekonomik gücü ve başarısı uluslararası arena için tehdit olarak görülmüştür. Özellikle Çin'in ideolojik yapısına olan bağlılığı Batılı güçleri karşısına alma olasılığını da güçlendirmektedir. Örnek verecek olursak 2016

yılında kurulan Asya Kalkınma Bankası vb çok uluslu iktisadi kurum ve kuruluşlar sayesinde Dünya Bankası ve Uluslararası Para Fonu gibi yapılanmaların etkinliğini kıracak alternatifler oluşturulmuştur (Bechna ve Thayer, 2016).

Burada ABD mi yoksa Çin'in mi daha saldırgan politikaları izlediğini saptamak kolay değildir ancak taraflara göre karşı aktör saldırgan olarak nitelendirilecektir. Buradaki temel nokta hangi aktörün daha fazla saldırgan politikaları takip etmenin ötesinde siber alanın hangi tarafın kontrolünde olacağıdır. Çünkü bu yeni alan hegemon devlet olma anlayışını uluslararası arenaya yansıtacaktır.

3.3.3. ABD'nin Uluslararası İş Birlikleri ve Baskınlığı, NATO Örneği

Uİ disiplini içerisinde aktör sayısına bağlı birçok analiz mevcuttur. Bu analizler içerisinde Soğuk Savaş Dönemi iki kutuplu olarak ele alınmıştır. Bu dönemdeki hadiseler siyah ya da beyaz olarak nitelendirilen ABD ve SSCB arasındaki rekabet neticesinde incelenmiştir. Bu rekabet daha çok konvensiyonel silahlar aracılığıyla gerçekleşmiştir. Klasik silahlanma düzeni ilerleyen dönemlerde bilhassa II. Dünya Savaşı esnasında kullanılan atom bombaları sayesinde değişmiştir. Nükleer silah kapasitelerinin konvensiyonel silahlara nazaran daha fazla etkiye sahip olduğu onaylanmıştır. Uluslararası arena için SSCB ve ABD arasındaki gerilimin siyah ya da beyaz olarak nitelendirilen bu dönemde bilgi savaşlarının ön plana çıkması, geleneksel bakış açısını sekteye uğratmıştır. Özellikle teknolojik gelişmeler sayesinde fiziksel sınırlar geçerliliğini yitirmiştir. Soğuk Savaş sonrasında tecrübe edilen bilgi çağı ve ön görülemez teknoloji boyutunun temelleri de yine bu dönemde atılmıştır. Bilişim alanındaki yaşanan gelişmeler hem olumlu hem de olumsuz yönleriyle kendini göstermiştir. Toplumsal yaşamın kolaylaşmasının yanı sıra küresel alanda meydana gelen yeni tehdit unsurları devletlerin dikkatlerini çekmektedir. Ulusal Strateji Belgelerinde, başkanlık direktiflerinde ulusal güvenliğin sağlanması için bu yeni tehdit unsurlarına karşı alınacak olan önlemler üzerinde yoğunlaşmıştır.

Ulusal güvenliği tehdit eden bu yeni unsurların varlığı siber kavramını ön plana çıkarmaktadır. Siber alan fiziki şartların geçerliliğinin kalmadığının kanıtıdır. Çünkü siber ortam, hava, kara, deniz ve hatta uzayın ötesindedir. Siber ortam fiziksel, dizimsel ve semantik katmanlardan meydana gelmektedir (Libicki, 2009). 1999 Kosova Savaşı'nda NATO, Sırp kuvvetlerini hedef aldığı ilk kez siber saldırıyı tecrübe etmiştir. DDoS ve diğer zararlı virüsler aracılığıyla NATO'nun birimleri ve üyelerinin iletişim faaliyetleri hedef alınmıştır. Kara El (Black Hand) ismiyle ortaya çıkan Sırp hackerlere Rus ve Çinli hackerlardan destek gelmiştir. Bu destek BM Güvenlik Konseyi Daimî Üye statüsüne sahip olan Rusya ve Çin tarafından Konsey'in kararı olmaksızın verilmiştir (BBC News, 1998). İlk başlarda NATO için bu saldırılar sadece uyarı niteliğindeyken 9/11 saldırılarından sonra NATO'nun bakış açısı tamamen değişmiştir. Çünkü küresel terör tehdidi olarak nitelendirilen 9/11 saldırıları sonrasında uluslararası arena da karmaşa

ve kaos hakimdir. Bu noktada 9/11 saldırılarının elektronik ya da dijital Pearl Harbour tehdit olasılığı gündeme gelmiştir (Mitchell, 2001).

NATO, bu saldırılar karşısında önlem alabilmek için NATO'nun güvenlik politikalarının revize edilmesini gündeme getirmiştir. 21 Kasım 2002 tarihinde Prag'da düzenlenen Zirve'de teknik hususlar üzerinden siber saldırılara karşı alınacak önlemlerin altı çizilmiştir. Elbette bu noktada NATO'nun yaklaşımı daha çok askeri kapasite ekseninde değerlendirilmiştir. NATO Siber Savunma Programını ilan etmiş olup NATO Bilgisayar Olaylarına Müdahale Birimi (NCIRC) oluşturmuştur (NATO, 2002).

2007 yılına gelindiğinde ise NATO'nun siber güvenlik algısında köklü bir değişim 1947'de Kızıl Ordu'nun Tallinn'e girişinin sembolü olan Tallin'in Kurtarıcısı heykelinin yerinin değişmesi ile başlamıştır. Estonya için bu heykel 50 yıllık Rus işgalinin somut halidir. Ancak Rus kökenli nüfus aynı görüşü benimsememiştir. 26 Nisan 2007'de bu iki taraf karşı karşıya gelmiştir. Buradaki en önemli nokta Estonya halkının %75'inin internet erişim kapasitesidir. Çünkü Estonya'da gerçekleştirilen saldırıların ardından kritik altyapıların önemi ortaya çıkmıştır. Finans kurum ve kuruluşlarına yapılan saldırılar sonucunda kritik altyapıların önemini vurgulamıştır (Bıçakçı, 2014). 2008 yılında NATO'nun bir diğer Zirve'si Bükreş'te olup bilişim sistemlerinin güçlendirilmesi ve Brüksel'de NATO Siber Savunma Yönetim Ofisi (CDMA) kurulması için kararlar alınmıştır. Dolayısıyla 2008 yılında Estonya, Almanya, İtalya, Letonya, Litvanya, Slovakya ve İspanya'nın aracılığıyla NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (CCD COE) kurulmuştur (Ada, 2018). 2009 yılına gelindiğinde ise Güney Osetya hadisesinde Rusya ve Gürcistan çatışmaya siber saldırılar aracılığıyla müdahale söz konusudur. NATO bu olay neticesinde Hibrit savaş kavramından bahsederken DDos saldırı faaliyetleri NATO'yu daha etkin politikalara itmiştir. NATO, siber saldırılara maruz kalan ülkelere yardım amacıyla Hızlı-Tepki Takımlarını (RRRTs) kurmuştur (Bıçakçı, 2012). 2009 yılında tecrübe edilen bir başka gelişim de Strazburg-Kehl Zirvesi'dir. Bu zirvede geleceğe yönelik stratejik gelişmeler üzerinde durulmuştur (NATO, 2010). İlerleyen yıllarda 2013 yılında Cambridge Üniversitesi aracılığıyla siber savaş esnasında uygulanacak hukuk hakkında Tallinn El Kitabı'dır. Bu belge aracılığıyla NATO CCDCCOE Uluslararası Bağımsız Uzmanlar Grubu'na uluslararası hukuk ve normların siber alana nasıl entegre edilebileceğinin üzerinde durulmuştur (Schmitt, 2013).

NATO'nun temel amacı aslında siber alanda profesyonelce düşünürken kollektif katılım aracılığıyla stratejilerini gerçeğe dönüştürmektedir. Bu noktada Cyber Coalition dünya da ön plana çıkan siber kolektif savunma tatbikatlarını planlayan ve bu tatbikatları yürüten Müttefik Dönüşüm Komutanlığı'na bağlı bir yapılanmadır. Siber Koalisyon NATO Askeri Komite bünyesinde yer almaktadır. Bu koalisyon dünyanın dört bir tarafından gelen 31 NATO müttefiki ve AB'den yaklaşık 1.000 katılımcı içermektedir.

Siber Koalisyon 2008 yılından bu yana ittifakın siber uzaydaki tehditleri caydırma, tehditlere karşı savunma ve karşı koyma kapasitesinin artırılmasını baz almaktadır. Siber Koalisyon tatbikatları, Tallinn'in NATO Müttefikleri ve Ortaklarını destekleyen en yeni siber organı olan Estonya Siber Güvenlik Tatbikatları ve Eğitim Merkezi veya CR14 sayesinde yürütülmektedir. NATO İletişim ve Bilgi Ajansı, İşbirliğine Dayalı Siber Savunma Mükemmeliyet Merkezi, Müşterek Harp Merkezi, Brunssum Müttefik Müşterek Kuvvet Komutanlığı ve NATO Karargahı, endüstri ve akademiden çok sayıda kuruluş da bu tatbikatlara katılmaktadır. 2021 yılında yapılan Siber Koalisyon aracılığıyla gaz tedarik boru hatlarına yönelik bir siber saldırı; birliklerin ve lojistiğin konuşlandırılmasını sekteye uğratan bir siber saldırı ve aşırı verilerinin çalındığı ve aşılama programlarının tehlikeye girdiği pandemiyle ilgili bir fidye yazılım gibi konular gündeme gelmiştir. 2022 Siber Koalisyon Estonya'da yeniden bir araya gelmiştir (Cyber Coalition: NATO's Flagship Cyber Exercise (t.y.), <https://www.act.nato.int/cyber-coalition>). Siber alandaki iş birliği ve tehditler karşısında alınacak önlemler noktasında NATO ön plandadır. Örnek olarak NATO Genel Sekreteri Jens Stoltenberg 2022 tarihinde Roma'da düzenlenen Siber Savunma Taahhüdü Konferansı'nda Rusya'nın Ukrayna'ya karşı yürüttüğü yasadışı savaşın bir parçası olarak uydulara, CI sistemlerine ve devlet dairelerine karşı gerçekleştirilen siber saldırılar üzerinde durmuştur. Bu noktada NATO devletlerden ya da devlet dışı aktörlerden kaynaklanan siber uzay tehdidini ciddiye almaktadır. 2016 yılında NATO'nun Varşova Zirvesi'nde kabul ettiği Siber Savunma Taahhüdü sayesinde müttefikler siber savunmaya daha fazla para, uzmanlık ve iş birliği açısından siber savunma kavramını ele almaktadır (NATO Secretary General Warns of Growing Cyber Threat (2022), https://www.nato.int/cps/en/natohq/news_208889.htm?selectedLocale=en).

Uluslararası alanda iş birliği daha çok ortak çalışmanın mantığını, neden, ne zaman ve nasıl iş birliği yapılacağı üzerinde temellendirilir. Örnek verecek olursak BM 1.Komitesi uzun yıllardır uluslararası güvenlik bağlamında bilgi ve telekomünikasyon alanındaki gelişmeleri aktif bir şekilde incelemektedir. Buna ilaveten Afrika Birliği bilhassa Afrika siber güvenliği için güvenilir bir yasal çerçeve oluşturulmasına ilişkin Afrika Birliği Sözleşme Taslağı'nı yayınlamıştır. AB ise AB'nin siber güvenlik stratejine ilişkin bir ortak bildiri yayınlamıştır. 27 üye ülkenin tamamı siber güvenlik konusundaki ortak görüşünü AB bünyesinde ilk kez bu bildiri de belirtmiştir. Uluslararası arenanın siber güvenliğe karşı ilgili açıktır. Ancak siber güvenlikle ilgili acil sorunlar için bir ulusal mevzuat kabul edilmeli ve bu mevzuatın uygulanmasının çok taraflı ilkelerin uygulanmasına bağlı olduğu unutulmamalıdır.

NATO, CCD COE aracılığıyla siber savunma alanındaki kabiliyet, iş birliği ve bilgi paylaşımının gelişmesini hedeflemektedir. Bu noktada CCD COE sadece NATO ve AB kuruluşlarıyla daha geniş bir iş birliği sağlamamaktadır aynı zamanda daha spesifik olarak Locked Shields adlandırılan gerçek zamanlı bir ağ savunma tatbikatına sponsor ülkeler aracılığıyla yer vererek iş birliği sürecini pratikleştirmektedir. Burada CCD COE iki temel eğilim saptamıştır. Birincisi siber güvenlik stratejilerini giderek daha fazla ülke benimsemekte olup çoğusu siber

güvenliği ulusal güvenlik bağlamında değerlendirmektedir. Ulusal Siber Güvenlik Çerçevesi El Kitabı'nda bu stratejiler karşılaştırılmaktadır. İkincisi ise hukukun siber güvenliğe nasıl entegre edileceğidir. Siber uzayın kara, deniz ve hava gibi korunması gerekmektedir (Talihärm, 2013).

2008'de CCD COE'nin kurulması, 2012 Chicago Zirve'nde ittifakın siber savunmanın arttırılması, 2014 Galler Zirvesi'nde siber uzayda uluslararası hukukun geçerliliğin kabul edilmesi, 2016 Varşova Zirvesi'nde siber uzayın kara, deniz ve hava alanları da savunulmasının vurgulanması, 2018 Zirvesi'nde müttefiklerin ilk kez siber tehditleri caydırmak ve savunmak için tüm yeteneklerin kullanılmasının onaylanması ve 2020 Siber Uzay Operasyonları için Müttefik Ortak Doktrini'nin yayınlanması gibi birçok adım siber alandaki iş birliğinin önemi göstermektedir. NATO için kolektif hareket etmek için dört eylem planı belirlenmiştir. Bunlar; mahremiyetin atıf yoluyla ortadan kaldırılması ve gizli hareket etmenin zorluğunun gösterirken siber saldırı sorumluluğunun vurgulanması, NATO'nun kötü niyetli siber eylemlere karşı müttefik tepkilerinin netleşmesi için mevcut krizin kullanılması, yerel CI sistemlerinin dayanıklılığının oluşturulması ve siber güvenlik alanında stratejik öneme sahip ülkeler için siber kapasite oluşturma çabalarını arttırmaktır (Maigre, 2022).

İnternet yoluyla işlenen suçlara (telif hakkı ihlalleri, bilgisayarla ilgili sahtekarlıklar, çocuk pornografisi ve ağ güvenliği ihlalleri gibi) dair ilk uluslararası antlaşma Budapeşte Avrupa Konseyi Siber Suç Sözleşmesi'dir. Antlaşma 2001'de yürürlüğe giriş olup ABD, Kanada, Japonya ve Güney Afrika'nın müzakereleri sonucu geliştirilmiştir. 47 ülke bu antlaşmaya taraf olup diğer devletlerin imzasına açıktır. Bu nokta da Budapeşte Sözleşmesi gibi bir sözleşmenin siber güvenlik konusunda uluslararası iş birliğine katkıda bulunmak için geliştirilip geliştirilemeyeceği gündeme getirilebilir. Siber uzay ile belirlenen yasaları uyumlu hale getirmek, farklı yorum ve yaklaşımları ortak değerlerle entegre etme girişimleri mümkün olabilir. Değerler ve çıkarlar uluslararası iş birliğinde en başta gelmektedir. Ancak siber güvenlik söz konusu olduğunda sonuçlar o kadar geniş ki koordine edilmesi oldukça zordur. Belki devletler için bu kadar önemli olan bir alanda daha adil ve kapsayıcı normlar geliştirilebilir. Bu noktada geliştirilen normların büyük güçlerin etkisinde olmaması gerektiği önemlidir (Carr, 2016).

3.3.4. Çin'in Siber Alanda Gelişen Ekonomisi ve Yatırımlar

ABD ve Çin arasındaki rekabetin teknolojik alana nasıl yansıdığı esasen aktörlerin ekonomik güçleri ile doğru orantılıdır. Bu noktada öncelikli olarak ABD ve Çin'in ekonomik kapasiteleri hakkında bilgi sahibi olmak gerekir. Mao Zedong döneminde Çin ekonomisi şu anki durumuna nazaran daha zayıf bir etkisiz bir durumdaydı.

Bu durumun sebebi o dönemli Çin siyasetine dayanmaktadır. Çünkü Çin, Mao Zedong döneminde bilhassa ABD hegemonyasına ve politikalarının karşısındaydı. Çin 1970'li yılların

sonlarına doğru uluslararası sisteme yavaş yavaş entegre olmuştur. Özellikle bu dönemde Çin'de gerçekleşen Kültür Devrimi'nin etkileri büyüktür. 1972 yılına gelindiğinde ABD Başkanı Richard Nixon'un Pekin'e olan ziyareti ise bu 2 güç arasındaki diplomatik ilişkileri başlatan mihenk taşı olmuştur. Çin, bu ziyaret sonrasında ABD'den ticaret alanında destek almıştır. 1978 yılından sonra ise reform faaliyetlerine başlamıştır.

Deng Şiao Ping, sosyalist politikaları kapitalist önlemlerle ayakta tutmaya çalışmıştır. Bilhassa kapitalizme adapte olma süreci de başlamıştır. Kapitalizme entegre olma sürecinden 2018 yılına kadarki kısımda Çin ekonomisi neredeyse %10 oranında artmıştır (Van, 2018).

Bu gelişim sosyal ve ekonomik açıdan ülkenin gelişimine olumlu katkıya sebep olmuştur. Çin'in ekonomik büyümesinin bir başka kanıtı ise Çin'in dünya ihracatındaki oranıdır. 1978 yılında bu oran %1 iken 2015 yılına gelindiğinde dünyadaki ihracatın %14,7'si Çin aracılığıyla gerçekleşmektedir. Bu noktada Çin'in Almanya ve Japonya gibi aktörleri de geride bıraktığı göz ardı edilmemelidir. 2009 yılından itibaren Çin, dünyanın en fazla ihracat faaliyetlerini gerçekleştiren aktörüdür (Athukorala, 2017).

Çin'in ekonomik kalkınma da gösterdiği gelişim şüphesiz gör ardı edilemeyecek bir başarıdır. Ancak Uİ disiplini içerisindeki en önemli aktör olarak kabul edilen devletlerin sadece ekonomik alandaki kapasiteleri yeterli değildir. Bu noktada politik, sosyal, kültürel ve diğer alanlarda da ön plana çıkmaları gerekmektedir.

Bilgi teknolojisinin sürekli gelişmesi ve veri korumanın öneminin artmasıyla birlikte yerel siber piyasası da gelişmeye başlayacaktır. Ayrıca siber güvenlik noktasında yaşanan bu evrimin işletmeler ve kuruluşlara sayısız fırsat sağladığı da göz ardı edilmemelidir. Çin için ulusal verilerin güvenliği dair endişeler be dijital ekonomi de daha fazla kişisel verinin korunma ihtiyacı da siber yeteneklerin gelişimini zorunlu kılmaktadır. Örnek olarak 2021'de Çin'in siber güvenlik pazar ölçeği 2020 yılına nazaran 9,5 milyar RMB (1,3 milyar ABD doları) artışla 62,7 milyar RMB'ye (8,64 milyar ABD doları) ulaşmıştır. Bu büyüme oranı 2020 yılına kıyasla %17'dir. Bu oran ÇİN politik uyum ve endüstriyel iyileşmeden kaynaklanmaktadır. 2022 yılında Çin'in siber güvenlik pazar gelirinin 14,05 milyar ABD dolarına ulaşması beklenmekteydi. Siber alana ayrılan bölüm değerlendirildiğinde 9,42 milyar ABD doları hacmiyle bu oran en büyük pazar segmentini temsil etmektedir. Buna ilaveten MIIT 2021 politika planında telekomünikasyon gibi önemli sektörlerin 2023 yılına kadar BT yükseltme bütçelerinin %10'unu siber güvenliğe ayırmalarını zorunlu kılmıştır. Buna ilaveten Çin aynı yıl siber güvenlik sektörünün 250 milyar RMB'den (38,6 milyar ABD doları) fazla bir değere ulaşacağını öngörmektedir (Interesse, 2022).

MIIT, 2021-2023 yıllarını hedef alan siber güvenlik sektörüne 38,6 milyar ABD doları ayırdığı politikası Çin'in yıllık bileşik büyüme oranının %15'inden fazlasıdır. Plana göre Çin siber

güvenlik için çeşitli temel teknolojilerinde atılım yapacaktır ve 2023 yılına kadar ilerlemesini sürdürecektir. Buna ilaveten güvenlik korumasının sınıflandırılmasını ve diğer üretim işlevlerini daha da optimize etmek için veri güvenliği teknolojisinin araştırılması ve uygulanması güçlendirilmelidir (Xinyi ve Hongpei, 2021).

Siber alandaki ABD ve Çin rekabeti birçok alana yansayacaktır. Örnek olarak Xi Jinping Paulson Enstitüsü'nde, Apple Inc İcra Kurulu Başkanı Tim Cook ve Berkshire Hathaway'den Warren Buffett'ın da bulunduğu Seattle'daki ABD'li iş adamlarını ziyaret etmiştir. Boeing dünyanın en büyük uçak üreticisi, Çin'de 38 milyar dolar değerinde 300 uçaklık büyük bir sipariş vermiştir. Bu teklif dönemin başkanı Donald Trump'ın öfkesine yol açmıştır. Çin'de açılması beklenen tesisin Washington eyaleti için 737 üretimdeki istihdamı azaltacağı iddia edilmiştir. Bu noktada ABD'li yatırımcılar, telekomünikasyon ve finansal hizmetler gibi devletin hakim olduğu sektörlerle daha fazla erişim sağlayacak ikili bir yatırım anlaşmasını talep etmesi Çin'e karşı güven problemlerinin devam ettiğini göstermektedir. Ancak Xi Jinping, Çin reformlarının önemli bir parçasının, yabancıların yatırım yapamayacağı alanları daraltmak olduğunu belirtmiştir. Çin açık ve hukuk normlarının geçerli olduğu daha fazla yatırım alanlarına istekli olduğunu belirtmiştir (Martina, 2015).

Çin'in siber alandaki yatırımlarının uluslararası arenadaki diğer aktörler için nasıl tehdit oluşturabileceğine değinilecektir. Bu durumu iyi açıklayabilmek için Birleşik Arap Emirlikleri ve Türkiye örneğinden yola çıkılacaktır. 2010 yılında Çin, BAE'den 64.500 ton sıvılaştırılmış doğal gaz ithal etmiştir. Bu ithalatın değeri 23 milyon doları aşmıştır. Buna ilaveten Çin Petrol Mühendislik ve İnşaat Anonim Şirketi (CPECC) şirketi, Abu Dabi'nin Habshan'daki ihracat terminallerine günlük 1,5 milyon ham petrol taşıyan Abu Dabi Ham Petrol Projesi'ne yardım etmiştir. Bu boru hatlarıyla taşınan petrol İran'ın olası askeri saldırıya uğraması durumunda birçok kez kapatmakla tehdit ettiği Hürmüz Boğazı'na uzanmaktadır. BAE, 3,3 milyar dolarlık bu projeyi başlatmış olsa dahi süreç mükerrer gecikmelere maruz kalacaktır (Al Bawaba, 2012). Buradaki temel çelişki CPECC'nin boru hatlarını işletme faaliyetlerine hazırlanmasına karşın Abu Dabi Ulusal Petrol Şirketi (ADNOC) bünyesindeki Kıyı Petrol Operasyonları Şirketi (ADCO) sürece dahil edilmemiştir (Oil & Gas News, 2012). ADCO'nun boru hattı sürecinin dışında tutulması Çin tarafından CPECC aracılığıyla yasa dışı faaliyetlerde bulunmasıyla açıklanabilir. Keza Çin'in siber casusluğu ekonomik alanda kendisine kar sağlayabilir. Türkiye örneği ele alacak olursak Ankara 2015'te 2013 yılında gündeme gelen Çin'e ait bir devlet firmasıyla uzun menzilli füze sistemleri için 3,4 milyar dolarlık ihaleyi iptal ettiğini açıklamıştır (South China Morning Post, 2015). Çin Hassas Makine İthalat-İhracat Şirketi (CPMIEC) ile 2013 yılında başlayan müzakere süreci noktada Türkiye kendi füze sistemlerini geliştirmeye yöneldiği için olumlu sonuçlanmamıştır. Bu noktada özellikle CPMIEC füze sistemleriyle NATO füze savunma sistemlerinin uyumu çokça tartışılmıştır. Küresel siber bağımlılık ve ekonomik entegrasyon süreçlerinin bir ülkenin ulusal güvenlik algısına nasıl etki ettiği analiz edilmelidir. Dolayısıyla yukarıda bahsedilen anlaşmalar

sadece ekonomik nitelikte olmayıp aynı zamanda bu faaliyetler Çin'in siber araçları kullanarak ulusal gücünü arttırma çabaları olarak nitelendirilebilir. Çin uluslararası ekonomik politikaları sayesinde yatırım yaptığı ülke de siber casusluk sayesinde ekonomik istihbaratın yayılması için de fırsatlar elde edebilir. Çin karşısında BAE ve Türkiye'nin tutumu incelendiğinde bu ülkelerin ABD kadar yoğun ve doğrudan tepki vermemelerine karşın yine de Çin yatırımlarını kısıtlama eğilimine sahiptirler. Burada önemli olan ABD haricindeki büyük güçlerin Çin siber ekonomik siber casusluk faaliyetlerinin dünya siyaset ve ticaret çerçevesinde ele alınmadır. Zira Çin ekonomik ve askeri olarak yükselmeye devam ettikçe diğer ülkeler Çin karşısında güçlerini birleştirmek zorunda kalabilir. Bu aşama da siber ekonomik casusluğunu durdurmak için uluslararası siber izleme yapılarına ihtiyaç duyulmaktadır (Magen, 2017).

3.3.5. İki Ülkenin Dönüşen Dış Politika Kararlarında Siber Alan

Çin ve ABD siber alanda karşı karşıya gelen önemli aktör olduğu için bu aktörler arasındaki ilişki analiz edilmelidir. Çünkü bu analizin sonucu bizlere Çin ve ABD arasındaki diyalogun iş birliğini yoksa çatışmayı mı arttırdığını sunacaktır. Siber uzay son yıllarda daha önceki yüzyıllar da açık denizler ve hava alanlarında tecrübe edildiği gibi Uİ için artık kritiktir. Devletler arasındaki ilişki ve refaha etki ettiği kadar Uİ sisteminin istikrar ve refahına da etki edecektir. Bu nokta da ABD ilk günden itibaren siber uzayı bir devrim olarak ele almaktadır. Çin ise en az ABD kadar bu alana önem vermektedir. Bu konuda Çin Başkanı Xi Jinping, birçok kez Çin'in konuya dair hassasiyetini dile getirmiştir. Xi Jinping'e göre, Çin siber alandaki gücünü inşa etmek için bilişim teknolojilerinin gelişimine yönelik bu tarihi fırsatı değerlendirmek için hevesle stratejisini geliştirirken büyük bir çaba sarf etmelidir (Xinhua, 2018). Aynı zamanda Xi, Çin'in kalkınması için siber güvenlik ve bilişim teknolojilerinin geliştirilmesinin altını çizirken siber uzay vizyonunu modern bir ekonomi ve yüksek kaliteli kalkınma, yeni sanayileşme, kentleşme ve tarımsal modernleşme modelleri aracılığıyla da vurgulamıştır. Çünkü dijital ekonominin gelişmesi için internet, büyük veri, AI ve reel ekonomi arasında derin bir entegrasyon süreci vardır. Bu entegrasyonun teşvik edilmesi, imalat, tarım ve hizmet sektörlerinin daha fazla dijitalize olması gerekmektedir. II. Dünya Savaşı'ndan sonra Pax Americana dönemi olarak adlandırılan ABD'nin Uİ sisteminin oluşmasındaki rolü düşünüldüğünde bu dönemin etkisi artık azalmıştır. Barack Obama (Krauthammer, 2011)'nın "Arkadan Liderlik" ve Trump'ın "Önce ABD" rolü ABD'nin eylem ve politikaların da sağlam bir fikir birliği söz konusu değildir. Bu nokta da Çin'in askeri ve ekonomik büyümesi iki tarafı iş birliğinden çok çatışmaya itebilir (Jinghua, 2019).

Siber alana yansıyan ABD ve Çin rekabetini belli bir seviye de uzlaşmaya götürme çabaları Uİ sisteminde karşımıza çıkmaktadır. Carnegie Uluslararası Barış Vakfı bu konu da Siber Politika Girişimi'nde bulunmuştur. ABD ve Çin yetkilileri ve uzmanları siber uzay üzerinden gelen tehdit algılarını iyileştirmeye yönelmişlerdir. Bu noktada vakıf çalışmalarından biri nükleer istikrara yönelik siber tehditlerin tanımlanmasına eğilirken diğeri Çin Silahlı Kuvvetleri'nden emekli bir

albay olan misafir akademisyen Lyu Jinghu ve Ariel Levite'in liderliğinde ABD ve Çin'in farklılıklarına rağmen siber uzayda iş birliği yapabilme yeteneklerinin teşvik edilmesine yoğunlaşmıştır. Ancak Carnegie Siber Politika Girişimi henüz onaylanmamış olup girişiminin içeriğinin doğruluğuna ilişkin kesin bir görüş birliği söz konusu değildir (The Carnegie Endowment For International Peace, U.S.-China Cyber Stability). ABD ve Çin'in siber alandaki iş birliğinin ön plana çıktığı bir başka örnekte 2015 ABD-Çin Siber Güvenlik Anlaşması'dır. ABD ve Çin arasındaki istikrarsız ilişkinin dünya ekonomisi açısından zararlı etkileri ön plana çıkarıldığında bu iki aktör çatışma yerine iş birliğine itilmektedir. Siber alanın ekonomiyi, CI, komuta ve kontrol sistemlerini felç edecek kapasite ulaşması uluslararası arenayı tırmanan güvenlik ikilemiyle başa bırakmıştır. ABD ve Çin'e diğer ülkelere nazaran karşılıklı güvenin sağlanması, casusluk hakların ve temel farklılıkların kabul edilmesi ve ortak çıkarlar noktasında ilerleme için iş birliği noktasında daha fazla sorumluluk düşmektedir. Bu anlaşmanın temel noktası Çin'i yasadışı siber sömürü faaliyetlerinin caydırırken tarafların iş birliğinin avantajlı olduğuna inandırmaktır (Johnson, 2016-2017).

Siber alanda ABD ve Çin'in iş birliği kapasitesinin arttırılma çabalarına rağmen bu iki aktör arasındaki rekabet daha fazla ön plana çıkmaktadır. FBI Direktörü Christopher Wray, Çin'i hem ABD hem de İngiltere için en büyük uzun vadeli tehdit olarak nitelendirmiştir. Wray'a göre Çin, ABD teknolojik altyapısını çalmaya karardır. Bu yüzden Wray, ABD şirketlerini Çin ile iş birliği noktasında sürekli uyarmıştır. Donald Trump döneminde Çin'e karşı bir ticaret savaşı başlatılmıştır. Joe Biden göreve geldiğinde ise ABD ve Çin arasındaki ilişki düzeyi gelişmeye başlamıştır. Xi Jinping, Çin'in ABD tarafından stratejik olarak yanlış değerlendirilmesi üzerinde dururken Çin'in Tayvan'ı işgal etme çabası ve Rusya'nın Ukrayna işgali Çin'i zora sokacaktır (Barr, 2022). Özetle ABD ve Çin arasındaki gerilim iş birliğinin pasif kalmasına neden olacaktır. Çünkü bu iki ülke arasındaki güven ortamı iş birliğini taşıyacak kadar güçlü değildir.

SONUÇ ve ÖNERİLER

Uİ disiplini içerisinde siber alan ve küreselleşme ile ilgili bir bağlantı kurulabilir. Bu ilişki ülkelerin dış politika algılarına da etki edecektir. Küreselleşmeye bağlı olarak devletlerin güç dağılımlarında karşılaşılan değişiklik asimetrik güç ilişkilerini ortaya çıkarmıştır. Artık ulusal güç gereksinimleri farklı tanımlanacaktır. Bu noktada siber güvenlik ön plana çıkacaktır.

Siber güvenliği tanımlamak ve devletlerin güç ilişkilerinin yeniden yorumlanması noktasında uluslararası arenada birçok analiz sistemi geliştirilmiştir. BM ITU'nun 2017 yılında yayımlandığı Küresel Siber Güvenlik Endeksi Raporu ön plana çıkarılabilir. Bu rapora göre 25 gösterge açısından siber güvenlikle ilgili kanuna uygun hareket edilmesi, teknik, örgütsellik, kapasitenin geliştirilmesi ve iş birliği gibi 5 ana sütuna yer verilmiştir. Ancak rapor esas olarak siber saldırılar karşısındaki savunma kapasitelerini baz almaktadır. Bu rapora göre 2014 yılında siber saldırılar karşısında alınan önlemler ve devletlerin savunma kapasitesi bakımından güç ABD'ye aitken 2017 yılına gelindiğinde Singapur ABD'nin önüne geçmiştir. Dolayısıyla siber alan klasik mücadele alanlarının çok ötesindedir. Uluslararası arenadaki konumu açısından ABD ele alındığında her ne kadar Çin, ABD karşısında potansiyel anlamda en güçlü tehdit olsa dahi ekonomik, siyasal, askeri kapasiteleri bakımından görece daha zayıf bir devlet siber alanda saldırılara karşı daha fazla daha az tehdit altında olabilir.

Siber güvenlik ile ilgili bir diğer analiz ise Clarke ve Robert'ın siber tehditlere karşı dayanıklılığı ölçen 2010 yılında geliştirdikleri puanlama sistemidir. Bu analize siber güvenlik ve güç ilişkisi siber saldırı, bağımlılık ve savunma kriterlerine göre değerlendirilmiş olup Rusya en fazla puan alan devlettir. Ancak Rusya'nın siber bağımlılık konusunda en yüksek puana sahip olması siber güvenlik ve güç ilişkisini değerlendirirken gücün klasik anlamdan farklı yorumlanması gerekliliğini ön plana çıkarmıştır.

Siber alandaki mücadele devletlerin diğer alanlardaki mücadele biçimlerinden oldukça farklıdır. ABD ve Çin'in siber alandaki rekabetinin ele alındığı bu çalışmada da özellikle bu iki aktörün dış politikalarına siber alanı nasıl dahil ettikleri analiz edilecektir. İlk olarak ABD ele alındığında siber güvenlikle ilgili ilk belge 2003 yılında yayımlanmıştır. Bu Siber Güvenlik Belgesi aracılığıyla ulusal ve federal direktifler sayesinde devlet ve yerel yönetim kurumları, özel sektör firmaları, sivil toplum kuruluşları ve vatandaşlar arasında kolektif iş birliği amaçlanmıştır. ABD siber güvenlik ile ilgili belgeler 2011, 2013 ve 2015 yıllarında yayımlanmıştır. ABD siber alanı dış politikaya entegre etmek için sistemik olarak ilerleyen bir aktördür. Tüm ülkenin ABD'nin siber

güvenliğin sağlanmasında tek bir bütün olarak hareket etmesi amaçlanmıştır. Sadece siber güvenliği dış politikaya entegre etmek yeterli olmayacaktır. Çünkü bu yeni alan sayesinde saldırı, terör, tehdit ve savaş gibi birçok klasik kavramın yeniden tanımlanmıştır. Bu noktada ABD NATO'nun da siber alana entegre edilmesi konusunda maliyet arttırıcı önlemlere yönelmiştir ancak siber alanda etkin olmak için sisteme daha fazla entegre olunması aynı zamanda aktörün kendini savunmasız bir konuma getirmesine de olacak sağlamaktadır.

ABD'nin siber güvenlik politikalarını şekillendirirken başkanlık direktifleri, resmi açıklamalar, doktrinler ve resmi belgelerin yanı sıra NSA, FBI, USCYBERCOM ve DHS de ele alınmalıdır. Bu kurumlardan NSA istihbarat, FBI siber faaliyetlerinin yürütülmesi, USCYBERCOM senkronizasyon ve kaynak sağlama, DHS ABD değerlerinin ve yaşam tarzının korunması noktasında ABD'nin temel yapı taşlarıdır. ABD, siber alanda hegemon güç olma arzusunu bütün kurum ve kuruluşlarına yansıtmaktadır. Bu noktada maliyet arttırıcı önlemlerden kaçınmadan kendisi için en büyük tehdit olan Çin karşısında gücünü korumak için gerekli politikaları proaktif bir şekilde takip etmektedir.

Siber alanda Çin'e geldiğimizde ise UI disiplin içerisinde bazı taraflara göre Çin saldırgan olarak anılmaktadır. Özellikle ABD ve Batılı devletler kendi çıkarlarını korumak adına Çin'in gücünü abartmaktadır. Her ne kadar Çin kritik alt yapıya sızma yoluyla casusluk, askeri bilgi edinmek için teknolojik casusluk ve ekonomik avantaj elde etmek için endüstriyel casusluk faaliyetlerinde bulunsa da uluslararası arenadaki diğer devletler gibi devamlılığını sürdürmek isterken güçlü bir aktör olmayı hedeflemektedir. Ayrıca 2015 Dünya Bankası verilerine göre Soğuk Savaş sonrasında dünya ekonomisinin 2 kat, ABD 1,8 kat ve AB 1,5 kat büyürken Çin'in büyüme oranının %10 olması siber alanda yalnızca Batılı devletlerin hakim olma potansiyelini kırmaktadır. Ayrıca Çin 2001 yılında DTÖ üyeyken aktif bir üye olmasına karşın 15 yıl içerisinde GSMH'sını 8 kat arttırıp 6 sıradan 2'nci sıraya yükselerek ABD karşısındaki yerini almıştır.

Çin'in ekonomik alandaki hızlı gelişimi askeri kapasitesine etki edecektir. Özellikle ABD ve Çin'in siber alana yönelik ilgisi düşünüldüğünde Çin bilgi teknolojileri aracılığıyla PLA'yı siber alana entegre etmeye çalışacaktır. Çin ulusal düzeyde bilgi teknolojisine 1986 yılında Devlet Ekonomik Bilgi Yönetim Öncü Grubu (CLSGISI)'nu kurmuştur. Bu gelişim süreci 1999 yılına kadar devam etmesine karşın 2001 yılında Devlet Bilişim Öncü Grubu (SILG) sayesinde yeniden yapılanma sürecine girilmiştir. 2003'te SILG tarafından yayınlanan Belge 27 aracılığıyla ise siber güvenlikle ilgili önlem politikaları ve ulusal stratejiler ön plana çıkarılmıştır. 2012 yılında Çin, Danıştay Bilgi Ofisi (SCIO) bilgi güvenliği için Yeni Politika Görüşü (NPO)'nü yayımlamıştır. Bu noktada özellikle Çin askeri kapasitesinin gelişimi üzerinde durulmuş olup Genel Kurmay Başkanlığı'nın 3. ve 4. Daireleri'ne bağlı olarak PLA ve onun istihbarat faaliyetleri ön plana çıkarılmıştır.

Siber alanda ilk olarak 1990 yıllarda ABD ve Çin arasındaki rekabet ABD Başkanı Bill Clinton'un Bilgi Otoyolu Programı'nı ilan etmesiyle başlamıştır. George W. Bush yönetimi ise ABD Siber Uzay Stratejisi'ni ilan ederek kritik altyapı sistemlerinin güvenliğini ortaya çıkarmıştır. 1994-2008 yılları arasında ise Çin'deki internet kullanıcılarının sayısı ABD'yi geçmiştir. Obama yönetimi döneminde ABD ve Çin arasındaki sorunlar tırmanmaya başlamış olup 2012 Mandiant Raporu'na göre PLA, ABD şirketlerini, hükümetini ve altyapısını doğrudan hedef alan saldırıların kaynağı olarak gösterilmiştir. 2014 yılına gelindiğinde bu iki aktör arasındaki sorunlar giderek artmıştır. 2015 yılında ABD-Çin Siber Güvenlik Anlaşması imzalanmış olsa da Trump döneminde ABD Ticaret Bakanlığı, Çin teknoloji ve ürünlerine, internet şirketlerine, sivil ve askeri amaçlarla ürün üreten teknoloji şirketlerine karşı ulusal gerekçeler aracılığıyla Çin'e karşı ekonomik yaptırımları kabul etmiştir. Biden döneminde ise siber güvenlik ulusal güvenliğin ayrılmaz bir parçası olarak kabul edildiği için Başkan Trump'ın Çin'e karşı tutumu geçerliliğini koruyacaktır.

Siber alandaki ABD ve Çin arasındaki rekabet BM Siber Yönetim Yapısı'na da yansımaktadır. 2004 tarihinden itibaren Çin, BM'nin siber uzayda sorumlu devlet davranışlarını geliştirmeye yönelik Hükümet Uzmanlar Grubu (GGE)'nin içerisinde yer almasına karşın Rusya ile yakın ilişkisi ileri sürülerek Çin'in Rusya'nın destekleyicisi olduğu algısı hedeflenmiştir.

Siber alana hegemon olmak isteyen ABD karşısında yükselen en önemli güç olan Çin'in rekabeti analiz edildiğinde kimin daha saldırgan olduğunu saptamak kolay değildir. Bu noktada ABD ve Çin'in askeri kapasiteleri ele alınmalıdır. Çin'in PLA'yı siber savaş durumunda bilgi üretme, toplama, iletme, analiz etme ve kullanmadaki çabası PLA'nın dijital savaşa verdiği önemi göstermektedir. 2020 yılında Uluslararası Stratejik Araştırmalar Enstitüsü (IISS)'nin yayınladığı rapora göre ülkelerin siber alandaki kapasiteleri ve ulusal güçleri tartışılmıştır. İlk 15 ülke incelendiğinde ABD 1'inci sıradayken Çin 2'cidir. İngiltere, Rusya, Hollanda, Fransa, Almanya, Kanada, Japonya, Avustralya, Kuzey Kore, İsrail ve Hindistan ve daha birçok ülkenin de siber alanda ön plana çıktığı göz ardı edilmemelidir.

ABD ve Çin arasındaki rekabette kamuoyuna yansıyan görüntü Çin'in ABD'ye nazaran daha saldırgan bir aktör olarak ön plana çıkmasıdır. Mandiant Raporu'na göre Çin destekli hackerlar ABD'deki en az 6 eyalette siber saldırılar gerçekleştirmiştir. Siber Güvenlik ve Altyapı Ajansı (CISA)'na göre ise 2017 yılında en az 12 şirket, 2018 yılında ABD kritik altyapı sistemleri, 2020 yılında Covid-19'a karşı ilaç ve araştırma sektörlerini Çin tarafından tehdit edilmektedir. Çin ise bu suçlamaları kabul etmemesine karşın Internet Company 360 Raporu'na göre ise NSA'nın 47 ülkeyi etkileyen siber saldırılar noktasında 10 yılı aşkın bir süredir etkin olduğu iddiasını ileri sürmüştür.

Sonuç olarak siber alanda ABD karşısında yükselen en önemli güç Çin'dir. Bu noktada Çin'in ekonomik ve askeri kapasitesini ABD için tehdittir. Çin, ABD'nin Asya'daki çıkarlarını tehdit etmektedir. Bunun yanı sıra ABD için Çin aynı zamanda Batı'ya ait değerler olan demokrasi

ve insan hakları kavramlarını da tehdit etmektedir. Bu düşünceden hareketle ABD'nin Çin'i uluslararası arena da yalnızlaştırmak istediği kanısına varılabilir. ABD, Çin'in devlet rejiminin diğer devletlerin yönetim biçimlerine nazaran daha otoriter olmasını kullanmaktadır. ABD'ye göre Çin'in yönetim biçimi demokratik ilkelerden uzak, çoğulcu yaklaşımdan yoksun ve sınırlandırılmıştır özgürlüğü savunmaktadır. Siyasal alanda Çin'e karşı yapılan baskılar ekonomik anlamda da devam etmektedir. Çin bu yaklaşımları kabul etmemekle birlikte kendisine yöneltilen siyasal baskının yanı sıra ekonomik kısıtlamaları engellemek için 2016 yılında kurulan Asya Kalkınma Bankası vb çok uluslu iktisadi kurum ve kuruluşları sayesinde Dünya Bankası ve Uluslararası Para Fonu gibi yapılanmaların etkinliğini kırarak alternatifleri ön plana çıkarmıştır.

ABD'nin yoksa Çin'in mi daha saldırgan politikaları takip ettiğini saptamak kolay değildir. Uluslararası arenadaki hakim gücü ele alındığında ABD, siber alana hakim olma düşüncesinden caymayacaktır. Çin ise diğer devletlere nazaran ABD karşısındaki en büyük potansiyel tehdit unsuru olmaya devam edecektir. Ancak siber alandaki mücadele diğer tüm alanlardaki mücadeleden oldukça farklıdır. Uluslararası arenadaki her aktör ABD, Çin, Rusya, İngiltere gibi büyük güçleri tehdit ettiği gibi görece daha az güçlü devletleri de tehdit etmektedir.

KAYNAKÇA

- Ada, Mehmet (2018), **NATO Üyesi Ülkelerin Siber Güvenlik Stratejileri Açısından İncelenmesi**, Yüksek Lisans Tezi, Gazi Üniversitesi - Bilişim Enstitüsü.
- Adam, P. Liff ve Erickson, Andrew S. (2013), “Demystifying China's Defence Spending: Less Mysterious in the Aggregate”, **The China Quarterly**, 216: 805-830.
- AFAD (2014a), “2014-2023 Kritik Altyapıların Korunması Yol Haritası Belgesi”, **Başbakanlık Afet Acil Durum Yönetimi Başkanlığı**, Ankara.
- Akarşlan, Hüseyin (2015), **Bilişim Suçları**, 2.Baskı, Seçkin Yayınları, Ankara.
- Akyeşilmen, Nezir (2018), **Disiplinler Arası Bir Yaklaşımla Siber Politika & Siber Güvenlik**, Orion Kitabevi, Ankara.
- Al Bawaba (2012), “BAE Delays Project to Bypass of Hürmüz Boğazı”, <https://www.albawaba.com/business/uae-delays-project-bypass-strait-hormuz-408210> (12.04.2023).
- Al-Fadhat, Faris (2019), **Ekonomi Politik Jepang Di Asia Tenggara: Dominasi Dan Kontestasi Aktor-Aktor Domestik**, Pustaka Pelajar Publishers, Indonesia.
- Altınkaynak, Mustafa (2017), **Uygulamalı Siber Güvenlik ve Hacking**, Abaküs Yayınları, İstanbul.
- Angstrom, Jan (2005), **Rethinking The Nature of War**, 1th Ed., Routledge Publishers, England.
- Arı, Tayyar (1997), **Uluslararası İlişkiler**, Alfa Yayıncılık, İstanbul.
- Arı, Tayyar (2003), **Uluslararası İlişkiler Teorileri: Çatışma, Hegemonya, İş Birliği**, Alfa Yayınevi, İstanbul.
- Arı, Tayyar (2008), **Uluslararası İlişkiler ve Dış Politika**, Marmara Kitap, Bursa.
- Arıboğan, Deniz Ülke (1998), **Kabileden Küreselleşmeye Uluslararası İlişkiler Düşüncesi**, Sarmal Yayınevi, İstanbul.
- Arquilla, John ve Ronfeldt, David (1993), “Cyberwar is Coming!”, **Comparative Strategy**, 12(2), 141-165.
- Asan Forumu (2014), “Bu Zamandaki Bütçe: Çin'in Savunma Harcamalarını Ölçmek”, <http://www.theasanforum.org/the-budget-this-time-taking-the-measure-of-chinas-defense-spending/> (15.12.2022).

- Ashraf, Cameran (2021), “Defining Cyberwar: Towards A Definitional Framework”, **Defense & Security Analysis**, 37(3), 274-294.
- Athukorala, Prema Chandra (2017), **China’s New Sources Of Economic Growth**, The Australian National University, Australia.
- Atzili, Boaz (2014), “Siber Savaş ve ABD Ulusal Güvenliği”, **School of International Service**, 43-47.
- Austin, Greg (2014), **Cyber policy in China**, Polity Publisher, England.
- Austin, Greg (2018), **Cybersecurity in China: The Next Wave**, Springer International Publisher, Switzerland.
- Aydın, Mustafa (1996), “Uluslararası İlişkilerde Yaklaşım, Teori ve Analiz”, **Ankara Üniversitesi SBF Dergisi**, 51(01).
- Bachmann, Sascha (2015), “Hybrid Wars: The 21st-Century’s New Threats to Global Peace and Security”, **Scientia Militaria: South African Journal of Military Studies**, 43(1), 77-98.
- Balta, Evren (Ed) (2014), **Dış Politika Analizi, Küresel Siyasete Giriş: Uluslararası İlişkilerde Kavramlar, Teoriler, Süreçler**, İletişim Yayınları, İstanbul.
- Barr, Luke (2022), “FBI Director Calls China 'Biggest' US Threat; Authorities Warn Of North Korean Cyber Attacks”, ABC News, <https://abcnews.go.com/Politics/fbi-director-calls-china-biggest-us-threat-authorities/story?id=86336590> (12.04.2023).
- Barston, Ronald Peter (2006), **Modern Diplomacy**, Pearson Publishers, Londra.
- Başa, Şafak (2010), “ABD İç Güvenlik Bakanlığı” <https://www.academia.edu/9830086/> (15.12.2022).
- Bateman, Jon (2022), “US-China Technological Decoupling: A Strategy And Policy Framework”, **Policy Commons**.
- Bauman, Zygmunt (1997), **Küreselleşme: Toplumsal Sonuçları**, (Çev. Abdullah Yılmaz), Ayrıntı Yayınları, İstanbul.
- Bayrak, Muharrem (2020), “ABD ile Birleşik Krallık’ın AB ve NATO Çerçevesinde Siber Alanlarının Tarihsel Analizi”, **Cyberpolitik Journal**, 5(9), 22-51.
- Bayraktar, G. (2015), **Siber Savaş ve Ulusal Güvenlik Stratejisi**, YeniYüzyıl Yayınları, İstanbul.
- BBC News (1998), <http://news.bbc.co.uk/2/hi/science/nature/200069.stm> (15.12.2022).
- Bechná, Zinaida ve Thayer, Bradley A. (2016), “NATO’s New Role: The Alliance’s Response to A Rising China”, **Naval War College Review**, 69(3), 65-82.

- Bendrath, Ralph (2003), **In Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security**, (Çev. Robert Latham), The New Publisher, New York.
- Bıçakçı, Salih (2014), “NATO’nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik”, **Uluslararası İlişkiler**, 10 (40), 101-130.
- Bıçakçı, Salih (2019), “Siber Güvenlik ve Savunma”, **Güvenlik Yazıları Serisi**, 42.
- Bıçakçı, Salih (2012), “Yeni Savaş ve Siber Güvenlik Arasında NATO’nun Yeniden Doğuşu”, **Uluslararası İlişkiler**, 9(34), 209-210.
- Bıçakçı, Salih (2013), **21. Yüzyılda Siber Güvenlik**, İstanbul Bilgi Üniversitesi Yayınları, İstanbul.
- Bilgin, Pınar (2005), “Turkey’s Changing Security Discourses: The Challenge of Globalisation”, **European Journal of Political Research**, 44: 175-201.
- Birdişi, Fikret (2014), **Teori ve Pratikte Uluslararası Güvenlik**, Seçkin Yayınları, Ankara.
- Bloomfield, Alan (2012), “Time to Move On: Reconceptualizing the Strategic Culture Debate”, **Contemporary Security Policy**, 33(3): 437-461.
- Boozallen, “China’s Cyberattack Strategy Explained” (t.y.), <https://www.boozallen.com/insights/cyber/chinas-cyberattack-strategy-explained.html> (12.04.2023).
- Branigan, Tania (2010), “Çin Ordusu Siber Savaş Tehdidini Hedef Alıyor”, <https://www.theguardian.com/world/2010/jul/22/chinese-army-cyber-war-department> (12.04.2023).
- Bulduk, Sevdâ (2006), “Sputnik Sendromu”, **İstanbul Üniversitesi Sosyoloji Dergisi**, 12(3), 61-69.
- Burchill, Scott ve Linklater, Andrew (2012), **Analiz Çerçevesi Uluslararası İlişkiler Teorileri**, (Çev. Ali Aslan ve Muhammed Ali Ağcan), Küre Yayınları, İstanbul.
- Burns, Thomas, L. (1990), “The Origins of the National Security Agency (NSA):1940-1952”, **United States Cryptologic History**, 5, 107-108.
- Buzan, Barry (1983), **People, States and Fear: The National Security Problem in International Relations**, 2th Ed., Wheatsheaf Books Publishers, London.
- Buzan, Barry vd. (1998), **Security: A New Framework For Analysis**, Lynne Rienner Publishers, Colorado.
- Cambridge Dictionary (2022), <https://dictionary.cambridge.org/tr/s%C3%B6zl%C3%BCk/ingilizce%C3%BCrk%C3%A7e/intelligence> (02.02.2022).
- Carr, Madeline (2016), “Crossed Wires: International Cooperation on Cyber Security”, **Interstate-Journal of International Affairs**, 2015(2), 2-13.

- Caşın, Mesut Hakkı (2002), “Soğuk Savaş Sonrası Askerî Stratejik İstihbaratın Yeni Vizyonu”, **Avrasya Dosyası**, 8(2), 254-294.
- Caşın, Mesut Hakkı vd. (2007), **Küreselleşmenin Avrupa Birliği Ortak Güvenlik ve Savunma Politikasına Etkisi**, Nokta Kitap, İstanbul.
- Charles, Tilly (2004), “Terror, Terrorism, Terrorists”, **Sociological Theory**, 22(1), 8.
- Chen, Dongxiao, ve Chuanying, Lu (2021) “Competition Without Catastrophe: A New China-U.S. Cyber Security Agenda”, **Shanghai Institutes for International Studies**, <http://www.siiis.org.cn/Research/EnInfo/5259> (12.04.2023).
- China Internet Network Information Center-CNNIC (2008), “The Number Of Chinese İnternet Users Exceed The US For The Frst Time”, **Beijing Daily**, <https://it.sohu.com/20080725/n258380068.shtml> (12.04.2023).
- CISA (2021), “Chinese State-Sponsored Cyber Operations: Observed TTPs”, https://media.defense.gov/2021/Jul/19/2002805003/-1/-1/0/CSA_CHINESE_STATE-SPONSORED_CYBER_TTPS.PDF (12.04.2023).
- _____ (2021), “Çin Siber Tehditlerine Genel Bakış ve Öneriler”, <https://www.cisa.gov/china> (12.04.2023).
- _____ (2022), “People’s Republic of China State-Sponsored Cyber Actors Exploit Network Providers and Devices”, <https://www.cisa.gov/news-events/cybersecurity-advisories/aa22-158a> (12.04.2023).
- Clarke, Richard A. ve Robert, Knake K (2010), **Cyber War: The Next Threat to National Security and What to Do About It**, 1st Press, Harper Collins, New York.
- Clarke, Richard Alan, ve Robert K. Knake (2014), **Cyber War: The Next Threat To National Security And What To Do About It**, Old Saybrook: Tantor Media Publishers, Chicago.
- Clausewitz, Carl Von (1976), **On War**, (Çev. Peter Paret ve Michael Howard), Princeton University Publishers, New Jersey.
- Collin, Barry (1996), **The Future of Cyber Terrorism, Proceedings of the 11th Annual International Symposium on Criminal Justice**, The Issues University of Illinois Publishers, Chicago.
- Craigen, Dan vd. (2014), “Defining Cybersecurity”, **Technology Innovation Management Review**, 4(10).
- CSET (2021), “Outline of the People's Republic of China 14th Five-Year Plan for National Economic and Social Development and Long-Range Objectives for 2035”, <https://cset.georgetown.edu/publication/china-14th-five-year-plan/> (12.04.2023).

- Çakmak, Haydar ve Altunok, Taner (2009), **Suç, Terör ve Savaş Üçgeninde Siber Dünya**, Barış Platin Kitapevi Yayınları, Ankara.
- Çalış, Şaban ve Özlük, Erdem (2007), “Uluslararası ilişkiler Tarihinin Yapı Sökümü: İdealizm-Realizm Tartışması”, **Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, (18), 230-243
- Çıtak, Emre (2017), **Güvenlik ve İstihbarat**, Yeni Yüzyıl Yayınları, İstanbul.
- Çiftçi, Hasan (2013), **Her Yönüyle Siber Savaş**, TÜBİTAK Popüler Bilim Kitapları, Ankara.
- Çitlioğlu, Ercan (2006), **Gri Tehdit Terörizm**, Ümit Yayıncılık, Ankara.
- ÇKP Merkez Politbüro Yürütme Komitesi Toplandı (2017), http://news.xinhuanet.com/politics/2017-01/22/c_1120363831.htm (14.12.2022).
- Danilovic, Vesna (2001) “The Sources of Threat Credibility in Extended Deterrence”, **The Journal of Conflict Resolution**, 45(3), 341.
- Darıcı, Ali Burak (2014), “Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırıların Analizi”, **Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, (7)2, 7.
- _____ (2017), Demokrat Parti Hack Skandalı Bağlamında ABD ve RF’nin Siber Güvenlik Stratejilerinin Analizi. **Uluslararası Çalışmalar Dergisi**, 1(1), 1-24.
- _____ (2019), Türkiye’nin Siber Güvenlik Politikalarının Analizi; Türkiye’nin Siber Güvenlik Modeli için Öneriler, **TESAM Akademi Dergisi**, 6(2), 11-33.
- DARPA, (2019), “A Selected History of DARPA Innovation” <https://www.darpa.mil/Timeline/index.html> (02.02.2022).
- _____ (2019), “ARPANET”, <https://www.darpa.mil/aboutus/timeline/arpamet> (02.02.2022).
- _____ (2019), “ARPA Is Born”, <https://www.darpa.mil/aboutus/timeline/dod-establishes-arpa> (02.02.2022).
- _____ (2019), “ARPA Becomes DARPA”, <https://www.darpa.mil/about-us/timeline/arpa-name-change> (02.02.2022).
- DATAREPORTAL (2023), “Digital Around The World”, <https://datareportal.com/global-digital-overview> (19.02.2023).
- Davis, Susan (2019), “NATO in The Cyber Age: Strengthening Security & Defence, Stabilising Deterrence”, **NATO Parliamentary Assembly**.
- Dedeoğlu, Beril (2014), **Uluslararası Güvenlik ve Strateji**, Yeni Yüzyıl yayınları, İstanbul.
- Deepak, B. R (Ed) (2018), **China’s Global Rebalancing and the New Silk Road**, Springer Publishers, Singapore.

- Demirel, M. (2012), **Asimetrik Tehdit Kavramı Bağlamında 9/11 2001 Sonrası Dönem’de Amerika Birleşik Devletleri’ndeki Siber Tehdit Algılamasının ve Geliştirilen Güvenlik Politikalarının İncelenmesi**, Yayınlanmamış Yüksek Lisans Tezi, Kara Harp Okulu - Savunma Bilimleri Enstitüsü.
- Department of Defence (2017), https://www.stratcom.mil/factsheets/2/Cyber_Command/ (02.02.2022).
- _____ (2019), “Annual Report to Congress: Military and Security Developments Involving the People’s Republic of China 2019.” USA: Office of the Secretary of Defense, https://media.defense.gov/2019/May/02/2002127082/-1/1/2019_CHINA_MILITARY_POWER_REPORT.pdf. (14.12.2022).
- Department of Defence Dictionary of Military and Associated Terms (2021), http://www.dtic.mil/doctrine/new_pubs/jpl_02.pdf (29.11.2022).
- Deppa, Catherine S. (2017), “US Cyber Command: An Overview”, **American Intelligence Journal**, 34(1), 12-15.
- Dick, Steve J. (2019), 50 Years of NASA History, https://www.nasa.gov/50th/50th_magazine/historyLetter.html (02.02.2022).
- DOD (2011), “Department of Defense Strategy for Operating in Cyberspace”, <http://csrc.nist.gov/groups/SMA/isbab/documents/DOD-Strategy-for-Operatingin-Cyberspace.pdf> (21.11.2022).
- _____ (2013), “DOD Strategy for Defending Networks, Systems, and Data”, http://iac.dtic.mil/csiac/download/DDNSD_Public_Releasable_11132014.pdf (21.11.2022).
- _____ (2015), “The DOD Cyber Strategy. Washington: The Department of Defense”, https://www.defense.gov/Portals/1/features/2015/0415_cyberstrategy/Final_2015_DoD_CYBER_STRATEGY_for_web.pdf (21.11.2022).
- Dorman, Andrew vd. (2005), **The Falklands War**, University of London Publisher, Londra.
- Douglass, John Aubrey (1999), **The Cold War, Technology and The American University**, University Of California Publisher, California.
- Dunn Cavelty, Myriam (2007), **Cyber-Security and Threat Politics: US Efforts to Secure The Information Age**, Routledge Publisher, England.
- Dunn Cavelty, Myriam (2013), From Cyber-bombs to Political Fallout: Threat Representations With An Impact In The Cyber-security Discourse, **International Studies Review**, 15(1), 105-122.
- Dupont, Benoit (2013), “The Proliferation of Cyber Security Strategies and Their Implications for Privacy”, **Circulation Internationale De L’information et Securite**, 67-80.
- Efegil, Ertan (2012), **Dış Politika Analizi Ders Notları**, Nobel Yayınları, Ankara.

- Efrony, Dan (2021), "The UN Cyber Groups, GGE and OEWG—A Consensus Is Optimal, but Time Is of the Essence," **UN Just Security Report**.
- Elmer-Dewitt, Philip (1993), "First Nation In Cyberspace", **Time**, 6, 62-64.
- Ester, Peter, ve Nispen, Pieter Van (2013), "Foreign Policy and The Cultural Factor: A Research and Education Egenda", **The Mediterranean Academy of Diplomatic Studies**, 1-40.
- EU COM702 (F1) (2004), Critical Infrastructure Protection in the Fight Against Terrorism, Brussels: Communication From the Commission to the Council and the European Parliament,<http://ec.europa.eu/transparency/regdoc/?fuseaction=list&coteId=1&year=2004&number=702&language=EN> (12.12.2022).
- FBI (2017a), "About: Mission&Priorities", <http://www.fbi.gov/about-us/quick-facts> (02.02.2022).
- ____ (2017b), "National Cyber Investigate Joint Task Force" <https://www.fbi.gov/investigate/cyber/national-cyber-investigative-joint-task-force> (02.02.2022).
- ____ "Cyber Crime", <https://www.fbi.gov/about-us/investigate/cyber/ncijtf>, (07.12.2022).
- Feldbaum, H., & Michaud, J. (2010), Health Diplomacy and The Enduring Relevance Of Foreign Policy Interests, **PLoS Medicine**, 7(4), e1000226.
- Finkelstein, Claire Oakes, & Govern, Kevin H. (2015), **Introduction: Cyber and the Changing Face of War Cyber War: Law and Ethics for Virtual Conflicts**, OUP Oxford Publishers, England.
- Finkle, Jim (2013), "Mandiant Goes Viral After China Hacking Report. Reuters", <https://www.reuters.com/article/net-us-hackers-virus-china-mandiant-idUSBRE91M02P20130223> (12.04.2023).
- FireEye Labs (2015), "APT 30 And The Mechanics Of A Long-Running Cyber Espionage Operation", <https://www2.fireeye.com/rs/fireeye/images/rpt-apt30.pdf> (12.04.2023).
- Force, Cyber Intelligence Task (2013), Operational Levels of Cyber Intelligence, Intelligence and National Security Alliance (INSA) Report.
- Fourkas, Vassilys (2021), "What Is Cyberspace?", <http://www.waccglobal.org/en/20043-communication-rights-an-unfinished-agenda/495-What-is-cyberspace.html> (11.11.2022).
- Frankel, Joseph (1968), **The Making of Foreign Policy**, Oxford University Publishers, London.
- Fukuyama, Francis (1992a), **The End of History? The National Interest**, Free Publishers, New York.
- ____ (1992b), **The End of History and The Last Man**, Publishers, New York.
- Gabriel, Weimann (2006), **Terror on The Internet: The New Arena The New Challenges**, US Institute of Peace Press.

- GCI (2017), “Küresel Siber Güvenlik Endeksi”, https://knowledge4policy.ec.europa.eu/sites/default/files/02_-_global_cybersecurity_index_-_grace_acayo_0.pdf (03.04.2023)
- Gibson, William Gibson (1984), **Neuromancer**, (Çev. Melik Altıntaş), Gündüz Yayınları, İstanbul.
- Giddens, Anthony (1990), **The Consequence of Modernity**, Stanford University Press, California.
- Gierow, Hauke Johannes (2015), “Cyber Security in China: Internet Security, Protectionism and Competitiveness: New Challenges to Western Businesses”, **Mercator Institute for China Studies**, (22), 1-10.
- Girgin, Kemal (2003), **Uluslararası İlişkiler Modern İstihbarat ve Türkiye**, Okumuş Adam Yayınları, İstanbul.
- Goldberg, Leonard (Yapımcı), Badham, John (Yönetmen) (1983), **Savaş Oyunları**, Metro Goldwyn Mayer, Amerika.
- Goldstein, Joshua S. ve Pevehouse, Jon C, (2014), **International Relations**, Pearson Publishers, New York.
- Goodman, Seymour E. (2008), “Critical Information Infrastructure Protection”, **NATO Security Through Science Series E Human And Societal Dynamics**, 34, 24-31.
- Gorman, Siobhan (2009), “Electricity Grid in U.S. Penetrated By Spies”, **The Wall Street Journal**, <http://online.wsj.com/article/SB123914805204099085.html> (12.04.2023).
- Goswami, Namrata (2018), “China in Space: Ambitions and Possible Conflict”, **Strategic Studies Quarterly, Spring**, 12(1), 74-97.
- Göçoğlu, Volkan ve Aydın, Mehmet D. (2019), “Siber Güvenlik Politikası: ABD, Rusya ve Çin Üzerine Karşılaştırmalı Bir Analiz”, **Güvenlik Bilimleri Dergisi**, 8(2), 229-252.
- Gözen, Ramazan (2001), **21. Yüzyıl Eşiğinde Türk Dış Politikası**, Alfa Yayınları, İstanbul.
- Gözükeleş, İzlem (2014), “Tarihten Örneklerle Siber Savaş”, <https://bilimvegelecek.com.tr/index.php/2014/09/01/tarihten-orneklerle-siber-savas/> (01.01.2023).
- Graham, Edward (2022), “Danışma Kurulu, Çin’in Siber Yeteneklerinin ABD için Ciddi Bir Tehdit Oluşturduğu Uyarısında Bulundu”, <https://www.nextgov.com/cybersecurity/2022/11/chinas-cyber-capabilities-pose-serious-threat-us-advisory-panel-warns/379760/> (12.04.2023).
- Gray, Colin S. (1999), “Strategic Culture as Context: The First Generation of Theory Strikes Back”, **Review of International Studies**, 25(1): 51.
- Gressel, Gustav (2019), “Avrupa’yı Hibrit Tehditlere Karşı Korumak”, https://ecfr.eu/publication/protecting_europe_against_hybrid_threats/ (08.03.2023).
- Güntay, Vahit, (2020), “Geleceğin Güvenliğinde Yapay Zekanın Askerileştirilmesi ve Uluslararası Hukuk”, **TASAM 6. Güvenlik Konferansı**, İstanbul, Turkey.

- Haizler, Omry (2017), The United States' Cyber Warfare History: Implications On Modern Cyber Operational Structures and Policymaking, **Cyber, Intelligence, and Security**, 1(1), 31-45.
- Halder, Debarati (2019), "Siber Uzay Konsepti", <https://internetlegalstudies.com/2019/04/05/concept-of-cyber-space/> (05.04.2019).
- Hart, Stephen, vd. (2020), "Riskio: A Serious Game For Cyber Security Awareness And Education", **Computers & Security**, 95, 101827.
- Hathaway, Oona A. vd. (2011), **The Law of Cyber-Attack**, Law Review Publishers, California.
- Hekim, Hakan ve Başbüyük, Oğuzhan (2014), Siber Suçlar ve Türkiye'nin Siber Güvenlik Politikaları, **Uluslararası Güvenlik ve Terörizm Dergisi**, 4(2), 142.
- Hill, Christopher (2003), **The Changing Politics of Foreign Policy**, Palgrave MacMillan, New York.
- Hillman, Jonathan E. (2018), "How Big is China's Belt and Road?", **Center for Strategic and International Studies**, 3.
- Hjortdal, Magnus (2011), "China's Use of Cyber Warfare: Espionage Meets Strategic Deterrence", **Journal of Strategic Security**, 4(2), 1-24.
- Holsti, Kalevi J. (1968), "National Role Conceptions in the Study of Foreign Policy", **International Studies Quarterly**, 14(3), 233-309.
- Holsti, Kalevi J. (1992), **International Politics**, Prentice-Hall International Publishers, New Jersey.
- _____ (1995), **International Politics A Framework for Analysis**, Prentice-Hall International Publishers, New Jersey.
- Holton, Robert J. (1998), **Globalization and the Nation-State**, MacMillan Publishers, Londra.
- Huges, Rex B. (2009), "NATO Cyber Defence", <https://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf> (02.12.2022)
- Huiskens, Ron (2009), **Rising China: Power and Reassurance**, ANUe Publishers, Missouri.
- Huntington, Samuel P. (1997a), "The Clash of Civilizations?", **Foreign Affairs**, 72(3), 22-49.
- _____ (1997b), **The Clash of Civilizations and the Remaking of World Order**, Simon and Schuster Publishers, Londra.
- Huth, Paul K. (1999), "Deterrence and International Conflict: Empirical Findings and Theoretical Debate", **Annual Review of Political Science**, (2): 25-48.
- Insikt Group (2022), "From Coercion To Invasion: The Theory And Execution Of China's Cyber Activity In Cross-Strait Relations", **Threat Analysis**, <https://www.recordedfuture.com/from-coercion-to-invasion-the-theory-and-execution-of-china-cyber-activity> (12.04.2023).

- Interesse, Giulia (2022), "China's Cybersecurity Industry: A Market Analysis", <https://www.china-briefing.com/news/chinas-cybersecurity-industry-a-market-analysis/> (12.04.2023).
- Internet World Stats İnternet Sayfası (2021), "World Internet Users and Population Stats", <http://www.internetworldstats.com/stats.htm> (02.12.2022).
- ITU (2015), "Global Cybersecurity Index (GCI)", https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-SECU-2015-PDF-E.pdf (21.11.2022).
- ____ (2017), "Global Cybersecurity Index (GCI)", https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2017-R1-PDF-E.pdf (21.11.2022).
- ____ (2018), "Global Cybersecurity Index (GCI)", https://www.itu.int/en/ITU-D/Cybersecurity/Documents/draft-18-00706_Global-Cybersecurity-Index-EV5_print_2.pdf (21.11.2022)
- Jackson, Michael P., & ARMY WAR COLL CARLISLE BARRACKS PA. (2011), "USCYBERCOM and Cyber Security: Is a Comprehensive Strategy Possible?", **US Army War College**.
- Jamestown Foundation (2010), "China's Cyber Command?", 10(15), <https://www.refworld.org/docid/4c74e64d2.html> (12.04.2023).
- Jinghua, Lyu (2019), "Chinese-American Relations in Cyberspace: Toward Collaboration or Confrontation?", <https://carnegieendowment.org/2019/01/24/chinese-american-relations-in-cyberspace-toward-collaboration-or-confrontation-pub-78213> (12.04.2023).
- ____ (2019), "Çin'in Siber Yetenekleri ve Niyetleri Nelerdir?", <https://carnegieendowment.org/2019/04/01/what-are-china-s-cyber-capabilities-and-intentions-pub-78734> (12.04.2023).
- John, L. E. E. (2022), "Cyberspace Governance in China: Evolution, Features and Future Trends", **Center for Asian Studies**, 129, 1-35.
- Johnson, Maj J. (2016-2017), "The Implications Of Cyber On Us-China Relations", Canadian Forces College, <https://www.cfc.forces.gc.ca/259/290/402/305/johnsonj.pdf> (12.04.2023).
- Julian, Nicholas (2021), "United States'and China's Cybersecurity Policies: Collaboration or Confrontation?", SIR Journal, <http://www.sirjournal.org/research/2021/1/24/united-states-and-chinas-cybersecurity-policies-collaboration-or-confrontation> (12.04.2023).
- Kahn, David (2002), "İstihbaratın Tarihsel Teorisi", **Avrasya Dosyası**, 8(2), 5-20.
- Kakauridze, Gvantsa (2019), "Dış Politika Analiz Katmanları", Medium, <https://gvantsakakauridze.medium.com/layers-of-foreign-policy-analysis-bec7d1579e05> (06.03.2023).
- Kaldor, Mary (1999), **New and Old Wars: Organized Violence in a Global Era**, Stanford University Publishers, California.

- Kaplan, Yusuf (1991), **Enformasyon Devrimi Efsanesi**, (Çev. Yusuf Kaplan), Rey Yayınları, İstanbul.
- Kara, Mahruze (2013), **Siber Saldırıları-Siber Savaşlar ve Etkileri**, Yüksek Lisans Tezi, İstanbul Bilgi Üniversitesi-Sosyal Bilimler Enstitüsü.
- Kara, Mehmet ve Çelikkol, Soner (2011), “Kritik Altyapılar: Elektrik Üretim ve Dağıtım Sistemleri SCADA Güvenliği”, **4. IV. Ağ ve Bilgi Güvenliği Sempozyumu**, 25-26.
- Karanacak, Bilge (2011), “Kritik Altyapılar ve Kritik Altyapıların Korunması”, **Siber Savunma Sempozyumu**, 24-25.
- Kay, Sean (2004), **Globalization, Power, and Security**. *Security Dialogue*, 35(1), 9– 25.
- Kazgan, Gülten (2004), **Küreselleşme ve Ulus Devlet**, Bilgi Üniv. Yayınları, İstanbul.
- Keleştemur, Saim Atalay (2018), **Siber İstihbaratın Kamu Güvenliği için Rolü ve Önemi**, Yüksek Lisans Tezi, Gedik Üniversitesi - Sosyal Bilimler Enstitüsü.
- Kharpal, Arjun (2022), “China State-Backed Hackers Compromised Networks of at Least 6 U.S. State Governments, Research Finds”, **CNBC**, <https://www.cnbc.com/2022/03/09/china-state-backed-hackers-compromised-6-us-state-governments-report.html> (12.04.2023).
- King, Lisa (1991), “The Origins of the Cold War: A Unit of Study for Grades”, **ERIC**, 9-12.
- Kissinger, Henry (2014), **Diplomasi**, 16. Baskı, İş Bankası Yayınları, Ankara.
- Kjaersgaard, Morten (2022) “Siber güvenlik Politikacılar için En Büyük Öncelik mi? Dünya Politikası ve Siber Güvenlik”, <https://heimdalsecurity.com/blog/the-role-of-cybersecurity-in-world-politics/> (10.04.2023).
- Koçer, Gökhan (2005), “Soğuk savaş Sonrasında Uluslararası Güvenlik Ortamı ve Türkiye’nin Ulusal Güvenliği”, **Stratejik Araştırmalar Dergisi**, 3(5),286-304.
- Krauthammer, Charles (2011), “The Obama Doctrine: Leading From Behind”, *Washington Post*, https://www.washingtonpost.com/opinions/the-obama-doctrine-leading-from-behind/2011/04/28/AFBCy18E_story.html?utm_term=.762328a0beec (12.04.2023).
- Küçükalp, Derda (2012), “Siyaset Olgusunun Doğası”, Ali Yaşar Sarıbay (Ed.), **Siyaset Sosyolojisi**, 2. Baskı içinde (20-50), Anadolu Üniversitesi Yayınları, Eskişehir.
- Kydd, Andrew H. (2015), **International Relations Theory: The Game Theoretic Approach**, Cambridge University Publishers, Cambridge.
- Latham, Robert (2003), **Introduction. In Bombs and Bandwidth: The Emerging Relationship Between Information Technology and Security**, The New Publishers, New York.

- Lewis, James Andrew (2002), "Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats", http://www.csis.org/media/isis/pubs/021101_risks_of_cyberterror.pdf (02.02.2022).
- Li, Y., & Liu, Q. (2021), A Comprehensive Review Study of Cyber-Attacks And Cyber Security; Emerging Trends And Recent Developments, **Energy Reports**, 7, 8176-8186.
- Libicki, Martin C. (2009), **Cyberdeterrence and Cyberwar**, RAND Publishers, USA.
- Lieberman, Elli (2013), **Reconceptualizing Deterrence: Nudging Toward Rationality in Middle Eastern Rivalries**, Routledge, New York.
- Lieberthal, Kenneth ve Singer, Peter Warren (2012), **Cybersecurity And US-China Relations**, Brookings Publishers, Washington.
- Lindsay, Jon R. (2014), "The Impact of China on Cybersecurity: Fiction and Friction, **International Security**, 39(3), 7-47.
- Lingzhi, Fan vd., (2022), "Exclusive: China a Main Target of US NSA Cyberattacks, with Key Infrastructure Under Threat", **Global Times**, <https://www.globaltimes.cn/page/202203/1253697.shtml> (12.04.2023).
- Liotta, Peter H. (2002), "Boomerang Effect: The Convergence of National and Human Security", **Security Dialogue**, 33(4), 473-488.
- Lukasik, Stephen J. (2011), "Why the Arpanet Was Built, IEEE Annals of the History of Computing", **IEEE Annals of the History of Computing**, 33(3), 7.
- Machiavelli, N. (2004), **Prens**, Can Yayınları, İstanbul.
- Maffra, Lourrene (2021), "Foreign Policy Analysis Methodology to Understand The Diffusion of Brazil's Agri-Food Policy Under Lula's Government", **Social Sciences and Humanities Studies Association**, 77-88.
- Magen, Sharon (2017), "Cybersecurity and Economic Espionage: The Case of Chinese Investments in the Middle East", **Cyber, Intelligence, and Security**, 1(3), 3.
- Maigre, Merle (2022), "NATO's Role in Global Cyber Security", **GMF**, <https://www.gmfus.org/news/natos-role-global-cyber-security> (12.04.2023).
- Mallick, Maj Gen PK (2022), "China's Developing Cyber Warfare Capabilities", Centre For Land Warfare Studies (Claws), 323, https://indianstrategicknowledgeonline.com/web/IB-323_China%E2%80%99s-Developing-Cyber-Warfare-Capabilities.pdf (12.04.2023).
- Manson, George Patterson (2011), "Cyberwar: The United States And China Prepare For The Next Generation Of Conflict", **Comparative Strategy**, 30(2), 121-133.

- Marmon, William (2011), "Main Cyber Threats Now Coming From Governments As "State Actors", <https://www.europeaninstitute.org/index.php/136-european-affairs/ea-november-2011/1464-main-cyber-threats-now-coming-from-governments-as-state-actors> (21.11.2022).
- Martelle, Michael (2019), "Siber Brifing: Çin'in Askeri Siber Kullanımı", **National Security Archive**, <https://nsarchive.gwu.edu/news/cyber-vault/2019-01-17/cyber-brief-chinas-military-use-cyber> (12.04.2023).
- Martina, Michael vd., (2015), "China's Xi Promises Better Investment Climate, Cyber War Deal Seen", <https://www.reuters.com/article/usa-china-idUSKCN0RN18R20150924> (12.04.2023).
- Mary Kaldor, (1998), **New and Old Wars: Organized Violence in a Global Era**, Polity Publishers, England.
- Mattelart, Armand (1994), **Mapping World Communication: War, Progress, Culture**, University of Minnesota Publishers, USA.
- McLuhan, M. (1963), **The Gutenberg Galaxy**, University of Toronto Press, Canada.
- Miller, Gregory D. (2003), "Hypotheses on Reputation: Alliance Cehrice and the Show of the Past", **Security Studies**, 12(3): 40-78.
- Mintz, Alex ve Derouen, Karl (2010), **Understanding Foreign Policy Drecisin Making**, Cambridge University Publishers, New York.
- Mitchell, Alison (2001), "A Nation Challenged: Computer Security; To Forestall a 'Digital Pearl Harbor' U.S. Looks to System Separate From Internet", <https://www.nytimes.com/2001/11/17/us/nation-challenged-computer-security-forestall-digital-pearl-harbor-us-looks.html> (02.12.2022).
- Modelski, George (1962), **A Theory of Foreign Policy**, Praeger, New York.
- Morgenthau, Hans Joachim vd. (1960), **Politics Among Nations: The Struggle for Power and Peace**, Alfred A. Knopf Publishers, New York.
- NASA (2019), "A Brief History of NASA", <https://history.nasa.gov/factsheet.htm> (21.11.2022).
- NATO (1999a), "An Alliance for the 21st Century Washington Summit Communique issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Washington", http://www.nato.int/cps/en/natolive/official_texts_27440.htm (21.11.2022).
- _____ (1999b), "The Alliance's Strategic Concept, 24 Nisan 1999", http://www.nato.int/cps/en/natolive/official_texts_27433.htm (21.11.2022).
- _____ (2002), "The Prague Summit and NATO's Transformation", <https://www.nato.int/docu/rdr-gde-prg/rdr-gde-prg-eng.pdf> (21.11.2022).

- _____ (2003), “The Prague Summit and NATO’s Transformation”, <http://www.nato.int/docu/rdr-gde-prg/rdr-gde-prgeng.pdf> (21.11.2022).
- _____ (2010), “NATO 2020; assured security, dynamic engagement”, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2010_05/20100517_100517_expertsreport.pdf (21.11.2022).
- _____ (2011), “NATO CIS Cervices Agency, NATO Cyber Defence Management”, http://www.nato.int/cps/en/natolive/news_85161.htm (21.11.2022).
- _____ (2012a), “Chicago Summit Declaration”, <http://www.nato.int/cps/en> (21.11.2022).
- _____ (2019), “NATO Cyber Defence”, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2019_02/20190208_1902-factsheet-cyber-defence-en.pdf (21.11.2022).
- _____ (2019), “NATO London Declaration”, https://www.nato.int/cps/en/natohq/official_texts_171584.htm (21.11.2022).
- _____ (2022), “NATO Secretary General Warns Of Growing Cyber Threat”, https://www.nato.int/cps/en/natohq/news_208889.htm?selectedLocale=en (12.04.2023).
- NATO CCDCOE (2019), “Exercises”, <https://ccdcoe.org/exercises/> (21.11.2022).
- _____ (2019), “CCD COE”, <https://ccdcoe.org/> (21.11.2022).
- Neack, Laura vd (1995), **Foreign Policy Analysis: Continuity and Change in Its Second Generation**, Prentice Hall College Publishers, New Jersey.
- Neack, Laura (2008), **The New Foreign Policy: U.S. and Comparative Foreign Policy in the 21st Century**, Rowman & Littlefield Publishers, Maryland.
- Neal, Jeff (2021), “ABD siber savaşı mı?”, <https://hls.harvard.edu/today/is-the-u-s-in-a-cyber-war/> (10.04.2023).
- Nissenbaum, Helen (2005), “Where Computer Security Meets National Security”, **Ethics and Information Technology** 7(2): 61–73.
- NSA, (2022), “NSA Siber Güvenlik”, <https://media.defense.gov/2022/Dec/15/2003133594/-1/-1/0/NSA%20Cybersecurity%20Year%20in%20Review%20v20221219.PDF> (11.04.2023)
- _____ (2022), “The Creation of NSA - Part 2 of 3: The Brownell Committee”
- NSS (2022), “Ulusal Güvenlik Stratejisi”, <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf> (11.04.2023)
- Oğuzlu, H. Tarık (2007), “Dünya Düzenleri ve Güvenlik: Ulus-Devlet Güvenlik Anlayışı Aşılıyor Mu?”, **Güvenlik Stratejileri Dergisi**, (6)14,7-42.
- Oil & Gas News January (2012), “UAE Delays Oil Pipeline to Bypass Hormuz to June”, <http://search.proquest.com/docview/916274658?accountid=14765> (12.04.2023).

- Öğüt, Adem (2003), **Bilgi Çağında Yönetim**, 2. Baskı, Nobel Yayıncılık, Ankara.
- Örgün, Faruk (2001), **Küresel Terör**, Okumuş Adam Yayınları, İstanbul.
- Örmeci, Ozan (2013), “21.Yüzyılda ABD-Çin Rekabeti”, **SDÜ Fen Edebiyat Fakültesi Sosyal Bilimler Dergisi**, 29, 1-14.
- Özcan, Arif Behiç (2011), “Uluslararası Güvenlik Sorunları ve ABD'nin Güvenlik Stratejileri”, **Selçuk Üniversitesi İİBF Sosyal ve Ekonomik Araştırmalar Dergisi**, 11(22), 451-470.
- Özdağ, Ümit (2018), **İstihbarat Teorisi**, Kripto Basım Yayım Dağıtım, Ankara.
- Özden, Yüksel (2000), **Öğrenme ve Öğretme**, 4. Baskı, Pegem A Yayıncılık, Ankara.
- Pajurek, Monika (2017), “Cybersecurity Military Entities of the United States of America”, **Facta Simonidis**, 10(1), 163-178.
- Pardhi, Megha (2022), “China’s New Focus on US Cyber Activities”, <https://thediplomat.com/2022/04/chinas-new-focus-on-us-cyber-activities/> (12.04.2023).
- Paul, Thazha Varkey (1994), **Asymmetric Conflicts: War Initiation by Weaker Powers**, 3. Baskı, Cambridge University Publishers, England.
- Plotnek, Jordan J. (2019), “Siber-Fiziksel Terörizme Karşı Akıllı Şebeke Direncinin Ölçülmesi: Literatür Taraması ve Tez Önerisi”, https://www.researchgate.net/figure/Features-inherent-to-cyber-terrorism-as-defined-in-current-literature-grouped_fig6_335540611 (24.02.2023).
- Polanyi, Karl (2005), **Büyük Dönüşüm**, İletişim Yayınları, İstanbul.
- Ponta, Adina (2021), “Responsible State Behavior In Cyberspace: Two New Reports From Parallel UN Processes”, **American Society of International Law**, 25, 14.
- Prasso, Sheridan (2019), “China’s Digital Silk Road Is Looking More Like an Iron Curtain”, <https://www.bloomberg.com/news/features/2019-01-10/china-s-digital-silk-road-is-looking-more-like-an-iron-curtain> (02.02.2022).
- Radiantlunatic (2019), ARPANET, <https://www.radiantlunatic.com/wp-content/uploads/2013/10/ARPANET.pdf> (02.02.2022).
- Raud, Mikk (2016), “China and Cyber: Attitudes, Strategies, Organization”, **Tallinn Paper**, 5-34.
- Richard, Alan Clarke & Robert, Knake (2010), “Cyber War: The Next Threat to National Security and What to Do About It”, **Studia Politicae Universitatis Silesiensis**, (11), 316-320.
- Roberts, Tom vd., (2011), Cyber Intelligence: Setting the Landscape for an Emerging Discipline, **Intelligence and National Security Alliance**, 9, 1-20.
- Rolse, Gideon (1988), Neoclassical Realism and Teories of Foreign Policy, **World Politics**, 51(1), 144-172.

Rosenau, James N., (1966), **Pre-theories and Theories of Foreign Policy**, 1st Ed., Routledge Publishers, England.

Sandıklı, Atilla ve Emeklier, Bilgehan (2012), Güvenlik Yaklaşımlarında Değişim ve Dönüşüm, **Teoriler Işığında Güvenlik, Savaş, Barış ve Çatışma Çözümleri Bilgesam Yayınları**, 3, 70.

Sanger, David E. vd., (2013), “Chinese Army Unit Is Seen as Tied to Hacking Against U.S”, **The New York Times**, <https://www.nytimes.com/2013/02/19/technology/chinas-army-is-seen-as-tied-to-hacking-against-us.html> (12.04.2023).

Schmidt, Michael Nikola (2016), “Super-Empowering of Non-State Actors in Cyberspace”, **World International Studies Committee**, https://www.academia.edu/10088487/Super_empowering_of_Non_State_Actors_in_Cyberspace (21.11.2022).

Schmitt, Michael N. (Ed.). (2013), **Tallinn Manual on the International Law Applicable to Cyber Warfare**, Cambridge University Publishers, England.

Segal, Adam (2017), “How China Is Preparing For Cyberwar”, <https://www.csmonitor.com/World/Passcode/Passcode-Voices/2017/0320/How-China-is-preparing-for-cyberwar> (12.04.2023).

_____ (2022), “Hearing On China’s Cyber Capabilities: Warfare, Espionage, and Implications For The United States”, **The U.S.-China Economic and Security Review Commission**, 2-3.

Sen, Gautam (2019), “China’s Cybersecurity Strategy: Global Implications”, **Scholar Warrior Journal**, 128-134.

Seren, Merve (2006), “Siber Tehditlerle Mücadelede Farkındalık ve Hazırlık.”, **Siyaset, Ekonomi ve Toplum Araştırmaları Vakfı (SETA)**, 183,16-17.

Seren, Merve (2020), “Büyük Güçlerin Siber Savaşı”, <https://www.aa.com.tr/tr/analiz/buyuk-guclerin-siber-savasi/2086047> (21.11.2022).

Sertçelik, Aşır (2015), “Siber Olaylar Ekseninde Siber Güvenliği Anlamak”, **Medeniyet Araştırmaları Dergisi**, 2(3), 25-42.

Shaw, Martin (2000), **Theory of the Global State**, Cambridge University Press, England.

Siber Güvenlik Nedir? (2021), <https://www.kaspersky.com.tr/resource-center/definitions/what-is-cyber-security> (21.11.2022).

Singer, J. David (1961), “The Level-of-Analysis Problem in International Relations”, **World Politics**, 14(1), 77-92.

Snyder, Richard C. Vd. (2002), **Decision-Making as an Approach to the Study of International Politics Foreign Policy Decision-Making**, Pelgrave MacMillan Publishers, New York.

- Sondermann, Fred A. (1961), **International Politics and Foreign Policy: A Reader in Research and Theory**, Free Publishers, New York.
- South China Morning Post (2015), “Turkey Says ‘Yes’ to China’s Trade Initiative, ‘No’ to Its Missiles”, <https://www.scmp.com/news/china/diplomacy-defence/article/1879097/turkey-says-yes-chinas-trade-initiative-no-its-missiles> (12.04.2023).
- Sönmezoğlu, Faruk (1992), **Uluslararası İlişkiler Sözlüğü**, Beta Yayınları, İstanbul.
- _____ (2005), **Uluslararası Politika ve Dış Politika Analizi**, 4. Basım, Filiz Kitabevi, İstanbul.
- Spade, Jayson M. (2012), **Information As Power: China's Cyber Power and American 's National Security**, US Army War College, USA.
- Swaine, Michael D. (2013), “Chinese Views On Cybersecurity In Foreign Relations”, **China Leadership Monitor**, 42, 1-27.
- Szalai, Andras (2009), “Coping With the Security Dilemma: A Fundamental Ambiguity of State Behaviour Ambiguities”, **The Skepsi Editorial Board**, 2(2), 103-119.
- Taddeo, Mariarosaria (2018), “How to Deter in Cyberspace”, https://www.researchgate.net/figure/The-three-elements-of-Cyber-Deterrence-Theory-and-their-dependencies-How-to-Deter-in_fig1_338843339 (22.02.2023).
- Talihärm, Anna-Maria (2013), “Towards Cyberpeace: Managing Cyberwar Through International Cooperation”, <https://www.un.org/en/chronicle/article/towards-cyberpeace-managing-cyberwar-through-international-cooperation> (12.04.2023).
- Tandoğan, Uğur (2010), “Dünya Gazetesi”, <https://www.dunya.com/kose-yazisi/savasa-hazir-miyiz/7527> (06.01.2022).
- Taner Altunok ve Zeynep Kaya (Ed) (2009), **Suç, Terör ve Savaş Üçgeninde Siber Dünya**, Platin Kitabevi, Ankara.
- TASAM, (2004), <http://www.tasam.org>. (22.12.2022).
- TDK (2021), http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.55355d01abed21.36704295 (22.12.2022).
- _____ (2022), “Güncel Türkçe Sözlük İstihbarat”, http://www.tdk.gov.tr/index.php?option=com_gts&arama=gts&guid=TDK.GTS.5c894e4f166307.32122960 (22.12.2022).
- Ten, C. W. Manimaran vd. (2010), “Cybersecurity for Critical Infrastructures: Attack and Defense Modelling”, **IEEE**, 40(4), 853-865.
- The Carnegie Endowment For International Peace, (t.y), “U.S.-China Cyber Stability”, <https://carnegieendowment.org/programs/technology/cyber/uschinacyberstability> (12.04.2023).

- Tirrell, K. William (2012), **United States Cyber Security Strategy, Policy and Organization: Poorly Postured to Cope With a Post-9/11 Security Environment**, Master Thesis, Washington University, The George Washington University, Military Art and Science.
- TNETWORKS, (2021), <http://www.tnetworks.com.tr/cozumler/advanced-persistent-threats-apt> (22.12.2022).
- Tombul, Fatih (Ed) (2015), **Uluslararası Siber Güvenlik Perspektifinde Siber Güvenlik, Siber Suçlar: Tehditler, Farkındalık ve Mücadele**, Farkındalık ve Mücadele, Global Politika ve Strateji Yayınları, Ankara.
- Tüm Ordunun Birinci Sınıf Askeri Kurum ve Askeri Birimleri 84 Olarak Yeniden Yapılandırıldı ve Xi Jinping Talimatlar Verdi (2017), http://news.xinhuanet.com/politics/2017-04/19/c_129550371.htm (14.12.2022).
- Tzu, S. (2018), **Savaş Sanatı**, Salon Yayınları, İstanbul.
- U.S. Cyber Command (2019), <https://www.cybercom.mil/About/History> (02.02.2022).
- U.S. Department of Defense (2018), “Remarks by Secretary Mattis on the National Defense Strategy”, <https://dod.defense.gov/News/Transcripts/Transcript-View/Article/1420042/remarks-by-secretary-mattis-on-the-national-defense-strategy/> (13.12.2022).
- U.S. Department of Homeland Security Office (2020), “Çin Oluşturduğu Tehditle Mücadele Etmek İçin DHS Stratejik Eylem Planı”, https://www.dhs.gov/sites/default/files/publications/21_0112_plec_dhs-china-sap.pdf (11.04.2023).
- _____ (2016), “Siber Olay Müdahalesinde DHS’nin Rolü”, <https://www.cisa.gov/sites/default/files/publications/DHS%20Cyber%20Incident%20Response%20Fact%20Sheet%20v15%20-%200508%20Compliant.pdf> (11.04.2023).
- UN Group of Governmental Experts (2013), “Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,” A/68/98, 8.
- _____ (2015), “Report of the Group of Governmental Experts on Developments in the Field of Information and Telecommunications in the Context of International Security,” A/70/174, 7-8.
- URL, “China Accuses US Of 'Tens Of Thousands' Of Cyberattacks” (2022), <https://www.france24.com/en/live-news/20220905-china-accuses-us-of-tens-of-thousands-of-cyberattacks> (12.04.2023).
- _____, “Cyber Coalition: NATO’s Flagship Cyber Exercise”, <https://www.act.nato.int/cyber-coalition> (12.04.2023).

- _____, “Evaluating China’s Road to Cyber Super Power”, https://nsiteam.com/social/wp-content/uploads/2022/01/Williams_STRATCOM-2021-11-17D.pdf (12.04.2023).
- _____, “China’s Cyberattack Strategy Explained” (t.y.), <https://www.boozallen.com/insights/cyber/chinas-cyberattack-strategy-explained.html> (01.09.2023).
- _____, “Digital Around The World” (2023), <https://datareportal.com/global-digital-overview> (02.09.2023).
- US PCCIP (1997), Critical Foundations Protecting America’s Infrastructures. The Report of the President’s Commission on Critical Infrastructure Protection President’s Commission on Critical Infrastructure Protection, Washington, DC: White House.
- US-China Economic and Security Review Commission (2019), “Report To Congress Of The US-China Economic And Security Review Commission”, **US-China Economic and Security Review Commission**.
- USOM (2014), “Siber Güvenliğe ilişkin Temel Bilgiler”, <http://some.sdu.edu.tr/assets/uploads/sites/408/files/siber-guvenlige-iliskin-temel-bilgiler22092017.pdf> (11.11.2022).
- Ünal, Ahmet Naci (2015), **Siber Güvenlik ve Elektronik Bileşenleri**, Nobel Yayınları, Ankara.
- Van Epps, Geoff (2013), “Common Ground: US and NATO Engagement with Russia in The Cyber Domain”, **Connections**, 12(4), 15-50.
- Van Ness, Peter (2002), “Hegemony, Not Anarchy: Why China and Japan Are Not Balancing US Unipolar Power”, **International Relations of the Asia-Pacific**, 2(1), 131-150.
- Voo, Julia vd., (2020), “National Cyber Power Index 2020: Methodology and Analytical Considerations”, **China Cyber Policy Initiative Reports**.
- Wall, Mike (2017), “Sputnik 1! 7 Fun Facts About Humanity's First Satellite”, <https://www.space.com/38331-sputnik-satellite-fun-facts.html> (02.02.2022).
- Wallerstein, Immanuel (2013), **Bilginin Belirsizlikleri**, Sümer Yayıncılık, İstanbul.
- Waltz, Kenneth N. (1959) **Man, The State, and War: A Theoretical Analysis**, Columbia University Press, New York.
- _____ (2000), “Globalization and American Power”, **The National Interest**, (59), 46-56.
- Warner, Michael (2012), “Cybersecurity: A Pre-History”, **Intelligence and National Security**, 27(5), 781-799.
- Warner, Michael & Walker, Stephen G. (2011), “Thinking About The Role of Religion In Foreign Policy: A Framework For Analysis”, **Foreign Policy Analysis**, 7(1), 113-135.

- Wendt, Alexander (1999), **Social Theory of International Politics**, Cambridge University Publishers, England.
- West, Dave (2022), “Dijital Çağın Dağıtım Aşamasındayız”, <https://www.scrum.org/resources/blog/we-are-entering-deployment-phase-digital-age> (19.02.2023).
- WH (2003), “The National Strategy to Secure Cyberspace. Washington: The White House”, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf (21.12.2022).
- White, Bret Austin (2020), **Reordering The Law For A China World Order: China's Legal Warfare Strategy in Outer Space and Cyberspace**, Journal of National Security Law & Policy Publishers, USA.
- White, Brian (Ed.) (1989), **Analyzing Foreign Policy: Problems and Approaches, Understanding Foreign Policy Systems**, Edward Elgar Publishers, England.
- Wiener, Norbert (1948), **Cybernetics: or Control and Communication in the Animal and the Machine**, MIT Publishers, Paris.
- Williams, Paul D. (2008), **Security Studies: An Introduction**, Routledge Publishers, New York.
- Wolfres, Arnold (1952), “National Security As An Ambiguous Symbol”, **Political Science Quarterly**, 4(67). 481-502.
- World Bank (2019), <https://www.worldbank.org/en/country/china/overview#1> (02.12.2022).
- Wu, Ji (2017), **Calling Taikong: A Strategy Report and Study of China's Future Space Science Missions**, Springer Publishers, New York.
- Wuthnow, Joel ve Phillip C. Saunders (2017), **Chinese Military Reforms in the Age of Xi Jinping: Drivers, Challenges, and Implications**, National Defense University Publishers, Washington.
- Xinhua (2017), “China Focus: Be Ready to Win Wars, China 's Xi Orders Reshaped PLA”, http://www.xinhuanet.com/english/2017-08/01/c_136491455.htm (15.12.2022).
- Xinhua (2018), “Xinhua Headlines: Xi Outlines Blueprint To Develop China's Strength In Cyberspace”, http://www.xinhuanet.com/english/2018-04/21/c_137127374.htm (12.04.2023).
- Xinyi, Xiong ve Hongpei, Zhang (2021), “China Launches 3-Year Draft Plan For Cybersecurity Sector After Regulatory Actions”, **Global Times**, <https://www.globaltimes.cn/page/202107/1228461.shtml> (12.04.2023).
- Xu, Manshu, ve Lu, Chuanying (2021), “China–US Cyber-Crisis Management”, **China International Strategy Review**, 3, 97-114.
- Xuetong, Yan (2017), “Strategic Challenges for China's Rise”, **Carnegie-Tsinghua Center For Global Policy**, <https://perma.cc/J8VU-5E7V>, (12.04.2023).

- Yener, Yavuz (2014), “NATO ve Siber Güvenlik 2-Strateji”, **Siber Bülten**, <https://siberbulten.com/makale-analiz/nato-ve-siber-guvenlik-2-strateji/> (06.01.2022).
- Yılmaz, Sait (2007), “Güçsüz Güç”, **Güvenlik Stratejileri Dergisi**, 3(05), 67-103.
- Yılmaz, Sait ve Salcan, Olay (2008), **Siber Uzayda Güvenlik ve Türkiye**, Milenyum Yayınları, İstanbul.
- Zhang, Li (2012), “A Chinese perspective on cyber war”, **International Review of the Red Cross**, 94(886), 801-807.
- Ziegler, Jean (2004), **Dünyanın Yeni Sahipleri ve Onlara Direnenler** (Çev. Mahmut Nedim Demirtaş), Altın Kitaplar, İstanbul.

ÖZGEÇMİŞ

2014 yılında Erzurum Anadolu Lisesi'ni, 2019 yılında da Karadeniz Teknik Üniversitesi – İktisadi ve İdari Bilimler Fakültesi, Uluslararası İlişkiler Bölümü'nü bitirdi. 2021 yılında Karadeniz Teknik Üniversitesi, Uluslararası İlişkiler Anabilim Dalında yüksek lisans programına başladı. Uluslararası bir şirket için Kuveyt, Katar, B.A.E., Suudi Arabistan, Umman, Yemen, Lübnan, Ürdün, Mısır, Cezayir ve Tunus bölgelerindeki yatırım danışmanı olan Dila Nur ÖZHANCI şimdi kendi şirketini yönetmektedir.

ÖZHANCI, bekar olup İngilizce-Arapça dillerini ana dili gibi konuşurken orta düzeyde Almanca ve Rusça bilmektedir.