



**T.C.
BATMAN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER
ANABİLİM DALI**

YÜKSEK LİSANS TEZİ

**ÇİN HALK CUMHURİYETİ'NİN SİBER GÜVENLİK
POLİTİKALARI**

**Hazırlayan
Zelal ÇAĞLIN**

**Danışman
Doç. Dr. Fulya KÖKSOY**

**Haziran-2024
BATMAN
Her Hakkı Saklıdır.**

T.C.
BATMAN ÜNİVERSİTESİ
LİSANSÜSTÜ EĞİTİM ENSTİTÜSÜ
SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER
ANABİLİM DALI

YÜKSEK LİSANS TEZİ

ÇİN HALK CUMHURİYETİ'NİN SİBER GÜVENLİK
POLİTİKALARI

Hazırlayan
Zelal ÇAĞLIN

Danışman
Doç. Dr. Fulya KÖKSOY

Haziran-2024
BATMAN
Her Hakkı Saklıdır.

TEZ KABUL VE ONAYI

Zelal AĐLIN tarafından hazırlanan ‘‘Çin Halk Cumhuriyeti’nin Siber Güvenlik Politikaları’’ adlı tez alışması 06/06/2024 tarihinde aşığıdaki jüri tarafından oy birliğı ile Batman Üniversitesi Lisansüstü Eğitim Enstitüsü Siyaset Bilimi ve Kamu Yönetimi Anabilim Dalı, Siyaset Bilimi ve Uluslararası İlişkiler Programı’nda YÜKSEK LİSANS TEZİ olarak kabul edilmiştir.

Jüri Üyeleri

İmza

Başkan

Prof. Dr. Ahmet İLYAS

Danışman

Doç.Dr. Fulya KÖKSOY

Üye

Doç. Dr. Murat CİHANGİR

Yukarıdaki sonucu onaylarım.

Dr. Öğr. Üyesi Ömer Murat ÖTER
Lisansüstü Eğitim Enstitüsü Müdürü

TEZ BİLDİRİMİ

Bu tezdeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edildiğini ve tez yazım kurallarına uygun olarak hazırlanan bu çalışmada bana ait olmayan her türlü ifade ve bilginin kaynağına eksiksiz atıf yapıldığını bildiririm.

DECLARATION PAGE

I hereby declare that all information in this document has been obtained and presented in accordance with academic rules and ethical conduct. I also declare that, as required by these rules and conduct, I have fully cited and referenced all material and results that are not original to this work.

Zelal ÇAĞLIN

06/06/2024

ÖZET

YÜKSEK LİSANS TEZİ

ÇİN HALK CUMHURİYETİ’NİN SİBER GÜVENLİK POLİTİKALARI

Zelal Çağlın

Batman Üniversitesi Lisansüstü Eğitim Enstitüsü
Siyaset Bilimi ve Kamu Yönetimi Uluslararası İlişkiler Anabilim Dalı
Siyaset Bilimi ve Uluslararası İlişkiler Programı

Danışman: Doç. Dr. Fulya KÖKSOY
2024, 234 Sayfa

JÜRİ

Prof. Dr. Ahmet İlyas
Doç. Dr. Fulya Köksoy
Doç. Dr. Murat Cihangir

Soğuk Savaş sonrasında küreselleşmenin ivme kazanmasıyla beraber bilişim ve teknolojiye sürekli bir değişim ve dönüşüm gözlemlenmektedir. Bu değişim birçok alana etki ettiği gibi güvenlik alanına da etki etmektedir. Ekonomik, sosyal, toplumsal, siyasal, çevre, organize suçlar gibi birçok alanda farklı güvenlik sorunları karşımıza çıkmaktadır. Teknolojik gelişme sonrasında internetin daha çok yaygınlaşmasıyla beraber güvenlik sorunlarındaki çeşitliliğin kabuk değiştirdiği, siber uzayın güvenlik sorunlarından etkilenen alanlar arasında yerini almaya başladığı görülmektedir. Gerçek dünyadan yavaş yavaş uzaklaşan ve siber uzayın hâkim olduğu bu dönemde yeni sorunların beraberinde getirdiği risk ve tehditlere karşı güvenliği sağlamak adına siber güvenlik kavramı ortaya çıkmaktadır. Yakın bir geçmişe sahip olan siber güvenlik olgusu, her geçen gün daha da büyük bir soruna dönüşmektedir. Siber uzayda belli bir güç elde etme ve bu alanı kontrol altında tutma çabasına girilmesi, siber suçlar ve siber saldırıların artması gibi durumlar devletlerin, kamu kurum ve kuruluşların, özel sektörlerin vs. böylesine önem arz eden bu konu ile ilgili bir takım politika/strateji belirlemesine sebep olmaktadır.

Bu çalışmanın amacı; güç elde etme hususunda tek olma arzusuyla hareket eden ve özel olarak politikalarının bazı kısımlarını kamuoyuyla paylaşıp da genel olarak söz konusu politikalarının tamamını diğer devletlere karşı gizli tutan, aynı zamanda gelişmiş ülkelere göre internetle biraz daha geç tanışmasına rağmen günümüzde teknolojinin önde gelen isimlerinden biri hâline gelen ve teknolojinin gelişmesine büyük katkıda bulunan Çin Halk Cumhuriyeti’nin siber güvenlik politikalarını incelemektir. Çalışma kapsamında öncelikle siber kavramı üzerinde durularak, ilgili alanın gelişim süreci hakkında bilgi verilecektir. Akabinde Çin Halk Cumhuriyeti’nin uygulamış olduğu ulusal ve uluslararası güvenlik politikaları incelenerek siber güvenliğe nasıl geçiş yapıldığı ve bu süreçte izlenmiş olduğu politikalara değinilecektir.

Anahtar Kelimeler: Siber, Siber Güvenlik, Çin Halk Cumhuriyeti, Çin Halk Cumhuriyeti’nin Siber Güvenlik Politikaları

ABSTRACT**MS THESIS****CYBER SECURITY POLICIES OF THE PEOPLE'S REPUBLIC OF CHINA****Zelal AĞLIN**

**BATMAN UNIVERSITY INSTITUTE OF SOCIAL SCIENCES
DEPARTMENT OF POLITICAL SCIENCE AND PUBLIC ADMINISTRATION
POLITICAL SCIENCE AND INTERNATIONAL RELATIONS PROGRAM**

Advisor: Assoc. Prof. PhD. Fulya KÖKSOY**2024, 234 Pages****Jury****Prof. Dr. Ahmet İLYAS****Doç. Dr. Fulya KÖKSOY****Doç. Dr. Murat CİHANGİR**

With the acceleration of globalization after the Cold War, a constant change and transformation is observed in technology. This change affects many areas, as well as the security field. We encounter different security problems in many areas such as economic, social, political, environmental and organized crime. As the internet becomes more widespread after technological development, the diversity in security problems has changed even more and cyberspace has begun to take its place among the areas affected by security problems. In this period when the real world is gradually moving away and cyberspace dominates, the concept of cyber security is emerging in order to ensure security against the risks and threats brought by new problems. The phenomenon of cyber security, which has a recent history, is turning into a bigger problem every day. Situations such as efforts to gain a certain power in cyberspace and keep this area under control, and the increase in cyber crimes and cyber attacks cause states, public institutions and organizations, and private sectors to determine a number of policies/strategies regarding this important issue.

The purpose of this study is to examine the cyber security policies of the People's Republic of China, which is acting with the desire to be unique in gaining power, generally keeping all of its policies secret to other states, but sharing some parts of its policies with the public; furthermore, despite being introduced to the internet a little later than developed countries, which has become one of the leading names in technology today, and has contributed greatly to the development of technology. Within the scope of the study, the concept of cyber will be emphasized and information will be given about the development process of the relevant field. Subsequently, the national and international security policies implemented by the People's Republic of China will be examined and how the transition to cyber security was made and the policies followed in this process will be discussed.

Key Words: Cyber, Cyber Security, People's Republic of China, Cyber Security Policies of the People's Republic of China

ÖNSÖZ

Tez çalışmamın her aşamasında yolumu aydınlatan, engin bilgi ve tecrübeleriyle beni en güzel şekilde yönlendiren ve desteğini hiçbir zaman esirgemeyen değerli danışmanım/hocam Doç. Dr. Fulya KÖKSOY'a ve bu süreçte yükümü benimle birlikte sırtlayan sevgili aileme ve özellikle canım annem Kadriye ÇAĞLIN'a sonsuz teşekkürlerimi sunarım. Tezimi benim bu günlere gelmemde büyük emeği olan ve şuan yanımda olmasada bir yerlerden beni gördüğüne inandığım ve başarımla gururlanacağına inandığım 'Kahramanım' rahmetli babam Ali ÇAĞLIN'a ithaf ediyorum.

Tezimin, bu alanda çalışma yapan tüm araştırmacıların yoluna ışık tutması ve yararlı olması ümidiyle...

Zelal ÇAĞLIN

BATMAN-2024

İÇİNDEKİLER

ÖZET	iv
ABSTRACT.....	v
ÖNSÖZ	vi
İÇİNDEKİLER	vii
GİRİŞ.....	1
BİRİNCİ BÖLÜM	8
1. Kavramsal Çerçeve	8
1.1. Siber Kavramı	8
1.2. Siber Kavramının Gelişimi	9
1.2.1. Siber Uzaya Genel Bakış	10
1.2.2. Siber Saldırı ve Türleri.....	13
1.2.3. Siber Tehdit, Türleri ve Araçları	21
1.2.3.1. Siber Suç	26
1.2.3.2. Siber Terörizm	28
1.2.3.3. Siber Caydırıcılık	29
1.2.3.4. Siber İstihbarat ve Siber Casusluk	30
1.2.3.5. Siber Savaş	32
1.3. Güvenlik Alanında Oluşan Yeni Tehdit: Siber Güvenlik	33
1.3.1. Güvenlik Kavramı ve Dönüşümü.....	34
1.3.2. Siber Güvenlik Kavramı ve Tarihçesi.....	43
1.3.3. Siber Güvenlik Çalışmalarına Genel Bakış.....	48
İKİNCİ BÖLÜM.....	66
2. Dış Politika ve Ulusal Güvenlik.....	66
2.1. Tarihsel Gelişim.....	67
2.1.1. Devrim Dönemi (1949-1978).....	71
2.1.2. Reform Dönemi (1978 ve Sonrası)	79
2.2. Dış Politika.....	87
2.2.1. Dış Politikanın Oluşumundaki Faktörler ve Karar Verme Süreci.....	89
2.2.2. Dış Politikada Dönüşüm Süreci ve Süreklilik.....	92
2.3. Dönemsel Açıdan Dış Politika	93
2.3.1. Mao Zedong Dönemi (1949-1976)	93
2.3.2. Deng Xiaoping Dönemi (1978-1992)	95

2.3.3.	Jiang Zemin Dönemi (1993-2002)	98
2.3.4.	Hu Jintao Dönemi (2002-2012).....	100
2.3.5.	Xi Jinping Dönemi (2012-...)	104
2.4.	Genel Bir Perspektiften Ulusal Güvenlik Anlayışı	112
2.5.	Yeni Dönem Ulusal Güvenlik Anlayışı	118
ÜÇÜNCÜ BÖLÜM		125
3. Çin Bağlamında Siber Güvenlik		125
3.1.	Çin’de İnternetin Gelişim Süreci	125
3.2.	Çin’in Siber Güvenlik Politikaları	132
3.2.1.	Siber Güvenlik Yasası.....	158
3.2.2.	Çin’in Siber Güvenlik Aktörleri.....	163
3.2.3.	Çin ve Batı Dünyası Açısından Siber Güvenlik.....	167
3.3.	Çin Bağlamında Siber Saldırıları	171
SONUÇ		186
KAYNAKLAR		192

KISALTMALAR

AB	Avrupa Birliđi
ABD	Amerika Birleşik Devletleri
AGİT	Avrupa Güvenlik ve İşbirliđi Teşkilatı
AIIB	Asya Altyapı Yatırım Bankası
APEC	Asya-Pasifik Ekonomik İşbirliđi Örgütü
APEC	Asya Pasifik Ekonomik İşbirliđi Örgütü
APT	Advanced Persistent Threats-Gelişmiş Siber Tehditler
AR-GE	Araştırma Geliştirme
ARPANET	İleri Araştırma Projeleri Yerel Ağı
ASEAN	Güneydođu Asya Ülkeleri Birliđi
BKBY	Bir Kuşak Bir Yol
BM	Birleşmiş Milletler
BMGK	Birleşmiş Milletler Güvenlik Konseyi
BRICS	Brazil, Russia, India, China, South Africa
CANET	Çin Akademik Ağı
CD	Silahsızlandırma Konferansı
CEC	China Electronics Corporation
CERN	Avrupa Nükleer Araştırma Merkezi
CETC	China Electronics Technology Group
CIA	Central Intelligence Agency-Merkezi Haber Alma Teşkilatı
CNCERT	The National Computer Network Emergency Response Technical Team/Coordination Centre of China-Çin Ulusal Bilgisayar Ağı Acil Müdahale Teknik Ekibi/ Koordinasyon Merkezi
CNISTEC	Çin Bilgi Teknolojisi Güvenlik Deđerlendirme Merkezi
CTA	Orta Tibet İdaresi
CTBT	Kapsamlı Nükleer Test Yasağı Sözleşmesi
ÇHC	Çin Halk Cumhuriyeti
ÇKP	Çin Komünist Partisi
DDoS	Dağıtık Hizmet Aksatma Saldırısı
DoS	Hizmet Dışı Bırakma
DTÖ	Dünya Ticaret Örgütü
FBI	Federal Bureau of Investigation-Federal Araştırma Bürosu
GFC	Great Firewall of China-Çin'in Büyük Güvenlik Duvarı
ICANN	İnternet Tahsisli Sayılar ve İsimler Kurumu

IDC	International Data Corporation
IT	Bilgi Teknolojisi
ITU	Uluslararası Telekomünikasyon Birliği
KGAÖ	Kolektif Güvenlik Anlaşması Örgütü
KYG	Kuşak ve Yol Girişimi
MDN	Tayvan Milli Savunma Bakanlığı
MIIT	Ministry of Industry and Information Technology-Sanayi ve Bilgi Teknolojileri Bakanlığı
MLPS	Multi-Level Protection Scheme
MOFA	Tayvan Dışişleri Bakanlığı
MPS	The Ministry of Public Security-Kamu Güvenliği Bakanlığı
MSS	Ministry of State Security-Devlet Güvenlik Bakanlığı
NASA	National Aeronautics and Space Administration-Ulusal Havacılık ve Uzay Dairesi
NATO	Kuzey Atlantik Antlaşması Örgütü
NIP	Ulusal Enformatizasyon Planı
NPC	National People's Congress
NSA	Ulusal Güvenlik Teşkilatı
PLA	People's Liberation Army-Çin Halk Kurtuluş Ordusu
RAT	Remote Access Trojan- Uzaktan Erişim Truva Atı
SASTIND	State Administration for Science, Technology and Industry for National Defense-Ulusal Savunma Bilim, Teknoloji ve Sanayi Devlet İdaresi
SBKP	Sovyetler Birliği Komünist Partisi
SILG	State Informatisation Leading Group-Devlet Bilişim Öncü Grubu
SNISCS	State Network and Information Security Coordination Small Group Devlet Ağı ve Bilgi Güvenliği Koordinasyon Küçük Grubu
SSCB	Sovyet Sosyalist Cumhuriyetler Birliği
STK	Sivil Toplum Kuruluşları
ŞİÖ	Şangay İşbirliği Örgütü
TDK	Türk Dil Kurumu
UDHB	Ulaştırma Denizcilik ve Haberleşme Bakanlığı
UNODC	Birleşmiş Milletler Uyuşturucu ve Suç Ofisi
USCYBERCOM	Birleşik Devletler Siber Komutanlığı
USSSTRATCOM	ABD Stratejik Komutanlığı
VPN	Virtual Private Network-Sanal Özel Ağ

GİRİŞ

Soğuk Savaş sonrası dönemde küreselleşmenin ivme kazanmasıyla beraber 1990'lı yıllara gelindiğinde güvenlik olgusunda büyük bir değişim ve dönüşüm sürecine girildiği görülmektedir. Bilişim teknolojilerinin hızla gelişimi ve internet kullanımının artması, siber kavramının çeşitlenmesine ve siber kavramına ait alt başlıkların oluşumuna sebep olmaktadır. Nitekim siber suç, siber saldırı, siber savaş, siber tehdit vb. gibi kavramların yanında ülkelerin güvenlik algılarındaki değişim ile beraber daha da önem kazanan “siber güvenlik” olgusu ortaya çıkmaktadır. Güvenlik sorunlarının derinleşmesi ve güvenlik olgusunun çeşitlenmesiyle beraber askeri tehdit odaklı olan geleneksel güvenlik anlayışı yerine, teknolojinin gelişmesiyle artan ve siber alanda sıkça karşılaşılan risk ve tehditlere karşı yeni güvenlik anlayışı benimsenmektedir.

Bilgisayar güvenliği olarak da anılan siber güvenlik kavramı, “elektronik ortamlarda bilgisayar sistemlerine ya da verilerine internet aracılığıyla müdahale edilmesinin önüne geçmek, bu sistemleri ya da verileri korumak” şeklinde tanımlanmaktadır (Athanassouli, 2019: 41). Yeni bir dünya düzeninin oluşmasında büyük etkisi bulunan siber güvenlik olgusu, günümüzde birçok alanda karşımıza çıkmaktadır. Öyle ki kişisel bilgilerden gizli hükûmet bilgilerine, sağlıktan bankacılık işlemlerine, işletmelerin işleyişinden bilimsel araştırmalara kadar hemen hemen hayatımızın her alanındaki bilgiye internet üzerinden ulaşılabilir. Böylesi önemli bilgilere erişimin bu kadar kolay olması, bilgilerin ele geçirilebilme ve ifşa edilebilme gibi tehlikelerin bulunması devletleri çok ciddi zarara uğratacağından dolayı büyük endişeye sebep olmaktadır. Bundan dolayı bu bilgilerin himaye edilmesi devletlerin en önemli görevlerinden biri hâline gelmektedir.

Siber güvenliğin önem kazandığı yeni dünya düzeninde devletlerarasında öne çıkan güç yarışı ve yapılan savaşlarda ise bilişim teknolojileri ve internet üstünlüğü öncü bir rol oynamaktadır. Yeni dünya düzeninde siber uzayın kullanımı arttıkça yalnızca devletlerarası ilişkilerde değil aynı zamanda özel sektörde de siber saldırı sayıları artmaktadır. Karşılaşılan bu siber saldırıların ve tehditlerin artması hem sivil topluma hem de uluslararası barışa büyük hasarlar vermektedir. 1999 yılında yaşanan Amerika Birleşik Devletleri'nin (ABD) Belgrad'daki Çin Büyükelçiliğini bombalaması bu duruma en iyi örneği teşkil etmektedir. Bu olayda Çinli hackerlar ABD hükûmetinin internet sitesini okunamayacak duruma getirmiştir. Aynı şekilde ABD'li hackerlar da buna kayıtsız kalmayarak benzer şekilde karşılık vermiştir (Spade, 2012: 4). Yaşanan bu

ve benzeri olaylardan dolayı devletlerin özellikle 2000’li yıllara gelindiğinde siber alanda güçlenme yoluna gittikleri görülmektedir.

1949 yılında Çin Halk Cumhuriyeti’nin (ÇHC) kurulmasını sağlayan Mao Zedong’un içe dönük tutumunun ardından 1978 yılında ÇHC’nin başına gelen Deng Xiaoping’in gerçekleştirdiği “reform ve dışa açılma” politikası ile beraber hızlı bir büyüme sürecine giren ÇHC, günümüzde ABD’den sonra dünyada en büyük ekonomiye sahip ikinci ülke konumuna gelmektedir. Deng dönemiyle beraber hızlı bir büyüme gösteren ÇHC’nin sahip olduğu özellikler ve takip ettiği birtakım politikalar neticesinde küresel bir aktör hâline geldiği görülmektedir. Bu özellikler/politikalar (Köksoy, 2019: 338):

- Nüfus oranının yüksek seviyede olması,
- Uygulamış olduğu “reform ve dışa açılım” politikasıyla beraber küresel sisteme uyum sağlaması,
- Mao döneminde uygulanan içe dönük, reaktif dış politika eğiliminin terk edilmesi ve Deng ile beraber dışa dönük ve proaktif bir dış politika eğilimine gidilmesiyle beraber yükselen bir ekonomik profile ulaşılması,
- Asya-Pasifik coğrafyasının dışına çıkarak sergilemiş olduğu aktif politikalar dolayısıyla hem bölgesel hem de küresel ortamda ön plana çıkmaya başlaması,
- Birleşmiş Milletler Güvenlik Konseyi’nin (BMGK) daimi beş üyesinden birisi olduğundan dolayı veto hakkına sahip olması,
- Doğal kaynaklar açısından zengin olması,
- Sürekli gelişen teknolojiye sahip olması,
- Askeri kapasitesinin güçlü olması, şeklinde sıralanmaktadır.

Yukarıda belirtilen tüm bu maddeler doğrultusunda ÇHC, uluslararası sistemde var olan diğer aktörler tarafından merakla takip edilmekte ve dünya siyasetinde büyük öneme sahip bir devlet portresi çizmektedir. İşte tam da bu noktada ÇHC, son zamanlarda siber saldırılar hususunda en fazla hedef gösterilen ülkelerden biri olarak karşımıza çıkmaktadır.

Siber saldırılar hususunda tüm dikkatleri üzerine çeken ÇHC, uğramış olduğu saldırılar ve herhangi bir ülkeye yapılan siber saldırılarda hedef gösterilmesinden dolayı siber kapasitesini her geçen gün daha da güçlendirme yoluna gitmektedir. Teknoloji alanında bir dünya markası hâline gelen ve “teknoloji devi” olarak anılan ÇHC’nin önemi, siber uzayda da ortaya çıkmaktadır. İnternet kullanımının yaygınlaşmasıyla

beraber yapılan son arařtırmalar ışığında dünya nüfusunun %64,4'ü internet, %59,4'ü ise sosyal medya kullanmaktadır (Burma ve Özdemir, 2024: 6). 2024 verilerine göre, 1,4 milyarlık nüfusuyla dünyanın en kalabalık ikinci ülkesi olan ÇHC'de, 2023'te yapılan arařtırmayla 1 milyar 90 milyonluk internet kullanıcısına ulařıldığı belirtilirken, nüfusun %77,5'inin ise çevrim içi hâle geldiđi vurgulanmaktadır (Population, 2024; 24 Radyo, 2024). Nitekim 2023 yılı itibarıyla dünyadaki 5,16 milyarlık internet kullanıcısının neredeyse 2 milyarını Çinliler oluşturmaktadır (Kara, 2023). Bu durum siber güvenlik bağlamında ÇHC'nin önemini bir kez daha gözler önüne sermektedir.

Teknolojinin ilerlemesi, siber saldırıların artması ve ülkelerin siber güvenlik alanında gerekli iyileřmeyi yapmak adına vermiř olduđu mücadele doğrultusunda 2000'li yıllar itibarıyla siber alanda büyük ilerlemeler yaşanmaktadır. Siber alanla ilgili yapılan çalışmaların artmasıyla beraber ortaya konan çok yönlü arařtırmalar neticesinde, siber güvenlik hususunda en güçlü devletler sıralaması; ABD, ÇHC, İngiltere, Rusya vb. řeklinde ilerlemektedir (Tanrıverdi, 2020). Bu devletlerden özellikle ABD ve Rusya arasında devam eden siber rekabet alanına giren ÇHC'nin, 1978 yılından günümüze öncelik vermiř olduđu ekonomi odaklı politikasında deđişikliklere gittiđi görölmektedir. ÇHC bu deđişiklikle beraber, askeri kapasitesini ve ulusal güvenlik sistemini iyileřtirmeyi, aynı zamanda ekonomik kalkınmasını artırma gayesi doğrultusunda siber güvenlik politikasını güçlendirmeyi ve küresel boyutta bir siber güce dönüşmeyi hedeflemektedir. Kısacası, Soğuk Savaş sonrasında deđişen güvenlik anlayışıyla beraber, geleneksel güvenlik anlayışı terkedilip yerine yeni güvenlik konseptinin gelmesiyle devletlerin daha çok siber güvenlik odaklı politikalar geliřtirdiđi görölmektedir. Bundan dolayı ÇHC'de iç güvenliđini korumak ve istikrarını sağlamak adına savunma ve saldırı amacıyla siber güvenlik politikasını geliřtirmektedir (Balke, 2018: 139-140).

Genel olarak ÇHC siber güvenlik politikasını belirlerken siyasi, askeri ve ekonomik hususları gözeterek hedefler belirlemektedir. Söz konusu hedefler ise řu řekilde sıralanmaktadır (Chang, 2014: 8; Darıcılı ve Özdal, 2018: 4-5):

- Ekonomik yönden geliřip, büyüme ve istikrarı sağlama fikrini gözeterek siber casusluk operasyonlarına engel olmak amacıyla dijital teknolojiyi geliřtirmek,
- Çin Komünist Partisi'nin (ÇKP) yönetimdeki devamlılıđını sağlamak ve karřılařılacak toplumsal ayaklanma giriřimlerinin önüne geçmek adına;

interneti kontrol altına almak ve ÇKP'ye karşı gerçekleştirilebilecek siber casusluk operasyonlarını önlemek için aktif bir sistem kurmak,

- İnternet ve ağ teknolojilerine dair yapılacak olan bilgi harbi planlarını önlemek, tedbirler geliştirmek ve ülkenin içişlerine müdahale amaçlı yapılacak operasyonları ortadan kaldırmak,
- Potansiyel düşmanların askeri altyapılarını, gayelerini, motivasyonlarını, kabiliyetlerini ve siber alandaki sınırlamalarını incelemek ve anlamak,
- Askeri alanda karşılaşılabilecek olaylar için hazırlık yapmak ve askeriye vasıtasıyla karşılaşılabilecek herhangi bir siber çatışma durumunda askeri alanda üstünlük sağlamak.

Tüm bu bilgiler ışığında, ülkemizdeki siber alan ile ilgili akademik literatür incelendiğinde, gerek uluslararası sistemdeki önemi gerekse yükselen bir eko-güce dönüşen ve teknoloji devi olan ÇHC'nin siber güvenlik politikalarına ilişkin yapılan çalışmaların yetersiz olduğu tespit edilmektedir. Bu doğrultuda tez çalışmasının amacı; diğer ülkelere kıyasla internetle geç tanışmasına rağmen günümüzde en fazla internet kullanıcısına sahip ülkelerden biri olan, teknolojinin ilerlemesine büyük katkıda bulunan, uluslararası sistemde önemli bir yere sahip ve aynı zamanda küresel sorunların çözülmesi noktasında etkin oyuncularından biri olan ÇHC'nin siber alanda önem arz etmesi çerçevesinde ülkemizdeki akademik literatüre katkı sağlamaktır.

Siber güvenliğin önem kazanmasıyla beraber siber uzayda belli bir güce sahip olmak ve bu alanı kontrol altında tutmak oldukça önemli bir hâle gelmektedir. Bu doğrultuda uluslararası sistemde yer alan tüm aktörlerin dünyada gündemini koruyan siber güvenlik hususu ile ilgili birçok çalışması bulunmaktadır. Yapılan araştırmalarda siber güvenlik hususunda en güçlü devletler sıralamasında ilk sırada ABD olmasına rağmen, diğer devletler tarafından büyük tehdit olarak görülen ve aynı zamanda yapılan siber saldırılarda en fazla hedef olarak gösterilen ÇHC'nin, siber güvenlik politikaları ve takip ettiği politikaların gizliliği hususundaki tutumu diğer devletler açısından endişeye ve merakı sebep olmaktadır. Bu noktada ise tez çalışmasının temel araştırma problemi/sorusu ortaya çıkmaktadır.

Söz konusu tez çalışmasında: “Dünya gündeminde bu kadar mühim olan siber güvenlik olgusu ile ilgili; teknolojinin önde gelen isimlerinden ve son zamanlarda yaşanan siber saldırılarda en fazla hedef gösterilen devletlerden biri olan ÇHC ne yönde bir siber güvenlik politikası takip etmektedir?” sorusuna cevap aranmaktadır. Ana

araştırma sorusu çerçevesinde ortaya konan temel hipotez ise şu şekildedir: ÇHC, siber güvenliğin sağlanması noktasında diğer büyük küresel aktörlerden farklı olarak, kendine özgü ve milli bir temele dayanan siber güvenlik politikası takip etmektedir.

Temel araştırma sorusu ve bu noktada ortaya konan temel hipotezin doğrulanması noktasında söz konusu tez çalışması bazı alt araştırma sorularını da içermektedir. Bunlar şu şekilde sıralanmaktadır:

- Teknolojinin ön planda olduğu günümüz dünyasında “siber güvenlik” kavramının önemi nedir?
- Siber güvenlik çalışmalarında ilk dörde giren devletler söz konusu alanda nelere dikkat etmektedir? Mezbahis devletlerin belirlemiş oldukları siber güvenlik politikaları nelerdir?
- Çin dış politikasında önem arz eden ulusal güvenlik anlayışında siber güvenliğin sağlanması hususu ne yönde ele alınmaktadır?
- Siber güvenlik çalışmalarında ABD ilk sırada olmasına rağmen, neden tüm devletlerin gözü ÇHC’nin üzerindedir?
- Diğer devletlerin belirlemiş olduğu siber güvenlik politikalarında ÇHC ile ilgili değinilen noktalar nelerdir?

Temel araştırma problemine cevap bulunması noktasında tez çalışmasında “nitel araştırma yöntemi” kullanılmaktadır. Bu bağlamda konuya ilişkin birincil ve ikincil kaynaklardan elde edilen veriler doğrultusunda, söz konusu verilerin analiz edilmesi ve yorumlanmasına dayanan “betimsel analiz” yöntemine başvurulmaktadır. Betimsel analiz yöntemi, belirli bir konuda ya da alanda bir durum, olay ya da olguyla ilgili birbirinden bağımsız olarak ortaya konan çalışmaların ayrıntılı bir şekilde incelenip düzenlemesine yönelik kullanılan bir yöntemdir. Genel olarak “ne?” sorusuna cevap aranan betimsel analiz yönteminde elde edilen sonuçların, hedeflenen konulara yönelik olarak gelecekte planlanan çalışmalara yol göstermesi beklenmektedir. Güncel gelişmeleri kapsayan tez çalışmasında bazı konuları daha iyi kavrayabilme ve bu konuların gelişimini analiz edebilme noktasında eski tarihli kaynaklara da yer verilmektedir. Akabinde ise çalışmanın güncel gelişmeleri kapsamından dolayı; yakın dönemdeki internet odaklı açık kaynaklar, makale, bilimsel çalışma, kitap, tez, rapor, siber güvenlik strateji belgeleri, dokümanlar ve gazete yazılarında yer alan bilgilere dayanılarak hazırlanmaktadır.

Öte yandan tez çalışmasında bazı sınırlandırmalara gidilmektedir. Bu noktada ÇHC'nin siber güvenlik politikalarını daha iyi analiz edebilmek için diğer tüm devletler yerine siber güvenlik hususunda önemli güce sahip üç devlet olan ABD, İngiltere ve Rusya'nın siber güvenlik politikalarına değinilmektedir. Aynı zamanda çalışmada siber saldırılar ve siber güvenlik kapsamında yer alan bütün konular ele alınmayıp, ÇHC'nin siber güvenlik anlayışı çerçevesinin analiz edildiği bölümlerde bazı sınırlandırmalar yapılmaktadır. Söz konusu tez çalışmasında karışık ve dinamik yapıya sahip bir alan olmasından dolayı siber uzay, siber saldırılar, siber tehdit ve siber güvenlik politikaları noktalarına dokunulmaktadır. Akabinde, çalışmanın sınırlı kapsamı dâhilinde belirlenen devletlerden ABD, İngiltere ve Rusya'nın takip ettiği politikalarda özellikle ÇHC ile ilgili kısımlara dikkat çekilmektedir.

Üç ana bölümden oluşan tez çalışmasının birinci bölümü, “Kavramsal Çerçeve” başlığı ve onun alt başlıklarından oluşmaktadır. Bu bölümde siber güvenlik kavramını analiz etmek adına, öncelikli olarak siber kavramına ve sonrasında yaşanan süreçte göstermiş olduğu değişim dolayısıyla siber kavramının gelişimine yer verilmektedir. Genel anlamda bilgi teknolojileri alanında yer alan kavramların genel kabul gören tanımlamaları bulunmadığından dolayı, siber ile ilgili kavramların da genel kabul gören tanımları bulunmamaktadır. Bu doğrultuda siber ile ilişkili ortaya çıkan kavramların açıklanmasında birçok tanıma yer verilmektedir. Akabinde siber saldırı ve siber tehdit türlerine yer verilerek, yapılacak siber saldırılarda hangi araçların/türlerin/çeşitlerin kullanıldığına değinilmektedir. Siber güvenlik kavramını daha iyi anlama noktasında öncelikle güvenlik kavramına değinilerek, güvenlik kavramının dönüşümü ele alınmaktadır. Nitekim siber kavramının güvenlik olgusuyla nasıl ilişkilendirildiği ortaya konmaktadır. Son olarak, tez çalışmasının ana konusunu oluşturan “siber güvenlik” hususuna başka bir alt başlıkta daha detaylı olarak değinilerek, bu olgunun tarihçesi ve aynı zamanda bu alan ile ilgili yapılan çalışmalar ÇHC dışında siber güvenlik hususunda güç elde eden diğer devletlerden; ABD, İngiltere ve Rusya ekseninde incelenmektedir.

Tez çalışmasının ikinci bölümü, “Dış Politika ve Ulusal Güvenlik” başlığı ve onun alt başlıklarından oluşmaktadır. Değişen dünya düzeninde ülkelerin liderleri değiştikçe belirlenen politikalar ve çalışmalarda da değişimler gözlemlenmektedir. Bu bağlamda ülkelerin çıkarları doğrultusunda dış politikalar oluşturulduğu görülmektedir. Dış politikaların belirlenmesinde birinci dereceki temel unsurun ise ulusal güvenlik

olduğu bilinmektedir. Değişen dünya düzeniyle beraber ulusal güvenliği sağlamada en önemli noktalardan biri ise siber güvenliği sağlamaktır. Özellikle konuya ÇHC ekseninde yaklaşıldığında Pekin'in ulusal ve siber güvenliği eş bir düzlemde değerlendirdiği ve her iki kavramı birbiriyle ilişkili olarak ele aldığı görülmektedir. Bu doğrultuda söz konusu bölümde çalışmanın ana konusunda yer alan ÇHC'yi daha iyi analiz etmek adına öncelikle Pekin'in genel yapısı, ortaya çıktığı süreç ve bu süreç sonrasında yaşanan gelişmelere değinilmektedir. ÇHC'nin bugünkü noktaya gelmesinde büyük katkısı bulunan liderlerden Mao Zedong “devrim dönemi (1949-1978)”, Deng Xiaoping ise “reform dönemi (1978 ve sonrası)” başlıkları altında incelenerek, ÇHC'nin yükselişi noktasında izlenen yol ve politikalar analiz edilmektedir. Akabinde ise ÇHC'nin dış politika süreçleri ve bu sürece etki eden faktörleri ele alıp, ÇHC'nin takip ettiği dış politikalar dönemsel açıdan incelenmektedir. Bu süreçte liderlerin dış politika ile ilgili atmış oldukları adımlara, politikalara yer verilmektedir. Son olarak, ÇHC'nin güvenlik algısı ve oluşan yeni güvenlik konseptiyle beraber dönemsel olarak liderlerin bu alana yaklaşımı ele alınmaktadır.

Tez çalışmasının üçüncü bölümü ise “Çin Bağlamında Siber Güvenlik” başlığı ve onun alt başlıklarından oluşmaktadır. Çalışmanın temel konusunun ele alındığı bu bölümde ÇHC'nin siber güvenlik politikaları ortaya konmadan önce internet gelişimi ve aynı zamanda siber uzay, siber egemenlik, bilgi güvenliği ve oluşan siber güvensizlik hususları ÇHC bağlamında incelenmektedir. Akabinde, ÇHC'nin siber güvenlik açısından yapmış olduğu çalışmalara, yasalara ve politikalara detaylı bir şekilde değinilmektedir. Bu bölümde siber güvenlik ile ilgili Beyaz Kitap'ta yer alan kısımlara dönemsel olarak yer verilmektedir. ÇHC'nin çıkarmış olduğu Siber Güvenlik Yasası farklı bir başlık altında incelenerek detaylı bilgi verilmektedir. Öte yandan politika yapım sürecinde birçok aktörün aktif rol oynaması gerekmektedir. Bu noktada ÇHC'nin siber güvenlik politikaları belirlenirken hangi aktörlerin hangi görevleri üstlendiği ile ilgili analizlere “Çin'in Siber Güvenlik Aktörleri” adlı alt başlıkta yer verilmektedir. Son olarak, farklı bir başlık altında ÇHC ve Batı dünyası açısından siber güvenlik olgusu değerlendirildikten sonra, yeni bir başlıkta ÇHC bağlamında gerçekleştirilen siber saldırılar incelenmektedir. Bu başlıkta genel olarak ÇHC'nin yaptığı iddia edilen siber saldırılara yer verilerek, ÇHC'nin diğer güçler üzerinde bıraktığı etki ve diğer aktörler tarafından tehdit olarak görülme durumunun ispatı niteliğindeki örnek olaylara yer verilmektedir.

BİRİNCİ BÖLÜM

1. Kavramsal Çerçeve

Tanımlama açısından kavramlara bakıldığında, bilgi teknolojilerine ilişkin birçok kavramda olduğu gibi siber güvenlik kavramında da net bir tanım yapılamadığı görülmektedir. Bu nedenle siber güvenlik kavramını ele almadan önce siber (*cyber*) kavramının tanımlanması gerekmektedir. Değişen dünya düzeniyle beraber siber kavramı ile ilişkili birçok kavram ortaya çıkmaktadır. Bu bölümde siber güvenlik kavramına açıklık getirmeden önce siber kavramı ele alınmaktadır. Akabinde alt başlıklar ekseninde siber ile ilişkili diğer kavramlar incelenmektedir.

1.1. Siber Kavramı

Merriam-Webster dil bilimsel açıdan siber kavramını; bilgisayarlar veya bilgisayar ağları/internet ağları ile ilgili bir kavram olarak tanımlamaktadır. Yani bunların sanal gerçeklik anlamına geldiğini söylemektedir (Klimburg, 2012). Birleşmiş Milletler (BM) siber kavramını “internete bağlı bilgisayarların, iletişim alt yapılarının, çevrimiçi iletişim yapan kişilerin, veri tabanı ve bilgi sistem araçlarının oluşturduğu küresel bir sistem” şeklinde tanımlamaktadır (Andress ve Winterfeld, 2011: 2). Temeli *sibernetik* kelimesinden gelen siber kavramının kökeni, eski Yunanca *Küernetes* sözcüğünden ortaya çıkmaktadır (Heylighen ve Joslyn, 2011). Siber kelimesinden türeyen sibernetik kavramı, güncel anlamını 1948 yılında Amerikalı matematikçi Norbert Wiener tarafından yazılan *sibernetik* ya da *hayvanlarda ve makinalarda iletişim ve kontrol* isimli kitabı ile kazandığı görülmektedir (Wiener, 1965: 99). Teknoloji ve iletişim öğelerinin sürekli olarak değişmesinden dolayı iletişimi kontrol edebilme ve yönlendirme noktasında, bilgisayar ve internet ile ilgili olarak *sibernetik* kavramı kullanılmaktadır. Bu kavramın Türkçe’deki karşılığı ise *bilişim* sözcüğü ile ifade edilmektedir (Çakmak ve Altunok, 2009: 25-26).

Amerikalı yazar William Gibson’ın siber kavramının günümüzdeki kullanımına karşılık gelen sözcüğü, 1984 yılında yayımladığı *Neuromancer* adlı romanında gerçekte olmayan anlamına gelen “*sanal metafor*” olarak kullandığı görülmektedir (Wills ve Ashenden, 2012: 111). Son olarak, siber kavramının Oxford sözlüğündeki tanımına bakıldığında; bilgisayarlar, bilgi sistemleriyle bağlantılı ve bu iklimin doğal bir parçası anlamında kullanılmaktadır (Yılmaz, 2020: 21). Siber kavramı iletişim ve teknolojinin

sürekli gelişimiyle beraber farklı çeşitlerde karşımıza çıkmaktadır. Bu nedenle zaman içinde siber kavramının çeşitlenmesi durumunu ‘siber kavramının gelişimi’ başlığı altında daha geniş olarak ele almak faydalı olacaktır.

1.2. Siber Kavramının Gelişimi

Dünyanın birbirinden çok uzak mesafelerini birbirine yakın hâle getiren küreselleşme olgusunun, ortaya çıkmaya başladığı ilk zamandan itibaren temelde ekonomik, sosyal, kültürel, teknolojik ve siyasal alanlarda birçok değişim ve dönüşüme sebep olduğu bilinmektedir. Bu değişim ve dönüşümlerden devletler, toplumlar ve sistemler aynı zamanda bunlarla bağlantılı birçok alan etkilenmektedir. Küreselleşmenin bu etkisi ulus devletler tarafından kabul edilmekte ve hayatımızın çeşitli alanlarında yaşanan etkisiyle beraber olası olumsuz etkilere karşı önlemler alınmaktadır (Yılmaz, 2017: 25-27).

Bilgi çağı denilen teknolojinin sürekli yenilendiği ve bilgi sistemlerinin hayatımıza intisap ettiği 1990’lı yıllardan sonra, uluslararası ilişkiler disiplinde bulunan tehdit olgusu ve buna bağlı kavramların tanımlamalarında birtakım değişimlerin yaşandığı görülmektedir. 1990’lı yıllar öncesi klasik güvenlik anlayışına göre şekillenen ve eksik kalan tanımlamaların olması kavramları eksik bir şekilde öğrenmemize sebep olurken, bu durumun küreselleşme sonrası yani 1990’lı yıllardan sonra değişmesi gerektiği anlaşılmaktadır. Hayatın her alanında bulunan bilgi sistemlerinin kültür, eğlence, araştırma, sağlık, savunma gibi birçok alanda devrim yaratacak nitelikte etkileri bulunmaktadır. Günümüzde; online eğitimden konferanslara, online bilet satışından otel rezervasyonlarına, akıllı telefonlardan iş hayatına kadar birçok unsur bilgi sistemlerine konu olmaktadır ve hayatımızın her alanının bu sistemlerle iç içe geçtiği görülmektedir. Böylesine insan hayatını etkileyen değişimlerle beraber yapısal birçok değişiminde olduğu bilinmektedir. Yaşanan bu değişimler her zaman olumlu sonuçlar doğurmamaktadır. Bu durumun yaratmış olduğu birtakım sorunların ve tehditlerinde olduğu dolayısıyla teknolojiye olan bu bağlılık ve uzmanlaşmanın tehditleri de içinde barındırdığı ifade edilmektedir (Yılmaz, 2020: 25).

Küreselleşme sonrasında teknoloji ve iletişimde yaşanan büyük ilerleme ile beraber bilgisayar kullanımında yüksek oranda artış yaşandığı görülmektedir. Bu artış toplumda eşsiz değişime sebep olarak, insan yaşamında kolaylıklar sunmaya başlamaktadır. Bilgisayarın böylesine yoğun kullanımı internet kullanımını da

etkilemektedir. İnternet kullanımının artışı ile coğrafi sınırların ortadan kalktığı yadsınamaz bir gerçektir. Teknoloji alanında yaşanan bu gelişmeler ile birlikte, insanların her türlü elektronik bilgi hizmetine erişimini mümkün kılan ve “siber uzay” olarak tanımlanan yeni bir dünya oluşmuştur (Gibson ve Erle, 2006: 97). Bilgisayar ve internet kullanımının milyarlarca ulaştığı bu zaman diliminde siber uzayı daha geniş kapsamlı tanımlayıp ele almak faydalı olacaktır.

1.2.1. Siber Uzaya Genel Bakış

İngilizce karşılığı “cyberspace” olan ve Türkçe’de ise “siber ortam, siber alan” olarak anılan siber uzay kavramı ilk olarak 1982 yılında bilim-kurgu yazarı William Gibson’ın “*Burning Chrome*” adlı eserinde kullanılmaktadır. Siber uzay kavramının söz konusu eserde kullanılmasıyla birlikte yaygınlaştığı görülmektedir (Gibson, 1982: 248). Daha sonra Gibson 1984 yılında yazdığı “*Neuromancer*” adlı romanında siber uzay kavramını daha da tafsilatlandırarak; “*matematiksel kavramların öğretildiği çocuklar tarafından, her milletten milyarlarca yasal operatörün deneyimlediği, her gün yaşanan içgüdüsel ve tepkisel bir sanrı. İnsan sistemindeki tüm bilgisayar kümelerinden oluşturulmuş verilerin grafiksel gösterimi. Düşünülemez bir karmaşıklık. Belleğin imkânsızlığında, verilerin kümelerinde ve takımyıldızlarında gezinen ışık çizgileri*” şeklinde tanımlamaktadır (Gibson, 2016: 69-70).

Yukarı kısımlarda belirtildiği üzere bilgi teknolojileri alanına ilişkin birçok konuda olduğu gibi siber güvenlik alanında da net bir tanımlama bulunmamaktadır. Öte yandan siber uzay ile ilgili de net bir tanım yapılamamaktadır. Bu yüzden bu kavram ile ilgili birçok görüş ve tanımlar ortaya çıkmaktadır. Genel kabul görmüş bir tanımlı olmayan siber uzayı, yapılan farklı tanımlarla ele almak kavramı anlamak açısından faydalı olacaktır.

Bilgi ortamı olarak görülen siber uzay kavramı; “*içerisinde bulunan dijital verilerin çevrimiçi olarak yaratıldığı, saklandığı ve paylaşıldığı bilgisayar ağları ile kurulmuş bir sanal âlemdir*” (Singer ve Friedman, 2018: 289). Bir başka tanımda ise siber uzay; “*internet ağları, enerji sistemleri ağları, kapalı askeri ağlar, yazılım tabanlı sistemler gibi içinde yazılım ve donanım bulunduran yapılar bütünüdür*” şeklinde tanımlanmaktadır (Darıcı, 2017: 31).

ABD Savunma Bakanlığı’nın terimler sözlüğünde siber uzay; “*dâhili işlemci ve denetleyicilerin yer aldığı internet ağları ve bilgisayar sistemlerinin birbiriyle etkileşim*

hâlinde bulunduğu küresel bir yapı” olarak tanımlanmaktadır (Gürkaynak ve İren, 2011: 265). Türkiye’de ise Ulaştırma Denizcilik ve Haberleşme Bakanlığı’nın (UDHB) yapmış olduğu tanımlar bulunmaktadır. Bu tanımlardan 2016-2019 yıllarını kapsayan Ulusal Siber Güvenlik Stratejisi’nde geçen siber uzay kavramının; “dünyanın her yerine ve dâhi uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunlar arasındaki bağlantıyı sağlayan ağlardan oluşan veya bağımsız hâlde bulunan bilgi sistemlerinden oluşan sayısal ortam” şeklinde tanımlandığı görülmektedir (UDHB, 2016: 7).

Libicki tüm bu tanımlardan farklı olarak bir görüş ortaya koymaktadır. Libicki’ye göre siber uzay; *“deniz, kara, hava ve hatta uzaydan bile bağımsız olan, iletişim altyapılarını kullanan sanal ortamdır”* şeklinde ifade edilmektedir. Akabinde karşıtlıkları da içinde barındırdığı belirtilen siber uzay, her ne kadar hava, kara, deniz gibi diğer çekişme alanlarına benzetilse de yine de diğerlerinden farklı olduğu vurgulanmaktadır (Libicki, 2009: 11-12).

Son olarak, siber uzayın en genel tanımını ele almakta fayda olacaktır. En genel siber uzay tanımı; *“sistemlerin hem kendi aralarında etkileşime geçtiği hem de insanların birbirine bağlı ağlarla etkileşime geçtiği fiziksel olmayan alan”* şeklinde yapılmaktadır (Bıçakçı, 2014: 106). Yalnızca fiziksel alan olmayıp aynı zamanda gerçeklik ve sanal gerçeklik durumunu ifade eden siber uzay, fiziksel dünyadaki birçok iletişim türünün dijital ortama aktarıldığı alan olarak görülmektedir. Siber uzayda etkileşim ve iletişim sağlanırken bu tamamen zamandan ve mekândan bağımsız olacak şekilde gerçekleşmektedir (Whittle, 1996: 7).

Yapılan tanımlamalar neticesinde her alanın siber uzay olarak ifade edilemeyeceği ve bir alanın siber uzay olarak ifade edilebilmesi için gerekli bazı hususların olduğu görülmektedir. Bu hususlar Clark’ın belirlemiş olduğu dört katman ve Choucri’nin belirlediği siber uzaya has özellikler doğrultusunda ortaya konmaktadır.

Clark’a göre bir alanın siber uzay olarak ifade edilebilmesi için dört katmanın varlığından bahsedilmesi gerekmektedir. Bu katmanlar şu şekilde ifade edilmektedir (Clark, 2010: 1-4):

1. İlk katmanı insanlar oluşturmaktadır. Siber deneyime katılan bu insanlar iletişim kurarak, bilgiyle çalışarak, karar alıp ve planlar oluşturarak siber uzayın doğasını dönüştürmektedir. Bu katmanda çeşitli ilgi alanlarına ve farklı rollere sahip aktörler, kullanıcılar ve kuruluşlar bulunmaktadır.

2. İkinci katmanda siber uzayda depolanan, aktarılan ve dönüştürülen bilgiler bulunmaktadır. Paylaştığımız video ve müzikler, çevrimiçi kitap ve fotoğraflar, meta-veri, işletme ve işlem kayıtları, aktarılan ve dönüştürülen kodlanmış metinler ve diğer materyaller bilgi katmanını oluşturmaktadır.
3. Üçüncü katman mantıksal katmandır. Bu katman siber uzayın platform yapısını destekleyen, hizmetleri oluşturan ve etkinleştiren yazılım programlarının olduğu katman olarak ifade edilmektedir.
4. Dördüncü katman ise mantıksal öğeleri destekleyen fiziksel katmandır. Fiziksel iletişim altyapısı olarak da adlandırılmaktadır. Fiber-optik kablolar, iletişim şebekeleri, bilgisayar donanımları, baz istasyonları, sensörler, dönüştürücüler bu katmanı oluşturmaktadır.

Belirlenen dört katman dışında bir de siber uzayın kendine has özellikleri bulunmaktadır. Bunlar ise şu şekilde sıralanmaktadır (Choucri, 2012: 4):

1. Zamansallık; geleneksel olan zamansallığı anlıkla değiştirmektedir.
2. Fiziksellik; fiziksel ve coğrafi konumun kısıtlamalarını açmaktadır.
3. Nüfuz etme; sınırlara, yetki alanlarına ve yargı bölgelerine nüfuz etmektedir.
4. Akışkanlık; sürekli değişimleri, yeniden yapılanmayı ve adaptasyon yeteneğinin yüksek olduğunu ifade etmektedir.
5. Katılım; siber uzayın aktivizm ve politik ifade önündeki engelleri azalttığını belirtmektedir.
6. Atfetme; aktörlerin kimliklerini aynı zamanda o olayla olan bağlantılarının gizlenmesi atfetme özelliğini kapsamaktadır.
7. Hesap Verilebilirlik; bu özelliğe göre siber uzayda sorumluluk mekanizmaları kolayca yok sayılmaktadır.

Günlük hayatın vazgeçilmez bir gerçeği hâline gelen ve hayatımızın her yerinde bulunan siber uzay, internet ve internet aracılığıyla birbirine bağlanan milyonlarca bilgisayarın etkileşim içerisinde olması, gelişen ve gelişmekte olan dünyada söz konusu bilgisayar etkileşim sayılarının hızla artması, insan için önemli yeni bir gerçekliği yaratmaktadır. Bu oluşan gerçeklik neticesinde zamanla gelişim göstererek sürekli bahsi geçen siber uzayın oluştuğu görülmektedir (Choucri, 2012: 3). Hayatın büyük parçası hâline gelen siber uzay; finans sektörü, e-devlet uygulamaları, modern ulus-devletin tekelinde bulunan savunma sanayi, enerji alt yapıları, bireysel bilgisayar kullanımı, devletlerin ve özel sektörün ticaret alanlarına kadar internetleşen her şeyi içine

almaktadır. Bu sebeple siber uzay her geçen gün daha fazla büyüyen bir yapıyı oluşturmaktadır (Önaçan ve Atan, 2016: 14).

Geçmiş insan ve makine temelli haberleşme araçlarının kullanımına kadar eski tarihe dayanan siber uzay, objesel ve hibrit bir yapıya sahiptir. Sadece internet ile sınırlandırılmayacak kadar geniş bir kapsama sahip olan siber uzay; hücresel teknolojiler, fiber-optik kablolar, uzay temelli telekomünikasyon, telsizler, uydu sistemleri, insansız hava araçları, kablolu telefon ağları ve hatta televizyonlar dâhil bu alanı oluşturan öğeler olarak karşımıza çıkmaktadır (Gedik, 2018: 24).

Bir iletişim aracı olarak erişilebilirliği ve açıklığından dolayı hayatımıza fazlasıyla kolaylık ve fayda sağlayan siber uzayın olumlu yanlarının yanı sıra birde olumsuz sonuçları bulunmaktadır. Suç, tehdit, saldırı ve casusluk gibi eylemlere serbest hareket alanı sunan siber uzay güvensizlik oluşturmaktadır. Bu alana yapılacak olan girişlerde engellerin az olması ve suçun savunmadan ucuz olması siber alana olan güvensizliği büyük oranda artırmaktadır. Bundan hareketle Nye siberi, yersiz ve kanunsuz “Vahşi Batı” olarak betimlemektedir (Nye, 2014: 5).

Siber uzayın oluşumuna/dönüşümüne katkıda bulunan birtakım aktörler bulunmaktadır. Bu aktörler; kötü niyetli kişiler, bireysel veya grup hâlindeki suçlular, sanayi casusluğu yapmak veya rakiplerini ortadan kaldırmak isteyen ticari kuruluşlar, teröristler, siber uzayı casusluk, ekonomik kâr veya savaş aracı olarak kullanmak isteyen devletler, kurumlar, kuruluşlar, uluslararası örgütler, devletlerin silahlı kuvvetleri ve istihbarat örgütleri şeklinde sıralanmaktadır (Çeliktaş, 2016: 6).

Kısaca özetlenecek olursa; şu ana kadar yapılan tüm tanımlar doğrultusunda siber uzayın genel kabul gören bir tanımı bulunmamaktadır. Siber uzayın sürekli genişleyen bir doğasının olması belirsizliği artırmaktadır. İletişim ve teknolojinin sürekli gelişmesi siber uzayın daha da genişlemesine neden olmaktadır. Bu durumun oluşabilecek yeni siber saldırı, siber tehdit ve siber suçların yanı sıra güvenlik ile ilgili kavramlarında sürekli dönüşümüne sebep olduğu görülmektedir. Bu durum ise siber uzaya yönelik kavramların tanımlanmasında zorluğa sebep olmaktadır.

1.2.2. Siber Saldırı ve Türleri

Teknolojide yaşanan ilerleme sonucunda bilgisayar ve internet kullanımının yaygınlaşması kullanıcılara belirli kolaylıklar sağlasa da beraberinde çeşitli tehditleri, riskleri ve sorunları getirmektedir. Bu riskler ve sorunların başında ise kurumlar ve

devletlerin *siber saldırılarla* karşı karşıya kalması yer almaktadır. Öte yandan, siber saldırı kavramına bakıldığında diğer kavramlar gibi genel kabul gören tanımının olmadığı görülmektedir. Bundan dolayı söz konusu kavram ile ilgili birçok düşünce ortaya atılmaktadır (Emir, 2020: 20). Siber saldırı kavramını anlayabilmek için mevcut tanımlardan bir kaçını ele alınacaktır. 2016-2019 Ulusal Siber Güvenlik Strateji Belgesi'ndeki tanıma göre siber saldırı; *“ulusal siber uzayda bulunan bilişim sistemlerinin gizlilik, bütünlük veya erişilebilirliğini ortadan kaldırmak amacıyla, siber uzayın her hangi bir yerindeki kişi ve/veya bilişim sistemleri tarafından kasıtlı olarak yapılan işlemler”* şeklinde ifade edilmektedir (UDHB, 2016: 8).

Diğer taraftan, birçok ülke ve uluslararası örgütün siber saldırıları ve beraberindeki tehditleri analiz etmek için tanımlamalara başvurduğu gözlemlenmektedir. Bu tanımlamalardan dikkati çeken iki örnekten biri ABD, diğeri ise Şangay İşbirliği Örgütü (ŞİÖ) tarafından ortaya konmaktadır. İlk olarak ABD'de Birleşik Devletler Siber Komutanlığı'nın siber operasyonlarda kullanmak için yayımladığı (2011) sözlükte siber saldırı, *“bilgisayarın ve bununla ilgili ağların veya sistemlerin kullanımı aracılığıyla hedef unsurun mal varlığını, kritik hedef sistemlerini, fonksiyonlarını bozma veya tahrip etme amaçlı düşmanca hareket”* şeklinde tanımlanmaktadır. Yapılan tanıma göre, kritik alt yapılara yapılan saldırılar siber saldırı olarak kabul edilmektedir ve tanımın temel özelliğinin ise kritik siber sistemlere zarar vermesi düşünülen düşmanca eylemlerle sınırlandırılması olduğu görülmektedir (Hathaway vd., 2012: 824; Cartwright, 2011: 5).

ŞİÖ'nün, siber saldırılara ilişkin araç tabanlı bir yaklaşım benimseyerek ABD Siber Komutanlığı'nın yapmış olduğu tanımdan farklı olarak daha geniş kapsamda bir tanım yaptığı görülmektedir. ŞİÖ siber saldırıyı, *“sosyal ve ekonomik, sosyal ve politik sistemlerin yanında diğer devletlerinde manevi, ahlaki ve kültürel alanlarına yönelik zararlı bilgi girişini, bilgi güvenliğine yönelik tehditler”* şeklinde tanımlamaktadır. ŞİÖ'nün siber saldırı tanımına bakıldığında; siyasi istikrarı sabote etmek amacıyla siber teknolojinin kullanılmasına değinmesi ve söz konusu kavramı geniş bir tabanda ele alması açısından yapmış olduğu tanım önem kazanmaktadır (Hathaway vd., 2012: 825).

Başka bir tanıma ele alacak olursak; kritik altyapı kesimine saldırma, yemleme, hizmet dışı bırakma, zararlı yazılımlarla hasar verme, sosyal mühendislik, veri çalma ve değiştirme, açık mikrofon dinleme gibi yöntemler kullanarak devlet veya ticari kuruluşların internet sayfalarını bozarak, sistemdeki bilgilerini çalma, ifşa etme, silme

veya deęiřtirme amacıyla hedef olan kiři, kurum veya řirketin iletiřim altyapılarına veya bilgi sistemlerine yapılan planlı ve koordineli saldırılara siber saldırı denmektedir (Çakmak ve Demir, 2009: 29-30). Söz konusu bu saldırıların, bilgisayardan bilgisayara, cihazlara ya da cihazların içindeki bilgilerin gizlilik, bütünlük ve erişilebilirliğini tahrip etmek amacıyla yapıldığı ifade edilmektedir (O' Shea, 2003: 6).

Öte yandan, siber saldırıların ne şekilde yapıldığı kısaca özetlenecek olursa; altyapı işleyişini aksatma ya da küçük ölçekli e-posta dolandırıcılığı, kullanılabilirliğini kesintiye uğratma ya da kısıtlama, sunucu servislerine ya da bağlantılarına aşırı yüklenme, izinsiz silme, deęiřtirme ya da okuma yapılarak bilgileri riske atma şeklinde olduğu görölmektedir (NCSC, 2012).

Temelde insan kaynaklı eylem olarak görölen siber saldırılarda her ne kadar kullanılan araçlar ve hedef alınan noktalar sanal ortamdan ve verilerden oluşsa da söz konusu saldırıların sonuçları insanlara dokunmaktadır. Aynı zamanda yapılan saldırıların hedefleri de insanların ortaya koymuş oldukları amaçlara dayanmaktadır (Lu, 2014: 11). Bir işletim sisteminde oluşan sistemsel aksamalar ya da hatalar sonucu oluşan zararların, siber saldırı olarak tanımlanmaması gerekmektedir. Çünkü siber saldırılar; siber uzayda, hedef gösterilen bilgisayar işletim sistemlerinin zarar görmesini isteyen saldırganlar tarafından yapılan hareketler sonucu meydana gelmektedir. Yaşanan siber saldırı sonucunda ortaya çıkabilecek zarar; sosyal, kültürel, ekonomik ya da hükümet fonksiyonlarında, siber saldırının bir sonucu olarak etki edebilmektedir. Siber saldırılar doğrudan ve dolaylı olarak iki türlü sınıflandırılmaktadır. Doğrudan siber saldırılarda hedeflenen sistemin yok edilmesi amaçlanırken, dolaylı siber saldırılarda hedeflenen sistemin işlevselliğinin önlenmesi amaç olarak karşımıza çıkmaktadır (Kello, 2013: 19).

Siber saldırıyı gerçekleřtiren saldırganlar, bu saldırıları içeriden ve dışarıdan kaynaklanan saldırılar olarak ayırmaktadır. Bu ayrım hedef aldıkları kurum ve kuruluşlara göre belirlenmektedir. İçeriden kaynaklanan saldırılarda kurumun kendisinin vermiş olduğu yetki ile bu sistemlere erişebilme ve kullanım gerçekleşmektedir. Dışarıdan kaynaklanan saldırıların ise kurumun izni dışında olan kişiler tarafından gerçekleştirilen saldırı olduğu ifade edilmektedir. Kurumlarda meydana gelen bu saldırılar hackerler, suçlular ve vandallar tarafından kötü amaçlarla yapılmaktadır (Kara, 2013: 9).

Siber saldırılar; içerideki casuslar ve yetkili kullanıcılar, bilgisayar korsanları, teröristler, organize suç örgütleri, casusluk faaliyeti yapanlar, düşman ülke ve dış istihbarat ülkeleri tarafından planlı ve uyumlu bir şekilde yapılabildiği gibi sistem içerisindeki bilinçsiz kullanıcılar tarafından plansız olarak yani farkında olmadan da yapılabilmektedir (Çeliktas, 2016: 8). Diğer taraftan, siber saldırıları çekici kılan ve başvurulmasına sebep olan özellikler bulunmaktadır. Bu özellikler şu şekildedir (Yıkıcı, 2020: 11):

1. Yapılacak olan saldırının hangi faktörle ve kimlerle bağlantılı olduğunu ortaya çıkarma zorluğu yani ilişkilendirme sorunu denilen özelliğinin olması,
2. Coğrafi mesafeler sorun olmadan dünyanın ne tarafında olunursa olunsun saldırının saniyeler içinde yapılabilmesi,
3. Bu saldırıların düşük maliyetlerle gerçekleştirilmesi.

Öte yandan, siber saldırı ve klasik saldırı ayrımının yapılması siber saldırıyı anlamak açısından faydalı olacaktır. Siber saldırılar oldukça hızlı gerçekleşmektedir. Saldırıya uğrayanın daha ne olduğunu anlayamadan saldırıya maruz kalabildiği görülmektedir. Yapılan saldırılarda kullanılan araçlar ise büyük önem göstermektedir. Siber saldırılarda kullanılan araçlar klasik saldırılarda kullanılan araçlardan farklıdır. Siber saldırılarda dijital araçlar kullanılırken klasik saldırılarda kinetik silahlar kullanılmaktadır. Böylece siber saldırılarda fiziki durumda kısıtlamalar ortadan kalkmaktadır. Fiziki yönden sınırlamaların ortadan kalkması siber saldırıların aynı anda birden çok hedefi vurabilmesine olanak sağlamaktadır. Maliyet açısından bakıldığında ise siber saldırıların maliyeti, klasik saldırılara göre daha düşüktür. Bir diğer fark ise hedef unsurudur. Siber saldırılarda amaç; hedef gösterilen bir bilgisayara ve içerisinde yer alan bilgilere erişmektir. Yapılan saldırıların sonuçları fiziksel olarak hasar ortaya çıkarsa da oluşan hasar ilk önce dijital ortamda meydana gelmektedir (Singer ve Friedman, 2014: 68-69; Todd, 2009: 68-69).

Dijital ortamda karşılaşılan siber saldırıların birçok çeşidi vardır. Bu saldırı türleri ve daha sonra anlatılacak olan siber tehdit türlerinin birbirleriyle bağlantıları bulunmaktadır. Yani birçok tehdit zamanla saldırılara dönüşebilmektedir. Teknolojinin ilerlemesiyle bu çeşitlerin sayısı her geçen gün artmaktadır. 21. Yüzyılda karşımıza en çok çıkan siber saldırı çeşitleri şunlardır:

1. **Zararlı Yazılımlar (Malware):** Hedef gösterilen bilgisayarlara, kullanıcıların izni olmadan sızıp, zarar vermek amacıyla oluşturulan yazılımlardır. Yani bilişim sistemlerine zarar vermek amacıyla ya da kullanıcılarının amaçları dışında kullanılmak üzere o sisteme yerleştirilmektedir. Ayrıca zararlı yazılımlar internet üzerinden de bulaşabilmektedir (Yener, 2013: 4). Yoğun olarak zararlı yazılım bulunduran ülkeler Uzak Doğu ülkeleri olarak gösterilirken, Avrupa ülkelerinde bu oranın daha düşük olduğu ifade edilmektedir. Bunun sebebi olarak hukuki altyapının olması ve aynı zamanda gerekli önlem çalışmalarının alınması gösterilmektedir. Bilgisayarlara bulaşan zararlı yazılımların yoğun olduğu ülkelerde başta ÇHC bulunmaktadır. Akabinde ise Türkiye ve Tayvan gelmektedir (Eren, 2017: 39). Zararlı yazılımların çeşitli tipleri bulunmaktadır. Bunlar; virüsler, solucanlar, truva atları, casus yazılımlar, rootkitler vb. şeklinde sıralanmaktadır (USOM, 2014: 9). Bu tipler siber tehdit başlığı altında daha detaylı açıklanacaktır.
2. **Oltalama-Yemleme (Phishing):** İnternet saldırıları arasında en yaygın ve en tehlikeli olan *oltalama*; İngilizce password (şifre) ve fishing (balık avlamak) kavramının bir araya gelmesiyle oluşturulan pishing ifadesiyle kullanılmaktadır (USOM, 2014: 11-12). Bu saldırı türünde hedef gösterilen kişiye içerisinde genellikle banka, resmi kurumlar ve benzeri yerlerden gelmiş gibi görünen sahte bağlantı bulunan e-posta gönderilmektedir. Bu bağlantıya tıklanması durumunda hesapları, şifreleri veya kredi kartı bilgileri saldırgan tarafından ele geçirilmektedir. Kullanıcıların oltalama e-mail konusunda eğitilmiş olması ve gelen her bağlantıyı tıklamamak gerektiğini bilmesi bu tip saldırılardan korunmak için önemli bir durumu teşkil etmektedir (Pajunen, 2017: 21).
3. **Hizmet Engelleme Saldırıları (DoS- DDoS):** *Hizmet dışı bırakma (DoS)*, saldırganın hedef olarak belirlediği sistemin alışılagelmiş işleyişini bozmak ya da zarar vermek için yapılan saldırı türünü ifade etmektedir. Burada asıl amaç, kullanıcıların ulaşmak istediği kaynakları kullanmasını önlemektir. Bir diğer tür ise *Dağınık Hizmet Dışı Bırakma (DDoS)* olarak karımıza çıkmaktadır. Bu saldırı türüne verilmek istenen zarar daha büyük olduğu zaman başvurulmaktadır. DDoS saldırılarını DoS saldırılarından ayıran en önemli nokta ise burada tek bir merkeze

yönelik yapılan saldırıların birden fazla bilgisayar ile gerçekleştirilmesinden kaynaklanmaktadır (Keleştemur, 2015: 292-296; Lau vd., 2000: 2275). Uluslararası siber çatışmalarda en çok kullanılan saldırı türü olan DoS ve DDoS saldırılarında amaç, çok geniş bir yelpazeden ortaya konmaktadır. Bunlardan bazıları; web sitelerine erişimin veya radyo kanallarının dinlenmesinin engellenmesi, gemilerin limana yanaştırılmasının durdurulması ve banka hesaplarından para transferlerinin engellenmesi gibi amaçlar çerçevesinde gerçekleşmektedir (Krause ve Tipton, 2007: 18).

DoS saldırılarının genel özelliklerine bakılacak olursa (Bozgeyik, 2018: 43):

- Genel olarak Botnet/ Zombi bilgisayar ağı ile gerçekleşmektedir.
- Binlerce hatta milyonlarca zombi bilgisayarlar kullanılmaktadır.
- İtibar zedelenerek maddi zarara uğratılması amaçlanmaktadır.
- Saldırıyı gerçekleştirenlerin bulunması neredeyse olanaksızdır, şeklinde sıralanmaktadır.

DDoS saldırılarında, bilgisayar ve bilgisayar ağlarının mümkün oldukça yavaşlatılması ve kullanılamaz duruma getirilmesi hedeflenmektedir. Bu saldırı aynı anda birden fazla bilgisayar ile gerçekleştirildiğinden dolayı büyük zararlara sebep olmaktadır. DDoS saldırılarının gerçekleştirilmesi noktasında bazı kabiliyetlerinin olduğu görülmektedir. Söz konusu kabiliyetler şu şekilde sıralanmaktadır (Yıldırım, 2018):

- Hedef alınan siteye yönelik saldırı yapılarak erişilebilirlik engellenmektedir.
- Hedef alınan bant genişliğine yönelik saldırı yapılarak bağlantıda ciddi problemler oluşturulabilmektedir.
- Uygulamalar aracılığıyla hedef gösterilen bilgisayarın işlevi sonlanmaktadır.

4. **Açık Mikrofon Dinleme:** Zararlı yazılım aracılığıyla, kullanıcının izni olmadan bilgisayarda mevcut olan kamera ya da mikrofonun açık tutulmasıyla ortamın dinlenmesi veya görüntünün alınması hedeflenerek yapılan saldırı faaliyetidir. Bu yöntemin en ünlü saldırısı olan GhostNet saldırısında; zararlı yazılımın devlet kurumları ve elçiliklerin sistemlerine yüklenerek, toplanan bilgilerin ÇHC'ye gönderildiği iddia edilmektedir (Çiftçi, 2013: 165).

5. **IP Aldatması:** Bilgisayara izinsiz erişim gerçekleştiren saldırgan, güvenilir bilgisayarın gibi kendisini göstererek mesaj göndermektedir. Mesajdan sonra saldırgan hedeflediği bilgisayarın IP adresini ele geçirerek internet üzerinden farklı paketler yollayarak bilgi alışverişini başlatmaktadır. Saldırgan, yapılan alışveriş sonrasında IP adresini değiştirip güvenilir adres görünümü vererek saldırılarına başlamaktadır. Bu duruma ise IP aldatması denmektedir (Abdul-Mumin, 2011: 31). IP aldatmasında, hedef olarak belirlenen kişi güven ilişkisi içinde veri alışverişini yaptığını sanmaktadır. Fakat saldırgan karşı tarafın kimliğini kullanarak saldırısını kamufle etmektedir (BM Uluslararası Telekomünikasyon Birliği, 2008). Kısaca IP aldatmacası; saldırganlar tarafından yönetilen bilgisayarlara gönderilen paketlerin başlık bilgilerindeki kaynak IP kısmında değişiklik yapılarak ve saldırı gerçekleştirilen kaynağın başka bir kaynakmış gibi gösterilerek gerçek kaynak adresin gizlenmesi faaliyeti olarak ifade edilmektedir (Ünal, 2011: 27).
6. **DNS Saldırısı:** Kullanıcının erişmek istediği internet sayfası dışında farklı bir sayfaya yönlendirilmesine dayanan yöntem DNS saldırısı olarak ifade edilmektedir. Bu saldırı yönteminde, saldırganlar DNS tarafından çözümlenmekte ve bu aşamaya korsanlar tarafından müdahale edilmektedir. DNS sunucusu, veri tabanına sahip bilgisayar sunucusu olup, girilmek istenen site ismini IP adresine yönlendirmektedir. Bilgisayarlarda daha önce girilmiş internet adreslerinin listelendiği ‘host’ verilerine, zararlı yazılımlar aracılığıyla erişen saldırganlar, bankasının web sitesine erişmek isteyen kullanıcıyı doğru web sitesini yazmasına rağmen farklı adrese yönlendirerek burada kullandığı tüm kişisel bilgileri elde etmektedir (Gürsoy, 2015: 99).
7. **Mızrak-Kimlik Avı Saldırısı:** Bu saldırı türü genellikle aynı anda çok sayıda kurbanı hedef alacak şekilde tasarlanmaktadır. Mızrak avı olarak bilinen bu saldırı türü, yanlışlıkla dâhi olsa, kötü amaçlı yazılım alıcılarının sadece bir kısmının kötü amaçlı bir bağlantıyı tıklamasını ya da virüslü bir dosyayı indirmesini umarak aynı anda adreslerden birçok e-posta adresine ortak e-posta gönderme şeklinde gerçekleşmektedir (Dalha, 2019).

8. **Sosyal Mühendislik:** Saldırganlar için en etkili saldırı şekli olan sosyal mühendislikte sınır yoktur. Yani diğer saldırı türlerindeki araç gereçlerde sınırlamalar söz konusuysa bu saldırı türünde bu sınırlamalara ihtiyaç duyulmamaktadır. Sosyal mühendislikte saldırı hedef olarak belirlediği kişiye psikolojik yönden saldırarak kişi ile ilgili bilgileri elde etmektedir (Maan ve Sharma, 2012: 552). Bu saldırı yöntemi ile insanların güvenleri manipüle edilerek bir saldırı gerçekleştirilmektedir. Dolayısıyla gelişmiş güvenli bilişim sistemleri bile hedef kişiyi gerçekleştirilen saldırıdan koruyamamaktadır. Kolaylıkla saldırıya uğrayan hedef kişiler, internet sitesinde gezinirken, zararlı bağlantılara tıklayarak ya da herhangi bir şey yükleyerek zararlı yazılımlar aracılığıyla söz konusu saldırının gerçekleşmesine sebep olmaktadır (Conteh ve Schmick, 2016: 31).

Sosyal mühendislik “insanları kandırmak, dışarı bilgi vermelerine zemin hazırlamak ya da harekete geçmelerini olanaklı kılmak için manipüle etmek” anlamına gelmektedir. Burada insanların duyguları istismar edilerek veri toplanmaktadır (Mann, 2008: 11). Bilgisayar korsanı olmayan sosyal mühendisler, bilgisayar korsanlarının işini kolaylaştıran ve bilgiye erişimini mümkün kılan kişiler olarak ifade edilmektedir. Sosyal mühendislerin amacı; bilgiye ya da bilgi sistemlerine fiziksel ya da dijital yollarla erişim sağlamaktır. Sisteme erişim sağlandıktan sonra elde edilen verilerin bozulması, silinmesi ya da çıkarılması için bilgisayar korsanlarının sisteme girişine izin veren sosyal mühendislerin uyguladıkları teknikler basit izinsiz girişler olabileceği gibi yüksek teknolojilerin kullanımını da içermektedir (Thornburgh, 2004: 134).

İnsanların zayıflıklarını kullanarak veriler elde eden bu saldırı türü bir nevi sanal dolandırıcılık yöntemi olarak da görülmektedir (Öcal, 2022: 46). Günümüzde oldukça yaygın olarak kullanılan sosyal mühendislik yöntemleri ise şu şekilde sıralanmaktadır (Tatar, 2011: 9-14; Çifçi, 2013: 147; Keleştemur, 2015: 307):

- Güvenilir olduğuna ikna ettikten sonra, bilgi karşılığında para, hediye vs. önermek,
- Sahte senaryolarla karşı tarafı etkilemek,
- Sosyal paylaşım sitelerinde akraba, arkadaş vb. ortak tanıdıklar üzerinden yakınlık kurarak bilgi, para vb. elde etmek,

- Telefon ya da e-posta yolu ile başka birini taklit ederek sanki o kişiymiş gibi iletişim kurmak,
- Karşı tarafın duygularını kullanarak zor durumdaymış gibi davranıp yardım talep etmek.

1.2.3. Siber Tehdit, Türleri ve Araçları

Küreselleşme sonrası yaşanan değişim ve dönüşümlerden sonra, bilgisayar yazılımlarına olan bağlılığın daha da artmasından dolayı, devlet güvenliğine yönelik karşılaşılan tehditlerin artması durumu klasik tehdidin ötesine geçmektedir. Bunun üzerine devletlerde bu değişime ayak uydurmak zorunda kalmaktadır. Bilgisayar yazılımlarına olan bu bağlılığın gelecekte de devam edeceği ve savaşların silah üstünlüğünün de ötesine geçerek yazılım üstünlüğünü ele geçirme boyutuna geleceği kabul edilmektedir. Bundan dolayı devletlerin görevi sınırları korumanın yanında bir de ağlar üzerinden yönetilen temel altyapıları korumak olarak değişmektedir (Özdal ve Ermiş, 2013: 278).

Devletler ve özel şirketlerin kritik altyapılarına bakıldığında, oluşabilecek herhangi bir güvenlik açığında bilgisayar korsanlarının vereceği ekonomik zararlar göz önünde bulundurulduğunda, siber tehdit araçlarının bir silah olarak nitelendirilmesi gerektiği savunulmaktadır. Ancak '*siber silah*' terimi her ne kadar popüler kültürün bir parçası haline gelse de, tanımı konusunda ortak bir noktaya varılamadığı görülmektedir. Terimin kapsamı oldukça geniştir, web sitelerini yavaşlatmaktan nükleer tesislerini yok etmeye kadar her şeyi kapsayan bilgisayar kodu yığınlarını temsil etmektedir (Brown ve Metcalf, 2014: 137).

Öte yandan, bir silahın genel olarak, savunma ya da saldırı aracı olarak kullanıldığı ve insanları etkisiz hale getirme, zarar verme ya da öldürme maksadıyla tasarlanmış bir cihaz olduğu bilinmektedir. Bu tanımlama daha çok klasik silahları kapsamaktadır. Fakat siber silahların klasik silahlardan farklı olduğu görülmektedir. Siber silahları oluşturan zararlı yazılımların insanları öldürmek, zarar vermek ya da etkisiz hale getirmek maksadıyla tasarlanmadığı ve silah teriminin özündeki maksadı yakalayamadığı kabul edilmektedir (Arimatsu, 2012: 97).

Yapılan saldırıların siber silah olarak tanımlanabilmesi için yasal çerçevede bazı şartları yerine getirmesi gerektiği savunulmaktadır. Bu yüzden de kullanılan zararlı yazılımın ya da hizmet dışı bırakma saldırılarının hangi şartlarda siber silah olarak

tanımlanabileceğinin belirlenmesi gerekmektedir. Örneğin, siber silahların neden olduğu hasar düzeyine bakılmaktadır. Bir sistemin geçici olarak hizmet vermesini engelleyen DDoS saldırısı ile bir bilgisayarı kullanılamaz hale getiren saldırı amaçlı kullanılan zararlı yazılım, hedeflediği herhangi bir saldırıda gözle görülür şekilde fiziksel hasara neden olmadıysa bu durum siber silah olarak değerlendirilmemektedir (Mele, 2013: 13).

Diğer taraftan bakıldığında ise kişiler, kurumlar, örgütler ya da devletler için hayati önem taşıyan bilgilerin bulunduğu siber ortam, kötü niyetli kişilerin hedefi hâline geldiği görülmektedir. Bu kötü niyetli kişilerin siber saldırı yöntemlerini kullanarak ortaya çıkaracakları zararlar ve saldırılar tüm aktörler tarafından tehdit olarak algılanmaya başlamaktadır (Karadağ, 2019: 13). Böylesine önem arz eden siber tehdidin diğer kavramlar gibi genel kabul gören tanımı bulunmamaktadır. Yapılan tanımlar doğrultusunda siber tehdit kavramı analiz edilmektedir.

“Bir sistemin veya kurumun zarar görmesiyle sonuçlanacak istenmeyen bir olayın olma potansiyeline” tehdit denmektedir (UHDB, 2016: 7). *“Siber ortama yönelik yapılan her türlü yıkıcı, engelleyici, bozucu ve ele geçirici saldırılar ya da faaliyetlerin çeşitli araç ve yöntemler aracılığıyla kullanılması”* siber tehdit olarak tanımlanmaktadır (BTK, 2009: 8). Bir başka tanıma göre ise siber tehdit; *“internete bağlanmayı olası hâle getiren ve çevrim içi saldırılarla karşı karşıya kalmayı mümkün kılan araçların oluşturduğu unsurlar”* şeklinde ifade edilmektedir (Güntay, 2017: 88).

Siber tehdit, zararlı ya da kasıtlı faaliyetler sonucunda oluşabileceği gibi bazen de bilinçsiz kullanıcılar tarafından da gerçekleştirilen olaylardan kaynaklanmaktadır. Örnek verilecek olursa; herhangi bir program ya da sistemde yeni kullanıcı oluşturulduğunda verilen izinlerin yanlış yapılandırılması durumunda, istenmeden yapılmış bir hareketin olmasıyla beraber istenmeyen etkilerin oluştuğu gözlemlenmektedir (Ulutaş, 2018: 93). Belirgin ve açık bir düşman tanımı bulunmayan siber tehditlerde saldırganlar, 12-19 yaş grubu arasındaki ergen çocuklar olabileceği gibi bazı düşünceleri savunan teröristler, terörizme destek veren ‘haydut devletler’ ya da çıkarları yönünde hareket eden devletlerde olabilmektedir. Siber tehditlerin belirli bir merkezinin olmaması ve karmaşık yapıya sahip olması saldırganların amaçlarının, tehditlerinin ne olduğunu ve kanıtlanabilirliğini zorlaştırmaktadır (Kurnaz, 2016: 70).

Öte yandan, siber tehdit ile ulaşılmak istenen hedeflerin; “güç elde etmek, kontrolü ele geçirmek, sömürü yapabilmek, maddi kazanç elde etmek ya da intikam

almak” şeklinde sıralandığı görülmektedir (BGA Security, 2018). Siber tehditlerin kullanım hedeflerini özele indirgediğimizde ise bilişim teknolojileri vasıtasıyla, toplumların iç ve dış düzenini koruma refleksini zayıflatmak ya da tamamen ortadan kaldırma isteği oluşturmak olduğu vurgulanmaktadır (Güntay, 2018: 92).

Siber silah olarak da tanımlanabilen siber tehdidin hedeflerinin yanında bir de siber ortamda karşımıza çıkabilecek çeşitli araç ve yöntemleri bulunmaktadır. Bu araç ve yöntemlere kısaca değinmek faydalı olacaktır.

1. **Zararlı Yazılım:** Bilgi ve iletişim teknolojilerinin işleyişini bozma, zarar verme, sekteye uğratma ve verileri çalmaya yönelik tasarlanmış virüs, truva atı, solucan/kurtçuklar, bakteri, arka kapı, mantık bombası, casus yazılımı vb. siber silahlar zararlı yazılım olarak adlandırılmaktadır (Malware Definition, t.y.).
2. **Bakteri:** Herhangi bir programdan bağımsız olarak, kendi kendine çoğalabilen bakteriler birçok farklı türünü kendiliğinden yazabilen zararlı yazılımlar olarak bilinmektedir. Çoğalma sonucunda bulaştıkları sistemde hafıza ve disk alanını kaplayarak işlem gücünü zayıflatmaktadır. Akabinde ise bilgisayar performansında düşüklüğe sebep olmaktadır. Bakteriler genel olarak çalışma mantığından dolayı virüse benzetilirken, yapı olarak ise solucanlara benzetilmektedir (Çiftçi, 2013: 169).
3. **Solucanlar, Kurtçuklar:** Zararlı yazılım türlerinden olan solucanlar, tıpkı virüsler gibi bir cihazdan başka bir cihaza kopyalanmak üzere tasarlanmaktadır. Fakat solucanlar virüslerin aksine bunu kullanıcı müdahalesi olmadan kendiliğinden yayılarak ve kendilerinin birebir kopyalarını ağdan ağa dağıtarak gerçekleştirmektedir. Bilgisayarda bulunan dosya ya da veri transferi işlevinin denetimini ele geçiren solucanlar, sisteme bir kere bulaştıktan sonra kendi kendine yollarına devam ederek çoğalmaktadır. Solucanların en tehlikeli yanlarının ise büyük oranda çoğalma yeteneklerinin olduğu belirtilmektedir. Veri ve dosya alışverişi yapan kullanıcılar alışveriş yöntemlerini kullanarak kendilerini, iletişim hâlinde oldukları tüm bilgisayarlara ya da tüm e-posta adreslerine gönderebilmektedir. Solucanlar yayılmak için dosyaya ya da taşıyıcı programa ihtiyaç duymamasının yanı sıra sistemde bir tünel açarak başkasının bilgisayarının

uzaktan ele geçirilmesine olanak sağlayabilmektedir. Yeni çıkan solucanlar, güvenlik yazılımları tarafından henüz tanınmadığı için ilk etapta ağ trafiğini önemli ölçüde yavaşlatabilmektedir. (Öğün ve Kaya, 2013: 154-155).

4. **Virüsler:** Bilişim teknolojilerinin gelişmesiyle beraber virüs, bilgisayar dünyasında on yıllardır karşılaşılan kavram olarak karşımıza çıkmaktadır. Virüs kavramının, insanlar tarafından negatif bir şekilde yorumlanmasıyla beraber söz konusu yorumun bütün zararlı yazılımları kapsadığı düşünülmektedir. Fakat bu kullanımın doğru olmadığı düşünülmektedir. Çünkü her tür zararlı yazılım virüs olarak ifade edilememektedir. Gerçek anlamda virüsler, diğer dosyalara bulaşarak yayılan bazı zararlı yazılım türlerini belirtmek için kullanılmaktadır. Kendi kendine yeterli olmayan virüsler yayılmak için diğer dosyalara ihtiyaç duymaktadır. IBM-PC tabanlı 'Brain' olarak adlandırılan *boot sector* virüsü kayıtlara geçen ilk virüs olarak karşımıza çıkmaktadır. Söz konusu virüsün Ocak 1986 yılında ortaya çıktığı söylenmektedir (Graham, Howard vd., 2010: 198-199).

Virüsler çeşitli şekillerde karşımıza çıkmaktadır. Bunlar;

- Ön yüklemeli virüsler
- Yerleşik virüsler
- Çok şekilli virüsler
- Makro virüsler
- Çok parçalı virüsler şeklinde sıralanmaktadırlar (Çiftçi, 2013: 170).

5. **Truva Atları:** Yunan mitolojisinde bir hediye gibi görünen truva atı, gerçekte Truva Antik Kenti'ni ele geçirme amacı olan ve Yunan askerlerini içinde gizleyen tahtadan tasarlanmış ata verilen isim olarak bilinmektedir. Günümüzde siber suçların işlenme biçimlerinden biri olan truva atının; faydalıymış gibi görünen bilgisayar programlarının arka planında gizli bir kodun yer almasından dolayı bilgi işlem güvenliğini zedeleyen ve tehlikeye atan bir program olduğu ifade edilmektedir (Turhan, 2006: 47). Genel olarak e-posta, mesajlaşma programları, internet ile oynanan oyunlar ya da internet ile yüklenen ücretsiz ve lisanssız yazılımlar yoluyla yayılan truva atları, solucanlardan farklı olarak sisteme bulaştığı program hangisiyse o programın açılmasını beklemektedir. Yani bulaştığı program açılmadan aktifleşmemektedir. Doğrudan bilgisayarın işletim

sistemine zarar veren truva atları, bilgisayar ile işlemleri gerçekleştirerek tüm kontrolü ele geçirmektedir. Gerçek bir uygulamaya benzeyen zararlı program türü olan truva atları, virüs olarak nitelendirilmemektedir. Bilgisayarlarda güvenlik açığı oluşturarak zararlı programların, saldırganlar tarafından sisteme girmesine yol açmaktadır. Kendi kendini çoğaltamasa da virüs kadar yıkıcı etkisi olan truva atları, faydalı gibi görünse de bilgisayar sistemlerine girdiğinde gizli olarak zararlı eylemlerde bulunmaktadır (Gordon ve Chess, 1999).

6. **Mantık Bombası:** Truva atına entegre edilebilen mantık bombaları, bilişim sistemi ya da ağında bulunan program kodunun bir parçasını taşıyan ve bazı kötü niyetli eylemlerin yapılması amacıyla tasarlanan program olarak ifade edilmektedir. Kötü niyetli eylemleri gerçekleştirebilmek için doğru zamanı bekleyen ya da sürekli olarak faaliyet gösteren bir program olan mantık bombaları; bilgisayar sistemini bozmak, kullanılamaz hâle getirmek için tasarlanmaktadır (Turhan. 2006: 51).
7. **Arka Kapı:** Yalnızca siber saldırgan tarafından bilinen kimlik doğrulama düzeneklerine takılmadan sistemde oluşan açıklardan yararlanarak oluşturulmuş, genellikle gizli yollarla sistemi yönetme ya da şifreli sisteme giriş yapabilmek için oluşturulan yöntem ya da giriş noktaları ‘arka kapı’ olarak adlandırılmaktadır (Çiftçi, 2013: 172).
8. **Kök Kullanıcı:** Sistemde yapılan işlemleri, sistem bilgilerini ya da dosyaları işletim sisteminden saklayarak gerçekleştirilen zararlı yazılım türü, kök kullanıcıları olarak tanımlanmaktadır. Günümüzde sistemleri ele geçiren zararlı yazılım türü olarak kullanılan kök kullanıcıları, işletim sistemlerinde çekirdek olarak faaliyet göstermektedir. Dolayısıyla çekirdek düzeyinde faaliyet gösterdiği için tespit edilebilmeleri oldukça zorlaşmaktadır. Bunun için özel programların kullanılması gerekmektedir (Öcal, 2022: 42).
9. **Casus Yazılımlar:** Bir bilgi işlem sisteminde, kullanıcının rızası olmadan bilgisayar üzerinden kişi, kurum ya da kuruluşlar hakkında bilgi toplayan yazılımlar ‘casus yazılım’ olarak adlandırılmaktadır. Kullanıcıların internet

üzerindeki hareketlerini izleyen casus yazılımlar bunu kayıt altına alarak, istem dışı ticari tanıtım yazılımları göndermektedir (Janasson ve Sigholm, 2005: 1).

10. Köle Bilgisayarlar: Önceden sistemlere yüklenen program aracılığıyla kullanıcıları uzaktan kontrol edebilen ve saldırganların amaçları yönünde kanalize edilen sistemlere botnet yani köle bilgisayar denilmektedir. Hedef olarak belirlenen sistemin kullanıcısının haberi olmadan sistemi, saldırganın amaçları doğrultusunda hareket ettirmektedir. Özel yazılımlar sayesinde uzaktan yönetilebilen köle bilgisayarlar büyük saldırılarda kullanılmaktadır (Güngör, 2015: 45).

11. Gelişmiş Siber Tehditler: Hedefi net olarak belirlenmiş sürekli bir çalışma neticesinde tasarlanmış olan ve çok etkili siber saldırı gerçekleştirme kapasitesine sahip siber tehditlere ‘gelişmiş siber tehditler’ denmektedir. Genel olarak grup ya da devlet desteği ile belirli sistem veya kişileri hedef alan APT’ler, özel geliştirilmiş saldırı teknikleri ve hedeflere sızmak için gelişmiş tehditler kullanılmaktadır. Bundan dolayı söz konusu tehditler bulaştıkları sistemlerde yayılarak uzun süre fark edilmeden çalışabilmektedir (Bircan, 2012).

12. Fidye Yazılımları: Bu yazılım türü bilgisayar sistemine ve ağa sızarak verileri ya da bilgisayarı kilitleyerek kullanıcıları sistemde kötü amaçlı yazılım olduğuna inandırmaktadır. Bu doğrultuda uyarı niteliğinde olacak şekilde söz konusu durumdan kurtulmak için ödeme yapmaları gerektiğini, aksi takdirde sistem verilerinin silineceğini belirten bir ibare yollanmaktadır (Oğuz, 2021: 29). Ödeme yapıldıktan sonra bilgilerin sağlam bir şekilde verileceğinin garantisi bulunmamaktadır. Genel olarak online oyunlar aracılığıyla bilgisayara bulaşan fidye yazılımları, günümüzde aktif bir şekilde kullanılmaktadır (Arslan, 2021: 25).

Öte yandan, yapılan araştırmalar sonucunda siber tehdit kavramını beş alt başlıkta toplamanın mümkün olduğu tespit edilmiştir. Söz konusu başlıkların; siber suç, siber terörizm, siber caydırıcılık, siber istihbarat, siber casusluk ve siber savaş şeklinde sıralandığı görülmektedir.

1.2.3.1. Siber Suç

Küreselleşme sonrası bilişim teknolojilerindeki gelişmeler birçok alanda geleneksel hâle gelen anlayışın değişmesine ve yepyeni bir yaşamın ortaya çıkmasına sebep olmaktadır. Söz konusu gelişmeler, hayatı olumlu yönde değiştirdiği gibi aynı zamanda olumsuz birtakım gelişmeleri beraberinde getirmektedir. Siber alanda yaşanan kimi gelişmeler sonrasında geleneksel suç anlayışına uymayan yeni suç anlayışı ortaya çıkmaktadır. Bununla beraber literatürde siber suçlarla ilgili çeşitli tanımlamalar yapılmaktadır. Bilgisayarların kötüye kullanılması, bilgilerin çalınması, verilerin nakli ile ilgili kanun ve meslekte etik kurallarına aykırı davranışlar siber suç olarak görülmektedir. Bilişim suçu, bilgisayar suçları ya da bilgisayar bağlantılı suçlar gibi kavramlar ile ifade edilen siber suçların hepsinin bilgisayar vasıtasıyla gerçekleştiriliyor olması onların ortak özelliğini ortaya koymaktadır. (Çakır ve Kılıç, 2014: 21).

Bir başka tanımda siber suç kavramına bakılacak olursa; 2000 yılında BM siber suçu, *“bilişim teknolojilerindeki sistemlerin güvenliğini ya da veri işlemini hedef alan ağ vasıtasıyla gerçekleştirilen eylemler”* şeklinde ifade etmektedir. 2004 yılında Avrupa Konseyi Siber Suçlar Sözleşmesinde ise siber suç tanımı; *“izinsiz erişim, veriye ve sisteme yapılan müdahale, bilişim sistemi vasıtasıyla dolandırıcılık ya da sahtekârlık suçlarının yanı sıra bilgisayar ve veriye yönelik yapılan eylemlere ek olarak, bilişim sistemlerinin kullanılmasıyla ve özellikle internetin yaygınlaşmasıyla beraber niceliksel olarak ortaya çıkan çocuk pornografisi, yabancı düşmanlığının ve ırkçılığın önlenmesine ilişkin hükûmler, telif haklarına ilişkin ihlallerde siber suçtur”* şeklinde yapılmaktadır. (Şenol, 2018: 194-195).

Diğer yandan ise ‘siber alandaki cinayet’ şeklinde tanımlanan siber suçta, yaşanan olayın cinayet zanlısının bilgisayar olduğu düşünülmektedir. Siber suçlular, bilgisayardaki kişisel verileri ele geçirmek, ticari sırları öğrenmek ya da kötü amaçlı internet araştırmasını gerçekleştirmek maksadıyla söz konusu saldırıyı gerçekleştirmektedir (Ulutaş, 2018: 94). Genel olarak siber suça örnek verilecek olursa (Corell, 2000: 8):

- Kullanıcının izni olmadan bilişim sistemine girilmesi,
- Sistemdeki verilere girilmesi hususunda izni olmadığı halde erişimde bulunulması,
- Verilerin değiştirilmesi ve silinmesi,
- Sistemin kullanımını sekteye uğratması,

- İletişimin izinsiz izlenmesi ve kayıt edilmesi gibi hukuka aykırı eylemler, şeklinde sıralanmaktadır.

1.2.3.2. Siber Terörizm

Siber terörizmin kökenine bakıldığında; Fransızca “terreur” sözcüğünden dilimize “terör” olarak geçen terim, Latince kökenli olup “korkudan titreme”, “yıldırma” anlamlarına gelmektedir. Terör teriminin zaman içerisinde sonuna eklenen “-izm” eki terörün sistemli olduğunu göstermektedir. Akabinde eklenen bu ek, terör olaylarının siyasi amaçlarına ya da terör fikrinin harekete geçirilmesine atıfta bulunmak için kullanılmaktadır. Bununla birlikte, sıklıkla kullanılan terör teriminin uluslararası alanda genel kabul görmüş bir tanımının olmadığı tespit edilmektedir. Fakat yine de terör terimine bir tanım yapılacak olursa; “*terör, şiddet yoluyla yaratılan korku ve bu korku ortamını yaratan şiddet olaylarının kendisi*” şeklinde ifade edildiği görülmektedir. Terörizm terimi ise; “*bir takım ideolojik amaçlar için sistemli, örgütlü ve sürekli biçimde terörü araç olarak kullanmayı benimseyen eylem*” olarak tanımlanmaktadır (Yalman, 2018: 259).

Diğer yandan, siber uzay ile terörizm kelimesinin birleşiminden meydana gelen siber terörizmin tıpkı terörizm kelimesinde olduğu gibi genel kabul görmüş bir tanımının olmadığı görülmektedir. Kapsamlı bir tanım yapılacak olursa siber terörizm; “*ideolojik ya da sosyal hedefleri gerçekleştirmek amacıyla, devletleri ve vatandaşlarını korkutarak, aşağılayarak, baskı kurma yoluyla devletlerin politikalarını değiştirmek için bilgisayarlara, veri tabanlarına, ağ sistemlerine bilişim teknolojilerindeki kabiliyetleri vasıtasıyla gerçekleştirilen zarar verici saldırılar ve tehditler*” şeklinde ifade edilmektedir (Yayla, 2014: 194-195). Yapılan bu tanım doğrultusunda, siber terör eylemlerinde silah olarak bilişim sistemlerinin kullanıldığı sonucuna varılmaktadır. Bununla birlikte söz konusu olan sistemler kullanılarak, hedef olarak belirlenen kişiler, kurumlar ya da devletlere ait bilgisayar ve iletişim sistemleri ele geçirilerek siber saldırılar yapılmaktadır. Bu siber saldırıların, korku ve şiddet içermesinin yanı sıra can ve mal kaybına da sebep olduğu sonucuna varılmaktadır (Şenol, 2018: 195).

Ek olarak internetin, merkezi kontrolden uzak olması, herhangi bir sınıra sahip olmaması, erişiminin ucuz ve kolay olması, medyanın yoğun ilgisinin olması ve anonim olması nedeniyle teröristler tarafından yoğun bir şekilde kullanıldığı ortaya konmaktadır. Teröristler için iki temel amaçla kullanılan internetin ilk amacı, iletişim

ortamını sağlaması ve etkin bir eğitim olanağı sunmasıyken, ikinci amacın ise internetin, bilgisayar ve ağ sistemlerinin gerçekleştirecekleri siber terör eylemleri vesilesiyle siber uzayı oluşturmaları şeklinde ele alındığı belirtilmektedir. Böylelikle siber uzay ve terörizmin kesiştiği yerde siber terörizm kavramının ortaya çıktığı tespit edilmektedir (Çeliktas, 2016: 11-12).

Yukarıda sayılan sebeplerden dolayı siber uzayın ve internetin teröristlere cazip gelmesiyle beraber siber terörizmde artış yaşandığı saptanmaktadır. Bu noktada ise siber terörizm ve siber suçun birbirinden ayrı şekilde ele alınması gerektiği düşünülmektedir. İki kavramı birbirinden ayırırken, eylemi gerçekleştiren saldırganların motivasyon durumları göz önünde bulundurulmaktadır (Weimann, 2004: 4). Kısacası, siber suç ve siber terörizmi ayıran noktalar ele alındığında, bu ayrımın (Yalman, 2018: 260);

- Siber suçta, saldırganlar dijital ortamı kullanarak maddi/manevi menfaat sağlamayı ilke edinirken,
- Siber terörizmde ise, belirli bir ideoloji doğrultusunda saldırganların yapmış olduğu saldırının sonucunun fiziksel/finansal zarar verme eğiliminde olması, şeklinde olduğu belirtilmektedir.

1.2.3.3. Siber Caydırıcılık

Caydırıcılık kavramı Türkçede genellikle, “*korkutarak cesaret kırmak ve vazgeçirmek*” anlamına gelen ‘caydırmak’ kelimesinden oluşturulmaktadır. Türk Dil Kurumu (TDK) sözlüğünde ise caydırıcılık; “*bir saldırganlığı önlemek ve engellemek için önlem alma işi*” olarak açıklanmaktadır (Türk Dil Kurumu, t.y.).

Diğer yandan caydırıcılık kavramı, “*bir devlet ya da topluluğun, başka bir devlet ya da topluluğa karşı gerçekleştirilecek eylemlerden kaçınmak amacıyla gerekli önlemler alması*” şeklinde tanımlanmaktadır. “*Yaşanacak olan anlaşmazlıkların giderek büyüüp askeri güç kullanımını gerektirmesine engel olması durumu*” da caydırıcılığın bir diğer açıklaması olarak karşımıza çıkmaktadır. Bununla birlikte, uluslararası güvenlik kaynaklarında ise caydırıcılığın “*esirgeme*” ve “*misilleme*” olmak üzere iki farklı türünün olduğu görülmektedir (Güntay, 2017: 91).

Siber uzayda caydırıcılığın temel amacına bakıldığında ise saldırı yapabilecek olan aktörleri daha saldırıyı gerçekleştirmeden engellemek amacıyla politikalar oluşturulduğu belirtilmektedir. Saldırganın bu saldırıyı gerçekleştirmesi durumunda, karşısına çıkacak olan tehdit öğelerinin saldırganı saldırıdan caydırabileceğine ve farklı

yollardan çözüm arayışına girmesine fırsat verileceğine olanak sağlanmaktadır. Bununla beraber, tek bir aktöre yönelik olmayan caydırıcılık, birden çok aktörün aynı girişimlerde bulunması olasılığının önüne geçmeyi amaçladığı görülmektedir. Kısacası, farklı aktörlere karşı farklı caydırıcılık politikaları izlenmesi gerektiği söylenmektedir. Bu duruma örnek olarak, Birleşmiş Milletler Uyuşturucu ve Suç Ofisi (UNODC) verilerinde yapılan bir analiz gösterilebilmektedir. UNODC'nin verilerine göre; ÇHC, Japonya ve Almanya siber uzay üzerinden işlenen suçlarda siber suçlara has kanunlar yaparken, bazı devletler siber suçlara yönelik var olan ceza kanunlarını hem siber hem de klasik yöntemler vasıtasıyla işlenen suçları kapsayacak şekilde genişletmektedir. Öte yandan, siber suç işleyen kişiler aynı anda iki farklı suç işlemekle yargılanabilmekte ve böylece caydırıcılık bu yöntemle artırılmaktadır (Savçın, 2020: 36-37).

Ek olarak, Çinli filozof ve savaş stratejisti Sun Tzu'nun “En iyisi savaşmadan baş egmektir” söyleminden yola çıkarak siber caydırıcılık kavramını ele alacak olursak; söz konusu kavramı, “*siber uzayda bilişim sistemleri ve bunlarla alakalı altyapılarına saldırı yapacak olan saldırganı, saldırıdan vazgeçirmek*” şeklinde ifade ettiği görülmektedir. (Şenol, 2018: 209). Bir diğer tanımda ise siber caydırıcılık, “*siber alanda saldırganların hareketlerini boşa çıkarma veya cezalandırma yöntemiyle saldırıdan vazgeçirme ilkesi*” şeklinde açıklanmaktadır (Libicki, 2009: 29-30). Bununla birlikte siber caydırıcılık, korunma hâlinde olan bir devletin, daha büyük bir misillemeyle karşılaşacağı korkusuyla, hedefleme ve etkileme yolunu kullanarak düşmanın yapacağı siber eylemleri caydırmaya yönelik niyetlerinin olduğunu gösteren strateji olarak görülmektedir (Iasiello, 2014: 55).

Son olarak, tehditlerin nereden geleceği belli olmadığından dolayı siber caydırıcılığın, misillemeden çok savunma odaklı olduğu belirtilmektedir. Bu durumda, yapılacak herhangi bir saldırıda saldırganların yapmış oldukları güçlü savunma sayesinde hedeflerine ulaşmadan onları başarısızmış gibi gösterip buna ikna ederek saldırıdan vazgeçirmektedir. Bunu da saldırı sonrası bedel ödeyeceklerine ikna ederek yapmaktadır (Lupovici, 2011: 51).

1.2.3.4. Siber İstihbarat ve Siber Casusluk

İstihbarat ve casusluk, insanlık tarihi boyunca düşman olan ülke, devlet ya da topluluklar üzerinde otorite sağlamak veya avantaj elde etmek amacıyla yürütülen faaliyetler olarak görülmektedir. Kökü oldukça eskiye dayanan bu kavramların önemi

hep aynı kalsa da teknolojik gelişmelerden dolayı yöntemlerinde farklılıklar olduğu sonucuna varılmaktadır (Çiftçi, 2013: 289-290).

Arapça kökenli olan istihbarat kavramı; ‘istihbar’, ‘haber’ ve ‘bilgi alma’ kelimelerinin çoğullaşmış hâlinde oluşmaktadır. İstihbarat kavramının İngilizce karşılığı ise ‘intelligence’ olarak karşımıza çıkmaktadır. Bu da akıl, zekâ, bilgi, haber ve istihbarat anlamına gelmektedir. Türkçe karşılığına bakıldığında ise ‘malûmatın derlenmesi’ yani toplanan bilgilerin değerlendirilmesi anlamını taşıdığı görülmektedir (Özdağ, 2009: 34). Bununla beraber, birden çok bileşeni bünyesinde barındıran siber istihbarat kavramının ise; *“önderler, devletler, şirketler, örgütler veya kişilerin siber alan içerisinde çekişme hâlinde oldukları güçlerin gizli ve hassas verilerinin bilişim teknolojileri vasıtasıyla kanunsuz yollarla elde etmesi”* şeklinde açıklandığı tespit edilmektedir (Akyeşilmen, 2018: 231).

Diğer yandan, verilen tanımlar doğrultusunda siber istihbaratın veri ya da bilgi toplama yöntemlerinin olduğu görülmektedir. Bu yöntemler; sosyal mühendislik, casus yazılımlar, ücretsiz web hizmetleri, sosyal medya, uzaktan bağlantı, oltalama ve iletişimin dinlenmesi şeklinde sıralanmaktadır. Bunlara ek olarak, devletlerin istihbarat örgütleri tarafından çeşitli hedeflerle oluşturulan ‘bal küpleri’ de bu yöntemlerin arasında yer almaktadır. Bal küpleri, siber alandaki en iyi bilinen savunma aldatmacası olarak görülmektedir. Bal küpleri sayesinde net ve yeterli bilgiye zamanında erişim sağlanarak oluşacak tehditlere karşı önceden uyarı sağlanmaktadır. Bal küpü siteleri ile özellikle terör örgütlerinin siber alandaki faaliyetlerinin tespit edilmesi ve terör eğilimi olan kişi ya da kuruluşların önceden belirlenmesinde gereken istihbaratın toplanması sağlanmaktadır (Kotik, 2015: 16).

Bir diğer kavram olan casus kavramı ise Lahey Antlaşması’nın (1889) 29. maddesinde, *“gizlice veya sahte kimlikle, muharip bir devletin harekât sahasında bilgi elde eden veya etmeye çalışan kimse”* şeklinde tanımlanmaktadır (Bozgeyik, 2018: 29). Bunun yanında siber casusluk kavramının ise, *“devletlerin sahip olduğu dijital ortamdaki bilgi varlıklarının; sistemde bulunan zayıflıklar, oluşan açıklıklar, yapılan saldırılar ve tehditler, kasıtlı bırakılan açık kapılar vasıtasıyla kullanılan yazılım ve donanımlar üzerinden belirli bir çıkar için ele geçirme ya da bilgi sızdırma”* şeklinde açıklandığı görülmektedir (Sağiroğlu, 2018: 25).

Siber casusluk ile internette, ağlarda, yazılımlarda ya da bilgisayarda yasa dışı yöntemler kullanılarak siyasi, askeri, ekonomik avantaj sağlamak amacıyla kişilerin,

kurumların, devletlerin gizli, hassas, özel bilgileri ele geçirilmektedir (Nickolov, 2008). Amerikan İstihbarat Direktörü James R. Clapper Ocak 2016’da, “ÇHC; Amerika, Amerika’nın müttefikleri ve Amerikan Şirketleri’ne karşı başarılı bir şekilde siber casusluk eylemlerini sürdürmektedir” şeklinde açıklama yapmasıyla beraber ÇHC’nin siber casusluk eylemleri yürüttüğünü ve Amerika’nın bu eylemler hakkında bilgi sahibi olduğunu vurgulamaktadır (Bozgeyik, 2018: 29).

Sonuç olarak, siber istihbarat ve siber casusluk sonucunda elde edilen önemli bilgilerin ileride karşılaşılabilecek geleneksel savaş ya da siber savaş öncesi düşmana karşı bilgi üstünlüğü sağlayarak önlem alma noktasında yarar sağlayacağı görülmektedir (Singer ve Friedman, 2018: 130-131). Bu durum, iki kavramın ileride karşılaşılabilecek herhangi bir savaş hâlinde, bilgi üstünlüğü sağlama ve önlem alma noktalarında büyük önem taşıdığını göstermektedir.

1.2.3.5. Siber Savaş

Uluslararası literatürde genel kabul gören tanımı olmayan siber savaş kavramının, İngilizce “cyber war” teriminden Türkçeye çevrilerek kullanılmaya başlandığı bilinmektedir. İngilizce’de “cyber” sözcüğü siber, “war” sözcüğü ise savaş anlamında kullanılmaktadır (Yayla, 2013: 40). Bu doğrultuda siber savaş kavramı; *“ulusal bir amacı gerçekleştirmek maksadıyla ya da mevcut bir savaşı desteklemek amacıyla, düşman ülkelerin her türlü bilişim sistemlerine ve altyapılarına karşı gerçekleştirilen imha etme, engelleme ya da çıkarlarına göre kullanma ve buna karşı gelen tedbirler ya da süreçler”* şeklinde tanımlanmaktadır (Güntay, 2017: 97). En çok rağbet gören siber savaş tanımı ise Richard Clarke ve Robert Knake tarafından yapılmaktadır. Onlara göre siber savaş; *“bir devlet tarafından, başka bir devleti desteklemek ya da onun adına başka bir devletin bilgisayar sistemlerine ya da bilişim ağlarına zarar vermek, veri eklemek, değiştirmek, kesinti yaratmak, bozmak üzere gerçekleştirilen sızma faaliyetleri”* olarak ifade edilmektedir (Clarke ve Knake, 2011: 119).

Bir başka ifade ile siber savaş; *“bir ülkeye ait sivil, askeri ve hükûmete ait olan bilişim teknolojilerinin düşmanların siber saldırılarına karşı savunulmasıyla beraber politik, ekonomik ya da askeri sebeplerle hedef olarak seçilen ülkeye bilişim teknolojileri üzerinden organize saldırı eylemleri gerçekleştirilmesi”* şeklinde tanımlanmaktadır (Yazıcı, 2011). Verilen tanımlara ek olarak bir de siber savaş

yöntemlerinin olduğu tespit edilmektedir. Siber alanda meydana gelen siber savaş yöntemleri şu şekilde belirtilmektedir (Öcal, 2022: 29):

- Bilgisayar korsanlığı savaşı
- Komuta kontrol savaşı
- Elektronik savaş
- İstihbarat merkezli savaş
- Ekonomik bilgi savaşı

Öte yandan, önleme savaşı olarak nitelendirilen siber savaşta en önemli noktanın “çeviklik” olduğu belirtilmektedir. Önleme savaşını etkileyen unsurlar ve hükûmetlerin siber savaş stratejilerindeki önemli hususları bulunmaktadır. Bu hususlar şu şekilde sıralanmaktadır (Çiftçi, 2013: 66- 70):

- Ülkelerin desteklediği ulusal ya da uluslararası sözleşmeler ve düzenlemeler,
- Bir ülkenin yönetilme şekli, oraya ait demokrasi anlayışı ya da insan haklarına yaklaşımları,
- Ülkenin uluslararası alanda kendisini konumlandığı yer,
- Siber uzaydaki aktifliği ve bağımlılığı,
- Siber saldırı durumunda sergiledikleri savunma ve siber saldırı eylemleri.

Bunlara ek olarak, siber savaş kavramı ile beraber siber suç ve siber terörizm kavramlarının ilişkilerine değinecek olursak; siber savaş kavramı bu iki kavram ile aynı yöntemleri kullansa da amaç ve motivasyon noktasında birbirlerinden ayrıldıkları görülmektedir. Siber savaş bu kavramlara göre daha sistemli ve daha yoğun siber saldırıları içerisinde barındırmaktadır. Ayrıca siber suçlar ve siber terörizm eylemleri kişiler ya da gruplarca yapılmaktadır. Fakat siber savaşın taraflarını devletler ya da örgütler oluşturmaktadır. Yani siber savaşın devletler ve örgütler mihrinde oluşan bir kavram olduğu belirtilmektedir (Hathaway ve Crootof, 2012: 833).

1.3. Güvenlik Alanında Oluşan Yeni Tehdit: Siber Güvenlik

Dünya sürekli olarak bir değişim ve dönüşüm hâlinindedir. Yaşanan yıkımlar, yenilikler birçok alanda farklılık ve çeşitliliği beraberinde getirmektedir. Özellikle yaşanan savaşlar güvenlik kavramında büyük dönüşümlerin yaşanmasına vesile olmaktadır. Güvenlik algısının ilk olduğu süreçten, yaşanan dünya savaşlarına ve Soğuk Savaş sürecine kadar birçok değişime maruz kaldığı gözlemlenmektedir. Genel kabul görmüş bir tanımı olmadığı için alt başlıklar hâlinde; farklı görüşlerin güvenlik

algısına, Kopenhag Ekolü'nün güvenlik anlayışına ve bu süreçler aracılığıyla siber güvenlik kavramının oluşumuna ve sonrasında yaşanan gelişmelere kadar birçok konuya ilişkin analiz yapılmaktadır.

1.3.1. Güvenlik Kavramı ve Dönüşümü

İnsan yaşamının her alanında var olan ve sonrasında da varlığını sürdüren güvenlik kavramı; güvende olma arzusu, yeme, içme ve barınma gibi temel gereksinimler arasında yer almaktadır. Abraham Maslow'un oluşturduğu temel ihtiyaçlar hiyerarşisine göre fizyolojik ihtiyaçların ardından gelecek olan güvenlik basamağı en temel ikinci ihtiyaç olarak piramitte yerini almaktadır. İnsanın güvenlik ihtiyacı giderilmeden bir sonraki basamağa geçmenin mümkün olmadığı belirtilmektedir. Güvende olma arzusu karşılanmadan bir sonraki ihtiyaç olan aitlik, sevgi, saygı ve kendini gerçekleştirme gibi sosyal ihtiyaçlar oluşmamaktadır. Kısacası, Maslow'un da belirttiği gibi, güvende olmak ya da güvende hissetmek kişiliğin getirmiş olduğu en temel ihtiyaç olarak görülmektedir (Kula ve Çakar, 2015: 197). Temel ihtiyaçlar içerisinde yer alan güvenlik kavramı zaman içerisinde farklı anlamlar kazanarak değişkenlik göstermektedir. Güvenlik kavramının tanımlarından bahsedilmeden önce kavramın kelime kökenini bilmek gerekmektedir.

Latince kökenli olan güvenlik kavramı, *se* (olmaksızın) ve *cura* (endişe) sözcüklerinin birleşimi sonucu *securitas* kelimesinden türetilerek oluşmaktadır. *Securitas* kelimesi “endişeden uzak olma” anlamına gelmektedir (Arends, 2012: 5). Cicero ve Lucretius vasıtasıyla psikoloji ve felsefe literatüründe ilk kez gündeme gelen güvenlik kavramı, birinci yüzyıl ile beraber “Pax-Romana” bağlamında siyasi bir terim olarak kullanıldığı görülmektedir. Thucydides'in oluşturduğu ve Thomas Hobbes'in şekillendirdiği kavramın bir başka oluşumu ise otoriter ve süper devletin doğuşu anlayışının şekillenmesiyle meydana gelmektedir. Akabinde günümüz güvenlik kavramına bakıldığında ise üç düşüncenin birleşimiyle oluştuğu belirtilmektedir. Bu düşünceler şu şekilde sıralanmaktadır (Brauch, 2008: 2-3):

1. Atinalıların, imparatorluklarının yıkılmasını önleme çabaları,
2. Romalıların, 'securitas'ının siyasi ve dini çağrışımlar,
3. Hobbes'un felsefi fikir yapısı ile oluşturmuş olduğu Leviathan.

Diğer taraftan, kavramın tanımlarına bakıldığında, uluslararası ilişkilerde, o alana ait durumları tanımlamak için kullanılabilecek genel kabul görmüş tanım veya

kavramsallaştırmanın olmaması, alanın en büyük problemlerinden biri olarak karşımıza çıkmaktadır. Uluslararası ilişkilerin sosyal bilim olması ve uğraştığı konuların niteliklerinden dolayı bu tarz sorunlarla karşılaşabilmektedir. Güvenlik kavramının da bundan dolayı tıpkı küreselleşme ve terör gibi genel kabulden yoksun birçok anlama sahip olduğu bilinmektedir (Özcan, 2011: 447). Uluslararası alanda ‘security’ olarak ifade edilen güvenlik kavramının, en temel tanımı TDK tarafından, “toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet” olarak ifade edilmektedir (Türk Dil Kurumu, t.y.).

Güvenlik kavramının esnek ve çok çeşitli olmasından dolayı birbirinden farklı tanımlar ortaya çıkmaktadır. Bu tanımlara bakıldığında ise;

- Wolfers, “güvenlik, nesnel anlamda var olan değerlere ait bir tehdidin olmaması, öznel anlamda ise bu değerlere ait bir saldırı olabilmesi korkusu taşımama ” şeklinde tanımlamaktadır (Wolfers, 1952: 481-502).
- Miller, “tehlike ve tehdit durumunun olmaması” şeklinde ifade etmektedir (Miller, 2001: 16).
- Bir başka tanımda ise; “hükûmetlerin, toplumların, örgütlerin ve bireylerin varlıklarını koruma ve sürdürme yolundaki eylemleri ile bunları tehdit eden öğelerin ortadan kaldırılması” şeklinde yorumlanmaktadır (Dedeoğlu, 2004: 2).
- Son olarak Ullman’a göre güvenlik kavramı, “kişilerin, devlet dışı birimlerin, örgütlerin ya da hükûmetlerin var olan değerlere veya hayatlarına yapılacak herhangi bir saldırı ya da tehdidin olmadığı durum” olarak ele alınmaktadır (Levy, 2005: 40).

Genel olarak yapılan güvenlik tanımlamalarına bakıldığında, oldukça farklı tanımların yapıldığı görülmektedir. Kavrama göreceli ve değişken anlamlar yüklendiği için farklı tanımlamalar ortaya çıkmaktadır. Ayrıca düşünürlerin farklı görüş ve bilimsel bakış açılarına sahip olması, aynı zamanda yapılan tanımlamaların mekân ve zaman olarak farklılık göstermesi yapılan tanımlamanın çeşitlenmesi hususunda önemli bir faktör olarak görülmektedir. Fakat kavram nasıl yorumlanırsa yorumlansın ya da nasıl kullanılırsa kullanılsın güvenlikten söz edilebilmesi için; varlığın korunması ve sürdürülmesi amacıyla içten ya da dıştan bir veya birkaç tehdidin olmasının yanı sıra birde bu türden algılamaların olması gerekmektedir (Karabulut, 2009: 9-10).

Tanımlamalara ek olarak; açlık, küresel ısınma, bölgesel savaşlar, uluslararası terörizm, çevresel felaketler, siber güvenlik tehditleri gibi konular günümüz güvenlik faaliyetlerinin konusunu oluşturmaktadır. Bu durum güvenlik konularının evrildiğini ve çeşitlendiğini göstermektedir. Süreç ilerledikçe düşünürler güvenlik kavramının odağına insanların güvenlik anlayışlarına paralel olarak çeşitli unsurlar yerleştirmektedir. Bundan dolayı farklı dönemlerde farklı güvenlik anlayışlarının ortaya çıktığı görülmektedir (Öcal, 2022: 11). Bu doğrultuda söz konusu dönemlerin analiz edilmesi güvenlik anlayışını daha iyi anlama noktasında fayda sağlamaktadır.

1648 tarihli *Westfalya Barış Antlaşması* ile beraber geleneksel imparatorluk sürecinden, çağdaş devlet yapısına geçilmektedir. Yaşanan bu dönüşüm sürecinin olduğu dönem ‘Avrupa Devletler Sisteminin’ başlangıcı olarak kabul edilmektedir (Sönmezoğlu, 2002: 29). Devletler sistemine geçilen bu süreçle beraber bu dönemi takip eden süreç genel anlamda klasik güç dengesi olarak ifade edilmektedir. Akabinde yerel, bölgesel güç öğelerinin birbiriyle bütünleştirildiği bu süreçte sınırları belli bir merkezi yapı sistemi oluşturulmaktadır. Büyük güçlerin birbirleri karşısında yer alması bu dönemin güvenlik anlayışının oluşmasına sebep olmaktadır. Öte yandan, bu dönemde hâkim modern devlet yapısının yükselmesiyle beraber sistemde yeniden yapılanmaya gidildiği görülmektedir. Devletin gücünü koruyabilmesi için öncelikle hâkimiyetini koruması gerekmektedir. Bu durum uluslararası kararlılığın belirleyici unsurunu oluşturmaktadır. Yapılan bu yöntemin amacı; süreç boyunca oluşacak çatışmaların ve savaşların en az düzeyde tutulması olarak ele alınmaktadır. Bunun yanında, büyük devletlerin yapmış olduğu her türlü faaliyetin meşru olarak karşılanması dönemin en önemli özelliği olarak ifade edilmektedir. Burada savaş durumu güvenlileştirilmemiştir, sadece uluslararası toplumun bir çıktısı olarak görülmektedir (Buzan ve Hansen, 2009: 23-24).

Dünyanın şahitlik ettiği en büyük savaşlardan biri olan *Birinci Dünya Savaşı*’nın yaşandığı süreçte ise devletlerin güç odaklı politikalarının, güvenlik noktasında yetersiz kaldığı düşünülmektedir. Savaş sonrasında bu tür bir savaşın ve sorunun tekrar etmemesi için barışı ve güvenliği yeniden oluşturma fikri ortaya çıkmaktadır. J. Bentham, J. Locke, I. Kant ve H. Grotius’un ortaya koyduğu düşüncelerin bileşimi şeklinde W. Wilson’un (1938) ortaya attığı 14 ilke ile kendi düşüncelerini gösteren yaklaşım Milletler Cemiyeti’nin kurulması ile başlamaktadır (Toklu, 2004: 29). Diğer taraftan, bazı yaklaşımlarında güvenlik kavramının dönüşümüne katkı sağladığı

görülmektedir. Bu doğrultuda, sonradan ortaya çıkan realistler kendilerini “idealist” olarak tanımlasalar da bu realistlerin kendilerini tanımlamaya yönelik gayretleri, idealistlerin tanımlanma ve tasvir edilmesine sebep olmaktadır (Eralp, 1996: 60).

Uluslararası İlişkiler disiplininin ortaya çıkmasıyla beraber öne sürülen bir diğer yaklaşım olan idealizm, iki büyük savaş arası dönemde ortaya çıktığı bilinmektedir. Savaş sürecinin başlamasıyla beraber devam eden yıkıcı olaylar sonucunda dünya barışının nasıl önleneceğine ilişkin savaş-barış teorisi olarak insanlığın genel problemlerine yapısal bir çözüm şeklinde olarak ortaya çıktığı söylenmektedir (Bakan ve Şahin, 2018: 139).

W. Wilson’un önderliğini yaptığı idealizm teorisinin üzerinde durduğu temel nokta, uluslararası barışı ve güvenliği sağlamak için karşılıklı olarak ulusların güçlerini birleştirmesi ve iş birliği içerisinde hareket edilen uluslararası bir toplumun oluşmasını sağlamaktır. Akabinde ise tüm devletlerin oluşturulan bu uluslararası toplumda barış hâlinde, yaşanabilir çatışmasız bir ortamın gerekliliğini addetmektedir. Bundan dolayı devletlerin savaş yanlısı olmadıkları demokratik bir yapının oluşturulması gerekliliğini vurgulamaktadır. Bunların yanı sıra, uluslararası hukukun üstünlüğü ve üst yargı mekanizmalarının varlığı ile uluslararası toplum düzeninin olabileceği, barış ve güvenliğin sağlanabileceği belirtilmektedir (Elmas, 2013: 46-47).

İdealizmin felsefi kökenine bakıldığında ise her ne kadar liberalizmle bazı konularda aynı temelde buluşsalar dâhi ayrıldıkları noktalar da olduğu görülmektedir. Bu noktalar şu şekilde ortaya konmaktadır: İdealistler, uluslararası politikada sosyal ve siyasal bir varlık olarak devleti ana aktör şeklinde görmektedir (Ateş, 2013: 61). Liberalizmi savunanlar ise güvenliğin asıl sağlayıcısının devletlerin yönetim şekli olduğunu söylemektedir. Onlara göre bir devlet totaliter rejime sahipse savaşa ve baskıya meyilli, demokratik rejime sahipse barış yanlısı olmaktadır (Kesgin, 2022: 5-6).

Birinci Dünya Savaşı’nın başlamasıyla beraber temelleri atılan idealist yaklaşımın barış ve güvenliği sağlamak için uyguladıkları engelleme çabaları İkinci Dünya Savaşı’nın başlamasıyla başarısızlık göstermektedir. Bu durum ise idealistlerin sonunu hazırlayarak 1945 yılından hemen sonra güç ve çıkar odaklı olan realist yaklaşımın uluslararası ilişkilere uygulanmasının yolunu açtığı ve idealizmin realizme dönüşmesine sebep olduğu belirtilmektedir (Aydın, 1996: 92).

Bu doğrultuda, realist anlayışa göre, güvenlik kavramı askeri unsurlar ışığında değerlendirilmektedir. Aynı zamanda dış politika ulusal güvenlik sorunları etrafında

şekillenmektedir. Bu durumda askeri ve siyasi sorunlar “yüksek politika”; ekonomi, çevre, sağlık ve diğer sorunlar ise “alçak politika” olarak nitelendirilmektedir (Oğuzlu, 2007: 14). Güç, çıkar ve insan doğasını temel alan ve devleti ana aktör olarak konumlandıran realist bakış açısı, güvenlik anlayışının odağında sürekli bir güvensizlik anlayışı ve güvende olamama durumunun yattığını savunmaktadır. Bu bakış açısı doğrultusunda realizm, devletlerin askeri güçleri ve çıkarları yönünde sürekli oluşabilecek tehdit ve risklere karşı hazırlıklı olmaları gerektiğini belirtmektedir. Ayrıca bu yöntem ile varoluşları doğrultusunda ulusal güvenliklerini koruyabilecekleri açıklanmaktadır. Öte yandan, güç ve kapasitenin artırılmasıyla, sürekli anarşinin hâkim olduğu bu ortamda, varlık ve söylemlerini kabul ettirilme olasılıklarının artacağı belirtilmektedir. Bu yöntem ile kişinin güvenliğinin sağlanabilmesi adına devletin ulusal güvenliğinin hâkim kılınması ilkesini ortaya atmaktadır. Realizmin güç ve kapasitenin artırılması noktasında süreklilik gerektiği düşüncesinin, Soğuk Savaş döneminin yaratmış olduğu ortam ile geliştiği gözlemlenmektedir (Sandıklı ve Emeklier, 2011: 6-7).

Soğuk Savaş süreci içerisinde realizm anlayışının da dönüşümle karşı karşıya kaldığı görülmektedir. Bundan dolayı, 1979 yılında Kenneth Waltz tarafından çıkarılan “Uluslararası Siyaset Teorisi (Theory of International Politics)” adlı kitapta, dış politikayı yalnızca insan doğasına ve hükûmetin kapasitesine indirgeyen görüş, dış politikayı yalnızca birey mihrinde değerlendiren liberalizmi ve üretim şekliyle sınıf çatışmasını temel odak noktası olarak belirleyen marksist görüşü eleştirdiği gözlemlenmektedir. Waltz, uluslararası sistemin bünyesinin ‘hiyerarşik’ ve ‘anarşik’ olarak iki türde olduğunu savunmaktadır. Ayrıca hükûmetlerin gayelerinin, varlıklarının sürekliliğini sağlamak ve hâkimiyetlerini korumaları gerektiği olarak belirtmektedir (Öcal, 2022: 13).

Bunlara ek olarak, realistlere göre güvenlik kavramı sadece güç ile sağlanabilecek iken neorealistlerin gücü, realistlerin düşüncelerine yakın olacak şekilde ortaya koyulduğu görülmektedir. Hans Morgenthau varlığının devamlılığını sağlamakla, Niccolo Machiavelli iyi bir yönetimle, Edward Carr, Kenneth Waltz ve realist düşüncayı savunan diğer düşünürler güç dengesi ve askeri kapasite ile güvenliğin sağlanabileceğini öne sürmektedir. Akabinde ise karşılıklı olarak ve anarşik düzenin bir sonucu olarak kapasite artırma yapan hükûmetlerin arasında yaşanan güvensizlik algısı

da John H. Herz tarafından ‘güvenlik ikilemi’ olarak ortaya konulmaktadır (Kesgin, 2022: 5).

Doğrudan güç yerine güvenlik üzerine yoğunlaşan neorealist anlayış, her ne kadar realist düşünceye yakın olsa da her iki kuramın birbirlerinin düşüncelerinden ayrıldığı noktalar da bulunmaktadır. İş birliğini savunan neorealistler aynı zamanda ittifaklar vasıtasıyla güvenliğini oluşturmanın gerekliliğini ileri sürmektedir (Sandıklı ve Emeklier, 2011: 25). Neorealizmi realist düşünceden ayıran bir diğer nokta ise güvenlik unsuruna ekonomik unsurları dâhil etme çabasına girmesi olarak ifade edilmektedir. Neorealistler, yalnızca askeri konuların güvenlik için yeterli olmayacağını bununla beraber ekonomin de güvenlik alanına girmesi gerektiğini savunmaktadır (Ayhan, 2016: 135).

Bir başka yönden, Soğuk Savaş sürecinin gevşemeye başlamasıyla birlikte hükûmet ve hükûmet dışı aktörlerin artması sonucu sistemin yeniden yorumlanması gerektiği düşüncesi ortaya çıkmaktadır. Küresel ölçekte varlığın sürekliliği ve güvenliğin sağlanması konusunda oluşturulan yorumlama; ekonomi, siyaset, kültür gibi birçok konuda güvenliğin oluşturulmasını da beraberinde getirmektedir (Dedeoğlu, 2020: 78).

Soğuk Savaş’ın bittiği sürece gelindiğinde ise birçok yeni olgu ve sorunun ortaya çıktığı görülmektedir. İktisadi, siyasi ve sosyal yansımaların olduğu yepyeni bir düzene girildiğinin sinyalleri ilk olarak 1990’lı yıllara girildiğinde verilmektedir. Yeni kurulmaya çalışılan ve pek çok sorunu içinde barındıran yeni düzeni tanımlayan bir isim henüz bulunamamaktadır. Günümüzde bile Soğuk Savaş sonrası dönem olarak adlandırılan bu dönem, yapılandırma aşamasında olan, bir geçiş dönemi olarak ifade edilmektedir. Soğuk Savaşın bitmesinden bu yana, yani yaklaşık yirmi yıllık süreçte, güvenlik kavramının tanımında ve anlayışında oluşan değişimler, dönemin dinamiklerini ve yapısını belirlemede büyük rol oynamaktadır (Bakan, 2007: 36). Soğuk Savaş sonrası süreçte, güvenliğin yeniden izahı ve güvenlik çalışmalarının uluslararası ilişkiler disiplini içerisindeki konumunun değişip, akademik gündemi meşgul eden ve üzerinde en fazla çalışma yapılan konulardan biri hâline geldiği gözlemlenmektedir (Öztürk 2014: 160).

Yaşanan süreçte güvenlik ile ilgili ortaya birtakım görüşler çıkmaktadır. Bu görüşlerde bir kesim, liberalizm ve uluslararası örgütlerin faydalarıyla barış ve iş birliğinin oluşturabileceği fikrini ortaya atarken diğer kesim ise medeniyetler arası ya da

etnik kökenli çatışmaların ve silahların çoğalıp yayılması ile beraber gelecekte anarşik ortamın oluşacağı düşüncesini savunmaktadır. Yeni dönemin oluşmasıyla birlikte tehdit ve risklerin artması ve dönüşmesiyle güvenlik kavramının yeniden ele alınması gerektiği düşüncesine varılmaktadır. Kavram yeniden ele alınırken eski dar düşünce kalıpları bir kenara bırakılarak, kavramın derinlemesine incelenmesi gerektiği vurgulanmaktadır. Bunlara ek olarak, Soğuk Savaş süreci iki kutuplu bir yapıyı beraberinde getirirken bu sürecin bitmesi ve yeni düzene geçilmesiyle birlikte sistemin yapısal dönüşümü iki kutupluluğu ortadan kaldırarak birden çok aktörün sistem içerisinde aktif olduğu bir yapı hâlini almaktadır (Krause ve Willams, 1997: 33).

Önceki dönemlerde güvenlik kavramının nasıl ele alındığına bakıldığında ise sınırların korunması ve ülke bütünlüğünün sağlanması şeklinde bir düşüncenin olduğu görülmektedir. Bununla beraber, dış politika amaçları denildiğinde her ne kadar klasik anlamda mevcut olan duruma ilişkin amaçlar akıllara gelse de artık bunun yanında güvenlik ve hayatî çıkar gibi amaçlarda gelmektedir. Fakat günümüze bakıldığında, küreselleşme ile beraber, bilişim ve teknolojinin gelişmesinin etkisiyle ülkeler arasındaki sınırların coğrafi olarak olmasa dâhi ekonomik ve siyasal boyutta netliğini kaybettiği göz önüne alınarak, güvenlik kavramının akıllara sadece sınırların korunması şeklinde gelmeyeceğinin açık olduğu görülmektedir (Bayır, 2013: 174). Daha önce askeri güvenlik anlayışı ve güç ön plandayken, sonraki dönemde bu düşünce karmaşılaşarak çevre güvenliğinden, bilgi güvenliğine kadar çok geniş alana yayılım göstermektedir. Bu genişleme; hükûmet, hükûmet dışı aktörler ve bireylerin güvenlik kavramını oluşturma evresinde yapılacak olan analiz seviyelerinde değişime sebep olmaktadır (Ergül, 2008:176).

Öte yandan, güvenlik kavramı ile ilgili oluşan yeni anlayış ile beraber etnik çatışmalar, doğal kaynakların yok olması, uluslararası uyuşturucu ve insan kaçakçılığı, yolsuzluk, mali suçlar ve çevre kirliliği gibi birçok risk ve tehdit konularını içine aldığı belirtilmektedir. Alanın bu denli genişlemesi karşısında yeni güvenlik yaklaşımı, devlet odaklı güvenlik anlayışının yerine bireyi odağa alan güvenlik anlayışını benimsemektedir. Ortaya çıkan bu yeni anlayışın; hesap verebilirlik, şeffaflık, denetime açıklık, hukukun üstünlüğü vb. ilkeleri de benimsediği görülmektedir. Tüm anlatılanlar ışığında, güvenlik ile ilgili sorunların Soğuk Savaş boyunca sürekli olarak askeri güç ile ilişkili bir şekilde ele alındığı tespit edilmektedir. Akabinde, bu süreçte askeri güçle ilgili olan unsurların devletin politikaları içinde yer aldığı gözlemlenmektedir. Devleti

merkeze alan ve güç odaklı uluslararası anarşik sistem yapısı bu dönemde etkili olsa da Soğuk Savaş sonrasında küreselleşmenin yaşanmasıyla beraber tehdit ve risk algılamalarında çeşitliliğin olduğu ifade edilmektedir. Kavramın çeşitlenmesi sonucu analizlerin yalnızca askeri temelde yapılması aşılıp, değerlendirmelere; nüfus, çevre, kültür, enerji sorunları ve ekonomik unsurlar gibi etkenlerin de dâhil edildiği görülmektedir (Şahin, 2020: 197).

Soğuk Savaşın bitmesiyle beraber bu süreci takip eden dönemde ise özellikle ABD’de 11 Eylül 2001 saldırılarının gerçekleşmesi, ulusal güvenliğin alanının ve algısının değişmesi yanı sıra güvenliğin sadece askeri ve fiziksel saldırılar karşısında alınan önlemler olarak görülmeyeceğini savunan bir yaklaşıma dönüştüğü vurgulanmaktadır. Yeni yaklaşımla birlikte siber saldırılar, terör, salgın hastalıklar ve ekonomik gelişmelerin engellenmesi de ulusal güvenliğin kapsamına girerek söz konusu alanın bir parçası hâline gelmektedir. Devletin hayatî önem taşıyan verilerinin korunması konusunun da ulusal güvenlik kapsamında önem kazandığı görülmektedir. Bununla beraber, yeni dönemle beraber devlet için önemli olan ulaşım, enerji, sağlık, finans gibi kritik altyapılar ile ilgili olarak siber suçlara ve tehditlere karşı siber politikaların da geliştirildiği ifade edilmektedir (Kesgin, 2022: 7).

Son olarak, güvenliğin dönüşümü ile ilgili yapılan çalışmalara önemli katkılarda bulunan Kopenhag Okulu’nun da analiz edilmesi konuya farklı bakış açısı kazandırmak adına önem arz etmektedir. 1990’lı yıllarda güvenliğin çok boyutluluğunu ön plana çıkararak kavramsal güvenlik çalışmalarında bir kırılma yaratan Kopenhag Okulu’nun, 21. yüzyılda güvenlik çalışmalarının merkezi hâline geldiği görülmektedir. Okul güvenlik kavramını; *“hükûmetlerin ve toplumların tehditlerden kurtulma arayışları ve düşman güçlere karşı bağımsız kimliklerini ve fonksiyonel bütünlüklerini koruma kabiliyetleri”* olarak tanımlamaktadır (Sandıklı ve Emeklier, 2011: 33). Okulun önemli teorisyenlerinden olan Barry Buzan güvenlik kavramına yönelik fikrini genişleterek klasik fiziksel güvenliğin yanı sıra siyasi, ekonomik, çevresel ve toplumsal güvenliği de güvenliğin konusu hâline getirmektedir. Diğer taraftan bakıldığında, 21. yüzyılda teknolojik gelişmeler doğrultusunda çok boyutlu güvenlik anlayışının yetersiz kaldığı düşüncesine varılmaktadır. Akabinde bu anlayışın değişmesi zorunlu hâle gelmektedir. Yaşanan teknolojik gelişmelerde göz önüne alındığında, önceki boyutlardan farklı olarak siber güvenlik adında yeni bir boyut daha kazandırıldığı görülmektedir (Hansen ve Nissenbaum, 2009: 1163).

Öte yandan, ilk başta güvenlik konusunda yapılan tartışmalara yönelik bir tepki ortaya koyan Kopenhag Okulu'nun, sonrasında güvenliği daha sistemli bir biçimde çalışmayı hedeflediği ifade edilmektedir. Sovyetler Birliğinin (SSCB) yıkılmasıyla beraber güvenliği bazı alt birimlere ayırarak hedeflenen çalışmalarına devam ettikleri görülmektedir. Bununla beraber, okul güvenlik unsurunu üç ana öğeye ayırmaktadır. Bunlar; bölgesel güvenlik alanları, güvenliğin boyutları ve güvenlikleştirme şeklinde sıralanmaktadır. Ayrıca Buzan güvenliği; askeri güvenlik, ekonomik güvenlik, çevresel güvenlik, siyasi güvenlik ve sosyal güvenlik olmak üzere beş farklı boyutta ele almaktadır (Buzan, 1983: 97).

Tüm bu anlatılanlara ek olarak, Kopenhag Okulu içerisinde sektörlerin seçimi sırasında bu sektörlerle beraber ortaya çıkan diğer boyutlar da büyük önem kazanmaktadır. Askeri güvenlik boyutu; hükûmetlerin sahip olduğu saldırı ve savunma yeteneklerinin karşılıklı etkileşimini ve diğer devletlerin algılayış biçimini içermektedir. Ekonomik güvenlik boyutu; hükûmetin sahip olduğu refah seviyesini ve gücünü kabul edilebilir aşamada tutmak ya da seviye olarak daha iyi konuma ulaştırmak için ihtiyaç duyulan maddi kaynaklara erişimi ifade etmektedir. Çevresel güvenlik boyutu; insanların tüm faaliyetlerinin bağımlı olduğu evrensel ve yerel biyosferin korunmasını ilgilendirmektedir. Siyasi güvenlik boyutu; hükûmetlerin yönetim şekli ve bu şekilde yasallık kazandıran ideolojileri kapsamaktadır. Sosyal güvenlik boyutu ise; geleneksel dil, din, kültür ve ulusal kimlik ile geleneklerin gelişimi için gerekli olan şartların devamlılığını içermektedir (Booth, 2007: 162).

Başka bir yönden bakıldığında, Kopenhag Okulu'nun güvenlik anlayışının temelini “*güvenlikleştirme*” kavramının oluşturduğu görülmektedir. Güvenlikleştirme; bölgesel ve sektörel güvenlik komplekslerinin aslında Buzan ve Weaver'in bireysel olarak yaptıkları çalışmaların ürünü olduğunu ifade edilmektedir. Güvenlikleştirme de Weaver'in imzası varken, sektörel ve bölgesel kompleksler Buzan'ın imzasını taşımaktadır (Açıkmeşe, 2008: 145). Okula göre güvenlikleştirme, “*siyasi bir toplulukta değerli bir öznenin varlığına yönelik bir tehdit olarak kabul edilen ve bu tehdide karşı acil ve olağanüstü önlemler alınması çağrısında bulunmayı sağlayan özneler arası bir anlayışın inşa edildiği başarılı bir söz edimi*” şeklinde açıklanmaktadır. Diğer kavramların açıklanmasında da anahtar kavram olarak kullanılan güvenlikleştirmede (Miş, 2011: 357) üç temel birim bulunmaktadır. Bu birimler; referans nesneleri, fonksiyonel aktörler ve güvenlikleştirme aktörleri olarak ortaya konmaktadır. İlk

aşamada yer alan belirli bir konunun belirli bir referans nesnesine yönelik tehdit olduğu varsayılmaktadır. İkinci aşamada, güvenlikleştiren aktör kitlelere bunun tehdit olduğunu ikna etmektedir. Üçüncü aşamada ise, güvenlikleştiren aktörlerin aldığı tedbirleri kapsamaktadır (Tokdaş, 2018: 16).

Yukarıda da belirtildiği gibi teknolojinin gelişmesiyle beraber güvenlik kavramının değişim ve dönüşümü sonucunda siber güvenlik kavramı ortaya çıkmaktadır. Tez çalışmasının kilit noktası olan bu kavram, farklı bir başlık altında ele alınarak daha detaylı bir şekilde incelenmektedir.

1.3.2. Siber Güvenlik Kavramı ve Tarihçesi

İnsan yaşamında büyük bir yere sahip olan güvenlik kavramı, küreselleşme sonrası teknolojinin daha da ilerlemesi ve internet kullanımının yaygınlaşmasıyla beraber çeşitlenerek karşımıza çıkmaktadır. Yaşanan bu değişim ve dönüşüm insan yaşamını kolaylaştırır da beraberinde risk ve tehditleri de getirmektedir. Bunun yanında, güvenlik kavramı tüm devletlerin, uluslararası örgütlerin ele aldığı önemli bir kavram olarak görülmektedir. Yukarıda da anlatıldığı üzere yaşanan dönüşümler siber kavramının ve onunla ilişkili diğer kavramların oluşmasına sebep olmaktadır. Tüm bu yaşananlarla birlikte dijitalleşen dünyada karşılaşılan tehdit ve riskten korunmak amacıyla siber güvenlik kavramı ortaya konmaktadır. Çalışmanın ana noktasını oluşturan siber güvenlik kavramı bu başlıkta ve sonrasında oluşturulacak başlıklar altında daha detaylı ele alınacaktır.

Soğuk Savaş ve sonrası süreçten başlayarak güvenlik tehditlerinde genişleme olduğu gözlemlenmektedir. Dolayısıyla güvenlik algısı bu yönde değişerek çeşitlilik göstermektedir. Oluşan yeni güvenlik anlayışıyla beraber yeni tehditler ortaya çıkmaktadır. Bu tehditler; ekonomik, gıda, çevresel, küresel salgınlar ve uluslararası terörizm vb. tehditler olarak genişlemektedir. Bu genişlemeyle beraber, küreselleşme ve sonrasında teknolojik gelişmelerin yaşanmasıyla ‘siber alan/uzay’ denen yeni alanın ortaya çıktığı belirlenmektedir. Bilgisayar ve dijital ağların sık kullanıldığı siber alanda, siber saldırı ve siber terör gibi tehditlerin güvenliğe zarar verdiği görülmektedir. Bu sorunlar her ne kadar başlangıçta tamamen teknik olarak görülse de siber alan ve diğer tehdit kaynakları arasında giderek iç içe geçen ilişki, siber güvenliğe çok daha fazla önem atfetmektedir. Böylece siber alanın kontrol edilemeyen yapısı ve özelliğinden dolayı, tehditler bu alanda çok boyutlu ve rahat bir şekilde yönetilmektedir. Bundan

dolayı, tıpkı diğer alanlarda olduğu gibi (kara, deniz, hava, uzay) bu alanında güvenlik yönünden önemli bir yere konulması gerektiği düşünülmektedir (Yangyue, 2015: 17-18).

Siber güvenlik kavramı, 1990'lı yılların başında ilk kez bilgisayar mühendisleri tarafından, ağa bağlı bilgisayarla ilgili oluşan bir dizi güvenlik problemlerini ifade etmek için kullanıldığı belirtilmektedir. Fakat daha sonra ortaya çıkan bu güvenlik problemlerinin yıkıcı sonuçlar doğurabileceği gerçeği ile karşılaşılnca, bu konu zamanla batı dünyasında özel şirketler, politikacılar ve medya açısından önemli bir tehdit olarak değerlendirilmeye başlanmaktadır. Bu tehditler 'Elektronik Pearl Harbor'lar olarak nitelendirilmektedir. Bunun yanında, ABD'de yaşanan 11 Eylül olayları; bilgisayar, bilgi teknolojileri ve güvenliğe akabinde ise özellikle dijital konulara gösterilen ilgiyi daha da artırdığı ifade edilmektedir. Bundan doğrutuda, bilgi ve iletişim teknolojilerinin alt yapılarının korunması, elektronik gözetim, teröristlerin interneti iletişim, haberleşme aracı olarak kullanması konularına odaklanılmaktadır (Hansen ve Nissenbaum, 2009: 1155- 1156).

İlk zamanlarda temel gayesi iletişimi sağlamak olan internetin geçmişi, telgrafın icadına (1837) kadar geri götürülebilmektedir (Cridland, 2008: 1). Daha sonrasında iletişimin sağlanması amacıyla Atlantik ötesine kablolar çekilmesi iletişimde var olan mesafe kavramını zamanla ortadan kaldırmaya başlamaktadır. İlk icat edildikleri zamanlarda kod çözme amacıyla üretilen ve büyüklüğü adeta bir ofis boyutunda olan bilgisayarlar, zamanla geliştirilerek teknolojide yeni bir çıkır açmaktadır (Öğün ve Kaya, 2013: 149).

Günümüzde böylesine önem arz eden siber güvenlik kavramına ilişkin birçok devlet, kurum ve kuruluş tarafından tanımlama yapılmaktadır. Fakat yukarı kısımlarda açıklaması yapılan diğer kavramlarda da olduğu gibi siber güvenlik kavramının da genel kabul görmüş ve ortak olan bir tanımı bulunmamaktadır. Her devlet tanımı ve politikaları kendine göre oluşturma yoluna gitmektedir. Ele alınan tanımlardan bazıları ise şu şekildedir: BM'ye bağlı olarak faaliyet gösteren Uluslararası Telekomünikasyon Birliği (ITU) siber güvenliği; *“siber uzayda kullanıcıların, kurum ve kuruluşların varlıklarını korumak amacıyla kullanılan politikalar, araçlar, güvenlik kavram ve önlemleri, eylemler, risk yönetimi yaklaşımları, uygulamalar, eğitimler ve teknolojilerin bütünü”* olarak tanımlamaktadır. Siber güvenlik; kuruluş ve kullanıcıların varlıklarını, bağlı oldukları bilgi işlem cihazlarını, bireyleri, altyapıları, hizmetleri, haberleşme

sistemlerini ve siber uzayda iletilen ya da saklanan bilgilerin tamamını içermektedir. Siber güvenlik ile gerçekleştirilmek istenen amaç ise kurum, kuruluş ve kişilerin güvenliğini ve varlıklarını siber alanda karşılaşılabilecekleri risk ve tehditlere karşı korumak ve bunun devamlılığını sağlamaktır (ITU, 2008: 2).

Ulusal Siber Güvenlik Stratejisi'ne (2016-2017) göre siber güvenlik kavramı *“siber alanı oluşturan bilgi ve iletişim sistemlerinin saldırılardan korunması, bu ortamda işlenen bilgi ya da verinin gizlilik, bütünlük ve erişilebilirliğinin koruma altına alınması, saldırıların ve siber güvenlik olaylarının tespit edilmesi, bu tespitlere karşı tepki mekanizmalarının çalıştırılması ve sonrasında ise sistemlerin yaşanan siber güvenlik olayı öncesi durumlarına geri döndürülmesi”* şeklinde ifade edilmektedir (UDHB, 2016: 8). Bir diğer tanım ise siber güvenliği; *“bilgi ve iletişim sistemlerini, ağları zarara uğratarak işlemez hâle getiren ya da çalışmasını engellemek amacıyla yapılan her türlü saldırı ve tehditlere karşı bu sistem ve ağları koruma çalışmalarının bütünü”* şeklinde yorumlamaktadır (Akleyek ve Tok, 2011).

Bir başka yönden siber güvenlik hususu analiz edildiğinde, 2007 yılının siber güvenliğinin, ulusal güvenlik için bir tehdit niteliği taşıyabileceği fikrinin oluşmasında önemli bir dönüm noktası olma özelliği taşıdığı gözlemlenmektedir. Bu tarihte, Rusya kaynaklı olduğu iddia edilen ve Estonya'ya karşı gerçekleştirilen siber saldırıların neticesinde ortaya çıkan zararlarla siber güvenliğinin, ulusal güvenlik için bir tehdit olabileceği düşüncesinin güçlendiği görülmektedir. SSCB döneminden kalan ve Tallinn Meydanı'nda bulunan Bronz Askeri Heykeli'nin taşınmasıyla, Rusya ve Estonya arasında gerilimin artarak devam etmesiyle beraber bu gerilimin etkilerinin siber uzayda da sürdürüldüğü ifade edilmektedir (Darıcı, 2015: 414). Her türlü hizmeti internet aracılığıyla sağlama olanağına sahip Estonya'da, yapılan bu saldırılar neticesinde hayatın aşağı yukarı durma noktasına geldiği söylenmektedir. Dünyanın farklı noktalarından, birçok farklı merkezlerden koordine edilerek gerçekleştirilen saldırılarda, ülkede en çok kullanılan internet siteleri, bankacılık ve finans sistemleri, devlet hizmetlerinin verildiği altyapı sistemleri vs. hedef alınarak, verilen zarar artırılmaktadır. Geniş kullanım alanına, gelişmiş internet ağına ve bu ağlarla birlikte bir organizasyona sahip olan Estonya'nın bunun yanı sıra siber uzaydan gelen saldırılara ve tehditlere karşı da açık ve savunmasız bir hâle geldiği belirtilmektedir (Eren, 2017: 36-37).

Öte yandan, yaşadığımız dönemde siber teknolojilerin; savunma, ulaşım, sağlık, eğitim, sanayi ve sosyal hayatın bir unsuru durumuna gelerek geniş bir alana yayılması,

bu alanlarda oluşacak tehdit ve saldırılara açık hâle gelmesine sebep olmaktadır. Bu durum siber güvenliğin önemini artırarak bu güvenliğin sağlanması gerektiği fikrini ortaya koymaktadır (Johnson, 2015: 26-29). Dolayısıyla yaşanan siber saldırılardan sonra devletlerin varlıklarını korumak ve vatandaşların güvenliğini sağlamak amacıyla daha aktif ve hukuksal tedbirler almak zorunda kaldığı görülmektedir. Bundan dolayı hem NATO, BM, Avrupa Birliği (AB), AGİT hem de diğer birçok devletlerarası örgütün bu konuda oluşturdukları politikalar ve savunma sistemleri ile siber güvenlik mekanizmaları revize edilmeye başlanmaktadır (Yılmaz ve Sağıroğlu, 2013: 159).

Söz konusu aktörlerin amaçları doğrultusunda donanım ve yazılımları birer araç olarak kullanarak, var oldukları fonksiyonel alanı güvenli hâle getirme gayreti gösterebilmek adına siber güvenlik aracılığıyla siber saldırıları ortadan kaldırmak ya da saldırıları en aza indirmek ve bu durumları politikalar üreterek onarmak aynı zamanda kritik alt yapıları korumak ve güçlendirmek amacıyla farklı yöntemler geliştirilmektedir. Oluşturulan politikaların temel amacı; izinsiz bir şekilde bireylerin, devletlerin ya da kurum ve kuruluşların özel bilgilerine ulaşılmasını engellemek ve var olan sistemleri kendi çıkarları yönünde manipüle etmelerinin önüne geçmektir. Ayrıca, var olan sistemler üzerinde yapılan tüm bilgi alma, bunları değiştirme, silme vs. gibi eylemlerin denetim altında yapıldığına emin olma amacı taşımaktadır (Limba, Plea, Agafonov ve Damkus, 2017: 560).

Anlatılanlara ek olarak, birçok yayında ya da çalışmalarda siber güvenlik kavramının yerine kullanılan '*bilgi güvenliği*' kavramı her ne kadar eş anlamlı olarak kullanılsa da siber güvenlik bilgi güvenliğine oranla, bilgi kaynaklarının korunmasının ötesinde birçok varlığın güvenliğini sağlamayı ifade etmektedir. Söz konusu varlıklar; bilgi, donanım, yazılım, baraj, kurum, şirket, bina, devlet ve insan diye sıralanmaktadır (Solms ve Niekerk, 2013: 99). Bunun yanında, bilgi sistemlerine kaydedilen, depolanan ve taşınan bilgilerin gizliliğinin korunması ve güvenliğinin sağlanması, bilgiye erişim hızının durumu ve kalitesinin korunması, veri bütünlüğünün sağlanması ve oluşacak zararı önleyerek işleyişinin devamlılığının sağlanması bilgi güvenliğinin amacını taşıdığı gözlemlenmektedir. Bu amaçlar siber güvenlik konusunun temelini oluşturan prensipler olarak da ele alınmaktadır (Sağıroğlu, 2011; Atalay, 2012: 43). "*CIA üçlüsü*" olarak da ifade edilen; gizlilik, bütünlük ve erişilebilirlik kavramları siber güvenliğin prensiplerini oluşturmaktadır. Bu prensipler şu şekilde açıklanmaktadır:

1. **Gizlilik:** Bilginin ya da verilerin korunması, izinsiz erişimin engellenmesini ve mahremiyetini içermektedir (Singer ve Friedman, 2018: 57).
2. **Bütünlük:** Sistemde bulunan bilgilerin yetkisiz bir şekilde değiştirilmemesini ifade etmektedir. Sözleşme yapıldığı zaman kimlik doğrulaması esnasında önem arz eden bütünlük prensibi, verilerin doğrulunun büyük öneme sahip olduğu sanayi tasarımları ve sağlık uygulamaları gibi alanlarda önemli bir nokta olarak karşımıza çıkmaktadır (Avrupa Komisyonu, 2013).
3. **Erişilebilirlik:** Yetkili kişilerin ya da gerekli izne sahip kişilerin bilgiye gereksinim duyduğu zamanda kaynaklara kesintisiz ulaşabilmesi, erişim hız ve kalitesinin korunması ve erişim kayıplarının önlenmesi olarak ifade edilmektedir (Karadağ, 2019: 34).

Yukarıda belirtilen siber güvenliğin üç prensibinin yanı sıra birde bilgi güvenliğinin prensipleri de bulunmaktadır. Bunlar şu şekildedir:

1. **İnkâr Edilemezlik:** Gönderen kullanıcının gönderdiği veriyi, alıcının ise aldığı veriyi inkâr edememe durumunu ifade etmektedir (Yılmaz ve Salcan, 2008: 86).
2. **Hesap Verilebilirlik:** Yapılan tüm eylemlerin hatta bu eylemi gerçekleştiren kişiyi dâhi takip edebilme durumu olarak açıklanmaktadır (Yeşilyurt, 2015: 170-172).
3. **Kimlik Doğrulama:** Veri gönderimi yapan kişiden, alıcının emin olmak için yapmış olduğu adımları ifade etmektedir (Karadağ, 2019: 35).

Diğer taraftan, yapılan araştırmalarda siber güvenlik ve siber savunma kavramlarının karıştırıldığı gözlemlenmektedir. Bundan dolayı son olarak siber güvenlik ve siber savunma kavramlarının birbirleriyle olan ilişkisini ele almak bu husustaki karışıklığı giderebilme noktasında faydalı olacağı düşünülmektedir. Siber savunma; *“düşmanın yapacağı ya da yapmaya çalışacağı herhangi bir saldırı durumunda bilgi ve iletişim sistemlerine yapılacak saldırı ve tehditlerin olumsuz etkilerinin önüne geçilmesi ve sistemlerin kalıcılığının sağlanması amacıyla alınması gereken önlemlerin tamamı”* olarak tanımlanmaktadır (Keleştemur, 2015: 315-316). Siber güvenlik ve siber savunma her ne kadar aralarında benzerlik taşısalar da ayrıldıkları noktalarda bulunmaktadır. Birbirlerinden ayrıldıkları bu temel noktalar; siber güvenlikte düşman saldırı yapmadan yani barış şartları içinde tedbirler alınırken

siber savunmada düşmanın saldırısı esnasında yani savaş sırasında tedbirler alınmaktadır (Cavelty, 2008: 12-13).

1.3.3. Siber Güvenlik Çalışmalarına Genel Bakış

Bilişim ve teknolojinin gelişmesiyle artan tehdit ve riskleri önlemek amacıyla ortaya çıkan siber güvenlik kavramının tüm dünyada büyük öneme sahip olduğu bilinmektedir. Böylesine önem arz eden bir durumda gerekli önlemleri almak amacıyla devletlerin her biri kendi koşulları doğrultusunda politikalar ya da stratejiler geliştirmektedir. Bununla beraber, siber güvenlik açısından güçlü ülkelere bakıldığında ABD, ÇHC, İngiltere ve Rusya gibi devletler çerçevesinde sıranın uzayıp gittiği görülmektedir. Yapılan çalışmanın asıl konusu ÇHC'nin siber güvenlik politikaları olduğundan dolayı üçüncü bölümde ÇHC'nin siber güvenlik ile ilgili yapmış olduğu çalışmalara detaylı yer verilecektir. Bu kısımda çalışmanın da sınırını oluşturan, siber güvenlik açısından güçlü olan diğer üç devletin siber güvenlik çalışmaları kısa bir şekilde analiz edilecektir. Bu devletler yukarıda da belirtildiği gibi ABD, Rusya ve İngiltere olacaktır.

ABD'nin 1990'lardan beri siber güvenlik kavramını ulusal güvenlik alanına yavaş yavaş dâhil etmeye çalıştığı görülmektedir. Bilişim teknolojilerinin gelişmesi ve internet kullanımının hızla yaygınlaşmasıyla birlikte 2000'li yılların ortalarına gelindiğinde artan ağ ve bilgisayar sistemlerinin ortaya çıkardığı güvensizlik sebebiyle ABD'nin siber güvenlik çalışmalarını hızlandırdığı belirtilmektedir (Wedermeyer, 2012: 10).

ABD'nin siber güvenlik ile ilgili yapmış olduğu çalışmalar incelendiğinde şu ana kadar ABD hükûmeti tarafından yayımlanan bir tanesi geçici olmak üzere toplam dokuz tane resmi belgenin bulunduğu görülmektedir. Yayımlanan bu belgelerin kısa bir şekilde içeriğinden bahsetmenin, ABD'nin ulusal siber güvenlik stratejilerini anlama noktasında fayda sağlayacağı düşünülmektedir. Yayımlanan belgeler sırasıyla şu şekildedir:

- Siber Uzayın Korunması ile ilgili Ulusal Strateji (2003)
- Siber Uzay Politika İncelemesi (2009)
- Siber Uzay Faaliyet Stratejisi (2011)
- Siber Güvenlik için Uluslararası Strateji: Refah, Güven ve Açıklık (2011)
- ABD Ulusal Güvenlik Stratejisi (2015)

- Siber Strateji Raporu (2015)
- Ulusal Güvenlik Stratejisi Belgesi (2017)
- Geçici Ulusal Güvenlik Stratejik Rehberliği (2021)
- Ulusal Güvenlik Stratejisi Belgesi (2022)

“*Siber Uzayın Korunması ile ilgili Ulusal Strateji*” belgesi, 2003 yılının Şubat ayında ABD hükûmeti tarafından yayımlanmaktadır. Belgenin içeriğine bakıldığında, ABD’nin kritik altyapılarının kamu ve özel kuruluşlarda; tarım, su, yiyecek, acil servisler, halkın sağlığı, savunma sanayi, hükûmet, enerji, ulaşım, bankacılık, bilgi ve telekomünikasyon, finans, kimyasallar ve zararlı maddeler, posta ve nakliyeden oluştuğu görülmektedir. Oluşturulan bu belge siber uzay sınır sistemine benzetilmektedir. Belgede bir takım stratejik hedefler oluşturulmaktadır. Bunlar; ABD’nin kritik altyapılarına yönelik saldırıların önlenmesi, siber saldırılara karşı ulusun savunmasızlığını azaltmak, karşı karşıya gelinen siber saldırının oluşturacağı zararı en aza indirmek ve kurtarmak, düzelme sürecini kısaltmak şeklinde ifade edilmektedir (United States Government, 2003: vii-viii).

Diğer yandan, belgede dikkat çeken hususun; ABD’nin kritik altyapılarının korunması amacıyla ulusal iş birliğinin sağlanması gerektiğini belirtmesi olduğu görülmektedir. Bu iş birliği hükûmet, özel sektör ve vatandaşlar arasında yapılmaktadır. Bunun yanında belgede bazı öncelikler belirlenmektedir. Bunlar ise ulusal siber güvenlik müdahale sisteminin kurulması, ulusal siber uzay güvenlik tehdidi ve güvenlik açığı azaltma programı; ulusal siber güvenlik bilinçlendirme ve eğitim programının uygulanması, hükûmetlerin siber uzayın güvenliğini sağlaması, ulusal güvenlik ve uluslararası siber güvenlik için iş birliğini sağlamak şeklinde ortaya konmaktadır (United States Government, 2003: x-xiii).

“*Siber Uzay Politika İncelemesi*” adlı belge 2009 yılında yayımlanmaktadır. Kısa ve orta vadeli eylem planlarının yer aldığı bu belgede, güvenlik ile ilgili politikaları belirleme yetkisinin Beyaz Saray’da olduğu söylenmektedir. Bunun sebebinin ise ABD’nin siber güvenlik konusundaki ciddiyeti olduğu vurgulanmaktadır (United States Government, 2009: 17).

“*Siber Uzay Faaliyet Stratejisi*” 2011 yılında yayımlanmaktadır. Yayımlanan bu strateji raporunda savunma bakanının, siber uzay görev ve sorumluluklarını ABD Stratejik Komutanlığı’na (USSTRATCOM), diğer muharip komutanlıklara ve askeri bölümlere devrettiği görülmektedir. Siber alanda daha iyi faaliyet gösterebilme ve

kaynaklarını verimli bir şekilde kullanabilme, organize etme becerisini sağlayabilme ihtiyacı göz önüne alınarak, ABD Savunma Bakanlığı USSTRATCOM'un bir alt birimi olarak Birleşik Devletler Siber Komutanlığı'nı (USCYBERCOM) kurduğu belirtilmektedir. Ulusal Güvenlik Ajansı (NSA) başkanı aynı zamanda USCYBERCOM'unda komutanlığını yapmaktadır. Diğer taraftan, söz konusu raporda yer alan savunma bakanlığının hedeflerine bakıldığında; siber alanın gücünden faydalanmak amacıyla siber alanın eğitilecek ve donatılacak aktif bir alan olarak değerlendirilmesi, savunma bakanlarının sistemlerinin ve ağlarının korunması, ABD'nin diğer hükûmet kurumları ve özel sektörlerle iş birliği içinde çalışması ve uluslararası müttefikler ile ortaklaşa siber güvenliği güçlendirmek için güçlü ilişkiler kurulması şeklinde ifade edildiği görülmektedir (U.S. Department of Defense, 2011: 5).

“Siber Güvenlik için Uluslararası Strateji: Refah, Güvenlik ve Açıklık” adlı raporun 2011 yılının Mayıs ayında yayımlandığı görülmektedir. Yayımlanan raporda; ABD, dünya genelindeki insanların ihtiyaçlarını gideren teknoloji vasıtasıyla bilgiye, düşüncelere ve birbirlerine bağlanmasına izin veren uçtan uca olacak şekilde birlikte çalışan internet ortamını desteklemektedir (United States Government, 2011: 8). ABD'nin diplomatik hedeflerinin bulunmasından ilk kez bahseden bu rapor, belirlenen hedefin uluslararası iş birlikleri oluşturarak siber alanı güvenli hâle getirmek olduğunu ifade etmektedir. Raporda, ABD'nin ulusal siber güvenliğini sağlama noktasındaki önemli hususta yer almaktadır. Rapora göre bu hususlar; ABD ordusunu siber saldırılara gücü yetecek hâle getirmek ve NATO üyesi ülkelerle iş birliği yaparak bir siber güvenlik politikası oluşturmak şeklinde açıklanmaktadır (United States Government, 2011: 21).

“ABD Ulusal Güvenlik Stratejisi” 2015 yılının Şubat ayında yayımlanmaktadır. Raporda, dönemin Başkanı Barack Obama ABD'nin karşılaştığı güvenlik tehditlerini ikiye ayırmaktadır. Birincisi, devam eden tehditler; dinci gruplar ve terörist eylemciler örnek verilmektedir. İkincisi ise, artan tehditlerdir ve bunlarda; siber güvenlik tehditleri, Rusya'nın sınır ihlali, iklim değişikliği ve hastalıklar olarak tanımlanmaktadır. ABD'nin uğrayabileceği riskler raporda kategorize edilmektedir. Bu risklerin birinci sırasında, ABD topraklarına, kritik altyapılarına gerçekleştirilecek saldırılar yer almaktadır. Diğer riskler ise şu şekilde sıralanmaktadır (United States Government, 2015: 1-2):

- ABD vatandaşlarına veya müttefiklerine karşı gerçekleştirilen saldırılar,
- Küresel ekonomik kriz veya yaygın ekonomik yavaşlama,

- Kitle imha silahlarının yayılması veya kullanımı,
- Şiddetli küresel bulaşıcı salgın hastalıklar,
- İklim değişikliği,
- Enerji piyasasındaki aksaklıklar,
- Güçsüz devletlerden dolayı karşılaşılan güvenlik tehdidi.

Yayımlanan rapor sonrasında ABD, kritik alt yapılarının güvenliğini ve özellikle siber güvenliği uluslararası güvenlik gündeminin birinci sırasına aldığı gözlemlenmektedir. Raporla, siber alana yapılacak herhangi bir tehdit durumunun sadece ABD'yi değil diğer devletleri de etkileyeceği ve bundan dolayı ortak bir çözümün gerekliliği ifade edilmektedir. Raporla değinilen bir diğer konu ise kritik altyapıya yapılacak saldırılarda ülkenin kendisini hemen toparlamayı hedeflediğini, uluslararası çerçevede hareket edeceğini ve diğer ülkelere de altyapılarından kaynaklanan tehditlere karşı yasa düzenlemelerinde yardıma bulunacağını açıklamaktadır. Bu rapor ile ilgili değinilecek olan son konu ise ABD bu rapor ile siber güvenliği ulusal güvenlik gündeminin ilk sıralarına alarak siber güvenliğin sağlanmasında kendisini dünya lideri olarak ilan ettiği görülmektedir (United States Government, 2015: 3-12).

“Siber Strateji Raporu” 17 Aralık 2015’de ABD Savunma Bakanlığı tarafından yayımlanmaktadır. Raporla belirtildiği üzere; Savunma Bakanlığı’nın ABD ulusal çıkarlarını, ayrıca diplomatik bilgi sistemlerine ait, askeri, ekonomik, hukuki, finansal, yaptırım araçlarını korumak amacıyla siber harekât düzenleyebilecek güce sahip olduğu bilgisi verilmektedir. Yayımlanan rapora göre ABD’nin beş stratejik hedefi bulunmaktadır. Bunlar şu şekilde sıralanmaktadır (The DoD Cyber Strategy, 2015: 3-26):

1. Siber alanda harekâtlar düzenleme ve harekâtları yürütmeye hazır kuvvetler kurmak,
2. Savunma Bakanlığına ait bilgi ağını ve verileri korumak,
3. ABD’yi ve çıkarlarını siber saldırılara karşı korumak,
4. Uygulanabilecek siber saldırı seçenekleri oluşturmak ve oluşturulan bu saldırıları çatışmaların arttığı durumlarda kullanmak,
5. Güçlü uluslararası ittifaklar oluşturup iş birliği içinde ortak tehditleri bertaraf etmek aynı zamanda uluslararası güvenliği ve dengeyi artırmaktır.

“*Ulusal Güvenlik Stratejisi Belgesi*” Donald J. Trump tarafından 2017 yılının Aralık ayında yayımlanmaktadır. Belgede öne çıkan ve diğer belgelerden farklı olan konular bulunmaktadır. Bunlar sırasıyla şu şekilde ortaya konmaktadır (Seren, 2018: 11-12):

- Ekonomik güvenlik, ulusal güvenliğin özünü oluşturan unsurlardan biri olarak tanımlanmaktadır. Bu durumda ÇHC’nin ekonomik yönden yapmış olduğu saldırılara dikkat çekilirken aynı zamanda adaletli ve karşılıklı ticaretin önemine vurgu yapıldığı görülmektedir.
- Rusya ve ÇHC, ABD’nin nüfuzuna, gücüne ve çıkarlarına meydan okuyan “rakip güçler” olarak tasvir edilmektedir.
- Bu belgede siber güvenlik ve göç konuları özel önem atfetmektedir.
- Barack Obama Dönemi’ndeki strateji belgelerinden ve var olan Pentagon yönetiminden farklı olarak Trump, iklim değişikliğini ulusal güvenliğe yönelik bir tehdit olarak saymamaktadır. Belgede, çevreyi korumanın öneminden bahsedilmektedir.

“*Geçici Ulusal Güvenlik Stratejik Rehberliği*” adlı belge Joe Biden hükûmeti tarafından 2021 yılının Mart ayında yayımlanmaktadır. Önümüzdeki dört yılın ana hatlarını ortaya koyan bu belge, stratejik boşlukların doldurulması amacı ile yayımlanmaktadır. Ara bir rehber olan bu belgenin yayımlanma sebebini Biden rehberin ön sözünde; “Amerika’nın dünyayla nasıl ilişki kuracağına dair vizyonumu iletmek için yayımlıyorum” ifadesiyle açıklamaktadır. Kapsamlı bir ulusal güvenlik stratejisi üzerinde çalışılmaya devam edilirken, Biden vakit kaybetmemek ve yeni dönem stratejisine uyum sağlamak adına, oluşacak keskin dönüşler karşısında kurumların şaşkınlığını ve aksaklık yaşamasını gidermek adına geçici bir stratejik belgenin yayımlanmasını gerekli görmektedir. Rehberde belirlenen hedefler şu şekilde sıralanmaktadır (Tavukçu, 2021):

- Ekonomiyi geliştirmek,
- Orduyu modern hâle getirmek,
- ABD’nin uluslararası kurumlardaki yerini geri almak,
- ABD’nin ortaklıklarını ve ittifak ağını yeniden canlandırmak.

Belgeye genel olarak bakıldığında; Covid-19 salgını, küresel iklim değişikliği, siber ve dijital tehditler, uluslararası ekonomik bozulmalar, insani krizler, ABD’ye rakip olan ÇHC ve Rusya gibi güçlerin yükselişi, yükselen milliyetçilik, teknolojik

değişimler, kitlesel silahların yayılması gibi konulara vurgu yapıldığı görülmektedir. Ayrıca, güvenlik kavramı kapsamlı olarak değerlendirilmektedir. Ekonomi güvenliğinden, çevre güvenliğine ve sağlık güvenliğinden, siber güvenliğe kadar birçok güvenlik alanına yer verilmektedir. Son olarak üzerinde durulan bir diğer önemli hususun ise uluslararası güç değişiminin farkındalığına vurgu yapılması olduğu görülmektedir. ABD'nin Rusya ve ÇHC gibi güçlü devletlerin yer aldığı rekabet ortamında özellikle askeri güçlerini ve nükleer kapasitelerini ve yeteneklerini yenilemesi, modernize edilmesinden bahsedilmektedir (Dingil, 2021).

Son olarak ele alınacak belge ise “*Ulusal Güvenlik Stratejisi Belgesi*” olarak karşımıza çıkmaktadır. ABD’de 2021 yılında geçici olarak çıkarılan Ulusal Güvenlik Stratejik Rehberliği belgesinden sonra 2022 yılının Ekim ayında Joe Biden tarafından yayımlanmaktadır. Yayımlanan bu belgeye göre ABD’nin küresel güç mücadelesindeki temel rakibinin ÇHC olduğu belirtilmektedir. Bununla beraber belgenin geneline bakıldığında; ABD’nin dış politika geleceği konusunda yapılacak olan ön görüşlerde önemli ipuçlarını barındırdığı gözlemlenmektedir. Bu çerçevede belge, ABD’nin küresel güç mücadelesinde rakip olarak gördüğü ÇHC ile ilişkilerinin ve mücadelelerinin nasıl şekil alacağını anlaşılabilmesi noktasında oldukça önem arz etmektedir (Başaran, 2022).

Genel olarak belgede temel noktanın ÇHC olduğu görülmektedir. ABD söz konusu belgede, ÇHC’yi Rusya ile beraber sınırlandırılması gereken aktör olarak tanımlamaktadır. Aynı zamanda belgede Pekin’in eylemlerine geniş olarak yer verilmektedir. ÇHC’yi otokratik rejimler arasında gören belge, Pekin yönetiminin yapmış olduğu eylemlerin uluslararası sistemde tehdit oluşturduğunu öne sürerek, Pekin’i revizyonist bir dış politika takip etmekle suçlamaktadır (National Security Strategy, 2022: 3-8).

Öte yandan yukarıda da belirtildiği üzere siber güvenlik çalışmaları açısından en güçlü devletler arasında yer alan bir diğer devletin Rusya olduğu bilinmektedir. Rusya, 2000’li yıllardan itibaren, siber uzayda etkisini göstermek amacıyla farklı plan ve stratejiler geliştirmektedir. Bu doğrultuda, 1979 ve 1989 yıllarında ortaya çıkan Afganistan Savaşı sırasında, SSCB Ordusu’nun psikolojik savaş yöntemlerini kullanamadığı görülmektedir. Ayrıca Moskova Başkanlığı’nın Afganistan’daki irtibatları ile etkili bir iletişim ve haberleşme sağlayamadığı belirtilmektedir. Bununla birlikte, 1994 ve 1996 yıllarında Çeçen Savaşı sürecinde de internet aracılığıyla yapılan

iletişim ve haberleşmenin başarısız olmasından dolayı savaş esnasında gelişmelerin Rusya perspektifinden bakıldığında oldukça olumsuz bir hâl aldığı görülmektedir. Yaşanan bu iki olumsuz gelişme sonrasında, Rus hükûmeti siber güvenlik, askeri bilişim ve ağ teknolojilerini hızla geliştirmeye başlamaktadır (Darıcılı, 2017: 420).

Rusya'nın siber güvenlik alanı ile ilgili yapmış olduğu çalışmalara genel olarak bakıldığında şu ana kadar uluslararası kamuoyuyla paylaştığı sekiz resmi belgenin olduğu görülmektedir. Bunlar şu şekilde sıralanmaktadır:

- Rusya Federasyonu Ulusal Güvenlik Konsepti (2000)
- Rusya Federasyonu'nun Bilgi Güvenliği Doktrini (2000)
- Askeri Doktrini (2010)
- Rusya Federasyonu'nun Silahlı Kuvvetleri'nin Bilgi Alanındaki Aktiviteleri Hakkında Kavramsal Görüşler Belgesi (2011)
- Rusya Federasyonu'nun 2020'ye Kadar Sürecek Uluslararası Bilgi Alanındaki Devlet Politikasının İlkeleri Belgesi (2013)
- Rusya Federasyonu'nun Siber Güvenlik Stratejisi (2014)
- Rusya Federasyonu'nun Bilgi Güvenliği Doktrini (2016)
- Rusya Ulusal Güvenlik Stratejisi (2021)

“*Rusya Federasyonu Ulusal Güvenlik Konsepti*” adlı belge 2000 yılının Ocak ayında yürürlüğe girdiği bilinmektedir. Genel olarak bakıldığında belgede; bilişim ve teknoloji güvenliğinin önemine değinilmektedir. Aynı zamanda bu konuda devlet çıkarları doğrultusunda gelişecek herhangi bir tehdide karşı alınacak önlemlerde belgede yer almaktadır (Darıcılı, 2017: 420).

“*Rusya Federasyonu'nun Bilgi Güvenliği Doktrini*” adlı belge 2000 yılının Eylül ayında Rusya'da siber güç olma yönündeki ilk belge olarak yayımlanmaktadır. Belgenin temelini; Rusya Federasyonu'nun bilgi güvenliği alanında devlet politikasının oluşturulması, ülkenin bilgi güvenliğinin yasal, bilimsel, teknik ve örgütsel desteğini geliştirmek maksadıyla öneriler hazırlanması, ülkenin bilgi güvenliğini sağlamak amacıyla belirlenen programların geliştirilmesi, tasarlanması gibi hedefler oluşturmaktadır. Doktrinde dikkat çeken noktalar şu şekilde sıralanmaktadır (Information Security Doctrine Of The Russian Federation, 2000):

1. Ulusal bilişim ve teknoloji ağlarının gelişimini sağlayacak yazılım ve donanımların üretilmesi,
2. Ülkenin menfaatine hizmet etmek için küresel ağlara bağlanması,

3. Ülkenin küresel bilgi toplumuna diğer ülkelerle eşit şartlar altında dâhil olması.

“*Askeri Doktrini*” belgesinin 2010 yılında yayımlandığı belirtilmektedir. Savaşın yeni alanı olan siber uzayın gündemde yerini yoğun şekilde almasıyla beraber, askeri AR-GE çalışmalarına ağırlık veren Rusya bu doktrini yayımlamaktadır. Doktrin, ulusal çıkar ve müttefiklerin çıkarlarını korumak maksadıyla siyasi ve bilgilendirici araçların kullanımını tartışmaktadır. Bu belge; askeri ve askeri olmayan güç ve yeteneklerinin modern askeri çatışmalar içerisinde kullanılması ile bilgi savaşının yaşanan bu çatışmalar içerisindeki rolünü tanımlamaktadır. Bununla beraber, yaşanacak olası bir savaş durumunda siber uzaydan gelebilecek olan tehditlere karşı ordunun hazırlık seviyelerini artırmak maksadıyla Rusya Silahlı Kuvvetleri içerisinde siber birliklerin kurulması fikri bu doktrin ile hız kazanmaktadır. Bununla birlikte, Rusya ulusal çıkar ve gayelerini gerçekleştirmek maksadıyla ileri ve karmaşık siber saldırı yöntemleri kullanmaktadır (European Parliamentary Research Service, 2014: 5).

“*Rusya Federasyonu’nun Silahlı Kuvvetleri’nin Bilgi Alanındaki Aktiviteleri Hakkında Kavramsal Görüşler*” adlı belge 2011 yılında yayımlanmaktadır. Bilgi alanında yaşanan gelişmeler bu alanda yetişmiş askeri personellere olan ihtiyacı artırmaktadır. Bundan dolayı bu belgede, askeri yeniliklerin yapılması gerektiğine yer verilmektedir. Herhangi bir çatışma ve krize karşı hazır olunması gerektiği vurgulanan belgede aynı zamanda silahlı kuvvetlerin dost devletler ve uluslararası kuruluşlarla birlik içinde olunması gerektiğini desteklediği, bilgi alanında uluslararası ortamda telafi edilemeyecek olaylara sebep olunacak davranışlardan uzak durulması gerektiği gibi ayrıntılara da yer verilmektedir. Ayrıca uluslararası bilgi paylaşımına önem veren uzlaşmacı bir tavır sergilendiği de gözlemlenmektedir (Ministry of Defense of The Russian Federation, 2011).

“*Rusya Federasyonu’nun 2020’ye Kadar Sürecek Uluslararası Bilgi Alanındaki Devlet Politikasının İlkeleri*” adlı stratejik planlama belgesinin 2013 yılının Şubat ayında yayımlandığı belirtilmektedir. Rusya Federasyonu’nun 2020 yılına kadar sürecek olan bu belgesinde belirtilen hedef ve gayelerine bakılacak olursa; uluslararası bilgi güvenliği sisteminin kurulması amacıyla uluslararası yasal rejimin kurulmasını özendirmek ve uluslararası bilgi güvenliği sistemini ikili, çoklu, bölgesel ve küresel düzeylerde kurmak olduğu ifade edilmektedir. Belirlenen hedeflerle beraber Rusya’nın öncelikleri arasında dikkat çeken hususun; bilişim teknolojilerinin hükûmetlerin

egemenliğini ve toprak bütünlüğünü, uluslararası barışı, güvenliği ve stratejik dengeyi tehdit etmek maksadıyla kullanılması riskini azaltmak olduğu görülmektedir. Belgeye bakıldığında dikkat çeken bir diğer hususta ise bilişim teknolojilerinin hükûmetlerin işlerine karışmak gibi aşırı uç gayelerle kullanılmasını engellemeyi hedeflediğini belirterek bilişim teknolojilerinin kullanılması ile ilgili hükûmetlerin teknolojik egemenliğe sahip olmalarının ve geliştirmekte olan ülkelerle gelişmiş ülkeler arasındaki bilgi eksikliğinin idame ettirilmesi gerekliliğinin altı çizilmektedir (Russian Federation, 2013).

Öte yandan, Rusya Federasyonu iletişim teknolojilerinin teröristler tarafından kullanılmasına karşın uluslararası iş birliği mekanizmaları kurulması gerektiğini savunmaktadır. Bundan dolayı, devlet politikalarını uygulamak maksadıyla federal otoriteler arasında uyumu sağlama görevi ile devletin bilişim teknolojileri hususundaki tavrını uluslararası alanda destekleme görevini Dış İşleri Bakanlığı'na devrettiği belirtilmektedir. Rusya'nın siber suçla savaşta iş birliği içinde olacağı ülke veya kuruluşlar; BM, ŞİÖ Üye Ülkeleri, Kolektif Güvenlik Anlaşması Örgütü (KGAÖ) Üye Ülkeleri, Bağımsız Devletler Topluluğu ve BRICS¹ üyeleri şeklinde sıralanmaktadır. Belgede belirlenen bilgi güvenliği hususundaki iş birliği yapılacak olan ülkeler ve uluslararası kuruluşlar ise; ŞİÖ, KGAÖ, Bağımsız Devletler Topluluğu, BRICS üyeleri, G-8 ve G-20 ülkeleri, Asya Pasifik Ekonomik İşbirliği Örgütü (APEC) ve uluslararası kuruluşlar şeklinde açıklanmaktadır (Russian Federation, 2013). Söz konusu belgede dikkat çeken bir diğer hususun ise internetin bilgi ve telekomünikasyon yönetiminin uluslararası boyuta gelmesi ve Uluslararası Telekomünikasyon Birliği'nin bu husustaki rolünün artırılması amacıyla uluslararası alanda ilerlemelerin olmasına önem verilmesi olduğu görülmektedir (Russian Federation, 2013).

“Rusya Federasyonu’nun Siber Güvenlik Stratejisi” adlı belge yaşanan tüm bu gelişmeler sonrasında 2014 yılında yayımlanmaktadır. Yukarıda açıklanan diğer belgelerin odağında bilgi güvenliği varken, bu belgenin odağını siber güvenlik stratejileri oluşturmaktadır (Federation Council of The Federal Assembly of The Russian Federation, 2014). Söz konusu belge, Rusya Cumhurbaşkanı Vladimir Putin tarafından 2013 yılında imzalanıp, 2020'ye kadar sürecek olan “Uluslararası Bilgi

¹ BRICS: Brezilya, Rusya, Hindistan, Çin ve Güney Afrika ülkelerinin İngilizce isimlerinin baş harflerinden meydana gelmektedir. (Brasil, Russia, India, China, South Africa).

Güvenliği Alanında Rusya Federasyonu Devlet Politikasının İlkeleri” belgesinde belirtilen ilke ve eylem planının bir parçası olarak ortaya konmaktadır. Ayrıca belge; Rus Güvenlik Konseyi, Savunma Bakanlığı, Dışişleri Bakanlığı, Adalet Bakanlığı ve İletişim Bakanlığı tarafından ortaklaşa imzalanmaktadır (Alioğlu, 2019: 183).

Belgede kavramları netleştirmek ve stratejinin daha anlaşılır olmasını sağlamak adına bazı kavramların açıklaması yapılmaktadır. Bu kavramlar; bilgi alanı, siber uzay, bilgi güvenliği ve siber güvenlik olarak ele alınmaktadır. Genel olarak bakıldığında, Rusya Federasyonu’nun yayımlamış olduğu diğer belgelerde siber güvenlik kavramı ile bilgi güvenliği kavramının birbirlerinin yerine kullanıldığından bahsedilmektedir. Bu belgede siber uzay kavramı “bilgi alanının bir unsuru olarak düşünülmelidir ve açıkça tanımlanmış sınırlara sahiptir” şeklinde ifade edilmektedir. Bilgi uzayı kavramı; “bilginin yaratıldığı, dönüştürüldüğü, iletildiği, kullanıldığı, depolandığı bireysel ve toplumsal bilinci, bilgi altyapısını ve bilginin kendisini etkileyen bir alan” olarak açıklanmaktadır. Bilgi güvenliği kavramının tanımı ise “bilgi uzayının zararlı ve yıkıcı etkilerinden bireyin mahremiyetinin, kurumların ve devletin korunmasıdır” şeklinde yapılmaktadır. Yapılan tanımlar bağlamında siber alan internet ve telekomünikasyon kanalları, teknolojik altyapı ve diğer kurumsal, özel, devlet kanallarından ortaya çıkan eylem alanı, siber güvenlikte siber alanın istenmeyen sonuçlardan en üst seviyede korunması amacıyla gerekli şartların oluşturulması anlamlarına gelmektedir (Federation Council of The Federal Assembly of The Russian Federation, 2014).

Belgeye göre Rusya’nın stratejik öncelikleri bulunmaktadır. Bu öncelikler şu şekilde belirtilmektedir (Federation Council of The Federal Assembly of The Russian Federation, 2014):

- Karşılaşılabilecek siber tehlikelere karşı özel bir ulusal savunma sistemi geliştirmek,
- Kritik bilgi altyapısının güvenilirliğini düzenli bir şekilde sağlayacak sistemler geliştirmek,
- Siber güvenlikle ilgili birey, hükûmet ve özel sektör arasında olan ortaklığa güç kazandırmak,
- Vatandaşların dijital okuryazarlığa sahip olmasını sağlamak,
- Uluslararası iş birliğini desteklemek.

Bunlarla beraber, yayımlanan bu strateji belgesi ile siber güvenlik hususunda devlet birimlerinin, işletmelerin ve halkın eşit konumda değerlendirileceği bir ortam

kurmak hedeflenmektedir. Bu hedef dışında belgede birtakım hedeflerinde belirlendiği görülmektedir. Söz konusu bu hedefler; kamu zihniyetindeki vatansever ve ahlaki ilkeleri güçlendirmek, Rus toplumunun çok uluslu yapısını korumak, forumlar, seminerler ve siber güvenlik sorunlarına odaklanmış kamuoyuna açık internet portalı açmak, eğitim sisteminin kültürel ve insani boyutunu geliştirmek şeklinde belirtilmektedir (Federation Council Of The Federal Assembly Of The Russian Federation, 2014).

“Rusya Federasyonu’nun Bilgi Güvenliği Doktrini” adlı belge ilk olarak 2000 yılında yayımlandıktan tam 16 yıl sonra 2016 yılının Aralık ayında bu doktrinin yenilenerek yeniden yayımlandığı görülmektedir. 2000’li yıllarda yayımlanan ilk doktrinde internetin o dönemlerde henüz yeni olmasından dolayı internetten bahsedilmediği dikkat çekmektedir. Fakat sonrasında yayımlanan ikinci doktrinin o dönemin şartlarına daha uygun ve güncel olmasından dolayı önceki strateji belgesinde belirlenen hükümlerin birçoğu geliştirilerek güncellenmiş olmasına rağmen ilk doktrin ile benzer yaklaşım öngörülmektedir (Alioğlu, 2019: 185).

Diğer yandan ise söz konusu belgenin bilgi güvenliği hususlarını üç aşamada ele aldığı görülmektedir. Bu aşamalar; bireysel, toplumsal ve devlet olarak sıralanmaktadır. 2000 yılında yayımlanan ilk doktrinde bireysel çıkarların öncelikler arasında olduğu belirtilmektedir. Fakat bu doktrinde önceliğin, bilgi alanında ulusal çıkarlar olduğu görülmektedir. Bundan dolayı, bilgi alanında Rus vatandaşlarının ulusal çıkarlarının korunması amacıyla mevcut yaklaşımlar güncellenmektedir. Belgede belirtilen ulusal çıkarlar şu şekilde ortaya konmaktadır (Russian Federation, 2016):

- Halkın anayasal hak ve özgürlüklerinin korunması,
- Sivil toplumun etkileşim içinde bulunduğu mekanizmalarını, demokratik kurumları ve devletini desteklemek,
- Rusya’da bulunan çok ırklı halkın tarihi, kültürel, manevi ve ahlaki değerlerinin korunması amacıyla bilgi teknolojilerini uygulamak,
- Yaşanacak herhangi bir saldırganlık durumu ya da yabancı eylemlere karşılık olarak barış ve savaş zamanında kritik bilgi altyapısının sürdürülebilir ve sekteye uğramadan işlemlerini sağlamak,
- Rusya’da bilgi teknolojileri ve elektronik sektörünü geliştirerek üretim, araştırma ve bilişim teknolojik topluluğun performansını iyileştirmek,

- Siber savunma ve siber güvenlik alanlarında ulusal ve uluslararası politikalar geliştirmek,
- Uluslararası siber güvenliği teşvik etmek.

Öte yandan belgenin kapsamını ele alacak olursak; askeri siber kabiliyetlerin kullanılarak geleneksel tehditlerin caydırılabileceğinin vurgusu yapıldığı görülmüyor. Aynı zamanda bu alanlarda siber güvenliğin sağlanabilmesi için iş birliğinin önemi vurgulanmaktadır. Belge de vurgulanan bir diğer hususun ise yönetimin güçlendirilerek bilginin merkezileştirilmesi olduğu ifade edilmektedir. Bu kapsamda bakıldığında, belge ile Rusya Federasyonu'nun karşılaştığı düşmanca bir ortamda uzun vadeli çatışma ortamını hazırlamak amacıyla savunma maksatlı ve saldırgan bir siber kabiliyet geliştirdiği açıklanmaktadır. Son olarak, siber güvenlik, gizlilik ve bilgi güvenliği konularının Rusya Federasyonu'nun milli çıkarları için oldukça önem taşıdığı vurgusunun yapılması bir diğer hususu oluşturmaktadır. Bunların korunması amacıyla kamu politikaları ile halkla ilişkilerin yanında birde bilgi güvenliğini artırmak için sistemlerin oluşturulması gerektiği savunulmaktadır (Russian Federation, 2016).

“Rusya Ulusal Güvenlik Stratejisi” adlı belgenin 2021 yılının Temmuz ayında Rusya Devlet Başkanı Vladimir Putin tarafından onaylandığı belirtilmektedir. Putin'in imzalamış olduğu başkanlık kararnamesi, Rusya Ulusal Stratejisi'nin 2015 yılında kabul edilen belge ile uyarlanan ve kapsamlı değişikliklerin yapıldığı bu yeni belgenin bir an önce yürürlüğe girmesini şart koşmaktadır. Sonrasında yürürlüğe giren belgenin önceliğinin, modern tehditlerle mücadelenin yanı sıra ÇHC ve Hindistan ile ittifakın güçlenmesi olması dikkati çekmektedir (Ceber, 2021). Oluşturulan bu stratejinin uygulanmasının, Rusya halkını korumaya, vatandaşların yaşam kalitesini iyileştirmeye, insan kabiliyetlerini geliştirmeye, ülkede savunma potansiyelinin artırılmasına, vatandaşlarının birlik ve uyumuna katkıda bulunmaya, ulusal kalkınma hedeflerine ulaşılmasına ve Rusya'nın rekabet potansiyelinin ve uluslararası alanda konumunun güçlendirilmesine yönelik olduğu vurgusu yapılmaktadır (Alpar, 2021).

Bir başka yönden ise söz konusu belgede siber güvenlik konusuna değinilecek olursa; bazı devletlerin, Rusya Federasyonu'nun iç işlerine karışmak maksadıyla bilişim teknolojilerini kullanması ve Rusya'ya yapılan siber saldırıların sayısında ciddi artışın olmasından dolayı Rusya'nın stratejik ulusal öncelikleri listesinde siber güvenliğin yerini aldığı belirtilmektedir (Ceber, 2021). Kısacası, 2021 yılında uygulamaya konulan belge, Rusya'nın karşı karşıya kaldığı tehditleri ortaya koymaktadır. Bundan dolayı bu

duruma karşı alınabilecek tedbirleri de içermektedir. Belgede ABD'nin, ekonomik ve askeri tehdit olarak görüldüğü açık bir şekilde ifade edilmektedir. Bundan dolayı, ABD'nin Asya-Pasifik bölgesindeki düşmanca göstermiş olduğu faaliyetleri karşısında, ÇHC ve Hindistan ile dostluğun geliştirilmesi gerektiği savunulmaktadır (Alpar, 2021).

Siber güvenlik alanında yapılan çalışmalara bakıldığında güçlü olan bir diğer devletin ise İngiltere olduğu görülmektedir. İngiltere'nin siber güvenlik ile ilgili birçok stratejik belge yayımladığı görülmektedir. Yayımlanan strateji belgeleri ise şu şekilde sıralanmaktadır:

- Birleşik Krallık Siber Güvenlik Stratejisi; Siber Uzayda Emniyet, Güvenlik ve Dayanıklılık Belgesi (2009)
- Ulusal Siber Güvenlik Stratejisi (2009)
- Siber Suç Stratejisi (2010)
- Belirsizlik Çağında Güçlü Bir İngiltere: Ulusal Güvenlik Stratejisi (2010)
- Birleşik Krallık Siber Güvenlik Stratejisi: Dijitalleşen Dünya'ya Birleşik Krallığı Taşımak ve Korumak (2011-2016)
- Ulusal Siber Güvenlik Stratejisi (2016-2021)
- Rekabetçi Bir Çağda Küresel Britanya: Güvenlik, Savunma, Kalkınma ve Dış Politikanın Entegre Gözden Geçirilmesi (2021)

“Birleşik Krallık Siber Güvenlik Stratejisi; Siber Uzayda Emniyet, Güvenlik ve Dayanıklılık” adlı belge, ilk siber güvenlik stratejisi olma özelliği taşımaktadır. 2009 yılının Haziran ayında Kraliçe'nin emriyle yayımlanan belge, İngiltere'nin siber uzaydaki politikalarını diğer güvenlik politikalarından ayırmaktadır. Belgede, siber uzaydaki tehditlerin yanında, söz konusu alanın getirmiş olduğu fırsatların İngiltere tarafından nasıl değerlendirildiğine dair bir çerçeve sunulmaktadır (Eren, 2020: 125). Bununla birlikte yayımlanan strateji belgesinin, suç örgütleri ve düşman ülkelere karşı oluşturulan savunma planlarını içerdiği tespit edilmektedir. Akabinde belge ile şirketler, devlet ve bireylerin karşılaştıkları siber saldırı durumunda risk altında oldukları açıklanmış olup, bu siber güvenlik stratejisi ile daha detaylı ve geniş olarak hazırlanan *“Ulusal Siber Güvenlik Stratejisi”* belgesinin beraber yayımlandığı görülmektedir (Alioğlu, 2019: 106).

Söz konusu belgede genel olarak; İngiltere'nin siber uzaydaki avantajını güvence altına almak maksadıyla bilgi, yetenek ve karar verme süreçlerini geliştirerek siber uzay kullanımından kaynaklanan riski azaltma ve fırsatları kullanma ile ülkenin

belirlemiş olduğu stratejik hedeflere ulaşmak için devletler, tüm sektörde var olan kuruluşlar, uluslararası ortaklar ve kamuoyunun iş birliği içinde çalışması gerektiği vurgulanmaktadır. Aynı zamanda tüm kesimlerin karşılaşabileceği dolandırıcılığın her türlü ile kimlik hırsızlığı ve teknoloji aracılığıyla işlenebilen siber suçlara karşı korunmanın nasıl sağlanacağı açıklanmaktadır (Cyber Security Strategy of the United Kingdom, 2009). 2009 yılının Haziran ayında, stratejik liderliği sağlamak ve Birleşik Krallık Siber Güvenlik Stratejisi'ni geliştirmek ve kontrol edebilmek amacıyla “Siber Güvenlik Ofisi” kurulduğu belirtilmektedir (Arslan, 2021: 57).

2010 yılının Mart ayına gelindiğinde İngiltere'nin “*Siber Suç Stratejisi*” adlı belgeyi yayımladığı görülmektedir. Haziran 2009 yılında yayımlanan ilk siber güvenlik strateji belgesinin üzerinden bir yıl geçmeden alınan kararlar sonuçlarını göstermektedir. Siber Suç Stratejisi adlı belgeye genel olarak bakıldığında; siber suçların tanımının yapıldığı, siber suçun niteliği ve çevrimiçi suçu yapan eylemcilerin hakkında bilgiler verildiği görülmektedir. Bunun yanında bazı konular için stratejiler oluşturulduğu tespit edilmektedir. Bu konular; finansal suçlar ve beraberinde çocuklara karşı gerçekleştirilen tehditler, taciz ve siyasi aşırılık, nefret suçları, halka karşı yapılan tehditler, çevrimiçi dolandırıcılık, mali suç, terörizm, kimlik hırsızlığı ve çocukların korunması şeklinde sıralanmaktadır. Aynı zamanda ulusal ve uluslararası ortaklık konuları ve yaptırımlara yönelik stratejiler de bu belgede yer almaktadır (Cyber Crime Strategy, 2010).

“*Belirsizlik Çağında Güçlü Bir İngiltere: Ulusal Güvenlik Stratejisi*” adlı belge 2010 yılının Kasım ayında İngiliz hükûmeti tarafından yayımlanmaktadır. Bu belge ile beraber siber güvenliğin sağlanabilmesi noktasında ortaya konan konuların, ülkenin ulusal güvenlik sorunlarından biri olarak sayıldığı görülmektedir. İngiltere siber güvenliği, ciddi ve öncelikli ulusal risklerden biri olarak görmektedir. Siber uzayda gerçekleştirilen eylemler, casusluk ve suç aracı olarak geliştirildiğinden, hükûmetler ve başkaları tarafından kullanılmak üzere bir askeri silah olarak büyüme göstermeye devam edeceğinden dolayı direk ulusal güvenlik ve ekonomik tehdit olarak gelişme göstereceğinin vurgusu yapılmaktadır (The National Security Strategy, 2010).

“*Birleşik Krallık Siber Güvenlik Stratejisi: Dijitalleşen Dünya'ya Birleşik Krallığı Taşımak ve Korumak*” adlı belge 2011 yılının Kasım ayında yayımlanmaktadır. Yayımlanan bu belgede Ulusal Siber Güvenlik Programı ve detaylarına yer verilmektedir (The UK Cyber Security Strategy, 2011). Siber güvenlik alanında köklü

değişikliklerin yapıldığı ve bu alanda birçok yeni kurumun oluşturulması maksadıyla çalışmaların başlatıldığı Ulusal Siber Güvenlik Programı'na 650 milyon pound bütçenin ayrıldığı söylenmektedir. Ayrılan bu bütçenin %59'u İngiltere'nin üç istihbarat ve güvenlik kuruluşu olan M16, M15 ve GCHQ para sağlayan fona, %14'ünü ise Savunma Bakanlığı'na ayırdığı açıklanmaktadır (Kınıkoğlu, 2012: 30). Öte yandan, söz konusu strateji belgesi ile daha dayanıklı ve güvenilir dijital bir ortam oluşturularak İngiltere'nin ekonomik refahının nasıl destekleneceği, ulusal güvenliğin nasıl korunacağı ve vatandaşın yaşam biçiminin nasıl korunacağı gibi konular üzerinde durulmaktadır. Aynı zamanda bu belge ile devlet içindeki kurumsallaşma ve strateji belgelerinin temelleri sağlamlaştırılmaktadır. Köklü değişimleri beraberinde getiren bu belge ile birlikte, İngiltere'nin siber güvenlik stratejisinde beş yıllık bir dönemde gerçekleşecek faaliyetler belirlenmektedir (Eren, 2020: 127). Bunun yanında, 2016 yılının Nisan ayında ise "Birleşik Krallık Siber Güvenlik Stratejisi 2011-2016: Yıllık Raporu" yayımlandığı da bildirilmektedir.

2011-2016 belgesi temelde üç bölümden oluşmaktadır. Bu bölümler şu şekilde açıklanmaktadır (The UK Cyber Security Strategy, 2011):

- **Birinci bölüm:** Bu bölümde, ağa bağlı olan dünyanın büyümesinde etkisi bulunan arka planın ve internetin sunduğu önemli sosyal ve ekonomik yararlardan söz edilmektedir. Aynı zamanda siber uzaya olan bağımlılığın artması durumunda yalnızca yeni fırsatlar değil, yeni tehditleri de beraberinde getirdiği belirtilmektedir. Yaşanan gelişmeler ile beraber siber uzay açık pazarları ve açık toplumları teşvik ederken bu açıklığın İngiltere'yi ciddi veri ve sistemlerinden taviz vererek ya da hasar vererek ülkeye zarar vermek isteyen suçlulara, bilgisayar korsanlarına ve yabancı istihbarat servislerine karşı daha güçsüz bırakabileceği vurgulanmaktadır.
- **İkinci bölüm:** Birinci bölümde bahsedilen tehditler bu bölümde açıklanmaktadır. Hissedilen etkilerin siber uzaya bağımlılığın artmasıyla daha da büyüyeceği belirtilmektedir. Artık günlük hayatta kullanılan ağların örgütsel ve ulusal sınırları aştığı görülmektedir. Bundan dolayı siber uzayda gerçekleşen olayların, geleneksel tepkileri geride bırakarak ciddi bir hızda meydana gelebileceğine değinilmektedir.
- **Üçüncü bölüm:** Bu bölümde ise devletin 2015'te İngiltere siber güvenliği vizyonu ile nereye ulaşmak istediğini ortaya koymaktadır.

2016 yılının Nisan ayında “Birleşik Krallık Siber Güvenlik Stratejisi 2011-2016: Yıllık Raporu” yayımlandığı bildirilmektedir. Belgenin hedeflerine bakıldığında, dört hedefin ortaya konduğu görülmektedir. Bu hedefler şu şekilde açıklanmaktadır (The UK Cyber Security Strategy 2011-2016 Annual Report, 2016:5):

- Siber suçlarla mücadele etmek ve ülkeyi siber alanda iş yapmak amacıyla dünyanın en güvenli yerlerinden biri hâline getirmek.
- Siber saldırı durumunda daha dayanıklı olmak ve siber alandaki menfaatlerini daha iyi koruyabilmek.
- Vatandaşın güven içinde kullanabileceği ve toplumları destekleyen açık, canlı ve istikrarlı bir siber alanın biçimlenmesine yardımcı olmak.
- Alınacak tüm siber güvenlik hedeflerini desteklemesi amacıyla ihtiyaç duyulan beceri ve kabiliyete sahip olmak.

Bununla beraber, 2011-2016 yılları arasında İngiltere bu programın geliştirilmesi amacıyla 860 milyon £ fonlama yaptığı belirtilmektedir (The UK Cyber Security Strategy 2011-2016 Annual Report, 2016:5).

“Ulusal Siber Güvenlik Stratejisi 2016-2021” adlı belgenin 2016 yılının Kasım ayında yayımlanmaktadır. Hükûmetin İngiltere’yi siber uzayda güvenli ve dayanıklı hâle getirme planının ortaya konulduğu ve 1,9 milyar sterlinlik dönüşümsel yatırımla desteklenen bu belgede, 2021 yılı için İngiltere’nin vizyonunun; karşılaşılan siber tehditlere karşı güvenilir olmak, saldırı sonrası çabuk toparlanmak ve sağlam durmak olduğu açıklanmaktadır. Belirtilen bu vizyonun gerçekleşebilmesi için caydırma, savunma ve gelişme konularına odaklanılması gerektiği vurgulanmaktadır. Odak olarak belirlenen bu konularda; vatandaşların, çalışanların ve kamu sektörünün kendilerini savunma potansiyellerine sahip olmaları gerektiğinden, ülkenin saldırganlar için zor bir hedef hâline geleceğinden ve saldırganlara gözdağı verip korkutarak geri adım atacaklarından söz edilmektedir. Bunun yanında belgede, İngiltere’nin dünyada büyük yere sahip olan bilimsel araştırma ve geliştirme kuruluşlarınca desteklenen, yenilikçi ve büyüyen bir siber güvenlik endüstrisine sahip olduğu savunulmaktadır (National Cyber Security Strategy 2016-2021, 2016).

Diğer yandan, İngiltere’nin siber güvenlik alanında yaptığı çalışmalarla kurumsallaşma yoluna gittiğinin en önemli örneği olarak ‘Ulusal Siber Güvenlik Merkezi’nin açılması gösterilmektedir. 14 Şubat 2017 yılında II. Elizabeth’in katılımıyla açılan ve ana binası Londra’da bulunan merkezin, İngiltere’nin siber

saldırılarına karşı savunma üssü olacağı belirtilmektedir (Corera, 2017). Kasım 2016'da yayımlanan strateji belgesinin odağında yer alan geliştirme eylemleri kapsamında İngiliz hükûmeti'nin 2020 yılına gelindiğinde belgenin yayımlandığı süreçten belirtilen süreye kadar gelineen süreçte, siber güvenlik teknolojilerini geliştirmek adına yaklaşık 10 milyon sterlin hibe ettiği görülmektedir (Siber Bülten, 2020).

“Rekabetçi Bir Çağda Küresel Britanya: Güvenlik, Savunma, Kalkınma ve Dış Politikanın Entegre Gözden Geçirilmesi” adlı belge 2021 yılının Mart ayında yayımlanmaktadır. Söz konusu belge son yıllarda yayımlanan en kapsamlı dış politika ve ulusal güvenlik revizyonunu içermektedir. Bu doğrultuda belgede, İngiltere'nin kötüleşen küresel güvenlik ortamına karşı daha dayanıklı bir duruş sergileyeceği ve bu alanda silahlı kuvvetlerini 20 yıl içinde bugüne kadarki en kapsamlı modernizasyondan geçeceği belirtilmektedir (Esen, 2021). Yayımlanan bu belgeyle beraber, İngiltere'nin artık daha fazla risk ve tehdit altında olduğu ve yeni bir güç yapılanmasını yürürlüğe sokacağı ve bundan dolayı hem İngiliz İstihbaratı hem de İngiliz Ordusu'nun önümüzdeki 30 yıl içinde çok boyutlu ve multidisipliner bir şekilde yeniden düzenlemeye geçirileceği görülmektedir (Şen, 2021).

Bunlara ek olarak belgede, İngiltere'nin yeni teknolojilerin geliştirilmesine öncelik verileceği söylenmektedir. Aynı zamanda geleneksel ve pahalı askeri donanımdan uzaklaşacağını belirten belgede bununla ilgili olarak, “yüksek teknoloji olanaklarının sunduğu avantajlar, drone'lar (SİHA) ve el yapımı patlayıcılar gibi ucuz ve kolayca elde edilebilen düşük teknolojili tehditler tarafından aşılabilir” ifadesinin belirtildiği gözlemlenmektedir (Esen, 2021).

Diğer taraftan belgede belirtildiği üzere, İngiltere'nin savunma politikasının odağında Rusya'nın ‘en şiddetli tehdit’ olduğu Avrupa-Atlantik bölgesinin yer almaya devam edeceği vurgulanmaktadır. Aynı zamanda, İngiltere'nin 10 yıl içinde Rusya'nın geniş Avrupa bölgesinde daha aktif olmasını beklemesi gerektiği ve devletin ilişkiler düzeline kadar Rusya'dan kaynaklanan her türlü tehditlere karşı aktif bir biçimde caydırıcı olacağı ve savunma yapacağı belirtilmektedir (Esen, 2021).

Son olarak belgede değinilen bir diğer konunun ise önümüzdeki on yılda “jeopolitik ve ekonomik çekim merkezinin doğuya yani ÇHC, Hindistan, Japonya gibi ülkelere kayacağı” olduğu görülmektedir. Akabinde Hint-Pasifik bölgesindeki Asya ülkeleriyle diplomatik ilişkilere öncelik verileceği bildirilmektedir. Bununla birlikte, ÇHC'nin yükselen gücünün, dünyadaki en önemli jeopolitik faktör olduğu ve Hint-

Pasifik bölgesinde etkisinin artmasıyla önemli zorluk oluşturacağı vurgulanmaktadır. ÇHC ile ilgili daha dikkatli ifadeler kullanılan belgede, ÇHC ye yönelik iddiaların artmasıyla beraber ortaya çıkan riskler ve insan hakları alanındaki güçlüklerle rağmen Pekin'e yönelik dengeli bir yaklaşım benimseneceği aynı zamanda ticaret ve yatırımlar alanında olumlu bir ilişki, küresel iklim değişimine karşı mücadele hususunda Çin ile ortaklığa önem verildiği belirtilmektedir (Köse, 2021).

İKİNCİ BÖLÜM

2. Dış Politika ve Ulusal Güvenlik

Değişen süreçlerle beraber devletlerin politika belirken izlemiş olduğu yollarda bazı değişim ve dönüşümler gerçekleşmektedir. Liderler değiştikçe belirlenen politikalar ve çalışmalar farklılaşmaktadır. Bu doğrultuda ÇHC'ye bakıldığında değişen liderler sonrası tamamen o politikayı ortadan kaldırmak yerine söz konusu politikalarda iyileştirilmeler ya da eklemeler yaparak yola devam edildiği görülmektedir. Nitekim ÇHC'nin, değişen liderleri ve politikaları sonrası, ardında kalan problemler dolayısıyla bir nevi bir kül hâline geldiğine, akabinde başa gelen yeni liderle beraber bir anka kuşu misâli yeniden küllerinden doğan, kendine özgü bir yapısı olduğu gözlemlenmektedir.

Öte yandan, tarihin her dönemine bakıldığında, devletlerin çıkarlarını sağlamak adına dış çevrelerine karşı eylemlerde bulunduğu ve çıkarları doğrultusunda dış dünyaya karşı bazı tutum ve davranışlar belirleyip uygulamaya koyduğu görülmektedir. Özellikle küreselleşmenin çok yoğun bir şekilde ilerlediği 21. yüzyılda ise devletlerin çıkarlarını sağlamak adına dış dünyaya daha önceki süreçte sergiledikleri tutum ve davranışlardan çok daha fazlasını sergilemek zorunda kaldığı tespit edilmektedir. Devletlerin dış çevrelerine yönelik sergilemiş oldukları tutumlarda çıkarlar ön plandayken, söz konusu çıkar türlerinden en önemlisinin güvenlik çıkarları olduğu ortaya çıkmaktadır. Bununla beraber devletin yapı taşı olan siyasal aktörlerin varolduğu günden günümüze kadar olan süreç içerisinde güvenlik olgusunun önemini koruduğu ve özellikle ulusal güvenlik çıkarlarının daima devletlerin dış politika belirlemede önemli bir faktör olduğu vurgusu yapılmaktadır. Kısacası, dış politikanın belirlenmesinde birinci derecede etkili olan unsurun ulusal güvenlik kavramı olduğu ortaya konmaktadır (Baharçiçek ve İnan, 2013: 102).

Genel olarak devletlerin ekonomik, sosyal, siyasal vb. çıkarlar elde etmek ve diğer devletlerin tutumlarını manipüle etmek adına dış politika geliştirdiği görülmektedir. Yukarıda da değinildiği üzere ulusal güvenlik unsuru devletlerin dış politikalarının şekillenmesinde büyük rol oynamaktadır. Diğer yandan bakıldığında ise günümüzde teknolojinin ilerlemesi ve internetin kullanım alanının genişlemesiyle beraber, siber alanın ulusal güvenlik içerisindeki rolünün de fazlasıyla arttığı gözlemlenmektedir. Bununla beraber gelecekte siber alanın ulusal güvenlikte ne kadar fazla ön sıralarda yer alacağı yadsınamaz bir gerçek olarak karşımıza çıkmaktadır.

Diğer taraftan ise Xi Jinping'in "siber güvenlik olmadan ulusal güvenlik olmaz" sözüne bakıldığında, siber güvenliğin ulusal güvenliğin önemli bir parçası olduğu bir kez daha gözler önüne serilmektedir. Xi Jinping'in sözündende anlaşıldığı üzere, ÇHC hükûmetinin ulusal güvenliği sağlamak ve ulusal çıkarları korumak adına politika belirlerken, siber güvenlik unsurunun önemi ve gerekliliği üzerinde durduğu saptanmaktadır.

Tüm anlatılanlar ışığında bu bölümde; öncelikle ÇHC'yi tanımak açısından ülkenin genel yapısı, tarihsel gelişimi ve yükselişinde rol oynayan devrim ve reform süreçleri ele alınmaktadır. Daha sonra, dış politika süreçleri ve dönemsel olarak dış politika ile ilgili atılan adımlara değinilmektedir. Son olarak ise genel bir perspektiften ulusal güvenlik anlayışı incelenip, akabinde yeni dönem ulusal güvenlik anlayışı analiz edilmektedir.

2.1.Tarihsel Gelişim

Bu başlık altında, ÇHC'yi tanımak adına öncelikle genel yapısı ile ilgili bilgi verilmektedir. Akabinde ÇHC'nin ortaya çıktığı sürece ve bu süreç sonrasında yaşanan gelişmelere değinilmektedir.

Çin olarak da anılan ÇHC, Pasifik Okyanusu'nun batı kıyısında ve Asya kıtasının doğusunda yer almaktadır. ÇHC'nin sınırlandığı yerlere bakıldığında; kuzeyi Moğolistan Halk Cumhuriyeti, kuzey doğusu Rusya Federasyonu ve Kuzey Kore, doğusu Sarı Irmak ve Doğu Çin Denizi, güney doğusu Güney Çin Denizi, Güneyi Vietnam, Laos, Hindistan, Birmanya, Butan ve Nepal, güney batısı ise Afganistan, Pakistan, Kırgızistan, Kazakistan ve Tacikistan ile sınırlandırılmaktadır. Dünya'da Rusya ve Kanada'dan sonra en büyük yüz ölçümüne sahip olan ÇHC'nin, 9 milyon 598 bin km²'lik bir yüz ölçümüne sahip olduğu bilinmektedir. Bunun yanında, her ne kadar tek çocuk politikası gibi politikalarla nüfusun hızı düşürülmeye çalışılsa da nüfus artışı hâlâ devam eden ÇHC, nüfus bakımından dünyanın en kalabalık ikinci ülkesi olarak karşımıza çıkmaktadır. 2022 verilerine göre ÇHC'nin nüfusunun 1 milyar 411 milyon 800 bin olduğu belirtilmektedir. 21. Yüzyılın ortalarına gelindiğinde ise bu sayının artmaya devam edeceği ve 1,6 milyar civarlarına ulaşacağı tahmin edilmektedir. Bununla beraber, ÇHC'nin nüfusunun %91,6'sını Han kökenli Çinliler, %16,7'sini ise aralarında Uygur Türklerinin de olduğu diğer azınlıklar oluşturmaktadır (Aljazeera Türk, 2014; Aytekin, 2023).

Öte yandan, dünyanın en eski medeniyeti olarak görülen Çin çok etnikli bir ülke olarak bilinmektedir. Çin ulusu kendilerini “Yanhuang’ın Torunları” ve “Ejderhaların Torunları” olarak adlandırmaktadır. Yaklaşık 5800 yıl önce ilk izlerinin görüldüğü Çin’de, ovalar çevresinde bir ülke oluşturmak amacıyla yerleşim toplumu ortaya çıkartmaktadır. Sonrasında ise birçok etnik grupların kaynaşmasıyla, hanedanlıklar oluşturulmaktadır. Fakat karşılaşılan birçok belirsizlikten dolayı Çin medeniyetinin ilk olarak hangi hanedanla ve ne zaman ortaya çıktığı kesin olarak bilinmemektedir. (Baidu Baike, 2023). Bununla beraber, Çin anakarası olarak adlandırılan bölgede binlerce yıllık süreç içerisinde birçok farklı devletlerin ve imparatorlukların kurulduğu söylenmektedir. Kurulan bu yapıların neredeyse tamamı Çin kültüründen etkilenip Çinlileşerek Çin toplumunun bir parçası hâline gelmektedir. Buna verilebilecek en son örnek ise Mançu-Qing İmparatorluğu (满清王朝) olmaktadır. Bu imparatorluk Çin imparatorluğunun sonuncusu olarak karşımıza çıkmaktadır. Çinlileşmenin etkisi altında kalan bu imparatorluk 1911 yılında Han Çinlisi milliyetçiler tarafından yıkılarak yerine Çin Cumhuriyeti (中华民国) adında yeni bir devlet kurulmaktadır. Böylelikle Konfüçyüsçü uygarlığın beşiği olan Çin anakarasında yeni bir dönem başlamaktadır. Bununla beraber, 2000 yıldır sürekli olarak hüküm süren hanedanlık dönemi sonra ererek yerini cumhuriyet dönemi almaktadır (Karluk, 2020: 103).

1949 yılında ÇHC kurulmadan önce birçok iç savaş ve karışıklıkların olduğu bilinmektedir. ÇHC böyle bir süreç sonrası kurulmaktadır. ÇHC’nin kurulma sürecine doğru giden yolda birtakım dönüm noktaları yaşanmaktadır. Bu dönüm noktalarının en önemlisinin, 1839 yılında baş gösteren Afyon Savaşı olduğu belirtilmektedir. Genel olarak bakıldığında Çin, kendi içine dönük ve izole bir toplum yapısına sahip ülke olarak varlığını sürdürmekteydi. Fakat karşılaşılan Afyon Savaşı sonrası bu durumun farklılaşmaya başladığı görülmektedir. Batı’nın ekonomik açıdan gelişmiş ülkeleri aracılığıyla zorlanarak uluslararası sisteme dâhil edildiği Afyon Savaşı sonrasında Çin’in izole olma durumu ortadan kalkmaktadır (Lee, 2018). Emperyalizmin dışında kalarak yaşamaya gayret gösteren Çin, Afyon Savaşıyla beraber emperyalist güçlerin yıkıcı yanıyla tanışmaktadır. Bunun yanın sıra, Çin’in klasik anlayışına göre, tüccarlar ekonomik anlamda kazanç elde etmek uğruna hiçbir şey üretmeyen sömürgeci asalaklar ve yabancılar ise tamamen barbar kişiler olarak görülmektedir (Sander, 2013: 271). Bu anlayış ile ilerleyen Çin uzun süre içe kapanık olduğu ve Batı ile olan ilişkilerini

minimal seviyede tutmayı başardığı görülmektedir. İstikrarlı giden bu durum İngiliz ticareti açısından önem arz eden bir ürün olan afyonun, Çin’de tamamen yasaklanması kararı sonrası değişmeye başlamaktadır. Çin’in emperyalizmin önemli aracı olan serbest ticarete yönelik yapmış olduğu bu hamle sonucunda İngiltere ve Çin arasında Afyon savaşının fitili ateşlenmektedir. Savaş sebebi oldukça basit gibi görünse de Henry Kissinger’in “iki dünya düzeninin çarpışması” olarak adlandırdığı bir hâl almaktadır (Kissinger, 2015: 73; Özdemir, 2022: 42-43).

Diğer taraftan İmparatorluk Dönemi; Afyon Savaşları, Boxer, Müslüman-Türk ve Taiping Ayaklanmaları gibi ÇHC’nin kuruluşuna giden yolda dönüm noktası niteliğindeki bu olaylar Çin’i zaman içerisinde yıpranmaktadır. Yukarıda da belirtildiği üzere İmparatorluk 1911 yılında burjuva devriminin lideri olan Sun Yat Sen tarafından yıkıldıktan sonra ülkede farklı aktörler gücü eline geçirme çabasına girmektedir (Oskay, 1967: 293). Bu doğrultuda Çin’in geleceği açısından önem arz eden iki partiden bahsedilmektedir. Bu partiler (Kissinger, 2015: 126);

- Çin Milliyetçi Parti- Kuomintang (Çan kay Şek önderliğinde kuruldu- 1894)
- Çin Komünist Partisi (Mao Zedong önderliğinde kuruldu- 1921), adıyla ortaya çıkmaktadır.

Yaşanan gelişmeler neticesinde, Sun Yat Sen’in hanedanlık sistemini yıkmasıyla sarsılan Çin toplumu, yeni cumhuriyetin kurulmasıyla beraber birtakım olumsuzluklarla karşı karşıya kalmaktadır. Yeni cumhuriyetle beraber Çin toplumunun, toplumsal istikrara yeniden kavuşamadığı, iç ve dış etkenlerden kaynaklanan bazı sorunlardan dolayı çaresiz kaldığı görülmektedir. Yaşanan bu olumsuzluklar karşısında Çinli aydınların 1921 yılında ÇKP’yi (中国共产党) kurduğu belirtilmektedir. Bu parti sonraki yıllarda, ülkede iktidar parti olarak görev yapan Çin Milliyetçi Partisi’ne (国民党) karşı önemli muhalefet olarak aktif rol oynamaktadır. Bununla birlikte, iki hareket arasında artan tansiyon zaman içerisinde iç savaşa dönüşmektedir. İkinci Dünya Savaşı sürecinde Japonya’nın Çin’e saldırmasından sonra bu iki hareket arasındaki iç savaşa bir süre ara verilmektedir. İkinci Dünya Savaşı’nın sona ermesiyle (1945) beraber- Japonya’ya atılan atom bombası sonucunda- Japonya yenilerek Çin’den geri çekilmektedir. Akabinde Çin’de iki hareket arasında yeniden iç savaşın patlak verdiği belirtilmektedir (Atawula, 2020:16).

İkinci Dünya Savaşı sonrasında ülkelerin yorgun düşmesi ve müdahale gücünü kaybetmesi sonucunda ve Mao Zedong’un taktik değiştirerek hem askeri gücüyle hem

de halkçı politikalarla kısa sürede Çin’de kontrolü ele geçirdiği görülmektedir. Bundan dolayı, Mao’nun halkın gözünde yükselmesi ve Çan Kay Şek’in, halk desteğinden yoksun kaldıkça otoritesini korumak adına olumsuz girişimlere yönelmesi, halkın gözünde Çan Kay Şek’in değerinin düşmesine sebep olmaktadır. Akabinde 1949 yılına gelindiğinde Çan Kay Şek yönetimindeki parti kesin yenilgiye uğrayarak Formoza adasına (Tayvan) kaçarak Çin Cumhuriyeti’nin burada devam edeceğini dünyaya ilan etmektedir. Günümüzde hâlâ devam eden Tayvan sorununun ana kaynağı, bu olay ile başlamaktadır (Çakan, 2017: 128-129).

1949 yılında Çan Kay Şek önderliğindeki Milliyetçilerin iç savaşı kaybedip Tayvan’a kaçmasıyla ve Komünistlerin Çin toprakların ele geçirmesiyle beraber Çin Halk Cumhuriyeti (中华人民共和国) adında yeni bir cumhuriyetin Mao Zedong önderliğinde kurulduğu ilan edilmektedir. 1 Ekim 1949 yılında, Pekin’deki Tiananmen Meydanı’nda düzenlenen ÇKP’nin 11. Merkez Komitesinin Üçüncü Genel Kurul Toplantısı ile kutlanan kurtuluş töreniyle beraber ÇHC’nin tarihi başlamaktadır. Çin Cumhuriyeti olarak anılan eski Çin’e halk kelimesi eklenerek Çin’de yeni bir cumhuriyet kurulmuş olmaktadır (Atawula, 2020: 16; Nabijiang, 2022: 16). Diğer yandan ise kuruluşundan sonra ÇHC’yi ilk tanıyan ülkenin; İkinci Dünya Savaşı sonrası Batı ve Doğu bloğu olarak ayrılan iki kutuplu dünyada Sosyalist Doğu Bloğu’nun öncüsü olan SSCB olduğu belirtilmektedir (Tosun, 2014: 25). Fakat ÇHC’yi ABD’nin başı çektiği kapitalist Batı Bloğu tanımamaktadır. Uluslararası alanda uzun süre boyunca Milliyetçi Çin iktidarındaki Çin Cumhuriyeti tanınırken, ÇKP yönetiminin ABD ve AB ülkeleri ile aralarındaki ilişkinin düzelmesiyle beraber 1971 yılına gelindiğinde Çin Cumhuriyeti’nin BM’den çıkartılarak ÇHC’nin uluslararası sisteme dâhil edildiği görülmektedir. Bununla beraber ÇHC 1971 yılından itibaren, BMGK’de daimi üye olarak varlığını devam ettirmektedir. Bunun yanında, günümüzde “Çin” ifadesinin ÇHC için kullanıldığı, “Tayvan” ifadesinin ise Çin Cumhuriyeti için kullanıldığı ifade edilmektedir (Çakan, 2017: 129).

Genel olarak bakıldığında, ÇHC ilk kurulduğu andan günümüze kadar sayısız olaylara sahne olmaktadır. ÇHC’nin gelişmesi adına ve günümüzdeki gücünü eline alması adına ilk kurulduğu andan itibaren birçok devrimler, politikalar ve reformlar gerçekleştirilmektedir. ÇHC’nin gelişim süreci iki dönemden oluşmaktadır. Bu dönemler; 1949-1978 yıllarını kapsayan Devrim Dönemi ve 1978 sonrasını kapsayan Reform Dönemi şeklinde karşımıza çıkmaktadır. ÇHC’nin gelişimi bu doğrultuda iki

farklı başlık altında incelenmektedir. Diğer yandan ise Mao Zedong ve Deng Xiaoping ÇHC'nin gelişimde katkıda bulunan önemli isimler olarak ÇHC tarihine adını yazmaktadır. Bundan dolayı, ÇHC'nin gelişimi ile ilgili analiz yapıldığında bu iki lider üzerinden yapılmasının faydalı olunacağı düşünülmektedir. Deng sonrası başa gelen isimlerden Jiang Zemin (1993-2002), Hu Jintao (2002-2012) ve Xi Jinping (2012-) gibi isimlerin yapmış olduğu çalışmalara daha detaylı şekilde farklı başlık altında yer verilmesi planlanmaktadır.

2.1.1. Devrim Dönemi (1949-1978)

1 Ekim 1949 yılında Mao Zedong önderliğinde kurulan ÇHC'de, ÇKP Başkanı olarak Mao Zedong görev yaparken, Başbakan ve Dışişleri Bakanı olarak da Chou Enlai'nin görev yaptığı görülmektedir (Sander, 1989: 366). “*Tek parti devleti*” olan ÇHC, ÇKP tarafından yönetilmektedir (Çalışkan, 2022: 6). Ülke sistemini kendi ideolojisine göre şekillendirmeyi amaçlayan Mao Zedong'un hedefi sosyalist bir devlet kurmaktır (Aktaş, 2019: 48). Bu bağlamda Mao, yeni devletin temel yol göstericisi olarak benimsediği ideolojilerin; Marksizm ve Leninizm olduğunu belirtmektedir. Bu ideolojileri benimsemesi ÇHC'nin tercihinin Sosyalist Blok'tan yana olduğunu göstermektedir. Bunun yanı sıra, yoğun savaş sürecinden çıkan ÇHC'nin ekonomik askeri ve sosyal alanda yardıma ihtiyacı olmaktadır. Bu durumda 1950 yılında SSCB ile 30 yıllık Dostluk, İttifak ve Karşılıklı Yardım Anlaşması'nın imzalandığı ifade edilmektedir (Adıbelli, 2006: 132). Buna ek olarak, Sovyet lideri Stalin'in ölümünden sonra Sovyetler'de, yönetimin yumuşayıp biraz daha özgürlükçü atmosferin hâkim olduğu söylenmektedir. Bu durum her ne kadar ÇHC yönetimini etkilese de Mao, eleştirilere kapalı ve güvensiz çizgide devam ederek SSCB'deki özgürleşmenin ÇHC'de etkili olmadığını yansıtmaktadır (Aslan, 2014: 31).

Öte yandan, Çinliler tarafından “aşağılanma yüzyılı” ya da “utanç yüzyılı” olarak anılan Afyon Savaşı ile başlayan (1849) ve 1949 yılında ÇHC'nin kurulmasıyla sona eren yaklaşık 100 yılı aşkın bir süre boyunca devam eden savaş ve mağlubiyet hâli ÇHC'yi ekonomik olarak fazlasıyla yıpratmaktadır. Bu durum ÇHC'yi ekonomik anlamda geride kalan bir ülke konumuna düşürmektedir. Akabinde 1950'lere gelindiğinde ise ÇHC'nin dünya ekonomisinin yaklaşık yüzde yirmide birlik dilimini oluşturduğu görülmektedir (Maddison 2007). Bununla beraber, ülkenin sistemini kendi ideolojisi doğrultusunda yapılandıran Mao Zedong ve Komünist Parti, ÇHC'nin rutin

olan klasik yönetim ve ekonomi modellerine reform uygulamaya başladığı görülmektedir. Ekonomik kalkınma politikasının amaçlandığı Mao döneminde (1949-1976), ÇHC tarihinde ilk kez olan, “*merkeziyetçi ve planlı ekonomi*” politikasının hayata geçirildiği ifade edilmektedir (Çakıroğlu, 2008: 3).

Çin’in kurulduğu tarihten bu yana ülkenin yönetiminde başa gelen Çinli komünist liderler ÇHC’yi güçlü, demokratik ve zengin bir ülke durumuna sokmayı başlıca amaçları olarak görmektedir. Geniş bir ülke yapısına sahip olan ÇHC’nin devlet başkanlarına göre bu durumun tek yöntemi; sanayileşmek, üretmek ve endüstrileşmek olarak belirtilmektedir. Bu bağlamda iş gücü hususunda endüstrileşmeye yönelen ÇHC, tarımı geliştirerek yaratıcılığı yükseltmeyi hedeflemektedir (Brunner ve Gökdere, 1969: 310). ÇHC’nin iç politikasında yaşanan sorunlar ve düzensizliklerden dolayı Mao’nun, ülkenin temelini geliştirmeye çalıştığı süreçte SSCB’nin ekonomi politikalarını örnek aldığı görülmektedir. Bu dönemde (1949-1976) ÇHC ekonomisi, *katı/emredici merkezi planlamaya dayalı ve dışa kapalı* özellik göstermektedir (Çalık, 2011: 310). ÇHC’nin gelişmesi adına yapılan çalışmalar ve dönemler arası izlenen politikalar kronolojik sırayla analiz edilmektedir. Bunun öncesinde genel olarak hangi dönem aralığında hangi konulara odaklanıldığını maddeler hâlinde belirtmenin faydalı olacağı düşünülmektedir.

ÇHC’nin dönemsel olarak izlediği politikalara genel olarak bakıldığında şu şekilde sıralandığı görülmektedir (Demirel, 2019: 32):

- 1949-1957 yıllarında, büyüme odaklı yol izlemektedir. Yani Mao bu süreçte, büyümeye, yeniliklere ve yeniden yapılanmaya odaklanmaktadır.
- 1949-1953 yıllarında, siyasi kontrolü ele almak amacıyla stratejiler üretilmektedir.
- 1953-1957 yıllarında ise, Sovyet tarzı endüstrileşme modeline öncelik verilmektedir.

Öncelikle 1949-1953 yılları arasındaki siyasi kontrolü ele geçirme adına atılan adımlara bakılacak olursa; ÇHC’nin “halkın demokrasi diktatörlüğü” adını verdiği bir sistemi açıkladığı görülmektedir. Bu noktada Mao, çalışan sınıfın üstün olduğu, işçilerin ve köylülerin birliğine dayanan, köylü sınıfı, işçi sınıfı, ulusal burjuvazi ve şehirli küçük burjuvazi sınıflarının egemen olduğu sistemi komünizm olarak ifade etmektedir. Bu doğrultuda bakıldığında Mao’nun ideolojisinde köylü kesim ön plandayken ve sistem bu doğrultuda şekillenirken, şehirli küçük burjuvazi sınıfı ile bağlarının zayıf olduğu belirtilmektedir (Dillion, 2016: 296-297).

1949-1950’li yıllarda ÇKP’nin başa gelmesiyle beraber uygulanan en önemli politikanın, “*Toprak Reformu*” olduğu görülmektedir. Bu yıllarda toprağın %40’ının yeniden dağıtıldığı belirtilmektedir (Mitter, 2012: 73-95). ÇHC kurulmadan önceki dönemlerde Çin köylüsü doğal afetler, feodalizm ve savaşlardan dolayı zor şartlar altında yaşamaktadır. Feodalizmin adaletsiz bir biçimde uygulandığı Çin’de, bu duruma ÇKP son vermek istemektedir. Bu bağlamda sorunun çözülmesi noktasında parti içinde önemli tartışmalar yaşanmaktadır. Köylünün yaşamış olduğu alt yapı sorunlarının çözümü yetersiz kaldığından dolayı toprak reformunun gündeme gelmesinin kaçınılmaz olduğu görülmektedir (Suyin, 1995: 48). Diğer yandan, 1950 yılına gelindiğinde ise ÇKP, toprak reformu programı çerçevesinde toprakları bütün sınıflar arasında dağıtmak amacıyla halk komünleri kurmaktadır. Bu bağlamda atılan bu adım feodal sistemden kapitalizme geçiş olarak ifade edilmektedir (Holcombe, 2016: 360). Reformun yapılmasındaki amaç; kırsal üretim güçlerini özgürleştirmek ve sanayileşmenin önünü açmak olarak belirtilmektedir (Dillion, 2016: 316).

Bu doğrultuda Mao şehirli ve ulusal burjuvazi sınıfını devlete daha bağımlı hâle getirmek adına 1951 yılında iki kampanya ortaya koymaktadır. Bu kampanyalar; “*Üç Anti Kampanyası*” ve “*Beş Anti Kampanyası*” adıyla düzenlenmektedir. Genel olarak kampanyaların yapılma amacı şu şekilde belirtilmektedir (Dillion, 2016: 296-297):

- Üç Anti Kampanyası: İsrâf, yolsuzluk ve bürokrasi kültürüne karşı yapılmış bir kampanya olan Üç Anti Kampanyası’nın amacı; ticaret dünyasında devlet görevlilerine yönelik yapılan mali teklifler ve bunun dışında farklı içerikte olan tekliflere dikkat çekmek olarak açıklanmaktadır.
- Beş Anti Kampanyası: Ulusal burjuvaziye hedef alan bu kampanya, vergi, rüşvet, dolandırıcılık, kaçırma, devlet mallarına yapılan hırsızlık ve devlete ait sırların açığa çıkarılmasına karşı yapılan şehirli bir hareket olarak düzenlenmektedir. Amacı; ÇKP’nin hedeflerini gerçekleştirmesi noktasında engel oluşturduğunu düşünülen ulusal burjuvazi iktidarını ve otoritesini yok etmektir.

Diğer taraftan, Mao’nun ÇHC’yi ekonomik ve siyasi anlamda geliştirmek adına birçok hamlesinin olduğu görülmektedir. Bu hamleler sırasıyla şu şekilde ele alınmaktadır:

- Birinci Beş Yıllık Kalkınma Planı (1953)
- Yüz Çiçek Kampanyası (1956)

- İkinci Beş Yıllık Kalkınma Planı- Büyük İleri Atılım (1958)
- Üçüncü Beş Yıllık Kalkınma Planı- Kültür Devrimi (1966)
- Dördüncü ve Beşinci Kalkınma Planı (1971-1980)

ÇHC'nin kurulmasına öncülük eden Mao Zedong, uzun süren savaş sonrası ülke içinde bulunan toplumsal bunalımı düzeltmeye çalışmaktadır. Uzun süren kargaşa sürecinden sonra Mao, birçok ülkenin de tartıştığı “*Sovyet tipi planlı ekonomi*” yönteminden etkilenecek, ülkenin altyapısını düzeltmek amacıyla bu modeli uygulamaya koymaktadır. Diğer ülkeler tarafından her ne kadar bu model eleştirilse de İkinci Dünya Savaşı sonrası dönemde dünya genelinde “planlı ekonomi” modeline geçildiği görülmektedir. Bununla beraber, 1953-1957 yılları arası Çin'in Sovyet tarzı endüstrileşmeye ağırlık verdiği dönem olarak ifade edilmektedir. Birçok ülke gibi ÇHC'nin de Sovyet tipi ekonomiden etkilenmesinden dolayı 1953 yılında “*Birinci Beş Yıllık Kalkınma Planı*”nı yürürlüğe koyduğu açıklanmaktadır. Planın uygulandığı dönem boyunca ÇHC, SSCB'den birçok alanda yardım almaktadır. Planın hazırlanması ve uygulanması sırasında teknik destekte bulunan Sovyetlerin kılavuzluğuyla ve eğitimiyle; mimari ve spor eğitiminden, endüstri mühendisliğine, bilimsel araştırma ve eğitim kurumlarına kadar hemen hemen her alan bu doğrultuda şekillendirilmektedir. Bu bağlamda, 1-2 yıllık gibi kısa dönemde yaklaşık 6000 Sovyet danışmanın ÇHC'ye gönderildiği ve 10.000'den fazla Çinli öğrencinin de SSCB'de öğrenim gördüğü belirtilmektedir (Naughton, 2007: 66).

Temel olarak sanayileşmeyi ve sanayiye dayalı ekonomik büyümeyi hedefleyen plan sonrası dönemin sonuçlarına bakıldığında; yüksek ekonomik büyüme ve sanayileşme hedeflerinde başarı elde edildiği görülmektedir. Bunun yanı sıra, altyapının büyük bir kısmının yeniden inşa edildiği ve enflasyonun aşağı çekildiği belirtilmektedir. Ayrıca SSCB ile yapılan işbirliği sonucunda “Doğu Bloğu” ülkelerle ticaretin arttığı vurgulanmaktadır (Özsoylu, 2006: 9-10). Aynı zamanda, ağır sanayi olan demir-çelik, çimento, madencilik gibi sanayi kollarında önemli başarılar yakalandığı gözlemlenmektedir. Planın sonuçları doğrultusunda devletin ekonomide ağırlığının arttığı ifade edilebilmektedir. Ekonomide ağırlık kazanan devlet, şehirlerde bulunan girişimci kesimi kamu kurumlarıyla çalışmaya ve iş birliği kurmaya zorlarken, kırsal kesimde bulunan çiftçileri ise kooperatiflere katılmaya zorlamaktadır. Tüm bu gelişmeler ışığında uygulanan politikaların sonucu olarak (Naughton, 2007: 67):

- 1954 yılının sonuna gelindiğinde kırsal kesimdeki çiftçilerin yalnızca %2'si kurulan kooperatiflere üyeyken, 1955 yılında bu sayı %14'e ve 1956 yılında ise %98'e yükselmektedir.
- Şehirde bulunan kesime bakıldığında ise, 1956 yılının başlarında özel işletmelerin devlet tarafından uygulanan yoğun kontrollerle kooperatiflere ya da " kamu-özel ortaklığına " dönüştüğü söylenmektedir.

Öte yandan, 1950'li yıllardan itibaren Mao Zedong'un benimsemiş olduğu *bir tarafa yönelme politikasıyla* ÇHC, SSCB'nin en yakın müttefiki olduğu bilinmektedir (Demirel, 2019: 33). Diğer yandan ise 1956 yılında Mao Zedong "Yüz Çiçek Kampanyası" adıyla, aydınların fikirlerini daha özgür bir ortamda dile getirmesini hedeflediği bir dönem başlatmaktadır. 1956'da başlayıp 1962 yılına kadar süren bu dönemde Mao, fikirlerin tartışılmasını isteyerek daha özgürlükçü bir ortamın oluşmasını sağlamaktadır. Akabinde ülkedeki kanaat önderlerinin, aydınların ve öğretmenlerin ülkenin sorunları hakkında konuşmasını ve eleştiri yapmasını istemektedir (Sander, 1966: 277). Zhou Hanedanı dönemi'ndeki "yüz çiçek açsın, yüz düşünce yarışsın" sloganından adını alan Yüz Çiçek Kampanyasıyla Mao bu dönemde, komünizmin toplumca benimsenmesi ve Marksist ideolojinin güçlenerek hâkim ideoloji hâline gelmesini istemektedir. Ancak sonuç, Mao'nun beklediğinden farklı gelişmektedir. Mao, aydınların feodaliteden hızla kurtulmanın yolları hakkında tavsiyeler ve teklifler getireceğini beklerken, özellikle aydın kesimin iktidara ve sosyalist yönetime karşı getirdiği ağır tenkitler hayal kırıklığının yaşamasına sebep olmuştur (Armaoğlu, 1984: 574).

Akabinde 1957 yılına gelindiğinde Mao ve Komünist Parti'nin Yüz Çiçek Kampanyası'nın sonuçlarından memnun olmadığı görülmektedir. Dönem içerisinde yönetime yöneltilecek liberal eleştirilerden dolayı toplumda liberalizme yönelim olmasından endişe edilerek birkaç ay içerisinde Yüz Çiçek döneminde sesini yükselten 800.000 aydın ve kanaat önderlerinin tutuklanıp cezalandırıldığı belirtilmektedir. Hatta kimilerinin işlerinden atıldığı ya da bazı durumlarda çalışma kamplarına gönderildiği ifade edilmektedir (Naughton, 2007: 69).

ÇHC tarihindeki en önemli zaman aralığı 1958-1962 (Büyük İleri Atılım) ve 1961-1980'li (Kültür Devrimi) tarihleri işaret etmektedir. Büyük felaketlerin başlangıcı olarak da görülen bu dönem aralıklarından ilk olarak 1958-1961 yıllarını kapsayan süreç ele alınmaktadır. Özgürlükçü ortamın hâkim olduğu Yüz Çiçek Dönemi'nin yok olmaya

başladığı süreçle birlikte, 1958 yılında *Büyük İleri Atılım (İleriye Doğru Büyük Hamle)* ve beraberinde *İkinci Beş Yıllık Kalkınma Planı* hayata geçirilmektedir (Çalık, 2011: 188). Çin ekonomisi Mao Zedong öncesi süreçte önemli oranda tarıma dayalı feodal bir sistemden oluşurken, Mao sonrası Büyük İleri Atılım politikasıyla beraber feodal tarım ekonomisinden komünizme hızlı bir geçiş yapılması hedeflenmektedir. Bu atılım doğrultusunda hayata geçirilen bazı hususlar bulunmaktadır. Bu hususlar şu şekilde ifade edilmektedir (Özsoylu, 2006: 10):

- Bu dönemde özel tarım üretimine yasak getirilmektedir. Buna devam eden ya da girişimde bulunan tarım işçileri “karşı devrimci” olarak nitelendirilmektedir.
- Çin toplumu devlet tarafından komünler şeklinde organize edilmektedir. Bundan dolayı Çin’de 100.00 ila 200.000 kişilik kapasiteden oluşan 24.000 komün inşa edilmektedir.
- Tarımsal üretimin yanında birde demir-çelik üretme birimlerine sahip olan komünler, ürettikleri ürünlerden ihtiyaçları doğrultusunda gerekli olan kısmını kendilerine ayırdıktan sonra, kalan kısmı devlete teslim etmektedir.

Mao bu dönemde, tarımın yanı sıra demir-çelik ocaklarını da komünlerde bulundurmasıyla sanayileşmeyi geliştirerek, tarım toplumundan sanayi toplumuna geçişi hedeflemektedir. Kırsal kesimin komünler şeklinde örgütlenmesiyle, kırsal sanayinin gelişimi sağlanmak istenmektedir. Bu proje sonucunda Mao, Çin’in çelik üretiminin İngiltere’yi 10-15 yıl içerisinde yakalayabileceğini ön görmektedir. Bu bağlamda, devletin ağır sanayiye yönelik yatırımları 1956 yılında %38 iken, 1958 yılında %56’ya yükselerek bu yatırımların büyük bir kısmının ağır sanayiye gittiğini göstermektedir. 1959 yılına kadar gayet başarılı ilerleyen proje, bu yıla gelindiğinde yaşanan kuraklık dolayısıyla sekteye uğramaktadır. Kuraklığın yanı sıra yanlış politikaların izlenmesi de bu başarısızlığın sebebi olarak görülmektedir. Başarısız politika ve kötüleşen hava sonucunda ÇHC’de açlık baş göstererek birçok insanın yaşamını yitirdiği belirtilmektedir. Bundan dolayı 1959-1962 yılları arası ÇHC halkı açısından oldukça felaket bir süreç hâline gelmektedir. İnsanlık faciasının büyük boyutlara ulaştığı ÇHC’de meydana gelen ölüm sayısı kesin olarak bilinmemektedir. Fakat bazı uzmanlar konuya ilişkin araştırmalar yaparak bazı rakamlar öne sürmektedir. Bu doğrultuda, Ansley J. Coale (1958-1961) bu sayının 16.5 milyon, John Aird ve Peng

Xizhe 23 milyon, Ashton, Hill, Piazza ve Zeitz ise 29.5 milyon ölü olduğunu ileri sürmektedir (Yang, 1996: 35).

Her ne kadar ölü sayısı net olarak bilinmese de büyüklüğünün açık bir şekilde ortada olduğu bu felaketin Mao yönetimine ve Çin devrimine büyük darbe vurduğu bilinmektedir. 1961 sonrasında ise bürokrasi de ciddi durgunluk ve hayal kırıklığı baş göstermektedir. Çin devriminin toplumsal motivasyonunu kaybetmesiyle Mao yönetimi daha ılımlı politikalar izlemektedir (Naughton, 2007: 73). Yaşanan bu olaylar sonrasında 1962-1968 yılları arasındaki süreç iyileşme dönemi olarak değerlendirilmektedir. Dönemin bu şekilde değerlendirilmesinin ana nedeni açlığın azalması ve sanayinin gelişmesi olarak ifade edilmektedir (Çalık, 2021: 23).

Mao'nun yaptığı hamlelerden bir diğeri olan *İkinci Beş Yıllık Kalkınma Planı'na* (1958-1962) bakıldığında ise ilk oluşturulan plandan tamamen soyutlanmadığı gözlemlenmektedir. Çünkü iki kalkınma planının da bir kolektifleştirme hareketi olduğu görülmektedir. Birinci Beş Yıllık Kalkınma Planı'nda yapılan en büyük hatalardan biri sanayi sektörünü ön plana çıkarmak ve tarım sektörünü göz ardı etmektir. İkinci Beş Yıllık Kalkınma Planı'nda bu hatadan ders çıkarılarak hareket edilmektedir. Bundan dolayı “iki bacak üzerinde yürümek” politikasıyla hem tarım sektöründe hem de sanayi sektöründe ilerlemeyi hedef alan ve bunu geliştirmeyi amaçlayan politika benimsenmektedir (Gökten, 2013: 17-18). Hatalarından ders almış gibi görünen Mao yönetimi yine ütöpik bir hedef belirlemektedir. Mao'nun belirlemiş olduğu bu hedef, sanayi sektörünün yıllık çıktısını %25 düzeyinde artırmak olarak ifade edilmektedir. Yani ülkenin sanayi çıktısının 3-4 yıl içinde bir kat artırılması ön görülmektedir. Belirlenen hedefin gerçekleşmesi hâlinde ülkenin göstermiş olduğu performans sonucunda hem kentsel işsizlik gerileyecek hem de kırsal alanda hafif sanayinin güçlenmesi yoluyla sektörel dengesizliklerin üstesinden gelineceği belirtilmektedir (Lippit, 1975: 104). Fakat hedefe ulaşmak adına üreticinin yaşam standartlarında ortaya çıkan gerileme görmezden gelinmektedir. Aynı zamanda hükûmetin krizi yönetememesi de bu duruma eklenince başarısızlık kaçınılmaz bir son olarak Mao'nun karşısına çıkmaktadır. Böylece başarısızlık zincirine bir halka daha eklenmektedir (Gökten, 2013: 18-19). ÇHC'nin sosyo-ekonomik yapısını etkileyen bu olay Mao'da büyük bir hayal kırıklığına sebep olmaktadır. Fakat yaşanan olumsuzluklara rağmen Mao ideolojisinden taviz vermeyerek idealindeki komünist toplumu oluşturmak adına çabalarına devam etmektedir (Erdoğan, 2020: 64).

Sosyalist dönüşüm adı altında yapılan projeler ve Büyük İleri Atılım projesinin yaratmış olduğu olumsuzluk sonrası ÇHC tarihinde “on yıllık kaos” olarak adlandırılan *Kültür Devrimi* süreci 1966-1976 yılları arasında gerçekleşmektedir (Sander, 1966: 137). 1966 yılında Üçüncü Beş Yıllık Kalkınma Planı’yla beraber hayata geçirilen Kültür Devrimi’nin asıl amacı, Çin halkını kapitalizmden uzaklaştırarak daha çok komünizm inancını güçlendirmektir. Kültür Devrimi tarihe; geçmişte yaşanan olumsuzlukların unutturulmaya çalışıldığı, ülkede bulunan aydınların, kanaat önderlerinin ve düşünürlerin siyasi baskı altında tutulduğu, bazı eyaletlerde insanlık suçlarının işlendiği, Kızıl Muhafızlarca tarihe ait kitap, tablo vb. eşyaların yakıldığı bir süreç olarak geçmektedir (Esherick, Pickowicz ve Andrew, 2006: 96-120). ‘Dört eskiyi; eski düşüncüyü, eski kültürü, eski adetleri ve eski alışkanlıkları yık’ sloganıyla harekete geçilen bu devrim ile 1957-1960 yılları arasında yaşanan gelişmelerde Mao’nun gücünü kaybetmesinin ardından, ülkedeki gençlerin desteğiyle kaybedilen gücün yeniden kazanılıp Mao’nun otoritesinin güçlendirilmesi hedeflenmektedir. Mao’nun burjuva unsurlarının ülkede yönetimi ele geçireceği endişesi sonrası bu durumun engellenmesi için çağrıda bulunduğu görülmektedir. Kızıl Muhafızların bu çağrıya kulak vermesiyle beraber toplumun tüm kesiminde beliren ‘yıkma, yok etme’ eylemlerine girişildiği ve halkın sokağa döküldüğü söylenmektedir (Aktaş, 2019: 49).

Bununla birlikte, alt-üst ilişkisi ve liderlik durumu bulunmamasından dolayı Kızıl Muhafızlar arasında ÇHC’nin bazı bölgelerinde çatışmalar yaşanmaktadır. Çatışmaların devam ettiği süre içerisinde bu durum iç savaşa sebep olmaktadır. Yaşanan bu olaylara engel olmaya çalışan Mao, Kızıl Muhafızları ÇKP etrafında yeniden toplamaktadır. Yankılarının sokak çatışmalarıyla devam ettiği sürece geline Kültür Devrimi’nde Mao, toplumda güvenliği sağlamak adına kendi eliyle kurmuş olduğu Kızıl Muhafızlar komitelerini orduya bağlayarak Yerel Devrimci Komiteler oluşturmaktadır. Fakat toplumsal isyanı bastırmak adına ordunun ileri gelen isimlerinin şartları bulunmaktadır. Bu şartlar; yönetimde söz hakkı ve devrim sürecinde tasfiye edilenlerden bir kısmının göreve iadelerinin talebi, şeklinde ifade edilmektedir. Bu şartlar doğrultusunda karşılıklı anlaşmayla beraber büyük çoğunluğu öğrencilerden oluşan 12-18 milyon arasında olan Kızıl Muhafızlar kırsal alanlara sürgün edilmektedir. 1968 yılına geldiğinde ise Mao’ya karşı tekrar silahlanan kızıl muhafızların, 1969 yılında kesin yenilgiye uğradığı görülmektedir. Akabinde Kültür Devrimi süreci de noktalanmaktadır. Her ne kadar toplumsal kriz bastırılsa da bu durum siyasal krizin

devam etme durumunu engelleyemeyerek bürokrasi kesimindeki mücadelelerin yaklaşık 7 yıl daha sürmesine sebep olmaktadır (Oktay, 2017: 53).

1966 yılında yapılan bir diğer hamle ise Kültür Devrimi'yle beraber uygulamaya konulan *Üçüncü Beş Yıllık Kalkınma Planı* olarak karşımıza çıkmaktadır. Uygulamaya konulan bu planda özellikle ulusal savunma ile ilgili hedefler ön plana çıkmaktadır. Bir diğer ana hedef ise ÇHC'nin karşılaşacağı herhangi bir savaş olasılığında ekonomik olarak bu savaşa hazırlıklı olması ve kendilerine yetebilecek kadar tarımsal üretim planının gerçekleştirilmesi olarak belirtilmektedir. Oluşturulan planın genel olarak istenilen hedefe ulaştığı görülmektedir. Gerçekleşen hedeflere bakıldığında; gayrisafi belirlenen %21,1 oranında gayrisafi sanayi üretimi ve %2,2 tarım üretimi hedefinin çok daha üstünde olduğu belirtilmektedir (Çalık, 2011: 191).

Söz konusu dönem içinde yaşanan ekonomik gelişmelere bakıldığında; 1967-1968 yıllarında öncesinde %5,7, sonrasında %4,1 oranında küçülme olduğu, akabinde 1969-1970 yıllarında ise öncesinde %16,9, sonrasında %19,4 oranlarında büyüme olduğu görülmektedir. Bu yüzden, 1967-1968 yıllarında yaşanan ekonomik daralmanın sebebi Kültür Devrimi'nde gerçekleşen yıkıcı etkiler olarak karşımıza çıkmaktadır. 1969-1970 yıllarındaki büyümenin sebebi ise ülke içinde siyasi ve toplumsal istikrarın yeniden sağlanamaması olarak ele alınmaktadır (Önür, 2021: 53).

Son olarak, 1971-1980 yılları arası Dördüncü ve Beşinci Kalkınma planının olduğu süreçler olarak bilindiği görülmektedir. 1971-1977 yılları arası *Dördüncü Beş Yıllık Kalkınma Planı*'nın uygulandığı dönem olarak değerlendirilmektedir. Planın uygulandığı süreçte ekonomik büyümede dalgalı bir görünümünden söz edilmektedir. Aynı zamanda artı bir büyüme oranının tutturulduğu da söylenmektedir. Bunun yanında, 28 Temmuz 1976 yılında ise Tagshan'da yaşanan deprem dolayısıyla gerçekleşen hasarla beraber bu durumun ekonomik göstergelere olumsuz yansıdığı bilinmektedir (Carayannis, 1976). 1977-1980 yılları arasına gelindiğinde ise bu dönemde *Beşinci Beş Yıllık Kalkınma Planı* uygulanmaktadır. 1976 yılında Mao'nun vefat etme durumundan dolayı o dönemde uygulanan ekonomik ve siyasi politikalarda köklü değişikliğe gidildiği görülmektedir. Bu planın gerçekleştirilmek istendiği dönemde Mao'nun etkisinin asgari düzeyde kaldığı söylenmektedir (Aktaş, 2019: 56).

2.1.2. Reform Dönemi (1978 ve Sonrası)

1970’li yıllarda hastalığa yakalanan Mao Zedong, 1976 yılında hayatını kaybetmiştir. Mao’nun ölümüyle beraber ÇHC’de reform dönemi başlamaktadır. 1976 yılından 1978 yılına kadar siyasi karışıklığın yaşandığı ÇHC’de, Mao’nun ölümünden sonra ekonomik durumun giderek daha fazla kötüleştiği bilinmektedir. Yaşanan iç siyasi mücadele dolayısıyla halkında yorulduğu bu ortama, liderlik etmek adına 1978 yılında Deng Xiaoping geçmektedir. Mao’nun varisi olan Deng buna rağmen Mao gibi ideolojik ilerlememektedir. Bu bağlamda Deng, ÇHC’yi modernleştirmenin yolunun ülke ekonomisini yeniden kurup geliştirmekten geçtiğini söylemektedir. Bundan dolayı ülkeyi yeniden dış dünyayla bağlamanın küresel ekonomik sisteme entegre etmek olduğunu bildirmektedir. Ekonomik reforma odaklanan Deng, dünyanın artık yeni bir döneme girdiğini ve bu yeni dönemde reformu gerçekleştirmek adına yönelinmesi gereken asıl hususun barış ve kalkınma olduğunu savunmaktadır. Bu doğrultuda Deng, ÇHC’de geri kalmış ekonomiyi modernleştirmek adına, 1978 yılında “*Reform ve Dışa Açılım*” politikasını yürürlüğe koymaktadır (Scobell vd., 2018: 16).

Diğer yandan komünizmin hâkim olduğu ÇHC tarihine bakıldığında, söz konusu dönemin genel anlamda ideolojik mücadele tarihi olarak nitelendirildiği görülmektedir. ÇHC kurucusu Mao’nun liderlik yaptığı süreçte devrim yapma ve bu devrimleri yapmak adına insanları ikna etme yoluna gidildiği tespit edilmektedir. ÇHC’de liderliği eline alan Deng ise ilk olarak ideolojik alandaki zorlukların aşılması gerektiğini belirtmektedir. Mao döneminde yaşanan devrim hareketleri sonucunda ortaya çıkan derin etkiler izlerini sürdürmektedir. Bundan dolayı Deng, ilk olarak bu derin etkileri silmek adına kendisinin başlatmış olduğu reform dönemi boyunca sürekli “*zihinlerin özgürleştirilmesi*” fikrini ve “*hakikati olgularda aramak*” gerektiğini detaylı bir biçimde vurgulamaktadır (Pu, 2015: 36).

1978’de Deng ile birlikte ÇHC’de büyük değişimlerin başladığı görülmektedir. Ekonomik açıdan ÇHC’nin altın çağı olarak anılan Deng döneminde, ÇKP’nin 11. Merkez Komite Toplantısı’nda alınan kararlar dönüm noktası olarak kabul edilmektedir. Bununla birlikte, dışa dönük politika izlemeye başlayan Deng, dışa açılırken teknoloji, sermaye ve piyasa ekonomisi düşüncesini ÇHC’de uygulamaya koymaktadır. Dünya genelinde olduğu gibi ÇHC’de de 1980’li yıllar neoliberal politikaların uygulanmaya başladığı dönem olmaktadır (Çakan, 2017: 103). Bu doğrultuda, ÇKP’nin yapmış olduğu toplantıda Mao’nun sürekli dile getirmiş olduğu sınıf mücadelesine son verdiğini ilan eden Deng, sosyalizmin asıl amacının, ülke kalkınması, güçlü ve zengin

olması gerektiğini vurgulamaktadır. Bundan dolayı ÇKP için yeni bir vizyon belirleyerek, ekonominin canlanması şeklinde hedefler ortaya koyduğu görülmektedir. Bu hedefi gerçekleştirmek adına 1978-1985 yılları arasında, “*Dört Modernizasyon Programı*” ya da “*Dörtlü Modernleşme*” olarak da anılan programı uygulamaya koyduğunu duyurmaktadır (Özsoylu, 2006: 15-16).

Dört Modernizasyon Programı dört alan için hedef belirlemektedir. Bu alanların; tarım, teknoloji, endüstri ve savunma alanları olduğu ifade edilmektedir. Belirlenen alanların modernleşmesi, batıyı örnek alması programın ortak hedefleri arasında yer almaktadır. Bunun yanında, Mao döneminde uygulanan birçok politika, kültürel devrim ve yabancı düşmanlığı dolayısıyla ÇHC iktisadi açıdan büyük zarara uğramaktadır. Deng, bu düşünce doğrultusunda Mao’nun uygulamış olduğu bazı ilkeleri ortadan kaldırarak durumun iyileştirilmesi adına adım atmaktadır (Saray ve Gökdemir, 2007: 664-665). Bu bağlamda Deng, ÇHC’nin reformlarda başarıyı yakalayabilmesi için, Batı’dan özellikle ABD ve Japonya’dan ve Asya Kaplanlarından (Tayvan, Singapur, Hong Kong ve Güney Kore) örnek alınması gerektiğinin vurgusunu yapmaktadır (Demirel, 2019: 36-37).

Öte yandan, Mao’nun ÇHC adına belirlemiş olduğu en önemli amaç kendi kendine yetecek seviyeye gelebilme durumu olduğundan dolayı Çin’in, kapılarını dış dünyaya kapatarak tamamen kendi içinde belirlediği merkezi planlamaya yöneldiği gözlemlenmektedir. Dış dünyaya kapalı bir tutum sergilemesi ÇHC’nin teknoloji hususunda geri kalmasına ve yabancı yatırımın ülkeye sokulmamasına neden olmaktadır. Deng döneminde ise bu tamamen tersi bir durum hâline gelmektedir. Deng bu dönemi, *kapıları dış dünyaya yeniden açmakla* başlatmaktadır. Mao döneminde teknoloji ve yabancı sermaye hususundaki gerilemeden sonra Deng dönemindeki Çin hükûmeti, *yabancı sermaye ve modern teknolojinin ülkeye gelmesi* önündeki engelleri kaldırmak amacıyla, 1980’li yılların başında birtakım politik ve yasal düzenlemeler yapmaktadır. Bununla birlikte, belirlenen yeni yasalarla beraber yabancı şirketlerin ÇHC’ye yatırım yapması ve Çinlilerin yabancılarla ortaklık kurması teşvik edilmektedir. Aynı zamanda bu süreçte, 1955 yılında askıya alınan Çin Anayasası yeniden düzenlenerek yürürlüğe konulmaktadır. Diğer yandan ise ÇHC’nin deniz kıyısındaki eyaletlerde özel bölge oluşturularak piyasa ekonomisine geçiş için örnek modeller geliştirilmeye çalışılmaktadır (Özsoylu, 2006: 19-20).

ÇHC'nin Deng dönemiyle beraber dışa açık bir yol izlemek adına yapmış olduğu düzenlemelere bakıldığında ise şu adımların atıldığı görülmektedir (Çalık, 2011: 193-194):

- İlk olarak 1979 yılında *Çin ve Yabancı Sermaye Ortak Girişimler Yasası* çıkarılmaktadır. Çıkarılan bu yasa ile yabancı yatırımlara resmen izin verilmektedir.
- 1983 yılında *Ticarî Markalar Yasası* oluşturulmaktadır.
- 1985 yılında *Patent Yasası* ve aynı yıl *Yabancılarla Ekonomik Sözleşmeler Yasası* yürürlüğe konulmaktadır.
- Yabancı sermaye alanında atılan önemli adımlardan bir diğeri ise 1986 yılında yabancıların ÇHC'de yatırım yapmak amacıyla sermayenin yarısına ortak olacak bir Çinli yatırımcı bulmalarına gerek duyulmasının önündeki engeli kaldıran *Tamamen Yabancıların Mülkiyetindeki İşletmeler Yasası* çıkarılması olmaktadır.
- 1988 yılında ortak işletmelerle ilgili yeni düzenlemelere gidilmesi noktasında yeniden *Çin ve Yabancı Sermaye Ortak Girişim Yasası* çıkarılmaktadır.
- 1990 yılında kentsel toprakların uzun dönemli oluşturulmasına ilişkin yönetmelikler uygulamaya konulmaktadır.
- Yabancı yatırım ve serbest piyasa ekonomisinin güçlendirilmesi adına atılan bir diğ er önemli adımlar; 1991 yılında *Telif Hakları Yasası* ve 1993 yılında *Şirketler Yasası*'nın çıkarılması olduğu belirtilmektedir.
- 1994 yılında yürürlüğe giren yasalar; *Haksız Rekabetin Engellenmesi Yasası*, *Tüketici Hakları Yasası*, *Dış Ticaret Yasası* ve *Ticarî Bankalar Yasası* şeklinde sıralanmaktadır.
- 1997 yılında *Fiyat Yasası*, 1998 yılında *Hisse Senetleri Yasası*, 2002 yılında *Kırsal Arazi Kiralama*, 2003 yılında *Bankacılık Düzenleme Yasası*, 2007 yılında *Mülkiyet Yasası* ve 2008 yılında ise *Tekelleşmeyi Önleme Yasası*'nın çıkarıldığı görülmektedir.

Bu bağlamda, 1978 yılı itibariyle serbest piyasanın, yabancı yatırımların, para ve sermaye piyasalarının güçlendirilmesi adına ÇHC'de birçok yasal düzenlemelere gidildiği görülmektedir. Bu yasal düzenlemeler uzun süreçleri kapsamaktadır. Yasal

düzenlemeler dolayısıyla kurulacak olan yeni ekonomik yapının hukuksal zemininin bu şekilde hazırlanmış olması planlanmaktadır.

Tüm bu gelişmeler ışığında, 1978 yılından beri ekonomiye öncelik veren ÇHC'nin, 1980'lerden itibaren kesintisiz olarak ekonomik büyümeye sebep olacak reformlara imza attığından dolayı, bu duruma ekonomik kalkınma literatüründe “Çin özgünlüğünde sosyalizm” dendiği görülmektedir. Bu reformların iki ayağı bulunmaktadır. İlk ayağı; kolektif tarım üretim sisteminden vazgeçilmesi, tarımda yapılan özelleştirmeler ile özel teşebbüs faaliyetlerine ve yabancı sermayeye müsaade verilmesi, düşüncesi oluşturmaktadır. 1980'li yılların sonuna gelindiğinde ise reformların ikinci ayağı devreye girmektedir. Reformların ikinci ayağında; devlete ait bazı sanayi kuruluşları özelleştirilmektedir. Aynı zamanda fiyat kontrolleri önemli oranda gevşetilmiş ve korumacı sanayi politikalarından vazgeçildiği belirtilmektedir. Ancak, enerji ve bankacılık gibi stratejik öneme sahip sektörler devlet kontrolünde kalmaya devam etmektedir (Aslan, 2014: 31-32).

Diğer taraftan, Deng'in iktidara gelmesiyle beraber yapılan reform hareketlerinin birtakım ideolojik ve politik tepkilere maruz kaldığı görülmektedir. Bu tepkilerin bir kısmı özgürlük ve demokrasi isteyen öğrenciler tarafından gelmektedir. Öğrencilerden gelen tepkiler/protestolar ilk olarak 1986 yılında başlamaktadır. Fakat 1989 yılında yapılan protestoların ÇHC tarihine büyük bir etki bıraktığı görülmektedir. 4 Mayıs 1989 yılında ÇHC'nin başkenti Pekin'de yer alan Tiananmen Meydanı'nda bir araya gelen öğrenciler hükûmetten bazı taleplerde bulunmaktadır. Öğrencilerin talepleri şu şekilde belirtilmektedir (Adıbelli, 2016: 85-86):

- Politik ve ekonomik reformların hızlandırılması,
- Anayasal özgürlüklerin garanti altına alınması,
- Yolsuzluklara karşı mücadele edilmesi,
- Basın özgürlüğünün sağlanması.

Yapılan bu gösteriler karşısında kaygılanan Çin hükûmeti olaylara nasıl müdahale edeceği konusunda kararsız kalmaktadır. Tiananmen Meydanı'na protestocuların çadırlar kurup açlık grevi çağrıları yapmasıyla beraber Çin hükûmeti ilk olarak sıkıyönetim ilan etmektedir. Daha sonra yapılan protestoların büyümesi sonucunda kendi rejimini tehdit ettiğini hisseden Çin hükûmeti olaya askeri müdahale kararı almaktadır. Askeri müdahale ile oldukça sert bir şekilde protestoları bastıran Çin ordusu bu müdahale sonucunda çok sayıda protestocunun öldürüldüğünü

açıklamaktadır. Dünya kamuoyu tarafından kınanan bu sert müdahalenin akabinde, ABD ve AB başta olmak üzere birçok ülke ÇHC'ye yaptırım uygulamaya başlamaktadır (Aras, 2018: 52-53).

Bunun yanı sıra, Deng döneminde gerçekleştirilen reform sürecinde karşılaşılan bir diğer önemli olay ise 1992 yılında Deng'in ÇHC'nin güneyine seyahat ederek özel ekonomik bölgeleri gezmesiyle gerçekleşmektedir. Söz konusu bölgede yer alan eyaletlerde oluşturulan özel ekonomik bölgeler, önemli bir büyüme göstermektedir. Ön görülen büyüme oranından çok daha yüksek bir büyüme ile karşılaşılmaktadır. Büyük ölçekli yatırımlar yapılan bu bölgelerdeki gelişmelerden çok memnun olan Deng, gezi sonunda ÇHC'de iktisadi reformların daha da genişletileceği ve sürekliliğinin sağlanacağını ilan etmektedir. Bu netice doğrultusunda, 1992 yılının Ekim ayında yapılan ÇKP'nin 14. Kongresinde “*sosyalist piyasa ekonomisine*” geçiş resmen kabul edilmektedir (Özsoylu, 2006: 25).

Başka bir yönden bakıldığında, SSCB'nin yıkılması ve küreselleşmenin ivme kazandığı süreçlerde birçok ülkenin olumsuz yönde etkilendiği görülmektedir. ÇHC'nin de bu süreçte gücünün kaybedileceği düşünülse de tam tersi bir durum yaşandığı belirtilmektedir. Yani bu durumda 21. yüzyıla güçlü bir devlet olarak giren ülkelerden biri olan ÇHC, özellikle iktisadi yönden önemli bir konuma ulaşmaktadır. Bununla beraber, sosyalist piyasa ekonomisi atılımlarını devam ettiren Deng, aynı zamanda sanayi atılımlarına da hız kesmeden devam etmektedir. 1992 yılından sonra yaşanan olumsuzluklara rağmen Çin liderleri özgüvenine yeniden kavuşmaktadır. Aynı zamanda Deng ekonomik reformunu yeniden canlandırmak adına olumlu yönden sinyaller vermektedir. Bu durum da ikinci reformun başlamasını sağlamaktadır. Böylece ÇHC'de ikinci reform dalgasının başlamasıyla, kaynak ve ham maddeye olan ihtiyaç Pekin'in geliştirmekte olan dünyaya ilgisini daha da artırmaktadır (Scobell vd., 2018: 18-19).

Öte yandan, 1997 yılına gelindiğinde Deng'in hayatını kaybettiği bilinmektedir. Her ne kadar 1993 yılında iktidar değişikliği açısından yapılan bir tercihle Jiang Zemin ÇHC'nin başına gelse de Deng' in ölümüne kadar olan sürede ÇHC siyasetine önderlik ettiği bilinmektedir. Reform süreci boyunca Jiang, Deng'i desteklemektedir. Bundan dolayı yönetime geçtikten sonra dahi Deng'in hayata geçirdiği reformların sürekliliğini koruyarak yeni reform projelerini yürürlüğe koymaktadır. 2002 yılına gelindiğinde ise ÇHC Hu Jintao önderliğinde yeni bir liderlik yönetimine geçmektedir. Hu genel olarak inandıkları hususlarda inatçı bir kimlikle tanınmaktadır. Jiang döneminde yürütülen

kampanyalarda aktif rol oynamaktadır. Yoksullukla mücadele hususunda yaptığı çalışmalarla dikkat çeken Hu döneminde ÇHC ekonomisinin oldukça hızlı büyüdüğü görülmektedir. Fakat bu dönemde yolsuzluk ve eşitsizlikten dolayı tepkilerle karşı karşıya kalınmaktadır. Hu döneminin sonlarına doğru ekonomide yavaşlamaların olması ve yabancı firmaların ÇHC'den çekilmesinden dolayı işsizlik oranında hızlı artış olmaktadır. Hu döneminin sonlarına doğru ortaya çıkan çatışmacı politikalarla beraber Deng döneminde başlatılan reform döneminden daha farklı yeni bir döneme gelindiği söylenmektedir (Atawula, 2020: 21-24).

Bu doğrultuda, 2012 yılına gelindiğinde ÇHC'de yeni bir dönem başlamaktadır. ÇKP 18. Kurultayında Xi Jinping ÇHC Devlet Başkanı seçilerek ülkenin başına geçmektedir. Xi'nin başkan olmasıyla sadece liderlik değişimi gerçekleşmemektedir. Aynı zamanda 1978'den beri süre gelen reformlarında değiştiği belirtilmektedir. Xi döneminden sonra ÇHC, tarihindeki en güçlü konumuna ulaşmaktadır. Deng'le başlayan ekonomik büyüme Xi ile tamamlanmaktadır (Çalışkan, 2022: 9). Bu bağlamda, Xi liderliği eline aldıktan sonra Deng'in ilerletmiş olduğu kalkınma modeline yeni bir boyut kazandırarak Eylül 2013'te "Bir Kuşak Bir Yol (BKBY)" ya da diğer bir adı "Yeni İpek Yolu Projesi" olan projeyi başlatarak kalkınmada yeni bir dönemin başlamasını sağlamaktadır (Çakan, 2017: 130). Bunun yanı sıra, Deng'den sonra ÇHC'de lider olan isimler hakkında detaylı analiz farklı başlıklarda yapılmaktadır. Fakat kısaca, ÇHC'nin 21. yüzyıla geldiğinde güçlü devletler arasında yer almasını sağlayan önemli noktalardan söz etmek gerekmektedir. Çünkü bu hususlar ÇHC'nin gelişiminin önemli parçalarını oluşturan zincirin birer halkasını oluşturmaktadır.

Genel bir değerlendirme yapılacak olursa, ÇHC'nin 20. yüzyıl ve 21. yüzyıllarda önemli farklılıklarının olduğu görülmektedir. ÇHC'de her ne kadar 20. yüzyılda savaşlarla, ekonomik sıkıntılarla, ülkenin parçalanma tehlikesiyle ya da siyasi dengesizliklerle mücadele edilse de tüm bu olumsuzlukların ardından 21. yüzyıla geldiğinde çok daha güçlü bir varoluşla karşılaşılmaktadır. Dünyanın en hızlı ekonomik büyümesine sahip olan ÇHC, yürütülen politikalar dolayısıyla ekonomik ve sosyal alanda dengesizliklere maruz kalmaktadır (Mitter, 2012: 11-12). ÇHC yaşanan onca olay neticesinde 21. yüzyıla geldiğinde güçlü devletlerarasında yerini almayı başardığı tespit edilmektedir. ÇHC'nin bu başarıyı sağlamasına sebep olan atılımlar şu şekilde sıralanmaktadır:

- Karma ekonomiye geçiş yapması,

- ÇHC'nin birleşmesi,
- Kentleşme Devrimi,

Yukarıdaki maddelerde belirtildiği üzere ÇHC'nin 21 yüzyılda güçlü devletlerarasına girmesini sağlayan başarılarından ilkinin, *karma ekonomiye geçmesi* olduğu söylenmektedir. Karma ekonomiye geçiş yapılan dönemde özel ekonomik bölgelerin sayısında artış görülmektedir. Bunun yanında, yabancı sermaye ve teknoloji transferinin de gün geçtikçe daha çok büyüdüğü söylenmektedir. ABD'den sonra dünyanın en büyük ikinci ekonomisine sahip olan ÇHC'nin ekonomisinin ilerleyen yıllarda daha fazla güçleneceği ön görülmektedir. Başarı elde etmesinde ki bir diğer durum, *ÇHC'nin birleşmesi* olduğu belirtilmektedir. ÇHC'de siyasi birliği sağlamak imparatorluk döneminden bu yana oldukça önemli bir hâl almaktadır. ÇHC'nin siyasi birliğini sağlamak adına bu dönemde iki önemli gelişme yaşanmaktadır. Bunlar; 1997'de Hong Kong'un, 1999 yılında ise Makao'nun ÇHC topraklarına katılmasıdır. Bu bölgelerin söz konusu topraklara katılımıyla beraber ÇHC'nin ekonomisinin giderek daha güçlendiği vurgulanmaktadır (Kavala, 2019: 221-227).

21. yüzyılda gerçekleşen en önemli atılımlardan bir diğerinin ise *Kentleşme Devrimi* olduğu belirtilmektedir. Tarım toplumu olan ÇHC için kırsal alanlar oldukça önem arz etmektedir. ÇHC'nin 1978'den sonra sanayileşmeye başlamasıyla kentleşmenin de giderek hız kazandığı görülmektedir. Diğer yandan, uzay araştırmalarının başlaması 21. yüzyılda ÇHC'nin dünyada önemli güç olduğunu gösteren bir diğer husus olarak karşımıza çıkmaktadır. Bunun yanında bir diğer gelişme ise, iki kutuplu dünya düzeni oluşturmak adına Asya Bloğunu yaratmaktır. Bu bloğu oluşturmadaki amaç; tek kutuplu dünya düzenine karşı, anlaşmalı devletlerin, bilhassa ekonomik anlamda, ortaklaşa hareket edebilecekleri kutupları oluşturmaktır. Bu dönemde yaşanan gelişmeler ışığında ÇHC, giderek önemli bir güç hâline gelmektedir (Kavala, 2019: 221-239).

Son olarak dışa kapalı bir ülkeyken dışa açık bir devlete dönüşen ÇHC'nin bu hususta yapmış olduğu önemli olaylardan biri, 2008 yılındaki olimpiyatların ÇHC'de düzenlenmesidir. Olimpiyatların ÇHC'de düzenlenmesi bir dönüm noktası niteliği taşımaktadır. Bir diğer önemli olay ise 2001 yılında Dünya Ticaret Örgütü'ne katılımın gerçekleştirilmesi olarak karşımıza çıkmaktadır. Aynı zamanda dışa açılmak adına atılan önemli adımlardan bir diğerinin, 2004 yılında yapılan anlaşma ile ÇHC'ye sınırsız ihracat yapma hakkı tanınması olduğu söylenmektedir. Bu durumda yüksek

kapasiteli tesisler ve ucuz emek ile ÇHC kendine önemli bir pazar payı almış bulunmaktadır (Karamanoğlu, 2020: 47-48).

2.2. Dış Politika

Devletlerin, belirlemiş oldukları hedefler ve ilkeler doğrultusunda bir başka devletlerle kurduğu bağlantı dış politikaların en geniş tanımı olarak karşımıza çıkmaktadır. Dış politikalar uluslararası sisteme bağlılığından dolayı dönemsel olarak farklılık göstermektedir. Bu farklılıklarda söz konusu olan hususlar; dış politikada egemen ya da öne çıkan temalar, tercihler ya da yaklaşımlar, uluslararası ilişkilerin dünya çapında büründüğü biçimler olarak belirtilmektedir. Dış politikalarda genellikle doktrinlerin ya da faydacılığın, ulusal çıkarların ya da ideolojilerin öne çıktığı tercihler ön plana çıkmaktadır. Birçok ülkede farklı dönemlerde değişen dünya koşulları dolayısıyla o dönemin şartlarına göre uyarlanan dış politikalar bulunmaktadır. Bu durum ÇHC’de, kurulduğu 1949 yılından beri geçerli olmaktadır. Yani ÇHC’de farklı dönemlerde değişen dünya düzeni doğrultusunda dış politikalar uygulamaktadır (Güler, 2001: 283).

Bununla beraber, ÇHC’nin gelişim süreci sonrasında, dünya ekonomisi başta olmak üzere bölgesel ve küresel hadiselerde söz sahibi olan önemli güçlerden biri hâline geldiği görülmektedir. Küreselleşmenin etkisinin belirgin bir şekilde görüldüğü ve Soğuk Savaş’ın sona ermesiyle izlerinin devam ettiği 1990’lı yıllar sonrası tek kutuplu dünya düzeninin yerini çok kutuplu dünya düzeninin alması, ÇHC’nin dünyaya karşı bakışının ve dış politikasının değişmesine sebep olmaktadır. Soğuk Savaş sürecinde güç ve savaş odaklı saldırgan bir politika izleyen ÇHC, savaş sonrasında bu politik tutumunu terk ederek yerine barış ve kalkınma temelli dış politikasını benimsemektedir (Harris, 2014: 64).

Öte yandan, BMGK’de veto yetkisine sahip olması ve nükleer silah kapasitesinin olması durumu politika üzerindeki etkisini güçlendirmektedir. Bundan dolayı uluslararası siyasette önemli bir aktör olan ÇHC’nin, dış politikasına bakıldığında çok yönlü bir politika geliştirdiği görülmektedir. Bu bağlamda, ekonomik yönden gelişmeye önem veren ÇHC’ye göre barış ve ekonomik kalkınma iç içe geçmiş konular olarak karşımıza çıkmaktadır. Yurtiçi ve yurtdışı barış ortamının sağlanması durumunda ekonomik kalkınmanın sağlanacağı düşünülmektedir. Bunun sağlanması

içinde başarılı bir dış politikaya ihtiyaç duyulmaktadır. ÇHC dış politikası şu çerçevede şekillenmektedir (Ekrem, 2003: 66):

- Büyük ülkeler ile ilişkilerini güçlendirmek,
- Kendi gibi gelişmekte olan ülkelerle ortaklık yapmak,
- Komşu ülkelerle ilişkilerini güçlendirmek.

Diğer taraftan ise ÇHC ekonomik alanda her ne kadar gelişim gösterip büyük bir güce sahip olsa da askeri ve siyasi olarak tam anlamıyla bir süper güç olamamaktadır. Bundan dolayı diğer devletlerle olan ilişkilerinde ve dış politikasında halkın çıkarlarını göz önünde bulundurarak bağımsızlık ilkesini resmi söylem olarak ele almaktadır. Bununla beraber, ÇHC'nin dış politikasındaki ideolojiyi oluşturan hususlar şu şekilde sıralanmaktadır (Sayın, 2013: 229):

- Millet egemenliği ve toprak bütünlüğüne saygı çerçevesinde dünya barışını inşa etme,
- İnsan haklarına saygı,
- Ticari ilişkiler kurulan ülkeler ile ortak kalkınma,
- Uluslararası ilişkilerde dostça ilişki kurmak, bu ilişkileri geliştirmek ve sürdürmek.

Bu doğrultuda, “barış içinde bir arada yaşama” prensibi ile barışçı bir tutum sergilediğini ve bu yönde hareket ettiğini gösteren ÇHC'nin uluslararası barışı sağlamak adına beş ilkesi bulunmaktadır. Bu ilkelerin gerçekleşmesinin gerekliliği ön koşul olarak görülmektedir. Söz konusu ilkeler şu şekilde sıralanmaktadır (Qimao, 2005: 57):

1. Eşitlik
2. Egemenlik ve toprak bütünlüğüne saygı
3. Karşılıklı barış içinde yaşama
4. Karşılıklı saldırmazlık
5. İç işlerine karışmama prensibi

“Barışçıl Yükseliş” politikasını temel alan ÇHC dış politikasında öncelikli olarak önem verilen husus; ulusal güvenliği sağlamak ve uluslararası alanda istediği yumuşak güç imajını iyileştirmek olduğu düşünülmektedir (Aktaş, 2019: 8).

Ek olarak, ÇHC'nin dış politikasının köklerine de bakılacak olursa; tarihsel miras, dünya görüşü, milliyetçilik ve Marksizm, Leninizm ve Maoizm faktörlerine dayanmaktadır. Söz konusu faktörler, ÇHC'nin ekonomik ve askeri yeteneği, yönetsel yapısı ve karar verme süreciyle birleşerek güvenlik, bağımsızlık, egemenlik,

toprak bütünlüğü ve ekonomik gelişme gibi önemli dış politikalarını oluşturmaktadır (Karaaslan, 2012: 138). Çin dış politikasının oluşumuna etki eden etmenler ve karar verme süreçleri, değişimi ve sürekliliği gibi hususlar ayrı başlıklar altında incelenmektedir.

2.2.1. Dış Politikanın Oluşumundaki Faktörler ve Karar Verme Süreci

Dış politika oluşturulurken iki türlü etmenin karşımıza çıktığı görülmektedir. ÇHC liderleri de bu iki etmen çerçevesinde dış politikaları oluşturmaktadır. Söz konusu etmenler iç etmenler ve dış etmenler olarak ayrılmaktadır. ÇHC açısından iç etmenlere verilebilecek en önemli örneğin ‘ekonomi’ olduğu belirtilmektedir. ÇHC’nin elde ettiği başarının en önemli aracı olan ekonomi, ÇKP yönetimini meşrulaştıran en önemli faktör olarak karşımıza çıkmaktadır. Ekonomi hususunda yaşanacak herhangi bir gerileme ÇKP yönetiminin meşruluğuna ve aynı zamanda ÇHC’nin kararlılığına darbe vuracağı öngörülmektedir (Harris, 2014: 182-183). ÇHC açısından dış etmenlere bakıldığında ise, bu etmenler ÇHC’nin niyetlerine, hedeflerine ve algısına göre değişmektedir. Uluslararası ortamın önemli güçlerin hesaplarını da göz önünde tutma zorunluluğu bulunmaktadır. Bu güçler; ABD, Japonya, Rusya ve diğer güçler olarak sıralanmaktadır (Harris, 2014: 67).

Bunun yanı sıra dış politikaların, değişen dünya düzenine uygun bir şekilde, o dönemin koşullarına göre uygulandığı görülmektedir. Bundan dolayı ÇHC’nin dış politikasına ve karar verme sürecine etki eden bazı faktörlerin olduğu tespit edilmektedir. Söz konusu faktörler şu şekilde ele alınmaktadır:

- **Kültür Faktörü:** Bir devletin dış politika içeriği ve hedeflerini belirlemede etkili olan faktörlerden biri olan kültür, yönlendirici özelliği dolayısıyla birçok hususa telkin etmektedir. Bu hususlar kısaca; değer arayışı belirleme, karar vericileri etkilediğinden dolayı devletin dış politikasını belirleme, dış politika yapım mekanizması ve süreci, temel siyasi sistemi, dış politika uygulama ve uygulama araçlarının belirlenmesi şeklinde sıralanmaktadır. Söz konusu hususlar ülkenin kültürüne göre şekil almaktadır. Yalnızca diplomatik kararları etkileyen kültür, tek başına belirleyici bir faktör olmamakla beraber diğer faktörlerle birleştiği ve içine girdiği zaman etkili olabilmektedir. Bundan dolayı bir ülkenin dış politikasının kültürel bir bakış

açısıyla incelenmesi ve tetkik edilmesi, dış politika çalışmalarına farklı bir bakış açısı kazandırmaktadır (Qingmin, 2003: 36-38).

- **İdeoloji Faktörü:** Dış politikaların uygulanması noktasında etkili olan ideoloji faktörü, dolaylı ve mekanizması karışık bir faktör olarak karşımıza çıkmaktadır. İdeoloji faktörünün dış politika açısından 3 özelliği bulunmaktadır. Bunlar; davranışa rehberlik etme, rasyonalizasyon ve toplumsal bütünleşme işlevi şeklinde sıralanmaktadır. Herhangi bir ülke diğer ülkelerin gerçek politika isteklerinin bilinmesini istemiyorsa, kendisini gizleyerek dış politika konumunun adaletle uyumluluğunu gösterme durumunda ideolojiyi kullanmaktadır. Bazı durumlarda ideoloji gizlense de, ülke içinde, tüm sosyal grubun beraberliğini sağlamada ‘birlik için çimento rolü’ oynamaktadır (Xiao vd., 2003: 5-7).
- **Enerji Faktörü:** Askeri ve ekonomik güç için büyük bir öneme sahip olan enerji, ulusal güvenlikte yaşamsal bir konuma sahip olan siyasallaştırılmış bir sermaye olarak karşımıza çıkmaktadır. Enerji isteğinden dolayı diğer petrol ithalatçısı ülkelerle çatışma olasılığı artan ÇHC, aynı zamanda enerji ithalatçısı bir ülke olarak petrol ithalatı tehdidi almaktadır. Bu durum ÇHC’nin diğer ülkelerle çok yönlü organizasyonlarda daha fazla seferberlik yapmasına sebep olmaktadır. ÇHC’nin istikrarlı bir şekilde hızla büyüyen enerji talebi uluslararası ortam oluşturma hususunda etkin rol oynamaktadır. Oluşan bu ortam ekonomik kalkınmaya elverişli olduğundan, ÇHC’nin dış ülkelerle olan ilişkilerde işbirlikçi bir yaklaşım benimsemesini sağlamaktadır. ÇHC’nin ilkelerinden biri olan ‘iç işlerine karışmama ilkesi’ dolayısıyla daha güvenilir enerji kaynakları arayışına yardımcı olmaktadır (Chigurh, 2006: 37-39).
- **Uluslararası Durum Faktörü:** Ülkeler arasındaki tüm karşılıklı ilişkilerin ve dinamiklerinin var olan durumu, uluslararası durum olarak ifade edilmektedir. İki kutuplu modelin ve birden fazla gücü ifade eden tek bir süper gücün uluslararası duruma ait olduğu söylenmektedir. Dünyanın gelişimi noktasında uluslararası durum göz ardı edilmemektedir. Uluslararası ortamın önemini belirten en iyi örnek yakın zamanda yaşanmaktadır. 2019 Aralık ayında başlayan Covid-19 salgınıyla beraber Çin diplomasisinin, salgına karşı yerel ve küresel mücadelede aktif rol oynadığı görülmektedir.

İnsanlık adına büyük bir sorumluluk üstlenen ÇHC, küresel yönetişimin maruz kaldığı sorunlarla karşı karşıya kalmaktadır. Bundan dolayı ÇHC, diğer büyük güçlerle ilişkilerini aktif olarak yönetmektedir. ÇHC'nin büyük güçlerle olan ilişkileri çerçevesinde genel olarak istikrarlı ve dengeli gelişim sağladığı belirtilmektedir (Nabijiang, 2022: 53).

Yukarıda söz konusu olan faktörlerin çeşitliliğinden dolayı ÇHC'de dış politikada karar verme sürecinin karmaşık bir hâl aldığı görülmektedir. ÇHC'de karar verme sürecine ilişkin bilgi erişimi sınırlı tutulmaktadır. Genel olarak dış politikada, siyasi rekabetle doğru orantılı görülen güç ve siyaset iç içe geçmiş bir hâl almaktadır. Batılı devletlerde siyasi rekabet kamuoyuna açık bir şekilde yapılırken ÇHC'de bu durumun tam tersi olduğu belirtilmektedir. ÇHC'nin karar verme sürecinde birden fazla aktör rol oynamaktadır. Belirtilen aktörler şu şekilde sıralanmaktadır (Demirel, 2019: 40):

- Politbüro Yürütme Komitesi
- Devlet Konseyi
- Dışişleri Bakanı
- Ordu (Genel Kurmay Departmanı, İkinci Topçu Birliği, Çin Halk Kurtuluş Ordusu)

Diğer yandan, küresel diplomasi ve bilgi kaynakları ÇHC dış politikasının karar verme sürecinde önem arz eden hususlar olarak karşımıza çıkmaktadır. Küresel diplomasiinin ekonomi ağırlıklı olduğu belirtilmektedir. Uluslararası entegrasyonda yaşanan artışlar ÇHC'de merkezi bakanlıklar ile kurumların örgütsel, ulusal ve uluslararası ajanslarla doğrudan ilişkilerini geliştirmektedir. Bundan dolayı, ÇHC'de konsoloslukların sayısında ciddi artışlar görülmektedir. Bilgi kaynaklarının ise, birçok ajansın yapmış olduğu analizler doğrultusunda karar alma süreçlerini etkilediği tespit edilmektedir. Bu doğrultuda internetin kullanımı, devletin sıkı kontrolünde olmasına rağmen dış politika karar verme sürecinde etkili olabilmektedir. Genel olarak, ÇHC dış politikası karar verme sürecinde birçok aktörün olmasından dolayı karmaşık bir yapı gözlemlenmektedir. ÇHC birçok alanda olduğu gibi bu alanda da kendine özgü bir biçimde gelişmektedir. Bu durum ise ÇHC'nin karar verme sürecinde ortak kararda uyuşmasını zorlaştırmaktadır. Neticede bu durum, ÇHC'nin uluslararası müzakere pozisyonunu karmaşık hâle getirmektedir (Harris, 2014: 45-62).

2.2.2. Dış Politikada Dönüşüm Süreci ve Süreklilik

ÇHC, 1978 yılı Deng dönemi itibariyle, barışçıl kalkınma stratejisinin başarılı olabilmesi için uluslararası sistemde ÇHC yararına barışçıl bir dış politikanın oluşturulması gerekliliğinin vazgeçilmez olduğunu sürekli vurgulamaktadır. Bundan dolayı Deng döneminde oluşturulan ÇHC'nin dış politikasında, ülkenin ekonomisine hizmet edecek çerçevede hareket edildiği görülmektedir. Bununla beraber, ÇHC'nin dış politika amaçları arasında uluslararası ekonomik düzeni değiştirme, iyileştirme fikri her zaman öncelikli hedef olmaktadır (Xiaoping, 1994; Yıldırım, 2017: 17).

Karmaşık bir yapıya sahip olan ÇHC dış politikası; ÇHC'nin dünyayı kavrama şekliyle uluslararası olayların, liderlerin fikirleri vs. gibi nedenlerden dolayı dönemsel olarak değişikliğe uğramaktadır. Söz konusu değişimler farklı başlık altında ele alınmaktadır. Diğer yandan, ÇHC'nin dış politika dönüşüm sürecine bakıldığında Soğuk Savaş sırasında ve Soğuk Savaş sonrasında belirlenen politikaların tamamen farklı olduğu görülmektedir. Bu farklılıklar dönemsel ve liderlere bağlı farklılık gibi görünse de aslında ÇHC dış politikası geçmişten gelen olaylara göre şekillenmektedir. Bu durum iki unsur ile ifade edilmektedir. Bunlar: “mağduriyet hissi” ve “hainlik sendromu” olarak belirtilmektedir. Mağduriyet algısı, Afyon Savaşları sonrasında “utanç yüzyılı” olarak adlandırılan dönemin vermiş olduğu bir etki olarak karşımıza çıkmaktadır. Bu dönemde ortaya çıkan mağduriyet algısı önemini yitirmiş olsa da etkisi hâlâ devam etmektedir. Bu algı ÇHC'de güvensizlik ve zayıflık hisleriyle bağlantılı tutulmaktadır. Bu durum ÇHC'yi tarihsel olarak şartlandırmış bir egemenlik hassasiyetine ve kapsamlı olarak güç geliştirmeye itmektedir. Bir diğer unsur olan hainlik sendromu ise ÇHC'nin 19. yüzyıldaki zayıflığı için bir başkasının suçlanması gereksiniminden ortaya çıkmaktadır. Hainlik sendromunu ortaya çıkaran bazı hususlar şu şekilde sıralanmaktadır (Harris, 2014: 17-30):

- Çinlilerin yabancıların gücüne göre daha zayıf konumda müzakerelere katılması,
- Bazı Çinli yetkililerin kendi çıkarları için Japon işgali sırasında yabancılarla iş birliği yapması.

Bununla beraber, ÇHC yetkililerinin her alanda olduğu gibi dış politika alanında da sürekliliği desteklediği görülmektedir. İster bölgesel olsun isterse uluslararası alanda olsun, yaşanılacak herhangi bir istikrarsızlık durumu ÇKP'nin otoritesinin sorgulamasına ve ÇHC'nin ekonomisinin kötüye gitmesine sebep olacağı

düşünülmektedir. Aynı zamanda küreselleşmenin etkiyle diğer ülkelerin de bundan olumsuz yönde etkileneceği vurgulanmaktadır. Neticede yaşanılacak istikrarsızlık durumunda, iç ve dış politikanın büyük oranda etkileneceği belirtilmektedir (Demirel, 2020: 42).

2.3. Dönemsel Açıdan Dış Politika

2.3.1. Mao Zedong Dönemi (1949-1976)

ÇHC siyasetinin ana kurucusu olan Mao Zedong aynı zamanda dış politikanın ana karar vericisi olmaktadır. 1949 yılında ÇHC'nin kuruluşuna önderlik eden Mao, bu sürecin başlangıcında dış politikayı şekillendirecek üç önemli siyasi karar önermektedir. Bunların; “Yeni Bir Soba Yakmak”, “Ev Temizlemek ve Sonra Misafirleri Davet Etmek” ve “Bir Tarafa Yaslanmak” şeklinde olduğu belirtilmektedir. Çin dış politikasının ana içeriğini oluşturan bu yönergeler; uluslararası kararda, uluslararası tanınma, uluslararası yardım ve ulusal güvenliğin korunması için çaba gösterme hususuna odaklanmaktadır. Bunun yanında ÇHC'nin stratejik tercihlerine bakıldığında ABD ve SSCB arasında tarafsızlığı koruyabilecek olanağa sahip olduğu görülmektedir. Fakat ÇKP, “tek tarafa yaslanma” politikasını daha önce uyguladığı için ABD'nin ÇHC'ye ait politikasının geçiş dönemini ve ABD ile uzlaşma fırsatını değerlendiremediği ifade edilmektedir. Bu durum, ÇHC-ABD çatışması gibi hususlara yol açmaktadır (Mianli, 2013). ÇHC'nin kuruluşuyla beraber belirlemiş olduğu üç politikayı açıklamak anlaşılmaması noktasında faydalı olmaktadır.

‘Yeni Bir Soba Yakmak’, “sıfırdan başlamak” olarak da adlandırılan bu politika, Xibaipo döneminde ÇKP tarafından oluşturulan dış politikalardan biri olarak karşımıza çıkmaktadır. Bu politikanın temel içeriği; yabancı devletler tarafından eski Çin’de görevlendirilen diplomatik kadroyu tanımamak ve Kuomintang ve diğer ülkelerin gerici hükûmeti tarafından kurulan diplomatik ilişkileri tanımamaktır. Söz konusu politikanın bazı önerileri bulunmaktadır. Bu öneriler; ÇHC’deki emperyalizmin ayrıcalıkları kaldırılmalı, ÇHC milletinin bağımsızlığı ve kurtuluşu gerçekleştirilmeli, her türlü aşağılayıcı diplomatik geleneğin prangaları kırılmalı ve diplomaside inisiyatif almalıdır, şeklinde belirtilmektedir. Bu bağlamda, Ocak 1949 yılında gerçekleştirilen Politbüro toplantısında Mao, emperyalizmin artık ÇHC’de meşru bir yeri olmadığını ve

emperyalizmi tanımak için acele etmediklerini vurgulamaktadır. Bu ifadelerle ÇKP dış politikasını netleştirmektedir (Sizhengwang.cn, 2021).

‘Evi Temizlemek ve Sonra Misafirleri Davet Etmek’ isimli politikada öncelikle ‘emperyalist güçlerin ülkedeki kalıntılarını temizlemek ve onlara faaliyet alanı bırakmamak, sonrasında ise diplomatik ilişkilerin kurulması hususunu ele almak’ düşüncesi yatmaktadır. Mao Ocak 1949 yılında, Stalin tarafından Xibaipo’ya gönderilen Sovyetler Birliği Komünist Partisi (SBKP) Politbüro üyesi Mikoyan ile yapmış olduğu görüşmede dış politika ile ilgili yaptığı konuşmasında; “diplomatik ilişkiler kurmadan önce evi temizlememiz ve ardından misafirleri davet etmemiz gerekir” demektedir. Yani ÇHC dış politikasının önceliği olduğuna vurgu yaparak gerçek arkadaşların önce gelebileceği fakat diğer konukların beklemesi gerektiğine dikkat çekmektedir. ÇHC’nin evi temizleme ve ardından misafirleri davet etme politikası, bağımsız ve barışçıl diplomasinin felsefesini yansıtmaktadır. Bu durum ÇHC’nin kendi egemenliğini sıkıca kavrama fikrini göstermektedir (Sizhengwang.cn, 2021).

‘Bir Tarafa Yaslanmak’ politikası Mao’nun, ÇHC’nin birleşik bir cephe oluşturmak adına SSCB, diğer ülkeler ve halk kitleleriyle bir ittifak kurmasının gerekliliğine inancı doğrultusunda, bu politikanın galibiyete ulaşmak adına ve bu galibiyeti sürdürme noktasında gerekli olduğu belirtilmektedir. ÇHC halkı ya emperyalizmden yana olmalı ya da sosyalizmden yana olmalı düşüncesini savunan Mao, üçüncü bir yolun olmadığını ve tarafsızlığın ise sadece bir kamuflej olduğunun vurgusunu yapmaktadır (Levi, 1953: 277). Söz konusu politika daha ÇHC kurulmadan önce Çinli liderler tarafından dile getirilmektedir. Komünist liderler, bu hususta başarılı olmanın SSCB desteğiyle olacağını hayati önemde görmektedir (Akdağ, 2023: 79). Bir tarafa yaslanmak dış politikasını çözmek ve uygulamak ülkenin sosyalist inşasına ve ileriki dönemde dış politikalar üzerinde derin etkiye sahip olmaktadır. Söz konusu politika, ulusal ekonominin inşası için acil kredi, ekipman, malzeme ve teknoloji gereksinimlerini çözmek ve ulusal ekonominin iyileşmesi ve güçlendirilmesine yardımcı olmaktadır. Söz konusu yardım noktasında, ÇHC kurulduğu andan itibaren SSCB’nin diplomaside aktif olarak destek verdiği görülmektedir (Nabijiang, 2022: 57).

Belirlenen bu politikalar dışında ÇHC’nin gelişimi hususu anlatılırken Mao Zedong’un izlemiş olduğu stratejilere daha önceki başlıklarda değinilmiştir. Mao Zedong ile ilgili ele alınan diğer hususlar da dış politikayı şekillendirecek adımlar

olarak karşımıza çıkmaktadır. Bu başlık altında yalnızca dış politikada önemli görülen hususlara yer verildiğini belirtmek gerekmektedir.

2.3.2. Deng Xiaoping Dönemi (1978-1992)

Mao Zedong'un vefat etmesiyle beraber 2 yıllık aradan sonra ülkenin başına geçerek önemli bir figür hâline gelen Deng Xiaoping, iyi bir stratejist ve düşünür olarak bilinmektedir. Bununla beraber, Deng yeni tarihsel süreçte dış ilişkilere rehberlik etmek adına eksiksiz ve sistematik bir düşünce sistemi oluşturarak biz dizi ilke ortaya koymaktadır. 11. ÇKP Merkez Komitesi'nin Üçüncü Genel Kurulu'ndan bu yana Deng partiyi, 'zihni özgürleştirme' ve 'gerçeği arama' ideolojik çizgisine bağlı kalmaya yöneltmektedir. ÇHC'deki temel çelişkilerin anlaşılması durumunun doğru şekilde çözülmesi, reform ve dışa açılım politikasının formüle edilmesiyle beraber aynı zamanda çağdaş dünyanın durumu ve özellikleri hakkında net ve gerçekçi bir anlayış kazanılmaktadır. Böylelikle doğru bir diplomatik stratejinin formüle edilmesi adına ideolojik temel sağlanmaktadır (Yi, 2004).

1990'lı yılların başında Deng, ÇHC'nin dış politikasının temel ilkesi olan "düşük bir profil izleme" adlı büyük stratejisini ilan ederek, ÇHC'nin düşük profil tutması ve belirsizlikler karşısında sakin kalması gerektiğini dile getirmektedir (Shambaugh, 2020: 14). Deng 1992 yılında yapmış olduğu bir konuşmasında ÇHC'nin hem ekonomik kalkınmaya odaklanarak hem de düşük bir profil izleyerek uluslararası ilişkilerde daha çok ağırlığa hâkim olunabileceğini vurgulamaktadır (Chen ve Wang, 2011: 197). 1990'lı yıllarda ifade edilen söz konusu stratejinin 1978 yılından itibaren fiili olarak uygulandığı söylenmektedir. Bir süre sonra "yirmi dört karakterli ilkeler" olarak anılan Deng'in dış politika stratejisinde söz konusu olan ilkeler şu şekilde ifade edilmektedir (Chen ve Wang, 2011: 197; Zhao, 2017: 296):

- Gelişmeyi sakince izleyin,
- Kendi konumunu güvenli hale getir,
- Yapılan değişikliklerin güvenle üstesinden gelin,
- Düşük profilde becerikli olun,
- Öne çıkmaktan kaçının,
- Bir takım katkılarda bulunun,

İlkelere genel olarak bakıldığında sabretmeye, dikkat çekmemeye ve önderlik etmemeye vurgu yapıldığı görülmektedir (Harris, 2014: 39).

Öte yandan, ÇHC'nin 1978 yılından itibaren ekonomik yapı, dış politika, içyapı vs. gibi hususlarda birtakım değişikliğe gittiği görülmektedir. Yapılan bu değişikliklerde en önemli faktörlerden biri, ÇHC dışındaki diğer Doğu Asya ülkelerinin büyük oranının daha yüksek bir ekonomik büyüme hızına sahip olması olarak gösterilmektedir. Yani ÇHC; Japonya, Hong Kong, Tayvan, Singapur ve Güney Kore gibi Doğu Asya ülkelerine oranla daha düşük hızla ekonomik ilerlemeye sahiptir (Westad, 2013: 406). Söz konusu Doğu Asya ülkeleri, diğer ülkelerin büyümediği kadar hızlı büyüme gösterdiğinden dolayı bu durum ÇHC'nin ekonomik sistemini yeniden yapılandırmaya itmektedir (Vogel, 2017: 2).

Bir diğer faktör ise karar alıcılardaki değişim ve aynı zamanda karar alıcıların kendi ülkelerinin gücüne ve uluslararası düzene yönelik algılarında yaşanan değişimi olarak karşımıza çıkmaktadır. Bu doğrultuda, 1978 yılında Deng'in başa gelmesiyle beraber ÇHC'nin dönüm noktası yaşanmaktadır. Deng kontrolü ele aldıktan sonra "reform ve dışa açılım" politikası dönemine girilerek barış ve kalkınma hususları ÇHC'nin önceliği hâline gelmektedir (Zhu, 2010: 21). Ekonomik kalkınma odaklı politika izleyen Deng ile beraber ÇHC'nin artık temek yönelimini belirleyen unsurun ekonomi olduğu belirtilmektedir. Bu bağlamda çağdaş bir ÇHC oluşturmak adına yapılan hamlelere bakıldığında; teknoloji, yatırım, yardım ve uzmanlığa katkı sağlayabilecek gelişmiş ülkelerle bağların iyileştirilmesi gibi hususların Deng ile beraber ÇHC dış politikasının önceliği hâline geldiği vurgulanmaktadır (Zhao, 2017: 304).

Diğer yandan, Deng'in dış politika adına çeşitli diplomatik düşüncelerinin olduğu belirtilmektedir. Bunlardan birinin, "tek hat" ve "geniş alan" stratejisi olduğu ifade edilmektedir. Bu strateji yeniden düzenlenerek büyük ülkelerle ilişkiler geliştirilmektedir. 1970'lerde ÇHC, SSCB'nin ciddi tehdidine direnmek ve SSCB'nin küresel hegemonyasını denetlemek adına başta ABD olmak üzere batılı ülkeleri bir araya getirmek istemektedir. ÇHC ve Japonya'dan Pakistan, İran, Türkiye'den Avrupa'ya ve oradan da ABD'ye uzanan hattaki tüm ülkelerin SSCB'ye karşı bir araya gelmesi ve uluslararası bir anti-hegemonik birleşik cephe oluşturması "tek hat" stratejisi olarak adlandırılmaktadır. Bununla birlikte, "tek hat"ı çevreleyen ülkeleri ifade eden "geniş alan" stratejisinin amacının; SSCB'nin genişleme ivmesine ortak bir şekilde karşı koymak adına tüm ülkeleri "tek hat" ve "geniş alan" içinde birleştirmek olduğu söylenmektedir. ÇHC'de bu iki stratejinin yeniden düzenlenmesi fikri ile beraber

ülkenin diplomatik çalışmalarının daha fazla öncelik ve esneklik kazanması sağlamaktadır. Akabinde bu strateji sayesinde ÇHC'nin uluslararası statüsü daha da artmaktadır (Nabijiang, 2022: 59).

Deng'in bir diğer diplomatik düşüncesi olan “Barış İçinde Bir Arada Yaşama” politikası hakkında bir önceki başlıklarda bilgi verilmiştir. Eşitlik, saldırmazlık, egemenlik ve toprak bütünlüğüne saygı, barış içinde bir arada yaşama ve iç işlerine karışmama gibi ilkeleri bulunan bu politika, uluslararası ilişkilerde karşılaşılabilecek herhangi bir problemle başa çıkmanın en iyi yolu olarak görülmektedir. Bir diğer diplomatik düşünce olan “tek ülke, iki sistem” kavramını ortaya koyan Deng, bu düşünce ile anavatanın yeniden birleşmesini teşvik etmektedir. Bu düşünce, tek Çin öncülü altında, devletin ana gövdesinin sosyalist sisteme bağlı olduğu, Hong Kong, Makao ve Tayvan'ın Çin'in ayrılmaz parçaları olduğu ve orijinal kapitalist sistemi ve yaşam tarzını uzun süre değişmeden sürdürdükleri anlamına gelmektedir (Huaqiu, 2004).

Dış politika adına birçok düşüncesi ve hamlesi bulunan Deng Xiaoping'in en önemli hamlelerinden biri Çin kapılarını dış yatırımlara açması olmaktadır. 1980'ler boyunca yapmış olduğu bu hamle ile dış ticaretini hızla geliştirmektedir. Bu sayede diplomatik bağları iyileşen ÇHC, bu dönemde 19 ülkeyle diplomatik ilişki kurduğu belirtilmektedir. Bir dönem SSCB ile araları bozulan ÇHC bu dönemde yeniden ilişkileri normale dönmektedir. Deng'in yapmış olduğu bir diğer hamle ise Dünya Bankası ve Uluslararası Para Fonu gibi uluslararası kuruluşlara katılmak adına girişimlerde bulunmaktır. Bununla birlikte, Deng'in 1980'li yılların başında “reform ve dışa açılım” politikası ile başlatmış olduğu iyimser hava 1989 yılında Tiananmen gösterilerinin sert bir şekilde bastırılmasıyla beraber ÇHC'nin uluslararası itibarının zarar görmesi ve Batı ülkeleriyle olan ilişkilerinin kısa süreliğine zayıflamasından dolayı yerini karamsar havaya bırakmaktadır (Shambaugh, 2020: 13; Akdağ, 2023: 84).

1989 yılında ÇHC'nin karşı karşıya kaldığı hususlar şu şekilde sıralanmaktadır (Rozman, 2017: 126):

- Batılı güçlerin Tiananmen olayından sonra yapmış olduğu yaptırımlar dolayısıyla ekonomik izolasyon,
- Uluslararası komünizmin çökmesinden sonra siyasi izolasyon,
- 1991 yılında yaşanan Körfez Savaşı sonrasında ABD merkezli bir tek kutupluluk,

- Rusya'nın Batı'ya eğilim göstermesi ve Japonya ile ABD arasındaki kuvvetlendirilmiş güvenlik ittifakının işaret ettiği gibi ÇHC, büyük güçler arasındaki gizli anlaşma riskiyle karşı karşıya kalmaktadır.

Öte yandan, 1990'lı yıllarda Soğuk Savaş'ın son bulmasının, ÇHC'nin büyük güçler arasındaki manevra alanını kaybetmesine sebep olduğu görülmektedir. Büyük güçler arasında etkili gücünü kaybeden ÇHC, bu gücü yeniden elde etmek adına strateji arayışına girmektedir. 1990'lı yılların ortalarına gelindiğinde ÇHC dünya ülkeleriyle yeniden bağ kurarak büyük bir başarı elde etmektedir. ÇHC'nin büyük güçlerle olan ilişkileri 1995-1996 yıllarında daha da yoğunlaşmaktadır. Bu bağlamda, Çin-Rusya arasındaki bağlantı, uluslararası sistemin çok kutupluluğa evrilmesi yönünde ilerlemektedir. Uluslararası toplumdan azda olsa dışlanan bir devlet olan ÇHC'nin, 1990'larla beraber bölgesel ve küresel sisteme daha fazla entegre hâle gelen daha normal bir aktöre dönüştüğü vurgulanmaktadır (Rozman, 2017: 125-126; Shambaugh, 2020: 14-15).

2.3.3. Jiang Zemin Dönemi (1993-2002)

1978 yılında Deng ile başlayan, ÇHC'yi kapsamlı olarak değiştiren ve kısa sürede tüm dünyayı önemli ölçüde etkilemeyi başaran dışa açılma ve reform politikalarının izlemcisi ve en önemli uygulayıcılarından biri olan Jiang Zemin, 1993 yılında ÇHC başkanlığını üstlenmektedir. Kasım 2022 yılında vefat eden Jiang'ın, ÇHC'nin küresel anlamda bir güç olmasında önemli katkıları bulunmaktadır (Durmaz, 2022). Bunun yanı sıra, 1993 yılında Deng döneminin sonlandırılması durumu yalnızca iktidar değişikliği açısından tercih edilmektedir. Nitekim Deng, 1997 yılındaki ölümüne kadar geçen sürede ÇHC siyasetine önderlik etmektedir. Bundan dolayı, Deng dönemi biçim olarak aslında 1993 yılında bitmektedir. Fakat Deng'in başlatmış olduğu reform dönemi günümüzde de izlerini sürdürmektedir (Atawula, 2020: 21).

Dış politika amacı hegemonyaya karşı savaşmak olan Zemin, bir taraftan hem dünya barışını sağlayıp hem uluslararası işbirliğini geliştirirken; öte taraftan ortak ekonomik kalkınmayı desteklemektedir (Zhu, 2001: 20). ÇHC, Soğuk Savaş sonrasında çok kutuplu dünya sistemine uyum sağladığı için dış politikada daha çok işbirlikçi bir tavır sergilemektedir. Bu çerçevede Jiang'ın yapmış olduğu hamlelere bakıldığında söz konusu hamleler şu şekilde belirtilmektedir (Tosun, 2015: 71):

- 1991 yılında Asya-Pasifik Ekonomik İşbirliği Örgütü'ne (APEC) üye olması,

- 2001 yılında Dünya Ticaret Örgütü'ne (DTÖ) üye olması.

Bununla birlikte, ÇHC'nin DTÖ'ye üye olmasıyla Mao dönemine geri dönülemeyeceği anlaşılmaktadır. Bu hamleyle reform sürecinin sürekli devam edeceği algısı oluşmaktadır. ÇHC 1982 yılında DTÖ'ye gözlemci olarak katılırken 15 yıllık müzakere sonunda, Jiang'ın liderliğinin son yıllarına doğru örgüte üye olabilmektedir. Jiang, ÇHC'nin yönetiminde olduğu süre boyunca çatışmadan uzak ve işbirlikçi bir dış politika çizgisinde ilerlemektedir. Fakat bazen küresel aktörlerle bazen de ABD ile güvenlik sorunları yaşamaktadır (Atawula, 2020: 21).

Diğer taraftan Deng'in teorisini miras alıp geliştiren Jiang'ın, diplomatik alanda özellikle de “yeni güvenlik konsepti”nde bir dizi yeni bakış açısı ve öneri ortaya koyduğu tespit edilmektedir. Bu doğrultuda geleneksel güvenlik kavramına bakıldığında, askeri ittifaklara ve silahlanmanın bir araç olarak iyileştirilmesine dayandığı görülmektedir. Bu yüzden, dünyada kalıcı barışı sağlamadığı ve uluslararası güvenliğin garanti altına alınmasına katkıda bulunmadığı kanıtlanan eski güvenlik kavramı yerine Jiang'ın savunduğu yeni güvenlik kavramının, karşılıklı güven ve yarar, eşitlik ve iş birliğine odaklandığı gözlemlenmektedir. Söz konusu yeni güvenlik konsepti kavramı; Soğuk Savaş zihniyetini ve güç politikaları zihniyetini terk etmek, birbirlerine karşı kuşkulu olmamak ve düşman olmamak anlamına gelmektedir. Bu anlayışta, ‘tüm ülkeler istikrarlı bir şekilde diyaloglar yürütmeli ve büyük eylemler hakkında karşılıklı bilgilenmeli, güvenlik çıkarlarına saygı duymalı, karşılıklı yarar sağlanmalıdır’ düşüncesi hâkim olmaktadır. Bu konseptin özü; tek taraflı güvenlik kapsamının ötesine geçmek ve karşılıklı yarar sağlayan iş birliği yoluyla ortak güvenliği aramaktır (Hong, 2013).

Jiang Zemin, Deng'in barış ve kalkınma çağı ve yeni uluslararası siyasi ve ekonomik düzeninin oluşturulması hususundaki düşüncelerini daha da detaylandırmaktadır. Aynı zamanda çok kutuplaşma ve ekonomik küreselleşme eğiliminin sunduğu avantajları ve zorlukları derinlemesine tartışan Jiang, dünyanın çeşitliliğini tanıma ve saygı duyma ihtiyacına vurgu yapmaktadır. Jiang'ın savunduğu bir diğer hususun, çeşitli medeniyetlerin ve sosyal sistemlerin uzun soluklu bir arada barış içinde yaşaması gerektiği olduğu söylenmektedir. Kültürel diplomasi ve kamu diplomasisine önem veren Jiang, geleneksel Çin kültürünün yayılmasına ve medyayı etkilemeye çok önem verdiği gözlemlenmektedir. Bunun yanı sıra, Çin'e karşı oluşan önyargıları değiştirme hususuna değinen Jiang, ÇHC'nin iyi bir uluslararası imajını

biçimlendirmek adına yabancı halkla birebir iletişim kurulmasını önermektedir (Hong, 2013).

Bunlarla beraber, Jiang Zemin'in liderlik yaptığı dönemin 2002 yılında son bulduğu bilinmektedir. 1992-2002 yılları arasında görev yapan Jiang Zemin'in ÇHC Dış Politikası'na genel olarak bakıldığında şu şekilde özetlendiği görülmektedir (Demirel, 2020: 62):

- ÇHC, Deng döneminde kalkınma, reform ve dünyaya açılma politikalarını benimserken bu durumun Jiang'ın gelmesiyle de devam ettiği görülmektedir.
- Jiang yalnızca Deng'in mirasıyla ilerlemeyerek kendi savunduğu fikirleri de siyasete uyarlamaktadır.
- Teknokrat kökenli olduğu bilenen Jiang Zemin'in bu düşüncesi sebebiyle teknoloji ve bilimsel kalkınmayı odağa almasına, özellikle askeri teknolojiye yenilikleri savunması ve askeri harcamaların artmasına, dolayısıyla bölgede ve uluslararası alanda ÇHC'nin saldırgan bir dış politika benimsediği düşüncesinin yaygınlaşmasına aynı zamanda ÇHC'nin tehdit olarak kavranmasına neden olmaktadır.
- Son olarak Jiang'ın görevinin sonlarına doğru olan 2000'li yıllarda DTÖ'ye üye olması uluslararası ekonomi alanında ve bölgede etkinliğinin artmasına sebep olmaktadır. Bu durumda ÇHC'nin uluslararası alanda kendine güveninin artmasına ve aktif rol oynamasına neden olmaktadır.

2.3.4. Hu Jintao Dönemi (2002-2012)

Dördüncü kuşak lider olan Hu Jintao 2003 yılında göreve başlamaktadır. Hu, görevde kaldığı süre boyunca uluslararası alanda birçok olayla karşı karşıya kalmaktadır. ÇHC'nin yaşanan bu olaylar karşısında aktif rol oynayarak dünyayla bütünleştiği kanıtlanmaktadır. ÇHC'ye yüklenen 'yükselen güç' kavramından dolayı uluslararası alanda etkin rol oynadığı görülmektedir. Yani atfedilen bu kavram dolayısıyla ÇHC'nin, aktif bir dış politikaya sahip olduğu düşünülmektedir. Dünyanın en hızlı büyüyen ekonomisine sahip olan ÇHC, 2008-2009 yılların da meydana gelen küresel ekonomik krizde birçok ülkeden daha iyi konuma gelerek kendine güvenen ve dış politikada etkin rol oynayan aktör olarak karşımıza çıkmaktadır (Zhao, 2010: 358-360).

Hu Jintao'nun çağa ayak uydurarak dış politikaya; “halk için diplomasi”, “harmonik/uyumlu dünya, uyumlu toplum, barışçıl yükseliş, barışçıl kalkınma, barışçıl gelişim” gibi bir dizi kavramlar getirdiği bilinmektedir. Hu Jintao sürecindeki dış politikayı anlamak adına bu kavramlar üzerinden gidilmesinin faydalı olacağı düşünülmektedir. Diplomasi kavramında büyük yenilikler yapan Hu Jintao, “halk için yönetim” ve “insan odaklı” kavramlarını dış politika bağlamında genişletmektedir. Bundan dolayı “*halk için diplomasi*” kavramını ortaya koymaktadır. 2009’un Temmuz ayında yabancı elçilerin 7. toplantısında önemli bir konuşma yapan Hu Jintao bazı hususların önemine vurgu yapmaktadır. Bunlar şu şekilde sıralanmaktadır (Hong, 2013):

- İlk kez kamu diplomasisini ve beşeri diplomasiyi güçlendirmenin,
- Çeşitli yabancı kültürel değişim faaliyetleri yürütmenin,
- ÇHC kültürünün sağlam bir şekilde yaymanın.

Bunların yanı sıra, Hu Jintao diplomaside ‘yeni dördü bir arada’ hedefini ortaya koymaktadır. Söz konusu dördü; “ÇHC’yi siyasi olarak daha etkili, ekonomik olarak rekabetçi, imaj dostu ve ahlaki açıdan çekici hâle getirmeye çalışmayı” kapsamaktadır. Kalkınma hususundaki bilimsel bakış açısının özü insan odaklı olmalıdır, düşüncesi hâkim olmaktadır. Diplomasi aynı zamanda “halk için diplomasi ve insan odaklı diplomasi” fikrine bağlı kalmalı ve halkın çıkarlarının her şeyden önce olduğu konusunda ısrar etmeli düşüncesi vurgulanmaktadır. İnsan odaklı “halk diplomasisi” kavramı, ÇHC’nin diplomatik faaliyetlerine giderek daha fazla yansımaktadır (Shikang, 2013).

Diğer taraftan, uluslararası alanda giderek önem arz eden bir aktör hâline gelen ÇHC’nin yükselişi, Batı ülkelerinde olmak üzere dünyanın birçok bölgesinde endişeye sebep olduğu için bu durumun, “Çin tehdidi” algısının oluşmasına neden olduğu görülmektedir. ÇHC hükûmeti oluşan bu algıları ve kaygıları azaltmak için “*barışçıl kalkınma*” ve “*uyumlu dünya*” kavramlarını geliştirmektedir (Zhu, 2013: 123). ÇHC’nin yükselişi kaygılara sebep olurken Çinli yetkililer, ÇHC’nin uluslararası imajını olumlu yönde güçlendirmek adına “barışçıl yükseliş” ifadesinin de kaygı yaratacağını düşündüklerinden bu ifadeyi “barışçıl kalkınma” ile değiştirmektedir (Akdağ, 2023: 86). Bu bağlamda, 2000’li yıllarda ÇHC’nin dış politikasında öne çıkan söylemler şu şekilde sıralanabilmektedir (Deng, 2008: 3):

- Barışçıl yükseliş

- Barış ve kalkınma
- Çok kutupluluk ve küreselleşme
- Barışçıl kalkınma
- Yumuşak güç
- Uyumlu dünya/uyumlu toplum

Dış dünyaya seslenirken uyumlu bir dünyanın oluşturulması çağrısında bulunan Çinli liderler, ÇHC'nin dünyaya kendisini barışsever ve uyum arayışında olan bir devlet olarak göstermeye özen gösterdiğini belirtmektedir (Lynch, 2015: 155-204). ÇHC'nin öne sürmüş olduğu stratejilerden biri olan “*barışçıl kalkınma*”; ÇHC için münasip bir uluslararası çevre oluşturmayı ve bilinçli olarak böyle bir çevreyi biçimlendirmeyi, devamlı yeni fırsatlar yaratmayı ve kalkınma adına daha kapsamlı bir alan açmayı amaçlamaktadır. Söz konusu strateji, ÇHC'nin bölgesel ve küresel sorunlarda yapıcı bir rol oynamasını gerektirmektedir. Yapıcı tutumda ilerletilen bu politika, ÇHC'nin gerektiğinde uluslararası sorumluluklar üstlenme cesaretine sahip olması gerektiği anlamını taşımaktadır (Zhu, 2010: 52).

ÇHC'nin bu dönemde dış ilişkilerindeki temel stratejilerinden biri ise “*yumuşak güç*” stratejisi olduğu söylenmektedir. Genel olarak bu dönemde ÇHC dış politikada imajını iyileştirme ve uluslararası alanda kendisi ile ilgili oluşan kaygıyı aza indirmeye adına yoğun çaba vermektedir. Mevcut uluslararası sistemin ÇHC'nin yükselişi için oldukça uygun bir ortam olduğunu düşünen Çinli politika yapımcıları bu doğrultuda adımlar atmaktadır. ÇHC'nin barışçıl yükseliş hususundaki başarısı genellikle uluslararası toplumla etkileşime girerek geçirmiş olduğu içsel dönüşümden kaynaklanmaktadır. Uluslararası toplumla sürekli olarak etkileşim hâlinde olan ÇHC'nin bu sayede, revizyonistlikten tarafsız eğilime geçtiği ve ardından statükocu bir güce dönüştüğü görülmektedir. ÇHC'nin bu süreçteki tüm kimlik değişimi, kurumsal seçimi ve norm kabulü barışçıl çerçevede gerçekleşmektedir. Hu Jintao 2009 yılında Çinli karar vericilerin dünya görüşlerini yansıtan beş ilke ilan etmektedir. Bu ilkeler şu şekilde sıralanmaktadır (Zhu, 2010: 22-40; Shambaugh, 2020:16):

- Köklü Dönüşüm
- Uyumlu Dünya
- Ortak Kalkınma
- Paylaşılan Sorumluluk
- Aktif Katılım

Bu ilkeler doğrultusunda ÇHC'nin köklü bir değişim sürecine girdiği ve aynı zamanda geleceğinin dış dünya ile bağlantılı olduğu ifade edilmektedir. Bundan dolayı Çin'in sadece uluslararası topluma aktif olarak uyum sağlamakla kalmayıp aynı zamanda ortak kalkınmayı arayıp, ona nazaran uyumlu bir dünya oluşturmada daha çok sorumluluk üstlenmesi gerektiği düşünülmektedir.

Hu Jintao dönemine genel olarak bakıldığında hızlı bir büyümenin mevcut olduğu görülmektedir. Dünya ekonomisini olumsuz yönde etkileyen 2008-2009 küresel krizinde yaşanan sarsıntıya rağmen kriz döneminde bile, ÇHC'nin ekonomisi en çok büyüyen ekonomilerden olduğu ifade edilmektedir. 2007-2010 yılları arasında yıllık olarak yaklaşık %10 büyüme oranını sürdüren ÇHC, krizlerde bile sürekli büyüeyebilen bir ülke hâline gelmektedir. Hu Jintao başkanlık ettiği süreçte ÇHC'nin imajını iyileştirmek ve ekonomik anlamda güçlenmek adına yapmış olduğu adımların meyvesini alarak, hem ekonomik başarıları ile hem de uluslararası alanda daha çok itibar kazanarak kendi sınırlarının çok ötesinde küresel bir perspektif kazanmaktadır. Bununla birlikte, 2008 yılında Pekin'de gerçekleştirilen 20. Yaz Olimpiyatları, Hu Jintao döneminde gerçekleşmektedir. Bu dönemde böylesine bir adım atılması ÇHC'nin imaj yönetimi ve ülke tanıtımı açısından çok önemli bir fırsat olmaktadır. 2001 yılında olimpiyatlara aday olup kazanan ÇHC, 2008 yılına kadar toplam 43 milyar dolar harcama yapmaktadır. Yapılan bu harcama, Dünya Olimpiyatlarına yapılan en çok yatırım olarak kayıtlara geçmektedir (Goldstein ve Pevehouse, 2014: 587; Tosun, 2015: 87-90).

Tüm bu olumlu süreçlerin yanında olumsuz hususlar da yaşanmaktadır. Hu Jintao döneminde yaşanan olumsuz hususlar şu şekilde sıralanmaktadır (Tosun, 2014: 70; Atawula, 2020: 23-24):

- Deprem ve sel gibi doğal afetlerin yaşanması,
- Sars salgınının yaşanmasıyla ÇHC'de ekonomik gelişimin ve toplumsal istikrarın olumsuz etkilenmesi,
- Bölgeler arasında denksiz kalkınma ve gelir dağılımındaki eşitsizlik,
- Çin sanayisinin tıkanmasıyla üretimin tüketimden fazla olması ve ihracatın fazla ürünleri yurtdışına satma ihtiyacını karşılayamamasıyla beraber Çinli şirketlerin iflas etmesi,
- ÇKP'nin siyasi meşrutiyetini gözetmek adına devamlı Çin Milliyetçiliği'ne sarılmasından dolayı hem yabancı düşmanlığının tetiklenmesi hem de Çinli

işçilerin haklarının savunması konusunda yetersiz kalınması durumu söz konusu olmaktadır.

Yaşanan olumsuzluklar doğrultusunda ÇHC dış politikada farklı bir yol izleyerek, özellikle toplumsal istikrarın bozulması, milliyetçiliğin başkaldırması ve rejimin güvenliğinin tehlikeye girmesi hususundan dolayı bencil ve sert/saldırgan bir tutum izlemeye başlamaktadır. Yani dış politikada güvenlik önlemlerini sertleştirmeye başlayarak çatışmacı bir dış politika izlemeye başladığı görülmektedir. Bu durumda Deng döneminde başlatılan reform döneminden farklı olarak yeni bir döneme girildiği dikkati çekmektedir.

2.3.5. Xi Jinping Dönemi (2012-...)

Hu Jintao'dan sonra 2012 yılında ÇHC'de göreve başlayan Xi Jinping günümüzde de görevine devam etmektedir. Özellikle dış politika alanında önemli değişimlerde bulunan Xi Jinping, ÇHC'nin bölgede ve uluslararası alanda küresel bir güç konumunda olmasını istemesinden dolayı bu değişikliklere başvurmaktadır. ÇHC'nin başına gelen her lider gibi Xi Jinping'de dış politika adına yeni kavramlar ortaya koymaktadır. “Çin rüyası” ve “Çin halkının ulusal yenilenmesi” gibi kavramlar üzerinde dış politikayı sürdüren Xi Jinping, Hu Jintao'nun benimsemiş olduğu “barışçıl gelişim” düşüncesini de ÇHC'nin dış politikasının temel ilkelerinden biri olarak görülmesinin devam etmesini sağlamaktadır. Bununla beraber, ÇHC'nin iç reformunun ve kalkınmasının uzun süreli olarak tanımlanmasını isteyen Çinli liderler, ülkenin büyük bir güç hâline gelebilmesi adına barışçıl ve istikrarlı bir dış politikaya ihtiyaç duyduğunu fark ettikleri için “barışçıl gelişim/barışçıl kalkınma” stratejisine önem vermektedir (Zhang, 2015: 8).

Genel olarak, ülkenin başına geçen her Çinli liderin dış politikasını temsil eden ve onu diğer liderlerden ayıran kavramların olduğu görülmektedir. Yukarıda da belirtildiği üzere Xi Jinping döneminde ÇHC'nin dış politikasının genel yönelimi olabilecek kavramlar bulunmakta ve bunlar üç kavram üzerinden açıklanmaktadır. Birbirleriyle bağlantılı olan bu kavramlar; “Çin Rüyası”, “ortak kader topluluğu” ve “başarı için çabalamak” şeklinde belirtilmektedir. Görüldüğü üzere Xi Jinping döneminde aslında birçok kavram göze çarpmaktadır. Fakat dış politika özellikle bu üç kavram üzerinden birbirleriyle bağlantılı bir şekilde ilerlemektedir. “Çin Rüyası” kavramı ilk olarak Xi Jinping dönemiyle ilişkilendirilse de aslında her üç kavram da bu

dönemin dış politikasını tanımlamaktadır. Yani bir arada ele alındıklarında ayırt edici bir bütünü oluşturmaktadır. Xi Jinping dönemini diğer dönemlerden ayıran bu kavramlar aynı zamanda bu dönemler arasındaki sürekliliği sağlamaktadır. Bu yüzden, 2013 yılından bu yana ÇHC'nin dış politikasına bakıldığında girmiş olduğu dönüşüm sürecinde devrimsel kopukluk yerine kısmi bir dönüşümün yaşandığı görülmektedir (Demir, 2020: 49).

Xi Jinping'in üzerinde durmuş olduğu bu kavramlara değinmeden önce belirlemiş olduğu yeni dış politikanın özünde bulunan özellikleri bilmek gerekmektedir. Xi' nin belirlemiş olduğu dış politikaların özünde üç özellik bulunmaktadır. Bunlar şu şekilde sıralanmaktadır (Poh ve Li, 2017: 88):

1. Xi Jinping dış politikasını belirlerken ÇHC ulusal çıkarlarını korumayı ön planda tutmaktadır. ÇHC'nin ulusal çıkarları; egemenlik, güvenlik ve gelişme/kalkınma çıkarları olarak ifade edilmektedir. Xi Jinping her ne kadar barışçıl gelişim/kalkınmaya bağlı kalınacağını ifade etse de ülkenin öz ulusal çıkarlarını da korumaya devam ettiğinin vurgusunu yapmaktadır. Bundan dolayı ülkenin sorumluluk alanını genişletmek istemesiyle beraber daha aktif bir dış politika benimseyen Xi Jinping, ulusal çıkarların kapsamının genişlemesine neden olmaktadır. Yani herhangi bir olay ÇHC'nin ekonomik kalkınmasını etkiliyorsa bu olay temel ulusal çıkar olarak kabul edilmektedir.
2. Barışçıl kalkınma/gelişim ilkesi yalnızca ÇHC tarafından değil, ÇHC'nin iletişim kurduğu diğer ülkeler tarafından da kabul edilmesi inancının bulunması, ÇHC'nin istikrarı sağlama ve ekonominin büyümesini sağlama noktasında önem arz etmektedir.
3. Son olarak ise Xi Jinping dış politika adına en üst düzeyde birimler tasarlamaktadır.

Bunlarla beraber, dış politika adına birçok hamlelerde bulunan Xi Jinping'in en çok anıldığı kavram olan "Çin Rüyasına" değinecek olursak; bu kavram Xi Jinping'in ortaya koyduğu bir kavram olmamasına rağmen, kavramı sürekli olarak vurgulaması ve onu uzun vadeli bir plan olarak ÇHC halkına sunması dolayısıyla son yıllarda kendisiyle en çok özdeşleşen kavram olmaktadır. Bu bağlamda, 28 Kasım 2012 yılında ÇHC Ulusal Müzesinde düzenlenen "Yenilenmeye Giden Yol" adlı sergide yapmış olduğu ziyaret sonucunda ilk kez Çin Rüyası ile ilgili açıklama yaptığı görülmektedir.

Sergide yapmış olduđu açıklamada “Herkes bir Çin Rüyası’ndan bahsediyor. Çin ulusunun yeniden canlanmasının, modern zamanlardan beri ulusun en büyük hayali olduđuna inanıyorum” şeklinde ifadelerde bulunmaktadır. Bu doğrultuda Xi Jinping, ÇHC’nin daha fazla uyum ve demokrasi ile daha zengin ve daha güçlü bir ülke hâline geleceğini düşündüğünü, ÇKP’nin 100. yıldönümü olan 2021 yılına kadar ülkenin orta derecede müreffeh bir topluma ulaşma hedefini gerçekleştireceğine inandığını ifade etmektedir. ÇKP, 18. Ulusal Kongre’ de, 2020 yılına gelindiğinde 2010 yılındaki kişi başına düşen milli gelirin iki katına çıkmasını sağlamak adına daha fazla çalışacağını açıkça belirtmektedir (Gang ve Shuang, 2012).

12 Mart 2013 yılında düzenlenen Ulusal Parlamento toplantılarında Devlet Başkanlığı makamını üstlenen Xi, burada da Çin Rüyası ile ilgili açıklamalarını sürdürmektedir. Bu toplantıda Çin Rüyasını gerçekleştirmede halka güvenme ve halka fayda sağlama sözü veren Xi Jinping, o dönemde nüfusu 1,3 milyar olan Çinli halkın rüyası kabul edilen Çin Rüyasını gerçekleştirmek adına halkın bu misyonu daima aklında tutması, bir bütün olarak bilgelik ile yenilmez bir güç olması gerektiğini belirtmektedir. Bu rüyanın gerçekleşebilmesi için ÇHC’ye özgü bir yol izlenilerek başarılabileceğini vurgulayan Xi, ÇHC halkını oluşturan tüm bu unsurların Çin’e özgü sosyalist sisteme inanması ve bu büyük ideali gerçekleştirmek adına ilerlemeye devam edilmesi gerektiğini belirtmektedir (Chinadaily, 2013).

Xi Jinping’ in ÇKP Genel Sekreterliği mevkindeki ilk döneminin sonuna geldiğinde Çin Rüyası toplumun olmasa da ÇKP’nin esas ideali hâline dönüşmektedir. 19. ÇKP Ulusal Kongresi Ekim 2017 yılında “yeni bir devirde ÇHC’nin kendine has olan sosyalizminin büyük başarısı için çaba harcamak ve Çin Rüyası olan milli canlanmanın gerçekleştirilmesi için bıkmadan çalışmak” teması ile gerçekleştirilmektedir. Bu kongrede Xi, Çin Rüyası kavramını detaylı olarak ele almaktadır. Bununla birlikte ÇKP’nin önüne 2021 yılı sonrası için ilk kez bir plan ortaya koymaktadır. Bu plan üç aşamada ele alınmaktadır (Jinping, 2018: 33-34):

- Planın birinci aşamasına göre, 18. Ulusal Kongre’de alınan karar doğrultusunda 2021 yılında gerçekleşecek olan ÇKP’nin 100. yıldönümüne kadar olan sürede ÇHC’de mutlak yoksulluk ortadan kaldırılarak ülkenin orta gelirli bir toplum hâline getirilmesi planlanmaktadır.
- İkinci aşamada, sosyalist modernizasyonunun gerçekleştirilmesi gayesine 2035 yılına kadar ulaşılacağı planlanmaktadır. Bu planın gerçekleşmesiyle

beraber ÇHC, ekonomik ve teknolojik kapasitesi ciddi bir şekilde gelişerek dünyanın önde gelen yenilikçi ülkesi olacağı düşünülmektedir.

- Son aşamada ise, 2049 yılında yani 21. yüzyılın ortalarına gelindiğinde Çin Rüyası'nın hedefi olan ulusal canlanma gerçekleştirilerek, zenginleşen Çin dünyada lider konumuna yükseleceği belirtilmektedir.

Xi Jinping Çin Rüyası ile ilgili hedeflerini gerçekleştirmek amacıyla Mart 2013'de Devlet Başkanlığı'na geçtikten hemen sonra dış politika ve iç politikanın ilerleyişinde değişiklikler yapmaktadır. Bununla birlikte, bu dönemde ÇHC'de yaşanan yolsuzlukla mücadele, eleştirel düşüncelere ve entelektüellere karşı baskıların artması ve siyasi iç meseleler gibi hususlardan dolayı Xi Jinping'in ÇKP'de ki konumunun güçlendiği görülmektedir. Bu durum ise dış politika alanında attığı adımlarda elini güçlendirmektedir. Dış politika alanında artan askeri harcamalar ve dış yatırımlar gibi alanlar Hu döneminin devamı niteliğinde olsa da Xi' nin bazı alanlarda önemli farklılıklar gösterdiği belirtilmektedir. Bu farklılıklar şu şekilde sıralanmaktadır (Demir, 2020: 50):

- ÇHC'nin komşularına verdiği önemin artması,
- Siyasi ve yurtiçi ekonomik gayelerin dış politika gayeleriyle aralarındaki bağlantının daha yakından kurulması,
- Proaktif bir dış politikaya yönelinmesi.

Öte yandan, Xi Jinping döneminde dış politika yapımı ile ilgili iki önemli adım atıldığı analiz edilmektedir. Bu atılan adımlarda amaç, Hu dönemindeki çok karışık dış politika yapımını değiştirmek ve daha bütüncül ve etkin dış politika izlemektir. Söz konusu adımlardan ilkiyle dış politikada karar vericilerin yenilenmesi ve böylelikle politika yapımının merkezileştirilmesi hedeflenmektedir. Bu adımın gerçekleştirilebilmesi için öncelikle Ulusal Güvenlik Komisyonu gibi yeni kurumlar oluşturulmaktadır. Bu kurumlar iç ve dış politika yapım süreçleri arasında düzeni sağlamaktadır. Sonrasında ise iç ve dış politika alanlarında Xi'nin önderlik ettiği çok sayıda gruplar oluşturulmaktadır. Bu gruplar ile ilgili detaylı bilgiler üçüncü bölümde verilmektedir (Grünberg, 2019; Lee, 2017; Wang, 2017). Oluşturulan gruplar sayesinde merkezi ve yerel yönetimler, hükûmet dışı aktörler ve dış politika süreçleriyle ilgilenen kuruluşlar aracılığıyla koordinasyon içinde çalışılması hedeflenmektedir. Bu sayede uygulanan politikalar uluslararası gelişmeler doğrultusunda zamanında düzenlenerek ve

karşılaşılan diplomasi sorunlarının üstesinden gelinebilecek şekilde yapılmaktadır (Jiechi, 2013).

Xi Jinping'in dış politika yapımı ile ilgili atmış olduğu ikinci adımda, politika belirlenirken karar alma ve uygulama süreçlerine yardımda bulunan tüm önemli aktörler öncelikle Komşu Ülkeler Hakkında Diplomatik Çalışma Konferansı'nda (Ekim 2013) daha sonra da Dış İlişkilere İlişkin Merkezi Çalışma Konferansı'nda (Kasım 2014) bir araya getirilecektir. Bu konferansların yapılmasındaki amaç, ÇHC'nin komşu ülkeleriyle ve diğer ülkelerle ilişkilerini bütüncül bir bakış açısıyla en üst seviyede belirlemektir. Uluslararası alanda yaşanan gelişmeleri/koşulları ve bölgesel koşulları bu toplantıda ele alan ÇKP, dış politika ile ilgili ilkeleri ve stratejik hedefleri belirleyerek 5-15 yıllık orta ve uzun vadeli planlar yapmaktadır (MFA, 2013; MFA, 2014).

Xi' nin Komşu ülkelere yönelik yapmış olduğu söz konusu politikalar Çin Rüyası'nın gerçekleştirilmesi noktasında büyük önem taşımaktadır. Bu politikalar doğrultusunda ÇHC komşularıyla ilişkilerini iyileştirmek ve düzenli olarak kalkınmayı sağlamak adına sağlıklı ortamın kurulması için çaba sarf etmenin ve komşu ülkelerin iyileşmesine katkıda bulunmaları gerektiğinin vurgusu yapılmaktadır (MFA, 2013). Bu durum her ne kadar ÇHC ekonomisine olumlu yansısı da bu politikalarla beraber ÇHC komşu ülkelerin kalkınması noktasında 'sorumlu' bir büyük güç olarak görüldüğünden, artık komşularıyla yakın ilişki kurmayla yetinmemesi gerektiği düşünülmektedir. ÇHC'nin, komşularıyla yakın ilişki kurmanın ötesine giderek artık yakın çevresini aktif bir şekilde biçimlendirme ve yönlendirme düşüncesi savunulmaktadır. Aynı zamanda küçük komşularına da destek olması ve böylelikle bölgesinde dengenin ve uyumun sağlanmasına katkı sunması gerektiğine ilişkin vurgu yapılmaktadır. Bu hedefler doğrultusunda, 2013 yılında Xi' nin, "*ortak kader topluluğu*" inşası ile Asya kıtasını dönüştürmek gibi ilgi çekici bir çaba içine girdiği görülmektedir (Demir, 2020: 49).

Bununla beraber, "ortak kader topluluğu" kavramında, Asya ülkelerinin ve aynı zamanda dünyanın kalkınma gayelerine ulaşmak ve düzeni sağlamak gibi sorunlarla karşı karşıya gelindiği durumlarda ÇHC'nin kendine has çözümlerine başvurulmasından söz edilmektedir. Karşılaşılan problemlere 'Çinli çözümler' üreterek dünyaya Çin'in bilgeliğini sunarak uluslararası alanda yaşanacak sorunlarda liderlik rolünü üstlenmektedir. Bu doğrultuda, ortak kader topluluğu kavramı ekonomik ve ticari ilişkilerin geliştirilmesi noktasında yapılan çalışmalarla somut bir eyleme

dönüşmektedir. Bu eylemlere verilecek en önemli üç örnek şu şekilde belirtilmektedir (Zhang, 2015: 15):

- Kuşak ve Yol Girişi (KYG)
- Asya Altyapı Yatırım Bankası (AIIB)
- İpek Yolu Fonu

Diğer taraftan, küçük ülkeler ile ilgili çalışmalar gerçekleştiren ÇHC'nin, 2014 yılında yeni bir toplantı yaparak komşu ülkeler dışında büyük ülkelerle de ilişkilerinin iyileştirilmesine, gelişmekte olan ülkelerle ilişkilerine ve çok taraflı diplomasiye odaklanılması gerektiği düşüncesini ortaya koyduğu görülmektedir. Bu bağlamda Xi Jinping toplantı sonrası dört katmanlı bir dış politika strateji belirlemektedir. Önceki dış politika stratejisinin devamı olan bu dört katmanlı stratejide yeni özelliklerde bulunmaktadır. Burada dikkat çeken strateji ise 1990 yılında Deng Xiaoping'in önermiş olduğu "düşük profil izleme" stratejisinden "başarı için çabalamak" olarak adlandırılan stratejiye geçiş olmaktadır. Bu iki strateji arasında farklar bulunmaktadır ve bu farklardan dolayı değişikliğe gidilmektedir. Söz konusu farklılıklar şu şekilde ele alınmaktadır (MFA, 2014):

- *Düşük Profil İzleme*: Ekonomi odaklı olan bu strateji, uluslararası sorunlarda bitaraf kalmayı ve diğer ülkelerle olan ilişkilerinde ekonomik çıkarların ön planda tutulmasını amaçlamaktadır.
- *Başarı İçin Çabalamak*: Siyaset odaklı olan bu strateji, komşu ile olan bağlarında stratejik ilişkilere odaklanan ve siyasi erdemin ön plana çıktığı bir strateji olarak karşımıza çıkmaktadır.

Bunun yanında, Çin yönetimi söz konusu stratejiyi izleyerek, asıl hedefi olan ulusal canlanmayı sağlamak adına ihtiyaç duyduğu istikrarlı ve huzurlu bir bölge ve uluslararası düzeni oluşturma alt hedefini birleştirmeyi amaçlamaktadır. Kısacası, "başarı için çabalamak" stratejisini izleyerek asıl hedef ile alt hedefin birleştirilmesi amaçlanmaktadır (Xi, 2014: 328-329; Xi, 2018: 22).

Bunlarla birlikte Xi'nin uluslararası ilişkilerinde sergilemiş olduğu tutuma bakıldığında; daha özgüvenli ve saldırgan bir tutum sergileme yolunda ilerlediği ve bu iddialı tutumuyla ÇHC ile toprak anlaşmazlıkları yaşayan komşuları arasında güvenlik kaygılarının arttığı görülmektedir. Güney Çin Denizi hususunda anlaşmazlıkların yaşandığı adalar ile ilgili ÇHC'nin, bu konuda ödün vermeye yanaşmadığı ve bu sorunlar ile ilgili kapsamlı iddiasını sürdürdüğü belirtilmektedir. Xi yönetimiyle ortaya

çıkan ÇHC'nin yeni dış politikası, bir yandan uluslararası ilişkilerde daha iddialı olmayı amaçlarken diğer yandan ekonomik ve askeri diplomasi ile karakterize edilebilmeyi hedeflemektedir. Bunun yanı sıra, çıkarları doğrultusunda stratejik olarak önem verdiği devletlerle diplomatik ilişkiler kuran ÇHC, bu ülkeleri desteklemek adına ekonomik yönden kabiliyetlerini ve yatırım programlarını kullanmaktadır. Xi yönetimiyle başlayan ÇHC'nin yeni dış politikasının, Güney Çin Denizi kısımlarındaki anlaşmazlıklarında ya da uçak gemilerinin faaliyete alınmasında daha iddialı bir duruş ile karakterize edilebileceği savunulmaktadır (Pradt, 2016: 197-201).

Tüm bu anlatılanlarla beraber aktif bir dış politika izleyen Xi Jinping döneminde gelişen bir diğer önemli olayın, çok taraflı gruplarla ilişkilerin iyileştirilmesi ve zirve diplomasisinin yapılması olduğu görülmektedir. Bu doğrultuda, ÇHC'de Xi Jinping başkanlığında yapılan zirveler şu şekilde sıralanmaktadır (Xi, 2018: 9):

- 2016 G20 Zirvesi
- 22. APEC Ekonomik Liderler Toplantısı
- 2017 BRICS Zirvesi
- I. Ve II. Kuşak ve Yol Forumu

Öte yandan, ÇHC'nin her anlamda lider durumunda olmasını isteyen Xi Jinping'in, ülkenin görünürlüğüne artırmak ve diğer ülkelerle olan ilişkilerini güçlendirmek adına birçok ülkeye ziyarette bulunduğu tespit edilmektedir. Nitekim 2013 yılında Devlet Başkanlığı'nı üstlendikten sonraki 7 ayın 33 gününü ülke dışında geçirerek ziyaretlerde bulunduğu gözlemlenmektedir (Zhang, 2015: 7-8). Bununla beraber, Xi Jinping döneminde en iddialı hamlenin 2013 yılının son aylarında "Kuşak ve Yol Girişimi" bir diğer adıyla "Bir Kuşak, Bir Yol" projesinin ilan edilmesi olduğu bilinmektedir. Genel olarak, bu dönemde yaşanan birtakım ekonomik ve siyasi sorunlar neticesinde geliştirme kararı alınan bu projenin oluşturulmasındaki başlıca nedenler şu şekilde belirtilmektedir (Kopuç ve Bayraç, 2021: 1355; Grieger, 2016: 1):

- Ekonomik büyüme hızının yavaşlaması,
- Arz fazlasının oluşmasından dolayı üretilen ürünlerin elde kalması,
- Ticari işbirliği yapanlar arasında yaşanan politik tikanıklar,
- ÇHC'nin iç bölgelerinde oluşan dengesiz ekonomik gelişmeler,
- Ekonomik ve siyasi olarak dünyadaki konumun daha da iyileştirilmek istenmesi.

Belirlenen bu nedenler doğrultusunda ortaya çıkan BKBY Projesi'nin amacı, Xi Jinping'in ifade ettiği beş ilke ile gerçekleşmektedir. Bu ilkeler şu şekilde ortaya konmaktadır (Dünya Ekonomik Formu, 2019):

- Ülkeler arasında bulunan karayolu bağlantılarını iyileştirmek,
- Toplumsal ve insanlar arasındaki etkileşimi artırmak,
- Politika iletişimde hızı artırmak,
- Engelsiz bir ticaret ağını özendirmek,
- Parasal dolaşım ve etkinliğini artırmak.

Avrupa ve Asya'da belirlenen güzergâhlar doğrultusunda geliştirilen ulaşım ağlarıyla bağlanıp Eski İpek Yolu'nu canlandırmayı hedefleyen bu proje aynı zamanda yukarıda belirlenen amaçların gerçekleştirilmesi adına kara, hava, deniz ve demir yollarının iyileştirilmesine yönelik, var olan ulaşım hatlarına alternatif bir proje olarak uygulamaya konulmaktadır (Li ve Schmerer 2017: 205).

Bir başka kaynak ışığında projenin, ÇHC'nin yakın çevresinin gelişimini kendi gelişimi doğrultusunda ilerletme hedefinin bir sonucu olarak ortaya çıktığı belirtilmektedir. Bu proje ile ÇHC, iç ve dış politika gayelerini ilişkilendirmeyi amaçlarken bu doğrultuda bir yandan altyapı yatırımlarıyla Avrasya ülkeleri arasındaki bağlantıyı ve iletişimi geliştirmeyi hedeflemektedir. Diğer yandan ise karşılaşılabilecek ekonomik, güvenlik ve siyasi meselelerin üstesinden gelmek niyetinde olduğu belirtilmektedir. Proje ilk olarak ÇHC'nin yakın komşularına yönelik başlatılmaktadır. Daha sonra Afrika, Orta Doğu ile Avrupa'yı da içine alarak genişletilmektedir. Son kertede söz konusu proje tüm dünya ülkelerine açılmaktadır. Böylelikle Çin Rüyası Avrasya Rüyasına dönüşerek ülkenin komşularının kalkınma gayeleri ÇHC'nin kendi kalkınması doğrultusunda şekillendirilmektedir (Demir, 2020: 55).

Xi Jinping döneminde değinilecek son hususun ise Covid-19 salgını olduğu görülmektedir. Bu salgın ile beraber, ABD ve diğer Batı ülkelerinde ÇHC'nin küresel yönetim kurumlarındaki etkisinin artmasıyla ilişkili olarak endişelerin yenilendiği gözlemlenmektedir. Bu doğrultuda küresel boyutta etki eden salgının, DSÖ tarafından halk sağlığı acil durumu olarak belirleme hususunda gecikmesi ve aynı zamanda Tayvan'ın bu acil durum kapsamına alınmaması durumu, ÇHC'nin artan etkisinin göstergesi olarak görülmektedir. ÇHC yönetimi salgının yoğunlaştığı süreçte yeterince şeffaf olmamasından ve sonrasında sert önlemler almasından dolayı eleştirilerin odağı hâline gelmektedir. Bu eleştiriler doğrultusunda ve salgın sürecinde yaşanan

istikrarsızlıktan dolayı ÇHC bu durumların üstesinden gelebilmek amacıyla yeni stratejiler geliştirmek zorunda kalmaktadır. Bu stratejilerin başında ise “aşı diplomasisi” gelmektedir. Bu stratejiyle beraber ÇHC, salgına maruz kalan birçok ülkeye aşı bağıışı ve her türlü tıbbi yardım yapmaktadır. ÇHC, yaşanan salgın sonrasında olumsuz yönde etkilenen uluslararası imajını yeniden iyileştirmek adına yapmış olduğu stratejilerle dış ilişkilerini titizlikle yürütmek zorunda kalarak durumu pozitif yönde ilerletmeye gayret göstermektedir (Haenle, 2020; Kobierecka, 2022: 1-7).

2.4. Genel Bir Perspektiften Ulusal Güvenlik Anlayışı

Güvenlik olgusu bireylerin kişisel yaşamının şekillenmesi noktasında oldukça önem arz eden bir husus olarak karşımıza çıkmaktadır. Bireyler kendilerini savunma durumunun gerçekleştiği ortamlarda oluşan güvenlik algısına göre hareket etmektedir. Bireyler için böylesine önem arz eden bir husus devletler için de büyük önem arz etmektedir. Bir devletin şekillenmesi, parçalanması vs. gibi durumlarda güvenlik algısı büyük rol oynamaktadır. Bu başlık altında ÇHC’nin güvenlik algısına kısaca değinilmeden önce güvenlik kavramının ne olduğunu değinilerek Pekin’in genel güvenlik anlayışı analiz edilmektedir.

Önemli olduğu düşünülen bir varlığa yönelik herhangi bir tehdit ve risk oluşturacak durum karşısında bu tehdide yönelik alınan önlemlerin bütününe *güvenlikleştirme* denmektedir (Buzan, 2008: 107). Siyaset Bilimci Paul D. Williams’ın güvenlik ile ilgili yapmış olduğu tanımında, dünya siyasetinin güvenlik kavramı olmadan var olmayacağı ve siyasetin/politikanın en güçlü aracının güvenlik olgusu olduğunu belirtmektedir (Williams, 2013: 1-2). Dünya geneline bakıldığında birçok devletin güvenlik kavramıyla varoluşlarını sürdürdükleri ya da bu yönde yaşamış oldukları eksikliklerden dolayı yok olma tehlikesiyle karşı karşıya kaldıkları görülmektedir. Bununla beraber dönemin şartlarına göre alınan güvenlik tedbirlerinin değişime uğradığı gözlemlenmektedir. Bu doğrultuda yaşadığımız yüzyılda dünya siyasetine bakıldığında, sürekli güvenlik meselelerinin artması ve tehlikelerin çoğalması sonucunda dünya devletlerinin silahlanmaya gittiği görülmektedir. Karşılaşılan risk ve tehditlerden dolayı dünyada ulusal politikalara sahip olan ülkeler yaşanan korku dolayısıyla güvenlik girişimlerini ön plana çıkarmaktadır (Bilgiç, 2011: 123-124).

Bu bağlamda tek olma, lider olma arzusu yüksek olan ÇHC’nin güvenlik algısına bakıldığında, ülke çıkarlarının ön plana çıktığı ve kendilerine has savunma

stratejilerinin belirlenmesiyle oluşan etmenler doğrultusunda güvenlik algısının şekillendiği belirtilmektedir. Bununla ilgili olarak Birinci Dünya Savaşı'nın ilk yıllarında yazmış olduğu "Tüm Savaşları Bitirecek Savaş" adlı kitabında, uluslararası sistemde felaketlerin yaşandığı yıllarda ulusal silahsızlanmanın uygulanabilirliği hususuna değinen H. G. Wells'in kitabına; silahlı barış egemenliğinin var olduğu süreçte, barış yanlısı olan ve bu niyetine güvenilebilen ülkeler arasına ÇHC'yi de eklediği görülmektedir. Wells, ÇHC'nin hiçbir dönem saldırgan/agrasif olmadığını iddia etmektedir (Wells, 2020: 34-35).

21. yüzyıla gelindiğinde durum bunun tam tersi bir hâl almaktadır. Soğuk Savaş döneminde birçok ülke güvenlik önlemlerini artırarak farklı savunmalarda bulunmaktadır. Söz konusu dönemde güvenlik olgusu; yabancı işgali, askeri saldırı, taktik ya da stratejik füze saldırıları ve kitle imha silahlarından korunma biçiminde algılanıp tanımlanmaktadır. Sert güvenlik (hard security) olarak da tanımlanan bu durum doğrultusunda toplumsal mekanizmaların büyük çoğunluğu buna göre yapılandırılmaktadır (Dedeoğlu, 2004: 15). Bu bağlamda, ÇHC'nin güvenlik olgusunu algılama biçiminden oluşan savunma stratejilerine bakıldığında, ilk girişimin 1964 yılında, ilk nükleer bombanın fırlatılmasıyla oluşturulduğu söylenmektedir. Uluslararası alanda sağlıklı ve sükûnet içinde bir ortamın oluşmasına engel teşkil eden ve büyük tehdit olarak kabul edilen en yaygın görüşlerden birinin, nükleer silah barındırma hususu olduğu vurgulanmaktadır. Bundan dolayı, nükleer enerji programlarının ve sistemlerinin geliştiği, nükleer silah kapasitesine ulaşabilme sayılarının artabildiği ve aynı zamanda nükleer silah üretimine olanak sağlayan bu durumun zehir teknolojisini yaygın hâle getirdiği görülmektedir. Böylesi tehlikeli bir durumu ortadan kaldırabilmek hayati bir önem taşımaktadır (Gül, 2021: 37-38).

Bu doğrultuda ÇHC'nin nükleer enerji oluşturma adımlarına bakıldığında, Dünya Nükleer Birliği'nin (World Nuclear Association) netlik içeren rakamlarda belirttiği üzere, 1970 yılında başlanılan bu adımların 2005 yılından sonra gelişiminin hızlandığı vurgulanmaktadır. Dünya Nükleer Birliği'nin 2011 yılının Aralık ayında yapmış olduğu araştırmalarda ÇHC'nin, 10 veya 20 yıl sonrasında nükleer enerjiyi, üretim sisteminin temeli hâline getireceğinden bahsedilmektedir (World Nuclear Association, 2023). Bunun yanı sıra söz konusu silahlar günümüz dünyasını birkaç kez yerle bir edebilecek potansiyele sahip olmaktadır. Bundan dolayı diğer silahlarla kıyaslanması mümkün olmamaktadır. Kimyasal ve biyolojik silahlar gibi kolay

üretilmeyen ve yaygın olmayan nükleer silahlara sahip olmak tehlikeli sayılmaktadır. Bu silahlara sahip olan ülkelerin en önemli ayrıcalığı güvenlik psikolojisi yaratmaktır. Birden fazla ülkenin bu silaha sahip olması durumunda psikolojik üstünlük durumu devreye girmektedir. Normal şartlarda bu silaha sahip olmayan ulusal aktörler üzerinde oluşan huzursuzluk dışında zamanla nükleer silah kullanan ülke sayısı arttıkça oluşan bu durum aza indirgenerek psikolojik üstünlük durumu başlamaktadır (Köse, 2007).

Diğer yandan ÇHC'nin genel güvenlik modeline bakıldığında; silahsızlandırılmanın gerekliliği üzerinde durulduğu görülmektedir. Bunu başarmak için ise kullanımının sınırlandırılması gerektiği belirtilmektedir (Bin ve Zhao, 2016: 2). Bu doğrultuda ÇHC 1995 yılında, Güneydoğu Asya Ülkeleri Birliği (ASEAN) kapsamında imzalamış olduğu Bangkok Antlaşması ile nükleer silahların üretimi, kullanımı ve bulundurulmasına yönelik sınırlayıcı olan bu antlaşmayı yürürlüğe koymaktadır. Bu hususta atılan adımlarda daha ayrıntılı bir programla Soğuk Savaş'ın sonlarına doğru, BMGK, Kapsamlı Nükleer Test Yasağı Sözleşmesi (CTBT) getirmektedir (United Nations, t.y.). Bu durum Nükleer Denemeleri Kapsamlı Yasaklanması ile sonuçlandırılmaktadır. Nükleer silahsızlanma ile ilgili yapılan son aşamanın Silahsızlandırma Konferansı (CD) olduğu bilinmektedir (Gül, 2021: 40).

Silahlanma güvenlik hususunda inkâr edilemeyecek bir durum olsa da silahsızlanmada emniyet açısından önemli bir olgu olarak görülmektedir. Dış politika oluşturulurken en önemli hedeflerden birinin güvenlik olgusu olduğu karşımıza çıkmaktadır. Fakat bu güvenlik hedefinin önünde büyük bir engel teşkil eden nükleer güç bulunmaktadır. Nükleer gücün güvenlik algısının merkezinde yer alması ve bu konuda yapılacak herhangi bir değişim, ulusal güvenlik anlayışında büyük rol oynamaktadır. Çinli liderler, nükleer silahsızlanma hususundaki ciddiyeti sıklıkla ifade etmektedir. Bu doğrultuda, kazanımlarının risk ve tehdit altında bulunmamasına yönelik bir girişim ya da hükûmetlerin dış politikalarındaki temel askeri hedefleri caydırma amacıyla bu sürece dâhil olmaktadır (Gül, 2021: 40).

ÇHC'nin dış politika belirlerken amaçlarından biri olan güvenliği sağlama ve kontrolü elinde tutma hususu ile ilgili bazı analizler yukarıda liderlerin uygulamış olduğu politikalar anlatılırken ele alınmıştır. ÇHC'nin başına geçen liderlerin belirlemiş olduğu dış politikaların çoğunluğu geleneksel ulusal güvenlik kapsamına girmektedir. Yukarıda değinilmeyen birkaç politika hakkında kısa bilgi aktarımları yapılarak geleneksel ulusal güvenlik ile ilgili de analiz yapılacaktır. Bununla birlikte, ülkelerin

ulusal çıkarları ve karşılaşılan tehditler değiştikçe iç ve dış politikalarda bu değişimler doğrultusunda şekillenmektedir. ÇHC, ulusal güvenlik çıkarlarını korumak ve bu duruma yönelik karşılaşılan tehditlere karşı önlemler almak ya da ortadan kaldırmak için birtakım strateji ve politikalar belirlemektedir. Yukarıda da ortaya konduğu üzere liderlerin belirlemiş olduğu strateji ve politikalar dönemin koşullarına göre değişkenlik göstermektedir.

Bu doğrultuda, dış politikalar belirlenirken güvenlik unsurunun da dikkate alındığı bilinmektedir. Mao Zedong dönemi dış politikaları genel hatlarıyla; ÇHC-SSCB ittifakı, ÇHC'nin yeniden bir araya getirilmesi, dışa kapalı süreç, Kültür Devrimi ve ABD'ye yaklaşma süreci biçiminde şekillenmektedir. Bu dönemde uygulanan en önemli ulusal güvenlik politikası ise nükleer silah hususunda yapılmaktadır. 1967 yılında ÇHC, atom bomba deneyimini gerçekleştirerek nükleer silah sahibi olmaktadır. Mao'ya göre uluslararası alan, çatışmacı ve her an savaş tehdidiyle karşı karşıya kalınan bir ortam olarak görülmektedir. Mao için ulusal güvenlik ve dış politika oldukça önemli bir konu olmaktadır. ÇHC'nin, ekonomik ve iç güvenlik yönünden kötü bir süreçten geçtiği dönemde dahi Mao bu iki hususta oldukça hassas davranmaktadır. Bundan dolayı ÇHC'yi askeri yönden güçlendirmeye oldukça fazla önem vermektedir (Atawula, 2020: 47-48).

Mao döneminden sonra ÇHC ulusal güvenlik kaygılarının yaşandığı ve ekonomik yönden zayıfladığı bir sürece girmektedir. Dışa kapalı bir tutum sergileyen Mao'dan dolayı ÇHC diplomatik olarak yalnız kalmaktadır. Aynı zamanda yaşanan iç huzursuzluklardan dolayı ideolojik olarak fikir ayrılıklarının yaşandığı bir süreçle karşı karşıya kalınmaktadır. Tüm bu süreçlerden sonra, ÇHC ikinci kuşak lider olarak Deng Xiaoping'i seçerek ekonominin yeniden canlanıp büyümesine sebep olmaktadır. Bu yönde ilerleyen Deng hem ekonomik ilerlemeyi sağlamak hem de Mao döneminde yaşanan ideolojik bölünmeyi iyileştirmek adına birçok strateji gerçekleştirmektedir. Deng döneminde yapılan en önemli stratejiler; Reform ve Dışa Açılma, Çince Sosyalizm, Dörtlü Modernleşme, Dengeleme politikası ve Çoğulcu Diplomasi şeklinde belirlenmektedir.

Bunların yanında, Deng'in güvenlik adına izlemiş olduğu politika olan çoğulcu diplomasi adlı politikaya da değinmekte fayda görülmektedir. Mao döneminde ülke uluslararası alanda bir yalnızlık içerisine girmektedir. Deng bu yalnızlığı gidermek ve ülke ekonomisini sürekli olarak geliştirmek amacıyla ÇHC'yi diplomatik ve finansal

yönden en yüksek konumda uluslararası sisteme entegre etmeye çalışmaktadır. Bu amaç doğrultusunda, 1980’li yılların başlarına gelindiğinde ÇHC’de açık kapı politikasının uygulandığı görülmektedir. Deng’in bu adımıyla beraber ÇHC, neredeyse bütün ülkelerle ve özellikle de Batıda bulunan gelişmiş Kapitalist ülkelerle diplomatik ilişkiler kurmayı hedeflemektedir. Deng’in bu hedefini büyük oranda başardığı gözlemlenmektedir. ÇHC’nin uluslararası alanda yalnızlaştığı süreç sonrasında atılan bu adımla beraber Deng döneminde, ÇHC’nin birçok uluslararası örgüte katıldığı ve anlaşmalara imza attığı bilinmektedir. Ayrıca, ÇHC’nin bu süreçte; yasadışı göç, uyuşturucu kaçakçılığı ve çevre kirliliği gibi hususlardan dolayı transnasyonal güvenlik sorunlarına karşı komşu ülkelerle iş birliği yapmaya başladığı gözlemlenmektedir (Wu, 2001: 278).

Diğer taraftan Soğuk Savaş’ın sona ermesiyle beraber bazı değişiklikler ortaya çıkmaktadır. Bu değişiklikler (Atawula, 2020: 49):

- İki kutuplu uluslararası sistemin çökmesi,
- ABD’nin tek süper güç olarak ortaya çıkması,
- Sovyet tehdidinin ortadan kalkması
- ABD’nin, ÇHC’ye karşı dışarıdan gelecek tehditlerde tek kaynak olarak görülmeye başlanması şeklinde sıralanmaktadır.

Soğuk Savaş sonrasında ÇHC’nin, her ne kadar ilk başta ABD’nin tek kutuplu egemenliğine meydan okuma hususunda geri adım atsa da zamanla artan baskılardan dolayı yeni bir uluslararası sistem arayışına girdiği görülmektedir. Bununla beraber, 1993 yılında ÇHC’nin yönetimine gelen Jiang Zemin, çok kutuplu bir uluslararası sistemi savunmaya başlayarak, güvenlik problemlerinin karşılıklı konuşma ve iş birliği ile çözülmesi gerektiğine sıklıkla vurgu yapmaktadır. Jiang Zemin sürecinde, ÇHC’nin en büyük endişelerinden biri olan ekonomik büyümenin yanı sıra bir de toplumsal istikrarın korunması hususu da iç güvenlik açısından gündeme gelmektedir.

Jiang Zemin’le beraber ÇHC’nin iç durumunda birçok önemli değişimler meydana gelmektedir. Bu değişimlerin en önemlisi ise güvenlik alanında karşımıza çıkmaktadır. ÇHC’nin ulusal güvenlik anlayışına yeni bir boyut kazandıran Jiang Zemin, “yeni güvenlik konseptini” ortaya çıkarmaktadır. Soğuk Savaş sonrasında değişen dünya düzeni ile beraber uluslararası alanda yeni güvenlik koşulları ortaya çıkmaktadır. Bu bağlamda ÇHC ortaya çıkan yeni güvenlik anlayışını, eski güvenlik anlayışında olan yalnızca askeri alana odaklanan anlayışla değil yeni koşullara da ayak

uyduran evrensel bir güvenlik konseptine dönüştürüp geliştirme yoluna gittiği görülmektedir. Bu görüş doğrultusunda ilerleyen ÇHC, 1993 yılından itibaren, Çinli karar vericiler ve akademisyenler aracılığıyla ülkenin güvenlik stratejilerini iyileştirmeye başlamaktadır. Sonuç olarak savunma, ekonomi, siyaset ve diplomasi alanlarını bir arada toplayan çok boyutlu yeni güvenlik konsepti oluşturan Jiang Zemin, ülkenin hedefi olan kalıcı olma ve büyüme hususuna büyük katkı sunmaktadır (Wu, 2001: 278).

Jiang Zemin sonrasında, 2002 yılında ÇHC yönetiminin başına gelen Hu Jintao, ulusal güvenlik problemlerinden biri olan deniz sınır güvenliğinin bu dönemde kötüleşmesiyle beraber, deniz problemlerine yönelik strateji ve politikalarını yeniden gözden geçirmektedir. Hu, deniz sınır güvenliğini korumak ve aynı zamanda deniz sınır anlaşmazlıklarından avantaj elde etmek adına, Güney Deniz’de yer alan askeri gücünü artırma yoluna gitmektedir. Bu şekilde, ABD’yi stratejik olarak ve onun müttefiklerini ise taktiksel anlamda caydırmaya çalıştığı görülmektedir. Deniz sınır anlaşmazlıklarının yanında bir de kara sınır anlaşmazlıkları ile ilgili problem yaşayan ÇHC’nin, Hu döneminde ülke ile komşuları arasındaki sınır anlaşmazlıklarını büyük oranda çözüme kavuşturduğu ifade edilmektedir. Bu anlaşmazlıkları ortadan kaldırmak adına yapmış olduğu müzakereler sonrasında, 2004 yılında ÇHC-Rusya arasındaki sınırların netleşmesi için doğu sınırları üzerine anlaşma imzalandığı vurgulanmaktadır. 2009 yılına gelindiğinde ise bu hususta atılan bir diğer adım olan, ÇHC ve Vietnam arasındaki kara sınırının belirlenmesi gösterilmektedir. Kara sınır anlaşmazlıkları adına birçok sınır problemlerini çözüme kavuşturan Hu yönetiminin yalnızca Hindistan- ÇHC sınır tartışmalarında netliğe kavuşamadığı gözlemlenmektedir (Atawula, 2020: 50). ÇHC’nin ulusal güvenlik gündeminde yer alan bir diğer husus olan ekonomik güvenliği korumak ve piyasada kontrolü elde tutmak adına devlete ait işletmeleri yeniden iyileştirmeye başladığına da değinmek gerekmektedir. Bu doğrultuda bakıldığında, Hu yönetimi 2003 yılında, ekonominin ilerlemesi ve partinin hedeflerine hizmet edebilmesi adına, devlet bankalarının devlete ait işletmelere sürekli borç vermesine karar vermektedir (Blumenthal ve Scissors, 2016).

2012 yılına gelindiğinde ise ÇHC’nin yönetiminde liderliği eline alan Xi Jinping’le beraber yeni dönem ulusal güvenlik anlayışı ortaya çıkmaktadır. Günümüzde liderliği devam eden Xi Jinping’in yeni güvenlik anlayışını farklı bir başlık altında ele almanın daha faydalı olacağı düşünülmektedir.

2.5. Yeni Dönem Ulusal Güvenlik Anlayışı

Değişen dünya düzeni dolayısıyla karşılaşılan tehdit ve çıkarlar ülkelerin her alandaki politikalarını, özellikle güvenlik alanındaki politikalarını, değiştirme gereksinimi doğurmaktadır. Bununla beraber, Xi Jinping 2013 yılında ÇHC yönetimini devraldığı süreçte Mao ve Deng dönemindeki ÇHC'den çok daha farklı bir toplum ve yönetimle karşı karşıya kalmaktadır. Yolsuzlukların yoğun bir şekilde gerçekleştiği, yönetimin kötüleştiği, teknolojinin zarar gördüğü ve bundan dolayı devlet işletmelerinin geri kaldığı, bürokrasinin giderek parçalandığı, koordine edilemediği, ekonomik yönden güç, bilgi ve örgütlenme yetkilerinin dağıldığı bir ortamla karşılaşan Xi, ÇHC toplumunun bu olumsuzluklardan daha da etkilenmemesi adına temkinli hareket etmeye çalışmaktadır. Bunun yanı sıra, Doğu Avrupa ve SSCB'nin çökmesi, Tiananmen krizi, Arap Baharı ve bazı devrim hareketlerinde edinilen tecrübeyi göz önünde bulunduran Xi, ÇKP rejiminin sabote edilmesine karşı duyduğu endişeden dolayı birçok gelişmeyi geri çevirmek durumunda kalmaktadır. Bu endişelerle beraber; 2014-2015 yıllarında Hong Kong ve Tayvan'da oluşan sivil hareketler, Doğu Türkistan ve Tibet'te yaşanan dönemsel huzursuzluklardan dolayı Xi'nin ÇHC'nin bölünme tehdidine karşı endişelerinin giderek arttığı görülmektedir (Lampton, 2015: 112).

Öte yandan, ÇHC'nin yükselmesi ve küresel bir güç hâline gelmesi, ulusal güvenlik tehdit ve çıkarlarının da küreselleşmesine sebep olmaktadır. Ekonomik alanda ilerleyen ÇHC'nin, yurtdışına yaptığı yatırımların artmasıyla ve giderek zenginleşen Çinlilerin farklı ülkelere açılmasıyla beraber tehdit ve risk boyutunun da arttığı görülmektedir. ÇHC'nin yükselişinden dolayı, yurtdışında sahip olduğu varlıkları korumak, enerji koridorlarının, kara ve deniz yollarının teminatını sağlamak ÇHC liderlerinin ulusal güvenlik gündeminde yerini almaktadır. Bu duruma en iyi örnek, 2014 yılında gerçekleştirilen Merkez Dış İlişkiler Çalışma Toplantısı'nda Xi'nin yapmış olduğu konuşma gösterilmektedir. Bu toplantıda Xi Jinping, sürekli olarak ÇHC'nin yurtdışındaki çıkarlarını koruma hususunun önemine vurgu yapmaktadır. Aynı zamanda koruma kapasitesinin geliştirilmesi ve seviyesinin artırılması gerekliliğinin altını çizmektedir (Xinhua, 2014).

Diğer taraftan, Soğuk Savaş sonrası güvenlik alanına ilişkin ÇHC'nin güvenlik algısının değişmesine sebep olan durumları biraz toparlamak gerekirse; büyük güç savaşının olmaması, küreselleşme, ABD'nin ortak ve rakip olması, geleneksel olmayan güvenlik sorunlarının yaşanması, enerji hususundaki güvensizlik ve en önemlisi

ÇHC'nin yükselişi gibi karşılaşılan altı eğilim dolayısıyla ÇHC'nin güvenlik anlayışının değiştiği görülmektedir (Kumar, 2012). ÇHC'nin yükselmesi ve zamanla küresel bir güç hâline gelmesiyle beraber, yurtdışındaki vatandaşları ve aynı zamanda varlıklarını koruma durumunu ulusal güvenlik politikasının temel görevi olarak tanımladığı belirtilmektedir. Bu duruma verilebilecek en iyi örnek ise 2015 yılında yayımlanan Beyaz Kitap'tır. ÇHC'nin yurt dışındaki güvenliğini ve çıkarlarını korumayı hedefleyen ÇHC, bunu sağlamak adına kitapta, PLA'nın sekiz stratejik görevinden birinin bu olduğunu söylemektedir (ÇHC Devlet Konseyi Basın Ofisi, 2015). Bunun yanı sıra, güvenlik hususunun sağlamlaştırılması ve genişletilmesi Xi döneminde her geçen gün yeni boyutlara ulaşmaktadır. 2013 yılında yönetime geldiği andan beri bunu yansıtan Xi, güvenliği açıkça siyasi projenin merkezine yerleştirmektedir (Nyman, 2023: 687). Xi Jinping, ülkenin yeni döneme girmesiyle beraber hem ideolojik açıdan hem de politik açıdan bu dönemin koşullarına uygun değişimlere imza atmaktadır.

- İdeolojik açıdan: Ülkenin değişen tehdit ve çıkarlarına uygun yeni bir ulusal güvenlik doktrini geliştirilmeye çalışılmaktadır.
- Politik açıdan: ÇHC'nin ulusal güvenlik hususunda görev alan karar alma mekanizmasını yeniden yapılandırma yoluna gitmektedir.

Tüm bu gelişmeler doğrultusunda genel bir yorum yapmak gerekirse, ÇHC'nin bu dönemde iç güvenlik hususunda alınabilecek önlemleri sertleştirdiği ve dış politikada ise agresif bir tutum sergilediği görülmektedir. ÇHC'nin hem politikadaki etkisini arttırmak hem de dönemin şartlarından dolayı ekonomide yaşanan durgunluğu önlemek amacıyla Xi yönetiminin iki önemli girişimi bulunmaktadır (Atawula, 2020: 54). Bu girişimler:

- Bir Kuşak, Bir Yol Projesi
- Asya Altyapı Yatırım Bankası şeklinde belirtilmektedir.

Xi Jinping döneminin politikalarını şekillendiren bu girişimlerden özellikle "BKBY" projesinin güvenlik bağlamında analiz edilmesinin faydalı olacağı düşünülmektedir. Bu bağlamda, Xi Jinping Eylül 2013'te, Kazakistan'da, ÇHC'nin nüfusu ve aynı zamanda ekonomisi ile paralel olan çok büyük bir proje ortaya koymaktadır. O dönemde ÇHC'nin bu proje dolayısıyla dünya gündeminin ilk sırasına hızlı bir giriş yaptığı görülmektedir. M.Ö. 2. yüzyıldan ve M. S. 16. yüzyıla kadar, bölgenin ticaretinde büyük öneme sahip olan İpek Yolu'nu yeniden canlandırmayı amaçlayan bu proje; Hindicini, Ortadoğu, Orta Asya, Kafkasya, Avrupa ve Avrasya

bölgeleriyle, içinde Türkiye'nin de yer aldığı 60'tan fazla ülkeyi kapsamaktadır. Bu ülkelerde bulunan yaklaşık 4,5 milyar insanı birbirine bağlamayı hedefleyen proje, 20 trilyon dolar değerinde bir maliyete sahip olmaktadır. Eski İpek Yolu gibi yalnızca karadan bağlantısı olmayan bu projenin iki ayağı bulunmaktadır. Hem karadan hem de denizden bağlantısı olan bu projenin; köprüler, limanlar, lojistik üsler, enerji santralleri, havalimanları, petrol ve doğalgaz boru hatları ile gerçekleştirilmesi planlanmaktadır (Erdoğan, 2020: 89; Önür, 2021: 42).

Bununla birlikte, ortaya koyulan BKBY projesi dolayısıyla ÇHC'nin yurtdışındaki çıkarlarının daha da genişlediği görülmektedir. Projeyle beraber, ÇHC'nin sermayesinin rastgele bölgelere yayılması, ülkenin yurt dışındaki varlıklarının tehditlere daha açık bir hâle gelmesine sebep olmaktadır. Söz konusu projenin kritik noktalarından biri güvenliği sağlamaktır. Bu durum Çinli uzmanların üzerinde durduğu bir husus olarak sürekli tartışma konusu hâline gelmektedir. Özellikle 2016 yılında Kırgızistan'daki ÇHC Büyükelçiliğine yapılan intihar saldırı sonrasında güvenlik hususu ile ilgili tartışmaların daha da arttığı belirtilmektedir (Mokry, 2016). Bu bağlamda, BKBY projesinin karşılaştığı güvenlik problemlerini dile getirmek amacıyla 4 Mayıs 2017 yılında Pekin'de "Kuşak ve Yol Güvenlik İşbirliği Diyalogu" düzenlenmektedir. Güvenlik sorunlarıyla ilgili düzenlenen ilk uluslararası konferans olma özelliğine sahip olan bu konferansa başta; Pakistan, Vietnam, Rusya, Türkiye, Suudi Arabistan, İspanya ve Belarus olmak üzere 20'den fazla ülkenin güvenlik bakanlıklarının katılımıyla bir takım hususlar üzerinde durulmaktadır. Bu hususlar şu şekilde belirtilmektedir (Xinhua, 2017):

- Kamu Güvenliği
- Terörle Mücadele
- Denizaşırı Çıkarların Korunması

Diğer yandan, yeni dönemde özellikle yurt dışındaki varlıklarının güvenliğini ve çıkarlarını korumak adına kara güvenliğinin yanı sıra deniz güvenliği üzerinde de duran ve bu doğrultuda stratejiler belirleyen ÇHC, karşılaşılan tehditlerle beraber daha sıkı önlemler alarak Çin Deniz Kuvvetleri'nin daha geniş bölgelerde harekete geçmesi yönünde çalışmalar yürütmektedir. Yeni dönemde güvenlik hususunda vizyonunu giderek genişleten ÇHC'nin bir diğer adımının ise Asya'ya yönelik olduğu belirtilmektedir. Asya'ya ait kendi güvenlik vizyonunu ortaya koyan ÇHC, 2014 yılında gerçekleştirilen "Asya'da Etkileşim ve Güven Oluşturma Önlemleri Konferansı'nda" bu

husus ile ilgili açıklamalar yapmaktadır. Konferansta, yeni Asya güvenlik konsepti ile ilgili vurgu yapan Xi Jinping'in bu husus ile ilgili; Asya'da yaşanan problemlerin Asya halkı aracılığıyla çözüme kavuşturulması ve buranın güvenliğinin Asya halkı aracılığıyla sağlanması gerektiği ile ilgili açıklamalarda bulunduğu görülmektedir (Xi, 2014; China Military, 2017). Bu husus ile ilgili 2017 yılında ilk politika belgesi yayımlayarak Asya Pasifik'te güvenlik iş birliğine değinen ÇHC, bölge ülkelerini "ittifaklar" yerine "ortaklıklar" kurmaya çağırmaktadır (Huotari vd., 2017: 27).

Başka bir yönden bakıldığında ÇHC'nin, yalnızca fiziksel dünyada değil aynı zamanda sanal dünyada da yükseldiği görülmektedir. Teknolojinin ilerlemesiyle beraber karşılaşılan siber problemler, ÇHC'nin sanal dünyadaki varlığının genişlemesiyle beraber sık sık karşılaşılan sorun olarak karşımıza çıkmaktadır. Bundan dolayı, siber ve uzay güvenliğini ülkenin ulusal güvenlik çıkarları listesine ekleyen Xi yönetimi, bu alanda gelişmeye büyük önem vermektedir. Xi Jinping'in bu alanda yapmış olduğu ilk çalışmalar (Huotari vd., 2017: 27):

- 2013 yılında Çin Askeri Bilimleri Akademisi aracılığıyla yayımlanan "Strateji Bilimi" ve 2015 yılında yayımlanan Beyaz Kitapta; ÇHC'nin siber alandaki altyapılarına düzenlenen saldırılardan dolayı, siber ve uzay alanları ülkenin stratejik rekabet alanları ve askeri mücadele alanları olarak gösterilmektedir.

Tüm bunlara ek olarak ÇHC açısından ulusal güvenlik anlayışına bakıldığında, söz konusu anlayış ülkenin hayatta kalması ve gelişmesi için bir ön koşul, halkın mutluluğu ve refahının temeli ve Çin özelliklerine sahip sosyalizm davası için önemli bir garanti olarak görülmektedir (Zhong, 2017). Xi Jinping ulusal güvenlik kavramını, ulusal kalkınmanın en önemli unsuru olarak görmektedir. İnsanların refahının sağlanmasında en temel hususun ulusal güvenlik olduğunu belirten Xi Jinping, bu düşüncesini geliştirmek adına bazı adımlar atmaktadır. Bu adımlar şu şekilde sıralanmaktadır (Chinadaily, 2017):

- Nisan 2014'te Merkezi Ulusal Güvenlik Komisyonu'nda düzenlenen ilk genel kurul toplantısında ilk defa "genel ulusal güvenlik konseptini" resmen ortaya koyduğu görülmektedir.
- Temmuz 2015'te, 12. Ulusal Halk Kongresi Daimi Komitesi'nin 15. Oturumunda, 15 Nisanı "Ulusal Güvenlik Eğitim Günü" olarak ilan ederek

ÇHC Ulusal Güvenlik Yasasını kabul ettiğini açıklamaktadır. Bu doğrultuda Xi'nin ulusal güvenliğe verdiği önemin altı bir kez daha çizilmektedir.

- Ocak 2017 tarihine gelindiğinde ise yeni dönemde karşılaşılan bütün ulusal güvenlik tehdit ve çıkar alanları Xi Jinping'in yeni ulusal güvenlik doktrini olan “kapsamlı güvenlik görüşü” adı altında birleştirildiği görülmektedir.

Bu bağlamda yeni dönemle birlikte değişen ÇHC'nin ulusal güvenlik anlayışı, Xi Jinping'le beraber daha da şekillenmeye başlamaktadır. Bundan dolayı Xi'nin, yeni dönemin başlaması sonucu ortaya çıkan yeni tehdit ve çıkarları yönetebilmek adına, ülkenin yeni durumuna uygun olabilecek şekilde kapsamlı bir ulusal güvenlik doktrini ortaya koyduğu görülmektedir. Bu yeni anlayış, temeli siyasi güvenlik olan ve siber güvenlik kadar geniş kapsamlı konuları içeren 11 farklı alandan oluşmaktadır. Bunlar şu şekilde belirtilmektedir (Chinadaily, 2017; Renminwang, 2019; Nyman, 2023: 687):

- Siyasi Güvenlik
- Sınırsal (Teritoryal) Güvenlik
- Askeri Güvenlik
- Ekonomik Güvenlik
- Kültürel Güvenlik
- Sosyal Güvenlik
- Teknoloji Güvenliği
- Veri Güvenliği
- Ekolojik Güvenlik
- Kaynak Güvenliği
- Nükleer Güvenlik

Bunun yanında, ulusal güvenliği karmaşık bir yapı olarak gören Xi Jinping, ÇHC'nin hâlihazırdaki ulusal güvenlik içeriğinin, zaman ve mekân boşluğunun tarihteki herhangi bir dönemdekinden daha zengin ve geniş olduğunu belirtmektedir. Tarihteki herhangi bir zaman aralığına bakıldığında ÇHC'nin iç ve dış faktörlerinin daha karmaşık olduğu görülmektedir. Bundan dolayı Xi Jinping, güvenlik hususunda eşitlikten yana olduğunu dile getirmektedir. Yani dış güvenlikle beraber iç güvenliğe, klasik güvenlikle beraber klasik olmayan güvenliğe ya da toprak güvenliğiyle beraber halkın güvenliğine eşit önem verilmesi gerektiğini savunmaktadır. Savunduğu düşünce dolayısıyla Xi'nin ortaya koyduğu Kapsamlı Ulusal Güvenlik Görüşü sözü geçen on bir farklı alandaki ulusal güvenliğin birleşiminden oluşmaktadır (Renminwang, 2019).

Genel olarak ÇHC’ nin ulusal güvenlik anlayışı değerlendirildiğinde; Soğuk Savaş anlayışı üzerine oluşturulduğu görülmektedir. Yani insani güvenlik göz ardı edilerek daha çok egemenlik ve toprak bütünlüğü gibi konular üzerinde durulmaktadır. Fakat Xi Jinping ÇHC’nin klasik güvenlik anlayışından farklı olarak Kapsamlı Ulusal Güvenlik Görüşü’nden daha çok insan güvenliğine dikkat çektiği görülmektedir. Xi’nin ortaya koyduğu bu görüşün dört ana hedefi bulunmaktadır. Bunlar şu şekilde belirtilmektedir (Li, 2015: 153-154; Liu, 2017: 39):

1. “İnsanların güvenliğini hedef olarak gören” Çin özelliklerine sahip bir ulusal güvenlik yolu izlemek.
2. Dış ve iç, geleneksel ve geleneksel olmayan güvenlik konularını bütünleştiren bir ulusal güvenlik sistemini oluşturmak.
3. Güvenlik ve kalkınmayı eşit bir temele oturtmak ve güvenlik ve kalkınma merkezli yeni bir zihniyet oluşturmak.
4. Diğer ülkelerin güvenliğini ÇHC’nin güvenliğiyle yakından ilişkilendirerek "uluslararası güvenliğin teşvikine dayalı" ortak güvenlik kavramını savunmak ve buna teşvik etmek.

Kapsamlı Ulusal Güvenlik Görüşü yalnızca günümüzde karşımıza çıkan ulusal güvenlik problemlerini değil aynı zamanda ileriki süreçlerde karşılaşılan problemleri ele alarak teorik bir çerçeve çizmektedir. Böylesi kapsamlı ulusal güvenlik zihniyetiyle beraber Xi Jinping’in ve önderliğindeki ÇKP’nin ÇHC’nin her ortamda ve hususta kendi otoritelerini korumayı düşündükleri görülmektedir (Zhong, 2017). Bu doğrultuda Xi Jinping’in sürekli olarak vurguladığı bazı hususların olduğu ifade edilmektedir. Bunlar şu şekilde karşımıza çıkmaktadır (Xinhua, 2018):

- Partinin ulusal güvenlik çalışmaları üzerindeki mutlak liderliğini sürdürmenin ve daha etkili liderlik ve koordinasyon uygulamanın gerekliliği,
- Parti Merkez Komitesinin otoritesini, merkezi ve birleşik liderliği kararlılıkla korumak ve sadık, güvenilir bir ulusal güvenlik birliği oluşturmanın gerekliliğinden söz edilmektedir.

Kapsamlı Ulusal Güvenlik Görüşünü bir tür ÇHC’nin genel stratejisinin açıklaması olarak gören ve bu stratejinin dışa yansımaları olarak ele alan Xi Jinping, Mayıs 2014’de Shanghai’da düzenlenen dördüncü zirve olan, Asya’da Etkileşim ve Güven Oluşturma Önlemleri Konferansı’nda “ortak çalışmaya dayalı, kapsamlı ve sürdürülebilir” yeni bir Asya güvenlik konsepti ortaya koymuştur. Bu ortaya atılan yeni

güvenlik konseptinin ÇHC'nin dış politika yönelimini yansıttığı görülmektedir (Renminwang, 2019). Yeni döneme girilmesinin ardından sürekli olarak savaş tehditlerine maruz kalan ÇHC'nin bu durumundan dolayı Xi Jinping, bir yandan barışçıl kalkınma yolunda ilerlerken diğer yandan da haklı çıkarlarını korumak adına kendilerinden ödün vermeyeceğinin vurgusunu yapmaktadır (Zhang, 2015; Li, 2015: 156).

Günümüzde de ulusal güvenlik üzerinde büyük bir titizlikle duran Xi Jinping, ÇHC'nin ulusal güvenliğini korumak adına ülkenin üst düzey ulusal güvenlik yetkililerini yaşanacak olası en kötü senaryoları düşünmeye ve güvenlik sistemlerini bu doğrultuda modernize etmeye çağırılmaktadır. 2023 yılının Mayıs ayı sonunda Xi Jinping, ÇKP'nin Ulusal Güvenlik Komitesi ile yapmış olduğu görüşmede “ülkenin şu anda karşı karşıya olduğu ulusal güvenlik sorunlarının karmaşıklığı ve zorluğunu, bu nedenle her türlü iç ve dış tehdide karşı koymak için çabaların yoğunlaştırılması gerektiğini” vurgulamaktadır. 2012 yılında iktidara geldiğinden beri ulusal güvenliği yönetişimin her alanında merkezi bir paradigma hâline getiren Xi Jinping'in, ulusal güvenlik kavramını; siyaset, ekonomi, kültür, savunma ve çevreden siber uzaya, hatta derin deniz, kutup bölgeleri ve uzayın yanı sıra büyük veri sistemleri ve yapay zekâya kadar her şeyi kapsayacak şekilde genişlettiği görülmektedir (Helmy, 2023).

Genel bir değerlendirme yapıldığında, ÇHC ulusal güvenliğinin ve ekonomik çıkarlarının korunması noktasında güvenlik ve kalkınma arasında daha yoğun bir koordinasyonun sağlanması gerektiğine odaklanmaktadır. ÇHC'nin ulusal güvenlik hususundaki amacı; dış dünyaya açılma durumunu daha güvenli hâle getirmek, korumak, kalkınma ve güvenliğin derin entegrasyonunu teşvik etmek aynı zamanda ulusal güvenliği sağlamak ve bu hususta reform yapma ihtiyacını etkili bir şekilde gerçekleştirmek için ÇHC çevresinde elverişli bir dış güvenlik ortamı oluşturmak şeklindedir. Bundan dolayı ÇHC, ulusal güvenliğini siyasi olarak sağlamaya yönelik yapmış olduğu en önemli çabaların; internet verilerinin ve yapay zekânın güvenlik yönetimini geliştirerek Pekin'in ve iktidardaki Komünist Parti liderlerinin karşılaşılabilecek herhangi bir dış müdahale durumunda ülkenin ulusal güvenliğini koruması amacıyla güvenlik risklerinin izlenmesini ve erken uyarılmasını sağlayan bir sistemin kurulmasını hedeflemektedir..

ÜÇÜNCÜ BÖLÜM

3. Çin Bağlamında Siber Güvenlik

Küreselleşme ile beraber hayatın her alanında birçok değişim ve dönüşümün olduğu gözlemlenmektedir. Bu değişimlerin en büyüğü teknoloji alanında gerçekleşmektedir. Bilişim çağının hâkim olduğu ve hayatımızın büyük bir parçası hâline gelen teknoloji ağırlıklı bu dönemde devletler, karşılaşılabilecek herhangi bir risk ve tehdide karşı kendilerini savunmak amacıyla çeşitli siber güvenlik politikaları belirlemek zorunda kalmaktadır. Siber uzayın hâkim olduğu ve gerçek ve sanal dünyanın içiçe geçtiği bu dönem yeni sorunları da beraberinde getirmektedir. Bundan dolayı, siber uzayda belli bir güce sahip olmak ve bu alanı kontrol altında tutmak oldukça önemli bir hâl almaktadır. Devletlerin, kamu kurum ve kuruluşların, özel sektörlerin vs. böylesine önem arz eden bu konu ile ilgili birçok çalışmaları bulunmaktadır. Bu noktada büyük önem arz eden siber güvenlik olgusu ile ilgili, teknolojinin önde gelen isimlerinden ve son zamanlarda yaşanan siber saldırılarda en fazla hedef gösterilen ülkelerden biri olan ÇHC ne gibi bir yol izledi? sorusu çalışmanın temel konusunu oluşturmaktadır.

Bu bölümde çalışmanın nihai konusu olan ÇHC'nin siber güvenlik politikaları ele alınmadan önce; internet gelişimi ve aynı zamanda siber uzay, siber egemenlik, bilgi güvenliği, oluşan siber güvensizlik gibi konular ÇHC bağlamında ele alınmaktadır. Akabinde, ÇHC'nin siber güvenlik ile ilgili yapmış olduğu çalışmalara, yasalara, politikalara vs. değinilmektedir. Son olarak, ÇHC'ye yönelik yapılan siber saldırılar/iddialardan söz edilmektedir.

3.1. Çin'de İnternetin Gelişim Süreci

ÇHC'nin internet gelişiminden söz etmeden önce genel olarak internetin ne olduğunu ve ilk olarak nerede ortaya çıktığı ile ilgili genel bir çerçeve çizilmesi, konunun detaylı olarak anlaşılması açısından fayda sağlayacaktır. Bundan dolayı ilk önce kısaca internetin tanımına ve ilk nerede, hangi amaçla ortaya çıktığına değinilmektedir. Akabinde ise ÇHC bağlamında internet gelişimi analiz edilmektedir.

Dünya genelinde binlerce bilgisayar ağını, bazı standart ve protokoller kullanarak birbirine bağlayan bir ağ olarak, iletişim ve haberleşme teknolojilerinin bilinen özelliklerinin sınırlarını zorlayan ve iletişim uygulamalarını büyük oranda

dönüşüme uğratan teknoloji *internet* olarak ifade edilmektedir (Lyytinen ve King, 2002: 97). 1950’li yıllarda bilgisayarın gelişmeye başlamasıyla oluşan internetin genel tarihine bakıldığında, ilk olarak 1960’lı yıllardan itibaren ABD’de askeri amaçlı bir proje ile ortaya çıktığı görülmektedir. 1970’li yılların başında ABD Savunma Bakanlığı askeri araştırma yapmak ve teknoloji ile bilimde öncü rol oynamak amacıyla *İleri Araştırma Projeleri Yerel Ağı* (ARPANET) adında bir bilgisayar ağı oluşturmuştur. Günümüzde bulunan internetin temelini oluşturan ARPANET adlı bu ağ yardımıyla askeri üsler arasında bilgi akışının sağlandığı belirtilmektedir. Nitekim, 1972 yılında düzenlenen konferans vasıtasıyla kamuoyuna tanıtılan internet, ilk olarak askeri amaçla geliştirilen bir proje olsa da zaman içerisinde başta üniversiteler olmak üzere, devlet kuruluşlarına ve özel şirketlere kadar geniş bir yelpazede kullanılmaya başlanmaktadır (Güçdemir, 2012: 373).

Özellikle 1990’lı yıllarda küreselleşmenin yoğunlaşmasıyla beraber internetin dünyada büyük bir yere sahip olduğu görülmektedir. Günümüzde ise hemen hemen her devlet internet ağına sahiptir. Yukarıda belirtildiği gibi ilk başlarda kullanım amacı askeri yönden sınırlı olan internetin, daha sonraları bilim kuruluşları ve araştırmalarda yoğunluklu olarak kullanıldığı ve günümüze bakıldığında kullanım açısından artık bu amaçlarla da sınırlı kalmadığı; iletişim, eğitim, medya, sağlık, ticaret, siyaset vs. her alanda farklı amaçlarla kullanıldığı yadsınamaz bir gerçek olarak karşımıza çıkmaktadır.

Günümüzde internet ve teknoloji alanında büyük yere sahip olan ÇHC’de internet gelişimi hangi adımlarla gerçekleşti? sorunun yanıtını alabilmek adına internet kavramı ve gelişimi, ÇHC bağlamında analiz etmek önem arz etmektedir. Geçen bin yıllık süreçte en dikkat çeken yeniliklerden biri olarak kabul gören internet ile ÇHC diğer gelişmiş ülkelere göre biraz daha geç tanışmaktadır. Fakat yine de günümüze bakıldığında ÇHC, internetin büyümesi ve gelişmesine büyük katkı sağlamaktadır (Verma, 2012). Çalışmanın ikinci bölümünde de belirtildiği üzere, ÇHC’nin ilk kurucu lideri olan Mao Zedong 1976 yılında hayatını kaybettikten sonra, de facto lider olarak 1978 yılında Deng Xiaoping’in başa geldiği bilinmektedir. Ekonomi odaklı politikalar izleyen Deng, ÇHC için büyük bir reform programı başlatmaktadır. Bu program ile ÇHC’nin, ekonomik yönden dışa açılmasını sağlayarak hızlı bir ekonomik yükselişe geçtiği görülmektedir. Yaşanan bu ekonomik büyüme ile beraber, 1980’li yılların ÇHC’nin internet ve bilgisayar teknolojisini adım adım keşfetmeye başladığı yıllar olduğu söylenmektedir. ÇHC’nin internetle tanıştığı ve internet açısından önemli

dönüm noktaları olarak bilinen yılların; 1986 ve 1987 yılları olduğu belirtilmektedir (Pekcan, 2020: 207). Nitekim ÇHC internet ile ilgili ilk adımını dönüm noktası olarak belirlenen 1986-1987 yıllarında atmaktadır. Bu adımlar şu şekilde ele alınmaktadır:

- Çin Bilim Akademisi Yüksek Enerji Fiziği Enstitüsü'nden Wu Weiming'in 25 Ağustos 1986 yılında, Pekin'den Cenevre'de Avrupa Nükleer Araştırma Merkezi'ndeki (CERN) Profesör Steinberger'e ilk e-maili göndermesi (Weimin, 2007: 7),
- 1987 yılında Pekin'de oluşturulan Çin Akademi Ağı'nın (CANet), "Çin Seddi'nin üzerinden dünyanın tüm köşelerine ulaşabiliriz" yazılı e-maili Almanya'da bulunan Karlsruhe Üniversitesi'nin iş birliği ile Almanya'ya göndermesi (Dazhou ve Kaishi, 2016: 158).

ÇHC'nin internet hususunda attığı ilk adımların akabinde, bu gelişmelerden sonraki süreçte internet teknolojilerini geliştirme yoluna gittiği görülmektedir. Bu maksatla ÇHC'nin, internet teknolojilerine daha fazla bütçe ayırmaya başladığı ve CERNET, ChinaNet, ChinaGBN gibi ulusal ağlar oluşturmaya başladığı gözlemlenmektedir (Dazhou ve Kaishi, 2016: 158). 1994 yılında ise ÇHC, sürekli devlet desteği alan ve ileri görüşlü hedeflerle tam işlevsel internet erişimine sahip ülke olarak kabul edilmektedir (Qiu, 2003: 1). Bununla beraber, 1995 yılından beri ÇHC'nin internetinin hızla geliştiği ortaya konmaktadır. ÇHC'de internet hususunda bir diğer dönüm noktasının, 1995 yılında internetin halkın kullanımına açılması olarak ifade edildiği görülmektedir. ÇHC, yaşanan bu gelişmelerle beraber internet altyapısına muazzam miktarda yatırım yapmaktadır. 1997 yılından 2009 yılına kadar 4,3 trilyon Yuan yatırım yapıldığı ve ülke genelinde toplam uzunluğu 8,267 milyon km olan optik iletişim ağı kablosu inşa edildiği ifade edilmektedir. İnşa edilen bu kabloların 840,000 km'sinin ise uzun mesafeli optik kablosu olduğu belirtilmektedir (Verma, 2012). Bunun yanında, ÇHC'de internete erişebilen toplam bilgisayar sayısının 1998 yılı itibarıyla 747,000'e ulaştığı söylenmektedir. Öte yandan, 1999 yılının Şubat ayında Çin Bilgi Teknolojisi Güvenlik Değerlendirme Merkezi'nin (CNISTEC) resmi faaliyetine başladığı görülmektedir. Aynı yılın Temmuz ayında ise china.com ABD'deki NASDAQ'da listelenen ilk Çinli ağ şirketi olarak kayıtlara geçmektedir (CNNIC, 2012).

Diğer yandan, 1999 yılında ÇHC'nin bilgi teknolojilerine daha çok önem vermesi yönünde iki önemli olayın yaşandığı görülmektedir. Bunlar; Falun Gong ve

ABD'nin Belgrad'da bulunan ÇHC Büyükelçiliği'ni bombalaması olayları olarak karşımıza çıkmaktadır. Yaşanan bu iki olay neticesinde internete verilen önemin artışı ve farklı adımların atıldığı ifade edilmektedir (Pekcan, 2020: 20). Bu doğrultuda Li Hongzhi tarafından 1992 yılında bulunan ve ÇHC'nin Changchun şehrinde halka tanıtılan *Falun Gong* ya da diğer adıyla *Falun Dafa*, dünyanın dört bir yanındaki milyonlarca insanın yaşamlarının bir parçası hâline gelen spiritüel bir uygulama olarak ortaya çıkmaktadır. Falun Gong kendi sitelerinde “yapılan bazı egzersizler ile evrenin en yüksek nitelikleri olan Zhen-Shan-Ren'e (Doğruluk-Merhamet-Hoşgörü) asimile olmayı hedefleyen bir disiplin” şeklinde tanımlanmaktadır. Falun Gong'da benimsenen inanca göre, disiplinli bir uygulama yolu izlenerek spiritüel gelişim sağlanmaktadır. Geliştirilen bu spiritüel sayesinde öğrenilen öğretilerle evreni yaşam merkezine alan ve bunu temel nitelik olarak kabul gören Falun Gong; doğruluk, merhamet ve hoşgörüye uyum göstermeye başlayarak zararlı alışkanlık ve takıntıları bırakmaya teşvik etmektedir (Falun Dafa, 2020).

Gösterilen bir dizi egzersizlerle beraber beden ve zihnin geliştirilerek bireyin iç huzura ve sağlıklı bir yaşam sürdürmesine yardımcı olan Budist ve Teoist öğretilere dayanan bir uygulama olarak ifade edilen Falun Gong, hızla tüm ÇHC'ye yayılarak kısa sürede en az 70 milyon insan tarafından uygulanmaya başlamıştır. Uygulamanın zamanla ÇHC ile sınırlı kalmayıp, tüm dünyaya yayılarak, birçok ülkeden destek gördüğü ve ödüle layık görüldüğü söylenmektedir. Başlarda ÇHC hükûmeti Falun Gong'a izin verse de zamanla bu düşüncenin değiştiği tespit edilmektedir. Önceleri ruhani bir uygulama olarak kabul gören Falun Gong, zaman içerisinde ‘mezhep’ ya da ‘tarikat’ olarak görülmeye başlayarak, yetkililer tarafından ‘şeytani din’ olarak ifade edilmektedir (Chan, 2004: 670).

Bununla birlikte, 25 Nisan 1999 yılında devletin kendilerine yönelik şüpheleri dolayısıyla yaklaşık 10,000 ila 30,000 Falun Gong uygulayıcısı Pekin'de toplanmıştır. Elleri Li'nin yazılarını tutan grupların sessizce oturup meditasyon yaparak protesto gösterisinde bulunduğu söylenmektedir. Devletin kendilerini itibarsızlaştırdığını düşünerek başlatılan protestolarda devlete açık bir mektup sunularak bazı taleplerde bulunmaktadır. Bu talepler; resmi tanınma ve ifade, basın ve toplanma özgürlükleri için anayasal haklar talep etme şeklinde kendini göstermektedir. Bunun yanı sıra, aynı yılın Mayıs ve Haziran ayları arasında yapılan protestolar sonrasında ÇKP

liderleri, uygulamayı yasaklayıp yasaklamama konusunda ikiye ayrılarak çelişkili mesajlar vermiştir (Lum, 2001: 2).

Sonuç olarak, ÇKP'nin yaşadığı fikir ayrılıklarına rağmen, 21 Temmuz 1999 yılında Falun Gong uygulaması yasa dışı ilan edilerek, liderlerinin de yasaklanması istenmiştir. Yaşanan bu sürecin akabinde, yüzlerce kişinin gözaltına alındığı ve sorgulandığı açıklanmaktadır. Aynı zamanda birçok kişinin hapishanedeyken hayatını kaybettiği vurgulanmaktadır (Ownby, 2008: 162). Falun Gong liderleri ise devlet savcıları tarafından, “devlet sırlarını yabancılara sızdırmak”, “kamu düzenini bozmak, adaleti engellemek, yasadışı toplanma vs.” gibi çeşitli suçlarla itham edilmektedir. Yapılan varsayımlar neticesinde, 150-450 grup lideri ve grup üyelerinin 18 yıla kadar hapis cezasına çarptırıldığı belirtilmektedir (Lum, 2001: 3).

Söz konusu protestolara ÇHC'nin bilgi teknolojilerine vermiş olduğu önemin artmasına katkı sunması yönünden bakıldığında, bu protestolarda en temel faktörün internet olduğu vurgusu yapılması, internetin gelişimine yönlük yapılan katkıyı bir kez daha gözler önüne sermektedir. Falun Gong liderlerinden birinin, yapılacak olan gösterilerde toplanmak maksadıyla kişileri yönlendirmek için interneti temel faktör olarak kullanması, internetin kitlesel bir eyleme yol açtığını göstermektedir. Bundan dolayı Falun Gong uygulamasında ÇHC'yi bilgi teknolojileri hususunda tetikleyen en temel nokta internet olarak karşımıza çıkmaktadır. Bu durum ise ÇHC'nin internet hususuna daha fazla eğilim göstermesine yol açmaktadır (Austin, 2014: 41). Yaşanan olaylar ışığında ise internetteki özgür bilgi dolaşımının ve bilgi toplumu düşüncesinin ÇKP'nin çıkarlarına ters düştüğü görülmektedir. Bu durumun toplumda kargaşaya ve örgütlenmeye sebep olduğu yaşanan olaylarla netliğe kavuşmaktadır. Tüm bu olaylar neticesinde, ÇHC'nin internet üzerinde sansür uygulama fikrinin temellerinin bu dönemde atıldığı ifade edilmektedir (Pekcan, 2020: 208).

Öte yandan, ÇHC'nin internet ile ilgili tutumunu ve söz konusu alandaki hâkimiyetini anlamak adına, internette uygulamış olduğu sansür uygulamasına değinmek gerekmektedir. Bu bağlamda, internet ile ilgili sansürleme çalışmalarının sıkça yaşandığı ÇHC'de, yapılan sansürleme adımlarından sonra kesin olarak ilk sansürlemenin 11 Temmuz 2003'te başladığı görülmektedir. Nitekim sansürleme ile ilgili yapılan 1998 yılındaki “Altın Kalkan Projesi'nin” (diğer adıyla “Çin Güvenlik Seddi” projesinin) 2003 yılına kadar etkinleştirilmediği belirtilmektedir. Projeyi hayata geçirmek amacıyla batılı ülkelerden internet güvenliği, video gözetleme, insan yüz

tanıma sistemleri gibi birçok yüksek teknoloji ürünü satın alınarak ve bu dev sistem için 30.000-50.000 civarında polis görevlendirilerek harekete geçildiği gözlemlenmektedir. Buradaki amacın ise ÇHC’de bulunan bütün yazılı, sesli ve görüntülü veri trafiğinin yoğun olduğu internetin, polisler tarafından izlenerek ülkenin internet güvenliğinin sağlanması olduğu ifade edilmektedir (Gülezer, 2014).

Diğer taraftan, 1999 yılında ÇHC’nin bilgi teknolojilerine daha çok önem vermesi yönünde gerçekleşen bir diğer olayın ise ABD’nin Belgrad’da bulunan ÇHC Büyükelçiliği’ni bombalamasıdır. 7 Mayıs 1999 yılında NATO, Yugoslavya’da Arnavutlara karşı gerçekleştirilen vahşeti durdurmak maksadıyla Sırp'lara yönelik hava harekâtına başladığı süreçte Belgrad’ı bombaladığı sırada 5 bombanın Belgrad’daki ÇHC Büyükelçiliği’ne isabet ettiği belirtilmektedir (Ponniah ve Marinkovic, 2019). Gerçekleşen bombalama sonucunda, 3’ü Çinli gazeteci olmak üzere 4 kişinin yaşamını yitirdiği ve 27 kişinin ise yaralandığı belirtilmektedir (Alperen, 2021). ABD Başkanı Bill Clinton, asıl vurmak istedikleri noktanın Yugoslav Federal Arz ve Tedarik Müdürlüğü olduğunu ve harita hatası yaparak kazara ÇHC Büyükelçiliği’ni vurduklarını dile getirip özür dilemiştir. Fakat birçok tanınmış gazetenin (the Guardian gibi) bu durumun böyle olmadığına ve NATO’nun ÇHC Büyükelçiliği’ni bilerek bombaladığına ilişkin haberler yaptığı görülmektedir (Sweeney ve Vulliamy, 1999). Bu olayın akabinde bazı uzmanların görüşleri doğrultusunda, ÇHC’nin kamuoyunu ve ordusunu etkileyen bu olayla beraber daha teknolojik bir savaş geliştirmek maksadıyla bu alana büyük yatırımlar yapıldığı açıklanmaktadır (Negro, 2017: 44). Bu doğrultuda yatırımların devam etmesiyle beraber, 21 Ağustos 2000 tarihinde, Pekin Uluslararası Kongre Merkezi’nde 16. Dünya Bilgisayar Kongresi’nin düzenlendiği ortaya konmaktadır. Düzenlenen kongrede Jiang Zemin’in; bilgi güvenliği yönetimini iş birliği içinde güçlendirmek ve internetin olumlu yanlarına tam anlamıyla yer vermek için bir sözleşmenin formüle edilmesini savunduğu görülmektedir (CNNIC, 2012). Bununla birlikte, 2000’li yıllara gelindiğinde ise yaşanan gelişmeler neticesinde internet teknolojileri hızla gelişerek devletin daha fazla önem verdiği bir husus olarak karşımıza çıkmaktadır. Bu duruma verilebilecek en iyi örneği, 8 Kasım 2002 yılında ÇKP 16. Parti Kongresi’nde ÇHC Devlet Başkanı Jiang Zemin’in konuşması oluşturmaktadır. Zemin bu konuşmasında; ülkenin bilim ve eğitim aracılığıyla canlanacağını aynı zamanda bilgi endüstrisinin gelişimini her şeyden önce tutup, finansal ve sosyal

gelişmenin tüm kapsamına bilgi teknolojilerinin (Information Technology- IT) uygulanması gerektiğini dile getirmektedir (Zemin, 2002).

Karşılaşılan gelişmelerden sonra bilgi teknolojileri ile ilgili dünya genelinde birçok adım atıldığı tespit edilmektedir. Nitekim 2005 yılında 2006-2020 yıllarını kapsayan Ulusal Enformatizasyon Planı'nın (National Informatization Plan- NIP) kabul edildiği görülmektedir. Kabul edilen bu planın hedefleri ise şu şekilde sıralanmaktadır (Austin, 2014: 2-3):

- Bilgi toplumunun desteklenmesi,
- E-devlet uygulaması,
- Bilgi teknolojileri alanında gerçekleşen rekabetin artırılması,
- Gelişmiş internet kültürünün oluşturulması,
- Yasal bir IT sisteminin desteklenmesi,
- Ulusal bilgi güvenliği sisteminin oluşturulması,
- İnternet kaynakları yönünde gelişimin artırılması,
- Yatırım, finansal ve araştırma politikaların geliştirilmesi.

Bu planın aksine ÇHC'de internet egemenliği ya da internet yönetimi devlete bağlı olmaktadır. Bundan dolayı farklı sistemler geliştirilmektedir. ÇHC, ülkenin internet kontrolünü sağlamak maksadıyla Türkçe karşılığı ÇHC'nin Büyük Güvenlik Duvarı olan *Great Firewall of China (GFC)* adında bir sistem uygulamaktadır. ÇHC'nin Büyük Güvenlik Duvarı ifadesi, 2002 yılında Charles R. Smith tarafından ÇHC'de bulunan yabancı ve zararlı düşüncelerden tek parti yönetiminin kurallarını korumak için uygulanan internet sansürünü tanımlamak için kullanılmaktadır (Shen, 2014: 599).

Bununla beraber, 800 milyonluk online nüfusu bulunan ve Google, Facebook, YouTube ya da New York Times'a erişimi içermeyen oldukça kısıtlı bir internete sahip olan ÇHC'nin GFC ile uyguladığı sansürün farklı eleştirilere maruz kaldığı görülmektedir. Sosyal düzenin ve ulusal güvenliğin korunması maksadıyla internette sansür uygulayan GFC'nin, bazı eleştirmenler tarafından amacı dışında bazı hususlara da sebep olduğunun altı çizilmektedir. Aynı zamanda GFC'nin internetin tek parti yönetimine karşı muhalif tabanı güçlendirme potansiyeli hususunda bir paranoyaya da sebep olduğu söylenmektedir. Öyle ki uygulanan sansür dolayısıyla ve devletin internete olan sürekli müdahalesi sonucunda dünyada online özgürlüğe sahip olamayan

devletlerin başında ÇHC gelmektedir. ÇHC'den sonra İran'ın ve Suriye'nin online özgürlüğü haiz olmayan devletler olduğu belirtilmektedir (Clark ve Chan, 2018).

Günümüze bakıldığında her ne kadar ÇHC'nin, online özgürlüğün sağlanması konusunda hareket kabiliyeti sağlamadığı görülse de bilgi teknolojilerinin gelişimi açısından oldukça önemli bir yol kat ettiği gözlemlenmektedir. Bu noktada ÇHC'nin teknoloji alanında böylesine gelişim göstermesi ve yükselmesi çeşitli siber saldırılarda hedef gösterilerek mevzubahis saldırılara maruz kalmasına sebep olmaktadır.

3.2.Çin'in Siber Güvenlik Politikaları

ÇHC'nin siber güvenlik algısı; siber uzay, siber egemenlik, bilgi güvenliği ve oluşan siber güvensizlik hususlarıyla beraber analiz edilmektedir. Öte yandan, ÇHC'nin yaşanan gelişmelerle beraber karşılaşılan risk ve tehditlere karşı siber güvenlik alanında belirlemiş olduğu politikalarına ve stratejilerine detaylı bir şekilde değinilmektedir.

İnsan yaşamında birçok değişimi ve dönüşümü beraberinde getiren küreselleşmenin ivme kazandığı 1980'li yıllarda başlatılan reform sürecinde ÇHC, ekonomik anlamda her ne kadar zorluklar yaşamış olsa da zaman içerisinde yüksek büyüme sürecine girmiştir. Durum bu şekilde ilerlese de ülkenin siyasi seçkinleri, içerisinde kırılan yeni kaynakları barındıran küreselleşme sürecini iki taraflı bir kılıç olarak görmektedir. Küreselleşmenin yaygınlaşmasıyla beraber siber silah gibi geleneksel olmayan tehditler giderek büyümektedir. Bu durum ise ÇHC'nin güvenliğine yönelik endişeleri artırmaktadır. Bundan dolayı küreselleşme süreci ile benzer şekilde siber uzay da iki tarafı keskin bir kılıç olarak ifade edilebilmektedir. Yaşanan bu değişimler sebebiyle ÇHC, güvenlik ile ilgili düşüncelerinin yeniden yapılandırılması gerektiği fikrini geç de olsa kabul etmiştir (Deng ve Thomas, 2004: 117). Diğer taraftan geniş yüzölçümü, nüfusu ve giderek daha da gelişen ekonomik yapısı ve askeri altyapısı kapsamında son yıllarda mühim bir küresel güç hâline gelen ÇHC'nin ekonomik, siyasi, askeri ve teknolojik alanlardaki fikirleri, planları ve stratejileri diğer devletler tarafından dikkatle takip edilmektedir. ÇHC'nin dünyadaki 3,4 milyar internet kullanıcısından 721 milyonuna sahip olduğu göz önüne alındığında küresel ölçekte siber güvenlik stratejileri belirleme hususunda harekete geçmesi durumunun tartışmasız olduğu görülmektedir. Yani böylesine büyük bir kullanıcı kitlesinin olması, en geniş siber güvenlik kadrosunu elinde bulundurması ve aynı zamanda geniş bir internet topluluğunun denetiminin,

yönetiminin kurumsal bir altyapı ve stratejisinin ve siber denetimin olması gerekliliğini ortaya koymaktadır (Darıcı ve Özdal, 2018: 2-3).

Bunların yanında, önceleri harekât alanları olarak; kara, deniz, hava ve uzay karşımıza çıkarken bilişim sistemleri ve teknolojinin hızlı gelişimi sonucu “siber uzay” da bu harekât alanlarında yerini almaktadır. Akabinde yaşanan gelişmelerle beraber diğer tüm harekât alanları siber uzayda hareket etmeye başlayarak, siber uzayın önemini bir kez daha gözler önüne sermektedir. Dünyada yer alan güçlü devletler ve ordular tarafından harekât ortamının beşinci boyutu olarak kabul edilen siber uzayın, 21. yüzyılda hükûmetlerin iç veya dış politikalarını belirleyen temel unsurlardan biri hâline gelmesinin yanında, savaş sahasında da önemli caydırıcılık gücüne sahip olma özelliği gösterdiği görülmektedir. Bu bağlamda, siber uzayın böylesine önem kazandığı günümüzde, ülkeler teknolojik imkân ve yeteneklerini geliştirme yoluna gitmektedir. Bu şekilde aktörler siber uzayda hak sahibi olabilmek ve nüfuzlarını artırmak istemektedir. Devletler teknoloji ve internete daha çok bağımlı hâle geldiklerinden dolayı siber saldırılara maruz kalma ihtimalleri de giderek artmaktadır. Karşılaşılabilecek bu siber saldırılar genellikle ülkeler için hayati önem taşıyan; elektrik, eğitim, sağlık, nükleer tesisler, tarım, sanayi, enerji, ulaşım, su, finans ve haberleşme gibi kritik alt yapı sektörlerine yapılarak çok büyük maddi zararlara, can ve mal kayıplarına sebep olmaktadır. Akabinde yapılan saldırı sonucunda da bu sektörlerden bir süre hizmet alınamamaktadır. Bundan dolayı devletler, ulusal siber güvenlik güçlerini tümüyle artırma ve güçlendirme yarışı içerisine girmektedir (Çeliktas ve Ünlü, 2018: 470).

Bu doğrultuda, Soğuk Savaş sonrası dönemde birçok devlet siber uzayda karşılaşılabilecek risk ve tehditlerden korunmak için siber güvenlik stratejileri geliştirmeye başlamaktadır. Bu dönemde teknolojik gelişmelere daha fazla önem vermeye başlayan ÇHC, bu alana yatırım yapan devletlerin başında gelmektedir. Bundan dolayı özellikle “siber uzay” ve “yapay zekâ” hususunda yaptığı yeniliklerle ABD ile dünyanın önde gelen devletlerin başında gelmektedir (Vinny Halo, 2021). Siber uzayda önemli bir aktör hâline gelen ÇHC, bunun yanı sıra internet kullanımında geniş kitleye sahip olması dolayısıyla dünyada internet kullanıcılarının dörtte birini kendi bünyesinde barındırmaktadır (Eroğlu, 2022: 62). Bununla beraber, 1980’li yılların sonuna gelindiğinde Pekin’in siber güvenlik hususuna yönelik politikalarını geliştirmeye başladığı görülmektedir. 1987 yılında internet kullanımına başlayan ÇHC hükûmeti tarafından, IP ile ilgili internet bağlantısı kullanımına ise 1994 yılında izin verilmiştir.

Bu doğrultuda bakıldığında aslında siber güvenlik konusunun ÇHC açısından oldukça yeni bir konu olduğu anlaşılmaktadır (Köksoy, 2019: 342).

Öte yandan, siber uzayı değerlendirme hususunda ÇHC'nin, diğer ülkelerden farklı olarak siber uzayın önemini “strateji” kavramında ele aldığı görülmektedir. Yani ÇHC için siber uzayın önemi stratejiden gelmektedir (Thomas, 2004). Kapsamlı ulusal güç düşüncesine dayalı olan ÇHC stratejisi, bütünsel boyutta ele alınmaktadır. ÇHC'nin bütünsel stratejik yaklaşımının özü, uluslararası sistemi ÇHC'nin kârına olabilecek şekilde manipüle etmeye dayanmaktadır (Korhan, 2018: 49). ÇHC'nin siber güvenlik stratejileri olduğu gibi genel olarak siber uzaya yönelik bazı stratejilerinin de olduğu gözlemlenmektedir. ÇHC'nin siber uzaya yönelik genel stratejileri şu şekilde ele alınmaktadır (Bey, 2018: 32-33):

1. Bilgi akışı, küresel ticaret akışı ve karşılıklı bağlantı ABD gibi ÇHC'nin de ekonomisinin temelini oluşturmaktadır. Bundan dolayı ÇHC, siber politikalar üzerine imzaladığı ad-hoc ikili anlaşmalarıyla birçok kesintiyi önlerken diğer ülkelerde gerilimi azaltmak adına söz konusu anlaşmaları gerekli görmektedir. Buna en iyi örnek; ABD ile endüstriyel casusluk için kullanılan siber saldırıları durdurmak amacıyla 2015 anlaşması gösterilmektedir. Bu tür anlaşmalarda, anlaşmaya uyulup uyulmadığına bakılmamaktadır. Asıl odak nokta; endüstriyel casusluktan korumaya çalışan bir teknolojiyi geliştirmektir. Bundan dolayı bu durum ÇHC için önemli bir hâl almaktadır. ÇHC' nin bu stratejideki önceliği; uluslararası siber normların kendi iç politikalarının bir yükümlülük hâline gelmesine yol açmayacak şekilde gelişmesini sağlamaktır.
2. ÇHC'nin belirlemiş olduğu siber uzay stratejilerinin ulusal güvenliğiyle yakından bağlantılı olduğu görülmektedir. Yoğun nüfusa ve geniş topraklara sahip olan ÇHC, bilgi akışını kontrol etmek amacıyla katı bir politika izlemektedir. Bilgi ve teknoloji çağının yaşandığı süreçte ÇHC düşman ülkelerin interneti, ÇKP'nin otoritesini baltalamak ve siber saldırı düzenlemek ya da bilgi yayılımı yaparak ülkeyi istikrarsızlaştırmak için kullanılabileceğinden endişe duymaktadır. Tüm bu risklerden dolayı ÇHC'nin bir diğer siber uzay stratejisinin ise “sansür” olduğu tespit edilmektedir. Başkan Xi Jinping, ÇHC'de sürmekte olan zorlu sosyo-ekonomik geçiş sırasında ideolojik uyumu artırmak ve siyasi muhalifleri

bastırmak maksadıyla sansüre yoğunluk vererek riski hafifletmek adına adımlar atmaktadır.

3. ÇHC her ne kadar siber operasyonlarındaki kabiliyetleri ve yapay zekâ gibi gelişmekte olan teknolojileriyle daha sofistike bir hâl almış olsa da Pekin'in büyük oranda Batı teknolojilerine bağımlı olduğu gözlemlenmektedir. Bu bağımlılığın ise Pekin tarafından "Made in China 2025" ile kırılması umulmaktadır. Yani ülke tamamen kendi teknoloji devlerini geliştirme çabasına girerek risk ve tehditleri ortadan kaldırmak için iki katı çaba sarf etmeye çalışmaktadır.

ÇHC'nin siber uzay ile birlikte üzerinde durmuş olduğu yapay zekâ hususuna da kısaca değinmek gerekmektedir. Genel anlamda ÇHC hükûmetinin uygulamış olduğu politikalara bakıldığında ülkenin ekonomik ve askeri gücünü mümkün olduğunca en üst seviyeye ulaştırmayı hedeflediği gözlemlenmektedir. ÇHC hükûmeti bunu yapmanın siber savunma temellerini güçlendirmeden geçtiğini belirtmektedir. Bundan dolayı yapay zekâ gibi teknolojik unsurlara büyük yatırımlar yapmaktadır. "Siber güvenlik olmadan ulusal bir güvenlik olamaz" sözüyle Xi Jinping hükûmeti, ulusal güvenlik doğrultusunda oluşturulan siber güvenlikle ilişkili politikaların önemini ve gerekliliğini bir kez daha göstermektedir. Bununla beraber, ÇHC kamu güvenliğinin ön plana çıkarıldığı bazı teknolojik hamlelerde bulunarak, büyük adımlar atmayı hedeflemektedir. Bunlara örnek olarak; yüz tanıma, araç ve akıllı telefon izleme, vatandaş gözetimi gibi adımlar verilebilmektedir. Bunun yanı sıra savunma mekanizmasını geliştirme girişiminde bulunan ÇHC'nin bu hususta da çeşitli faaliyetleri bulunmaktadır. ÇHC, hükûmete ait iki savunma elektroniği şirketi China Electronics Corporation (CEC) ve China Electronics Technology Group'un (CETC) yan kuruluşu olarak kabul edilen ChinaSoft ve China Cybersecurity vasıtasıyla faaliyetini devam ettirmektedir. Bunlar dışında yoğun hizmet ve ürün talebi dolayısıyla yüzlerce özel siber güvenlik şirketi giderek artış göstermektedir (Austin, 2018).

Yukarıda sıklıkla üzerinde durulduğu üzere, ÇHC'de "bilgi güvenliği" ya da "ağ güvenliği" kavramları olarak kullanılan siber güvenlik, ÇHC'de olduğu gibi tüm uluslararası sistemde yeni ve popüler olan bir husus olarak gündemde yerini almaktadır. Nitekim her geçen gün siber uzayda karşılaşılan risk ve tehditlerden dolayı siber güvenliğin önemi giderek artmaktadır. Bundan dolayı ÇHC'de diğer devletler gibi bu alanda çeşitli politikalar geliştirmeye çalışmaktadır. ÇHC'nin bu alanda belirlemeye

çalıştığı politikaların genel amacı; askeri, ekonomik ve siyasi yapılanmasını güçlendirmek, ABD ve Batı hegemonyasına karşı bir seçenek oluşturmak, küresel sistemdeki siber egemenliğini sağlam bir noktaya oturtmak şeklinde sıralanabilmektedir (Journal of Political Sciences & Public Affairs, 2017). Bu doğrultuda, bilişim ve teknolojiye yaşanan ilerlemeler sonucunda dünyanın dört bir yanında gelişim ve dönüşümler ortaya çıkmaktadır. Bundan dolayı ÇHC’de ülke içinde internet kullanım oranındaki artış gözle görülür bir hâl almaktadır. Bu artış dolayısıyla ulusal boyutta siber suç oranında da yükseliş görülmektedir. Diğer yandan, ülke dışından internet ağına uygulanan siber saldırıların yoğunlaşması gibi nedenler doğrultusunda ÇHC, siber güvenlik hususunu vazgeçilmez bir konu olarak gündeminin odak noktasına koymaktadır (ChinaDaily, 2017; Ivezic, 2017).

ÇHC’nin belirlemiş olduğu kanun veya politikalarda siber kavramı kısmen yer alsa da siber güvenlik ile ilgili hususlar bilgi güvenliği olarak ele alınmaktadır. ÇHC kültürü ve aynı zamanda ÇHC’nin Batı edebiyatına karşı olan itici tutumu buna sebep olmaktadır. ÇHC kültüründeki inanç doğrultusunda bakıldığında, bilgi birikimi bir güç olarak görülmektedir. ÇHC’nin belirlemiş olduğu stratejinin odağında da geleneksel gücün bilgiye dayalı güce evrilimi yatmaktadır (Patton, 2016: 9). Genel olarak bakıldığında ise ÇHC’nin siber güvenlik ile ilgili net bir tanımı olmadığı görülmektedir. Buna rağmen ÇHC siber güvenlik hususunu oldukça geniş bir yelpazeden ele almaktadır (Akyeşilmen, 2018: 114). Bununla beraber, diğer devletlerin siber güvenlik anlayışlarının, ÇHC’nin siber güvenlik anlayışıyla paralel olduğu görülmektedir. ÇHC’nin; internetin ulusal güvenlik, sosyal, ticaret ve bireysel menfaatlere karşı oluşabilecek zararlardan ya da zarar verici herhangi bir etkiden korunmayı sağlaması gerekliliğine yönelik bir siber güvenlik görüşü bulunmaktadır. ÇHC’nin burada belirlemiş olduğu çıkarlar/menfaatler şu şekilde sıralanmaktadır (Swaine, 2013: 3):

- Devletin ve toplumun savunma kapasitesi,
- Ekonomik boyutta güçlü bir biçimde rekabet etme kabiliyeti,
- Sosyal değerlerin korunması,
- Kişilerin mahremiyeti ve vatandaşların güvenliği.

Önceleri savaş stratejisine yoğunlaşan ÇHC, 1990’lı yılların ortalarında Körfez Savaşı’ndan sonra edinmiş olduğu tecrübeler neticesinde bu stratejisinde değişikliğe gitmektedir. Bu bağlamda, belirlemiş olduğu yeni strateji çerçevesinde ordusunu küçülterek yeni teknolojilere yatırım yapmayı planlayıp savaş birlikleri kurmaktadır.

Güç konusunda dünyada tek olma arzusu bulunan ÇHC; bilgi teknolojileri ve siber savaş hususunda da dünya üzerinde lider bir pozisyonda olma hedefinin olduğunu dile getirmektedir. Akabinde bu konuyla ilgili yaklaşık 20 yıldır strateji belgeleri, raporlar ve doktrinler yayımlamaktadır. Bundan dolayı çeşitli politikalar geliştirmektedir. 1980’li yılların sonu ve 1990’ların başından itibaren ÇHC Ordusu, “bilgileştirme” adıyla teknolojinin hâkim olduğu sürece ayak uydurmak için siber uzay ve bilgi teknolojileri hususunda etkin bir güç olma yolunda planlar yürütmektedir (Alioğlu, 2019: 124). Tüm bunların yanında, ordu merkezlerinde siber savaş eğitimleri verilmektedir (Gül, 2012: 19-20).

Daha önce Xi Jinping’in siber güvenlik adına söylemiş olduğu sözde de vurgulandığı gibi, ÇHC yönetimi için siber güvenlik ulusal güvenliğin vazgeçilmez bir parçası hâlini almaktadır. ÇHC, 1993 yılından itibaren bilgi güvenliği stratejilerini geliştirecek bazı gruplar tayin etmektedir. Bu gruplar kurulduğu yıla göre şu şekilde sıralanmaktadır (Kotik, 2015: 60; Darıcılı ve Özdal, 2018: 12-14):

- Devlet Ekonomik Bilgi Yönetimine Öncü Küçük Grup (1986)
- Devlet Enformatik Yönetim Grubu (1999)
- Devlet Ağı ve Bilgi Güvenliği Koordinasyon Küçük Grubu (2003)
- Merkezi Bilgi Ağı Güvenliği ve Enformatikleştirme Lider Küçük Grubu (2014)

Oluşturulan bu grupların başlıca amaçları; kurumlar arası iş birliği ve koordinasyonun sağlanması, bilgi teknolojilerinin yoğunluk kazandığı bu süreçte yerel teknolojilerin teşvik edilip güçlendirilmesi ve siber politikalar için belirlenen yatırımların artırılması şeklinde ifade edilmektedir. Belirlenen bu amaçlar aktif savunma² stratejisinin bir parçası olarak görülmektedir (Köksoy, 2019: 342). ÇHC siber uzayın ekonomik, askeri ve siyasi yönden tehdit oluşturduğunu bilse de bu durumun avantajlarını da bilerek hareket etmektedir. Bundan dolayı siber güvenliğe verilen önem her alanı kapsamaktadır. Çünkü oluşacak tehditler tek bir alan üzerinden gelmemektedir. Bu yüzden her alanda karşılaşılabilecek risk ve tehditlere karşı önlem alınması gerekmektedir. Aynı zamanda avantajları da fırsata çevirmek yararlı olacaktır.

² Aktif Savunma: Düşman saldırmadan saldırıya geçmeyip, saldırı gerçekleştikten sonra her türlü hücumu dayanan saldırıyı gerçekleştirmek olarak ifade edilmektedir (Chang, 2014: 20).

Öte yandan, ÇHC'nin siber güvenlik stratejisini ekonomik boyutta incelediğimizde, stratejinin ülke ekonomisinin siber uzay sayesinde büyümesini sağlamak ve ülke sınırları içinde oluşacak siber suçları engellemek gibi hedefleri olduğu belirtilmektedir. Kalabalık bir nüfusa sahip olan ÇHC, halkın taleplerini karşılayabilmek amacıyla ekonomik gelişmenin daimi olmasını istemektedir. Bundan dolayı da endüstriyel siber casusluk faaliyetlerinde bulunan ÇHC'nin, söz konusu faaliyetlerle rakip ekonomilere zarar verdiği iddia edilmektedir. Ortaya atılan ABD kaynaklı bu iddiaları ise ÇHC hiçbir şekilde kabul etmemektedir. Buna rağmen ABD Ulusal Kontrespiyonaj Dairesi'nin yapmış olduğu açıklamaya göre ÇHC dünyanın en ısrarcı ve en yoğun endüstriyel siber casusluk faaliyetlerini gerçekleştirmektedir (Chang, 2014: 21-22). Bunun yanında, 2014 yılında Amerikan Adalet Departmanı'nın ÇHC hükûmeti ile alakası olduğu ileri sürülen 5 siber ajana dava açmasıyla beraber ABD ve ÇHC arasındaki siber gerilimin tırmandığı görülmektedir. İki ülke arasında tırmanışa geçen bu siber gerilimin ise Yonyou ve Inspur gibi ÇHC bilişim teknolojileri şirketlerinin hisse senetlerinin artmasına sebep olduğu söylenmektedir (Chang, 2014: 6).

Ulusal siber güvenlik konusuna büyük önem veren ÇHC, siber casusluk faaliyetlerine karşı oldukça yüksek önlemler almaktadır. ÇHC hükûmeti, ülkede var olan yabancı yazılımların siber casusluk faaliyetlerini artıracağı yönünde endişeleri içinde barındırmaktadır. Bu doğrultuda, 2003 yılında Çin Devlet Konseyi tarafından, siber güvenlik ile ilgili ilk strateji planlarından biri olan "Doküman 27" (diğer adıyla "Belge 27") yayımlanmaktadır. Bununla birlikte Çok Katmanlı Koruma Planı'nı devreye girdiği görülmektedir. Bu plana göre belirli katmanlar oluşturulmaktadır. Bunlar şu şekilde sıralanmaktadır (Gierow, 2014: 5):

- 1. ve 2. katmanı bireyler ve küçük şirketler,
- 3. katmanı işletmeler ve stratejik öneme sahip sektörler (finans, altyapı ve diğerleri),
- 4. ve 5. katmanı ise kamu kurumları/yetkilileri oluşturmaktadır.

Oluşturulan planın birçok devlette etkisi olduğu görülmektedir. Bu bağlamda Microsoft'un artık Windows işletim sistemini ÇHC'li yetkililere satmadığı söylenmektedir. Kaspersky ve Symantec gibi virüsten koruma yazılımları gibi yabancı yazılımlarda artık 3. katmandaki stratejik öneme sahip sektör ve işletmelerde kullanılmamaktadır. ÇHC hükûmeti, her ne kadar yerli yazılımları etkin olmaması ve işletim sorunlarının yaşanması gibi nedenlerle arka planda bıraksa da yine de

oluşabilecek herhangi bir sızmanın verebileceği zararın çok dahageniş bir etki doğurabileceğinden dolayı tüm katmanlarda yerli yazılım kullanımını teşvik etmektedir (Gierow, 2014: 2-5). Buna bağlı olarak, ilk sivil belge özelliğine sahip Belge 27 adlı dokümanla ÇHC'nin, bilgi teknolojisini hem ekonomik fırsat hem de güvenlik problemi olarak ele aldığı gözlemlenmektedir. Söz konusu dokümanın belirli hedefleri bulunmaktadır ve bu hedefler şu şekilde sıralanmaktadır (Raud, 2016: 11):

- Kritik altyapıların korunması maksadıyla aktif bir savunma politikası oluşturulması,
- Dinamik gözlemlene, gelişimi destekleme,
- Ekonomik bilgilerin yönetimi grubuyla ve devlet organlarıyla iş birliği yapmak yoluyla siber güvenlik politikalarının şekillendirilmesi.

Siber uzay ekonomik açıdan olduğu gibi siyasi açıdan da birtakım risk ve tehditleri beraberinde getirmektedir. ÇHC, yönetimin hedeflerinden biri olan ÇKP ideolojisini yaymak ve korumak düşüncesi doğrultusunda atmış olduğu adımlardan biri olan Altın Kalkan Projesi'ni devreye sokmaktadır. Bu proje ile halkın, hükûmetin belirlemiş olduğu bazı yabancı web sitelerine erişimi engellenmekte ve geniş çaplı internet sansürü uygulanmaktadır. Proje ile beraber verilerin ülke dışına ya da içine girmesi engellenmektedir. İnternet ve bireylerin özgürlüğünü kısıtlayan ve ABD başta olmak üzere diğer birçok batılı ülkenin eleştirilerine maruz kalan Altın Kalkan Projesi kapsamında iki güvenlik sistemi oluşturulmaktadır. Bu projeler şu şekilde karşımıza çıkmaktadır:

- Çin'in Büyük Güvenlik Duvarı (*Great Firewall of China*),
- Yeşil Baraj (*Green Dam*) Projeleri.

Great Firewall, ÇHC'nin iç politik dengesini korumak maksadıyla siber uzayda bilgi akışını kontrol etme çabası olarak algılanmaktadır. Bu projeye yapılan eleştiriler çoğunlukla birey özgürlüğüne odaklandığı için ÇHC'nin siber uzayı "egemenlik sınırları dâhilinde bir alan" olarak gördüğü gözden kaçırılmaktadır (Zhang, 2012: 805). Green Dam ise, ÇHC hükûmeti tarafından 2009 yılı itibariyle başlatılmaktadır. Bu proje ile internet akışı izlenmekte, yasaklı sitelere erişim engellenmekte ve yabancı ülkeler tarafından bilgisayara yüklenmiş olan zararlı yazılımlar tespit edilmektedir. Oluşturulan bu iki güvenlik sisteminin en temel özelliği, karşılaşılabilecek herhangi bir siber savaş tehdidinin algılandığı durumlarda ÇHC'nin siber uzayı bloke ederek dünyanın geri kalanından tecrit edilmesine imkân sağlamaktır. Bu durum, ÇHC'nin sahip olduğu

askeri stratejisi ve siber güvenlik politikasıyla hazırlanmakta olduğu herhangi bir siber savaş durumunda Pekin'e büyük avantajlar sunmaktadır (Alioğlu, 2019: 125). ÇHC, Altın Kalkan Projesi ve Great Firewall kapsamında sahip olduğu siyasi organizasyon ve fikirleri doğrultusunda ülke güvenliğinin yanı sıra siber güvenlik alanını da büyük oranda ordunun denetimine bırakmaktadır (Gül, 2012: 18).

Ekonomik ve siyasi boyutun yanı sıra, askeri boyutta ÇHC'nin hedefine bakıldığında ise güvenlik hususunda siber savaşa hazır bir devlet konumunda olmayı hedeflediği görülmektedir. Bu bağlamda, teknolojinin hızlı bir şekilde ilerlemesi ve gelişim göstermesiyle ÇHC ordusu da siber savaşa hazır olmak maksadıyla bütün birimlerinde enformatikleştirmeyi³ sağlamayı ummaktadır (Kanwal, 2009: 15). 2000'li yıllarının başlarında Çin Merkez Askeri Komisyonu, enformasyonelleştirme koşulları altında halk savaşının incelenmesi çağrısında bulunmaktadır. Akabinde ÇHC'nin, 2004 yılında Milli Savunma Beyaz Kitabı yayımladığı görülmektedir. Kitap, bilgilendirmenin silahlı kuvvetlerin savaşma yeteneklerini artırmada kilit faktör hâline geldiğini belirtmektedir. ÇHC askeri doktrini ise çatışmanın ilk aşamalarında siber ve elektronik savaş yeteneklerinin bir kombinasyon içerisinde kullanılması gerektiğini belirtmektedir (Lewis ve Timlin, 2011: 8).

2004 yılında yayımlanan Beyaz Kitap'ta askeri bilişim ve teknolojik sistemlerin güçlendirilmesi maksadıyla kapasitenin artırılması hedeflenmektedir. Kitabın ikinci kısmında belirtildiği üzere, bilim ve teknoloji ile güçlü bir ordu kurulması amaçlanmaktadır. Çin Halk Kurtuluş Ordusu - PLA (*People's Liberation Army*), bilişim ve teknolojik ilerlemelerden faydalanarak savaş kabiliyetlerini geliştirmeye çalışıp, yalnızca niceliksel bir ölçek yerine nitel verimlilik oluşturmayı ve aynı zamanda insan gücünün yoğun olduğu orduyu teknolojinin yoğun olduğu bir orduya dönüştürmeyi hedeflemektedir. PLA, 'Yetenekli İnsanlar İçin Stratejik Proje' adlı bir çalışma uygulayarak, yeni tipte yüksek kalibreli askeri personelin eğitilmesine odaklanmaktadır (China's National Defense, 2004).

2006 yılına gelindiğinde ÇHC, bilgi teknolojisindeki savunmasızlığını anlayarak bu savunmasızlığı azaltmayı hedeflemektedir (Janeliūnas ve Tumkevič, 2020: 129). Bu düşünceden hareketle 2006 yılında ÇHC Danıştay tarafından açıklanan "Orta ve Uzun Vadede Bilim ve Teknolojinin Geliştirilmesi Ulusal Programı (2006-2020)"

³ Enformatikleştirme: Endüstri toplumunu bilişim teknolojilerindeki gelişmeler aracılığıyla bilgi toplumuna dönüştürmek olarak tanımlanmaktadır (Chang, 2014: 13).

yayımlanmaktadır. Bu program ÇHC'nin modern teknoloji ve bilişim alanındaki gelişimi hususunda kritik bir önem arz etmektedir. Bilişim teknolojilerinin yerli kaynaklarla geliştirilmesini temel hedef olarak gören ÇHC, belirlemiş olduğu bu hedefin ÇHC halkının mevcut standartları kabul etmek yerine yaşam kalitesini ve standartlarını yükseltme amacına uygun olması gerektiğini ortaya koymaktadır. Bununla beraber, 2006 yılına kadar birçok kurumda bilişim ve teknoloji alanlarında koordinasyonunun kurulmasında başarı elde edilememiştir. Kurumlar arasındaki koordinasyonun ise bu program sayesinde sağlandığı gözlemlenmektedir. Program, ÇHC'nin teknolojik anlamda gelişmesinde ve teknolojinin bugünkü seviyesine ulaşmasında önemli bir adımı teşkil etmektedir. Askeri bir amacı bulunmayan mevzu bahis program çeşitli planlar önermektedir. Bu planlar şu şekilde ortaya konmaktadır (Raud, 2016: 12):

- Bilişim sektörünün teşvik edilmesi,
- Enerji kaynaklarının artırılması,
- Su ihtiyacının tesisi,
- Çevre teknolojilerinin geliştirilmesi,
- Fikri hakların teşvik edilmesi,
- ÇHC'nin rekabetçi ekonomik yapısına sahip olması.

Sonuç olarak, 21. yüzyılda yaşanan bilim ve teknoloji devrimiyle beraber birçok ülkede ekonomik ve sosyal görüş açısından köklü değişiklikler yaşanmaktadır. ÇHC'nin de bilginin, teknolojinin ve AR-GE çalışmalarının önemli bir rol oynadığı söz konusu süreçte büyük adımlarından biri olan bu program ile yenilik odaklı bir devlet inşa etmeyi hedeflediği gözlenmektedir (Clarke ve Knake, 2011: 32-33).

Kamu hizmetlerinde ve resmi kurumlarda bilişim ve teknolojinin geliştirilmesi amaç olarak belirtilerek 2006 yılında Beyaz Kitap yeniden yayımlanmaktadır. Siber güvenliği ordu aracılığıyla sağlayan ÇHC, siber güvenliğin yönlendirilmesi ve siber altyapının genel durumu gibi hususlarda önemli sorumluluklar alarak siber güvenlik alanında aktif rol üstlenmektedir. Bu bağlamda, Genelkurmay bünyesinde önemli faaliyetler gerçekleştiren ve ÇHC'nin siber güvenlik ağını kontrol etmek maksadıyla Mavi Ordu adı verilen bir birimin kurulduğu görülmektedir (Güntay, 2016: 132). PLA bünyesinde bulunan Genelkurmay Başkanlığı 3. ve 4. departmanlarının çeşitli görevleri bulunmaktadır. Bu görevler; 3. ve 4. departmanların diğer kuvvetler ile sistemli bir şekilde ülke dışındaki sinyallerin toplanması, ele geçirilmesi ve analizi, ÇHC sınırları

içerisindeki iletişim sistemleri ağlarının kontrolünün sağlanması, elektronik harp, bilgi harekâtı ve siber saldırıların uygulanması gibi görevleri olduğu ifade edilebilmektedir (Raska, 2015). Ayrıca, PLA bünyesindeki Genelkurmay Başkanlığının 3.departmanı, ÇHC ordusunun sahip olduğu bilişim altyapısının ve aynı zamanda ağların güvenliğinden ve sinyal istihbaratından sorumludur. Elektronik bilginin toplanması, kullanılması ve analiz edilmesinden sorumlu olan 3. departmanın yanı sıra, farklı 3 adet araştırma kuruluşu da ülkenin siber güvenliğini sağlama ve geliştirme amacıyla sürekli AR-GE çalışmaları yürütmektedir. Bununla birlikte, siber güvenlik hususunda ÇHC'nin ileri gelen üniversiteleri, bu çalışmalara destek olmaktadır (Gül, 2012: 18). PLA bünyesindeki bir başka birimin ise 2006 yılında faaliyete geçen Birim 61398 olduğu ifade edilmektedir. Birim 61398'in, şu zamana kadar birçok batılı üst düzey firma ve devlet kurumuna karşı siber saldırılar gerçekleştirdiği düşünülmektedir (Sanchez, 2014). Bu birim dışında 2002 yılında kurulduğu ifade edilen, kabiliyetli siber korsanlardan, akademisyenlerden ve devlet adına çalışan hackerlerden oluşan “Gönüllü Bilgi Teknolojileri Milis Birimleri” (başka bir ifadeyle “İnternet Milis Birlikleri”) bulunmaktadır. ÇHC'nin siber ordusu da denilen bu grubun, ÇHC kaynaklı diğer devletlere yapılan birçok siber saldırının arkasında olduğu düşünülmektedir (European Parliamentary Research Service, 2014: 5; Çiftçi, 2015: 43).

Tüm bunların yanı sıra, gelecekte karşılaşılabilecek savaşlarda yeni nesil savaş stratejileri arasında yer alan ve PLA'nın hazırlamış olduğu “Entegre İletişim Ağı Elektronik Harbi” (*Integrated Network Electronic Warfare*) adlı stratejinin bulunduğu görülmektedir. Oluşturulan bu strateji, muhtemel bir savaşta düşman bilişim sistemlerinin çalışamaz hâle gelmesi amacıyla kullanılan siber saldırılar, elektronik harp ve konvansiyonel silahlarla saldırı görevlerinin birlikte kullanılmasını kapsamaktadır. Bu strateji kapsamında 2011 yılında PLA bünyesinde Çin Milli Savunma Bakanı sözcüsü tarafından “Online Mavi Ordu” adı verilen bir birim oluşturulmaktadır. Bu birim siber saldırılar karşısında ülkeyi korumakla görevlendirilmektedir. Söz konusu birim, bilgisayar sistemleri, haberleşme ağları, istihbarat, keşif ve gözetleme sistemleri içerisinde kör noktalar oluşturan, gerek duyulduğu durumlarda bu kör noktaları istismar ederek mevzubahis sistemlere elektronik harp ve uydular ile saldırı düzenleneceğini öngören bir saldırı birimi olarak görev yapmaktadır (US-DoD, 2009: 14; Beech, 2011; Raska, 2015). Diğer yandan, siber güvenliği ulusal güvenlik aktörlerinden biri olarak gören ÇHC, var olan siber

güvenliğini geliştirmek maksadıyla ülkede bulunan en iyi üniversiteler ile düzenli bir şekilde siber alan/uzayda AR-GE faaliyetleri yürütmektedir. Bu anlamda siber savaş, uzay silahları ve elektronik savaş için gerekli olan personelin eğitimi hususuna büyük önem verilmektedir. Her zaman lider olma arzusu olan ÇHC siber güvenlik ve siber savaş alanında da dünyanın en etkili gücü hâline gelmeyi amaç edinmektedir. Bundan dolayı stratejiler ve projeler üretilmesinin yanında bir de saldırgan savunma stratejisinin uygulanması boyutunda ordunun eğitildiği merkezlerde düşmanın bilişim teknolojilerine ve bilgisayar ağlarına hasar verilmesi ile ilgili hususlara dayalı olarak siber savaş üzerine eğitimler vermektedir. Aynı zamanda personel ihtiyacını karşılamak adına askeri birlikler, genç siber savaşçıların keşfedilmesi, yetiştirilmesi, siber orduya katkı sağlanması ve muhtemel bir siber savaş etkinliğini artırmak maksadıyla siber korsanlık üzerine yarışmalar düzenlenmektedir (Ventre, 2010; Wedermyer, 2012: 17; Çeliktas, 2016: 67-69).

Öte yandan ÇHC, 2010 yılında Savunma Raporu yayımlamaktadır. Bu raporda, siber güvenliğin milli savunma sisteminde önemli bir yere sahip olduğundan bahsedilmektedir. Bunun yanı sıra, siber uzayın gelişmesi ve güçlenmesi için önemli yatırımların yapılacağı vurgulanmaktadır. (Kesgin, 2022: 48). Aynı zamanda raporda birtakım siber saldırılardan söz edilmektedir. Bu saldırılar ÇHC hükûmetinin siber uzay hususunda önemli bir güce eriştiğini göstermektedir. Yapılacak olan bu siber saldırıların askeri harekâta üç önemli alanda katkı sağlayacağı belirtilmektedir. Bunlar şu şekilde ifade edilmektedir (US- DoD, 2015):

1. Rakip devletlerin verilerine siber casusluk yoluyla erişmek,
2. Diğer devletlerin internet tabanlı lojistik, iletişim ve ticari faaliyetlerini hedef alarak düşmanlarının harekâtlarını kısıtlamak ve verecekleri tepkinin sürelerini yavaşlatmak,
3. Çatışma, savaş ya da kriz durumunda konvansiyonel silahların da kullanılması yoluyla kuvvet çarpanı olarak hizmet etmesini sağlamak.

ÇHC hükûmetinin siber güvenlik hususunda yapmış olduğu çalışmalara bakıldığında, yönetimin teknolojik gelişmeye, öz sermaye kullanarak milli ve yerli yazılım üretimine ve üretim süreçlerinin devlet desteğiyle sürdürülmesine büyük önem verdiği görülmektedir. Tüm bunların akabinde özellikle 2010 yılı sonrasında Pekin'in, siber güvenlik alanında ve siber yönetim hususunda önemli girişimleri olduğu gözlemlenmektedir. Nitekim 2010 yılı sonrasında çeşitli kritik stratejik belgeler

hazırlanıp, yeni organizasyon yapıları oluşturulmaktadır (Darıcılı ve Özdal, 2018: 13-14). ÇHC'nin önerisi doğrultusunda siber uzay kurallarını belirlemek maksadıyla 2011 yılında BM Genel Meclisi'nde "Bilgi Güvenliği için Uluslararası Davranış Kuralları" adlı bir tasarı ortaya konmaktadır. ÇHC'nin siber güvenlik hususundaki resmi duruşunu ifade eden tasarı; Rusya, Tacikistan ve Özbekistan tarafından desteklenmesine rağmen genel olarak geniş çaplı kabul görmemektedir. Bu tasarı (Hsu ve Murrey, 2015):

- Tüm devletlerin egemenlik, siyasi bağımsızlığına saygı ve toprak bütünlüğü,
- Konuyla ilgili milli kanun ve düzenlemelerle uyum içinde olacak şekilde uzay bilgisi üzerinde hak ve özgürlüklere saygı,
- Bilgi güvenliği hususunda uluslararası kuralların belirlenmesi için BM'nin önemi, şeklinde siber politika hususunda 11 ilke içermektedir.

2012 yılında Danıştay Bilgi Ofisi tarafından "Yeni Politika Görüşü" adlı bir strateji ortaya konmaktadır. Teknoloji alanında faaliyet gösteren kurumlar arasında bilgi paylaşımının teşvik edilmesi bu stratejinin temel amacı olarak belirtilmektedir. Öte yandan, söz konusu stratejinin önceki stratejilerden temel bir farkı bulunmaktadır. Bu fark, 'belirlenen bu stratejinin ekonomik ve teknolojik gelişmeye izin vermekten de öte, devlet kurumları ve vatandaşların bilgi güvenliğinin sağlanması hususuna öncelik verilmesi' hususunun belirtilmesinden kaynaklanmaktadır Aynı zamanda stratejinin ağ teknolojilerinden kaynaklanan sosyal manipülasyon ve casusluk operasyonlarını önlemek gibi yeni amaçlara da sahip olduğu ortaya konmaktadır (Segal, 201).

2013 yılına gelindiğinde bir diğer Beyaz Kitap'ın yayımlandığı görülmektedir. Bu kitapta, ÇHC'nin milli güvenliğini, uzay ve siber uzay güvenliğini koruma hakkına sahip olduğu açıklanmaktadır. Aynı zamanda kitapta ÇHC'nin, "kendisine saldırılmadıkça saldırıda bulunmayacağı" beyan edilmektedir (Chang, 2014: 20). 2013'te karşımıza çıkan bir diğer gelişme ise Çin Askeri Bilimler Akademisi'nin 2013 yılında yayımladığı Askeri Strateji Belgesi olduğu görülmektedir. Bu belgede, ağ güvenliği ve ağ savaşları önemli bir yer tutmaktadır. Belge kapsamında Çin ordusunda 3 çeşit ağ saldırı birimi olduğu ifade edilmektedir. Bunlar şu şekilde belirtilmektedir (Varlık, 2015):

- Özel Askeri Network Savaş Gücü
- Orduya Bağlı Sivil Organizasyonlar
- Sivil Kuvvetler

2014 yılında “İnternet Güvenliği ve Enformasyon İçin Merkezi Grup” adlı yeni bir organizasyon kurulmaktadır. Bu grubun operasyonlarının ÇHC başkanları tarafından yönetilmesine karar verilmektedir. Böylece ÇHC’nin siber uzaydan kaynaklanan gelişmelere verdiği önem vurgulanmaya çalışılmaktadır. Grubun temel amacı; devlet kurumları arasında internet güvenliği ve bilişim sektörlerinin geliştirilmesi amacıyla gerekli koordinasyonun ve ortak siyasi önceliğin oluşturulması olarak belirlenmektedir. Söz konusu grubun ÇHC başkanlığında faaliyet göstermesi, siber güvenlik alanında hızlı ve kesin kararlar alınması açısından önemli bir stratejik yaklaşım olarak değerlendirilmektedir. Böylelikle karar verme sürecinde zaman kaybının önüne geçilmektedir. Bununla beraber, bürokrasiden kaynaklanan süreçler ve siber güvenlik alanındaki yanlış kararlar hususunda önemli gelişmelerin yaşandığı görülmektedir (Darıcılı ve Özdal: 2018: 15).

“İnternet Güvenliği ve Enformasyon İçin Merkezi Grup” adlı organizasyon ekseninde ‘bilgi teknolojileri konusunda aktörleri kategorilere ayıran çok aşamalı bir güvenlik şemasının (Multi- Level Protection Scheme-MLPS) oluşması’ ön plana çıkan önemli bir husus olarak karşımıza çıkmaktadır. Bahsi geçen şema doğrultusunda kişisel kullanıcılara, küçük firmalara, devlet kurumlarına, finans sektörlerine farklı seviyelerde güvenlik ölçütleri uygulanmaktadır (Gierow, 2014). Bu düzenlemeler neticesinde, ÇHC’de Batı kökenli YouTube, Facebook, Twitter vb. sosyal medya araçlarına ve birçok internet sitesine erişim yasaklanmaktadır. Aynı zamanda Batılı şirketlerin ÇHC’de satış yapmalarına izin verilmemektedir. Bu bağlamda sosyal medya araçlarına yönelik alternatifler sunulmaktadır. Fakat buna rağmen vatandaşlar kendi kimlik bilgileriyle bu platformlara giriş yaptıklarından dolayı sıkı denetimler yapılmaktadır. Bunun yanı sıra, internet ortamında varlığını sürdüren şirketler başta olmak üzere tüzel kişilerin de lisans alma zorunluluğu bulunmaktadır. Bundan dolayı hükûmetin her siteye, her kullanıcıya ve internette bulunan her türlü bilgiye ulaşımı mümkün olmaktadır. Bu durum her ne kadar sadece ÇHC’nin siber alan/uzayda egemenliğini güçlendirme hedefinin sonuçları gibi görünse de ÇKP ekseninde şekillenen tek partili yönetim sistemi yapısına dayanmaktadır. Aynı zamanda bu durumun, sistem içi eleştirilerin ve hükûmete yönelik yapılacak herhangi bir saldırının önüne geçilmesi amacından da kaynaklandığı görülmektedir (Köksoy, 2019: 343).

Öte yandan 2011 yılında Rusya, Tacikistan ve Özbekistan dışında geniş çaplı olarak kabul görmeyen “Bilgi Güvenliği için Uluslararası Davranış Kuralları” adlı

BM'ye sunulan tasarı, 2015 yılında ŞİÖ'nün altı üyesi olan ÇHC, Rusya, Kazakistan, Kırgızistan, Tacikistan ve Özbekistan tarafından güncellenerek yeniden BM'ye sunulmaktadır. İlk tasarıda olduğu gibi bu tasarı da birçok eleştiriye ve endişeye sebep olmaktadır. Sarah Mckune, bu durumun en önemli nedeninin siber uzayda devletlerin egemenliğine ve uluslararası insan haklarına yapılan vurgu olduğunu belirtmektedir. Tasarının içeriğinde; hükûmetlerin internetin uluslararası yönetim, güvenlik, devamlılık ve istikrarında eşit sorumluluk ve rollere sahip olması gerektiği ifade edilmektedir. Buna karşılık ABD ve diğer hükûmetler, internet politikasının yalnızca devlet tarafından belirlenmemesi ve çok paydaşlı bir yönetim modeline dayanması gerektiğini dile getirmektedir. Fakat ÇHC ve Rusya gibi devletler açısından bakıldığında, bu tasarının Batı'ya da fayda sağlayacağı düşünülmektedir (Mckune, 2015). Bu noktada insan hakları hususundaki yaklaşımın dile getirildiği tasarının 7. maddesinde “Medeni ve Siyasi Haklar Konusundaki Uluslararası Sözleşme göz önünde bulundurularak, bireyin çevrimdışı ortamda korunan hakları çevrimiçi ortamda da korunmalıdır” şeklinde bir ifadenin yer aldığı görülmektedir. Fakat “başkalarının hak ve itibarlarına saygı ile ulusal güvenliğin, kamu düzeninin, kamu sağlığının veya ahlakının korunması ile ilgili bazı kısıtlamalar söz konusu olabilir” de denmektedir. Bu madde, hükûmetlerin internet hususunda kendi ülkelerinde istedikleri sansürü uygulayabilmeleri anlamına gelmektedir. Bundan dolayı bu madde ile ilgili görüş birliği sağlanamamaktadır (Pekcan, 2020: 211).

Diğer taraftan, 2015 yılında ÇHC'nin Wuzhen şehrinde II. Dünya İnternet Kongresi düzenlenmektedir. Yoğun katılımın gerçekleştiği kongrede Xi Jinping açılış konuşması yaparak amaçlarının, ÇHC'deki 1.3 milyar insanın internetten yararlanabilmesini hedeflediklerini belirtmektedir. Aynı zamanda büyük bir enerji ve canlılık ile milli veri stratejisini, milli siber gelişim ve “İnternet Plus” eylem planını uygulayacakları ifade edilmektedir. Xi Jinping tüm bunların yanı sıra, küresel bir internet yönetim sisteminin oluşturulabilmesi için 2011 ve 2015 yıllarında BM'ye sunulan “Bilgi Güvenliği için Uluslararası Davranış Kuralları” adlı tasarıyla benzeyen bazı önerilerde bulunmaktadır. Burada dikkat çeken husus ise Xi Jinping'in temel ilkelerinden biri olan “siber egemenliğe saygı” ilkesinin yer almasıdır. Bu maddede, her hükûmetin bağımsız olarak kendi siber gelişim yolunu belirleyebileceği, kamu politikalarını ve siber düzenlemesini seçme hakkının olabileceği ve buna saygı duyulması gerektiği vurgulanmaktadır. Aynı zamanda hiçbir ülkenin siber

hegemonyaya sahip olma amacının olmaması ve diğer ülkelerin iç işlerine müdahale etmemesi gerektiği de söylenmektedir. Xi Jinping'in önerileri ise şu şekilde sıralanmaktadır (Xi, 2015):

- Küresel internet altyapısının oluşturulmasının hızlandırılması ve ağ-bağlanırlığının desteklenmesi,
- Karşılıklı öğrenme ve aynı zamanda kültürel değişim için online platform oluşturulması,
- Ortak refahı sağlamak amacıyla siber ekonominin yenilikçi gelişiminin teşvik edilmesi,
- Siber güvenliğin korunması ve düzenli bir şekilde gelişiminin teşvik edilmesi,
- Eşitlik ve adaletin teşvik edilmesi amacıyla internet yönetim sisteminin kurulması.

Bununla beraber, ÇHC'nin Milli Savunma Bakanlığı tarafından 26 Mayıs 2015 tarihinde ilan edilen yeni bir "aktif savunma" politikasını özetleyen, kamu ile paylaşılan ilk strateji belgesi olma özelliği gösteren Çin Askeri Stratejisi beyaz kitabını yayımladığı görülmektedir. Önceden yayımlanan dokuz ulusal savunma belgeleri arasında doğrudan askeri strateji odaklı ilk belge olarak karşımıza çıkmaktadır (USNI News, 2015). ÇHC'nin siber güvenliği ile ilgili önemli ipuçlarının yer aldığı belgeye göre, ÇHC kara, deniz, hava, uzay ve siber uzayın güvenliğini bir bütün olarak gören askeri bakış açısına sahip olmaktadır. Birçok ilkin yaşandığı belgede bir diğer ilk ise siber birim kurma hususunda gerçekleşmektedir. İlk defa ordu içerisindeki saldırı olarak siber operasyon yapma yeteneğine sahip siber birim kurma hususu resmi olarak açıklanarak hükûmetin ana hedefi bu kapsam doğrultusunda kendi sınırları içerisinde siber uzayda tam egemenlik kurmak ve bunu da iç ve dış tehditlere karşı savunma olarak belirtilmektedir (China's Military Strategy, 2015). Çin'in Askeri Stratejisi adlı belgede şu noktalara işaret edilmektedir (USNI News, 2015):

- Bilgi toplumunun hızlı gelişimi,
- PLA'nın oluşan bu yeni koşullarla uyumlu olabilecek yeni planlar oluşturması gerekliliği,
- Enformasyonizasyon.

Yerel çatışmaların dahi bu bilgilendirme sürecinden etkilenecek biçim değiştirmesi gerektiği, aynı zamanda PLA'nın savaş sistemlerini ve komuta yapısını ve

tüm askeri öğelerini ağ teknolojisi ile uyumlu hâle getirmesinin bir zorunluluk olduğu vurgulanmaktadır. Yaşanacak olan siber kriz ve siber operasyonları PLA'nın yeni bir tehdit olarak değerlendirdikten sonra bunlara karşı yeni önlemler alması gerektiği ifade edilmektedir (USNI News, 2015).

Çin'in Askeri Strateji belgesi kapsamında, uzayın uluslararası rekabette yeni bir alan hâline gelmesi dolayısıyla hükûmetler tarafından uzay politikalarının geliştirildiği görülmektedir. Bu durumun, uzayın silahlandırılmasına yönelik olduğu, aynı zamanda ÇHC'nin uzayın barışçıl bir ortam olmasından yana olduğunu fakat bu alanda var olan çıkarlarının da korunması gerektiğini ve uzay güvenliğine karşı olabilecek tüm risk ve tehditlere karşı mücadele verileceği belirtilmektedir. Milli güvenlik alanı hâline gelen siber uzay, ekonomik ve sosyal ilerlemenin yeni temeli olarak görülmektedir. Bundan dolayı birçok ülke tarafından siber kuvvet oluşturulmaktadır. Siber saldırıların başlıca kurbanlarından biri olan ÇHC, siber uzayın böylesine önem arz ettiği bu süreçte ve karşılaşılan risk ve tehditler dolayısıyla gerekli siber altyapının korunması maksadıyla gereken tüm önlemlerin alınacağını vurgulamaktadır. Bu kapsamda var olan siber kuvvetlerini güçlendirme yoluna gidileceği ve siber uzay alanında uyarı sistemlerinin geliştirilip, yerleştirilmesi ile siber uzay alanının korunabilmesi maksadıyla uluslararası boyuttaki alınan önlem ve faaliyetlere katılacağını belirtmektedir (China's Military Strategy, 2015).

Yayımlanan Askeri Stratejik belgesinde siber uzay 'stratejik rekabet alanı' olarak kabul edilmektedir. Bundan dolayı siber uzay alanında siber savunma birimi kurulacağı söylenmektedir. ÇHC ordusu bir taraftan siber savunma kabiliyetini geliştireceğini, yaşanacak olan herhangi bir siber kriz hâlinde milli bilgi ağını ve bilgi güvenliğini, ülkenin milli güvenliğini ve sosyal dengesini koruyacağını belirtmektedir. Diğer taraftan ise ülkenin uluslararası iş birliğini geliştirme çabasını desteklediğini söyleyerek siber uzayda uluslararası iş birliğine de açık kapı bırakmaktadır. Strateji belgesine bakıldığında, siber savunmanın bilgi güvenliği başlığı altında yer aldığı da dikkat çekmektedir (China's Military Strategy, 2015).

Siber güvenlik alanında yaşanan gelişmelere, oluşan yeni kurumlara ve uygulamalara bağlı olarak uzay teknolojilerinden kaynaklanan bilimsel gelişmeleri; askeri, ekonomik ve siyasi kapasitesini güçlendirmek maksadıyla yeni bir fırsat alanı olarak değerlendiren aynı zamanda uzay alanındaki siber kapasitesini geliştirme yönünde adımlar atan ÇHC hükûmeti, 2016 yılında "Ulusal Siber Uzay Güvenliği

Stratejisi” adlı belgeyi yayımlamaktadır. Belgede bahsi geçen hususlar şu şekilde sıralanmaktadır (National Cyberspace Security Strategy, 2016; Journal of Political Sciences and Public Affairs, 2017):

- Milli güvenlik hususunda siber uzay, yeni risk ve tehditlerin oluştuğu aynı zamanda öngörülmez bir şekilde güçlenmeye devam ettiği bir alandır.
- Siber alan/uzaydan dolayı oluşabilecek tehditlerin ortadan kaldırılması noktasında ÇHC hükûmeti bilimsel, yasal, diplomatik, teknik ve askeri olarak bazı önlemleri hayata geçirecektir.
- ÇHC hükûmeti, başta iç güvenliği hedef alan her türlü casusluk, sabotaj gibi müdahale girişimine karşı herhangi bir kararsızlık yaşamadan önlem alacaktır.
- Ülkede bulunan kritik altyapı sistemini korumaya yönelik önlemler alınacaktır.

Siber uzayı deniz, toprak, hava ve uzayla aynı öneme sahip yeni bir alan olarak gören ÇHC, yayımlamış olduğu bu belgede istikrarlı, güvenli ve sürekli güçlenen bir siber uzayın sadece ÇHC’de değil aynı zamanda bütün dünya için de büyük önem taşıyan bir ‘yeni alan’ olduğunu ifade etmektedir. Ulusal Siber Uzay Güvenliği Strateji belgesinde, milli rejimi yıkmayı ya da ağ yoluyla ortadan kaldırmayı hedefleyen bütün faaliyetlere itiraz edilmesi gerektiği vurgulanmaktadır. Kritik bilgi alt yapılarının gözetilmesinin hükûmetin, özel sektörün ve toplumun tamamının ortak sorumluluğu olduğu söylenmektedir (National Cyberspace Security Strategy, 2016).

ÇHC söz konusu belgede, ortak sorumluluğun sadece ülke içerisinde değil uluslararası düzeyde de yayılım göstermesi ve kazan-kazan (win-win) politikası gerekçesiyle siber uzayda ‘ortak kader topluluğu’ oluşturulması gerektiğine inandığının sözünü etmektedir. Fakat sözü edilen bu durum için ÇHC’nin Batı’ya karşı güvensiz tutumundan dolayı bugüne kadar herhangi bir adım atılamamaktadır. Bu bağlamda karşılıklı olarak ortada bir güvensizliğin olduğundan söz edilmektedir. Bu güvensizliğin temel nedeni, Batı toplumunun insan haklarına odaklanmasının ÇKP’nin ve ÇHC toplumunun istikrarı için bir tehdit olarak görülmesinden kaynaklanmaktadır. İnterneti Batı müdahalesinin bir aracı olarak gören ÇHC, Batı değerlerinin Çin toplumu içerisinde yayılmasından endişe duymaktadır. Bununla birlikte Batı’nın endişe duyduğu noktanın ise ÇHC’nin siber casusluk ve bilgi savaşı kapasitesi olduğu belirtilmektedir (Peiran, 2012: 38). Bu doğrultuda, siber uzayın gelişimi açısından ortak bir girişimin

olması önemli bir adım olarak görülsede karşılıklı olarak yaşanan bu güvensizlik sorunu devam ettiği müddetçe siber uzay ile ilgili ortak bir girişimin olması pek mümkün olmamaktadır. ÇHC ve Batı arasındaki bu problem her geçen gün arttığından dolayı ortak girişim için zorlukta artarak devam etmektedir.

Tüm bu anlatılanlar ışığında genel bir değerlendirme yapıldığında; siber güvenlik ile ilgili ÇHC'nin geliştirmiş olduğu planlar, ortaya koyduğu stratejiler, düzenlemeler ve oluşturulan kurumlar çerçevesinde şu hedeflere ulaşılmaya çalışıldığı ifade edilmektedir (Darıcılı ve Özdal, 2018: 17):

- İnternet, ağ teknolojileri ve bilişim sektörlerinin gelişmesi,
- Yerel teknolojilerin teşvik edilmesi,
- Devlet kurum ve kuruluşlarının, bireylerin siber güvenliğinin sağlanması,
- Diğer devletlerden olası siber operasyonların, casusluk ve manipülasyon faaliyetlerinin kısacası her türlü siber faaliyetin engellenmesi amaç edinilmektedir.

Yaşanan tüm bu gelişmelerden dolayı siber saldırı kapasitesini ve siber savunmasını geliştirmek adına birçok politika izleyen ÇHC, bu alanda yapmış olduğu çoğu adımla birlikte hem siber güvenliğin giderek daha fazla ön plana çıkması hem de bu alanda etkin bir küresel aktöre dönüşme gayesiyle siber güvenlik alanında yapmış olduğu önceki düzenlemelerin yasallaştırılması yoluna gitmektedir. Bu bağlamda 7 Kasım 2016'da kabul edilen ve 1 Haziran 2017'de yürürlüğe giren Siber Güvenlik Yasası'nı uygulamaya koymaktadır (ReedSmith, 2018). Siber Güvenlik Yasası'nın ayrı bir başlık altında daha detaylı bir şekilde ele alınması planlanmaktadır.

2019 yılına gelindiğinde bir Beyaz Kitap daha yayımlandığı görülmektedir. Oluşturulan bu kitapta ÇHC'nin yeni girdiği süreçteki ulusal savunması ele alınmaktadır. Bu kitapta, ÇHC ve Rusya ile rekabete ve oluşabilecek çatışmaya, terörle mücadele ve aşırıcılığa odaklanan ABD stratejisinde gerçekleşen büyük değişime açık ve detaylı bir cevap verilmektedir. ÇHC, ABD ile stratejik rekabetinde siber güvenliğin de önemli bir kriter olacağını bu kitapta belirtmektedir (Cordesman, 2019). PLA'nın var olan koşullarda yönetilme şekillerini ifade etmek maksadıyla inovasyonun, liderliğin ve komuta sistemlerinin iyileştirilme vurgusunun yapıldığı kitapta, aynı zamanda halk savaşının genel gücünü belirterek Mao Zedong'un doktrini desteklemeye devam edileceğine ilişkin vurgu yapılmaktadır. Kitapta, askeri güçlerin modernizasyonu ve genişlemesi tamamen savunmacı bakış açısıyla değerlendirilmektedir (Mallick, 2019).

Bu bağlamda PLA, bilgi odaklı bu dönemde yeniliklerden yararlanmayı ve yeni savaş yollarına hazırlanmayı hedeflemektedir. 2012 yılından 2021 yılına kadar bakıldığında, ÇHC'nin savunma alanında yapmış olduğu harcamaları 98 milyar dolardan 210 milyar dolara yükselttiği ve her geçen yıl bu yükselişin katlanarak arttığı tespit edilmektedir (Euronews, 2021).

ÇHC'nin silahlı kuvvetleri siber uzay kabiliyetlerinin güçlendirilmesinin belirtildiği 2019 Beyaz Kitap'ında, bu doğrultuda ulusal siber sınır, savunmasını geliştirip ağ müdahalelerini hemen tespit edip karşı koymak amacıyla inşa edilmektedir. İnşa edilen sınır, siber güvenlik ve bilgiyi koruyarak ulusal siber egemenliği, bilgi güvenliğini ve sosyal istikrarı kararlılık çerçevesinde sürdürmektedir. Tehdit ve risklerin çoğaldığı bu dönemde ÇHC, tehditleri algılama noktasında stratejik hayati çıkarların merkezine siber güvenliği almaktadır. Bu durum kitapta şu sözlerle belirtilmektedir (Mallick, 2019):

- *“Dışardaki alan, uluslararası stratejik rekabette kritik bir yerdir. PLA siber savaşta, düşmanın keşiflerini ve iletişim uydularını yok etmek, zarar vermek ve bunlara müdahale etmeyi amaçlamaktadır.”*

Bunun için yapılması istenilen şey ise “düşmanı kör ve sağır etmek” olduğu kitapta belirtilmektedir. Kitapta siber uzayın barışçıl kullanımı üzerinde duran ÇHC, bu bağlamda uyduları korumak, alana güvenli bir şekilde girmek, çıkmak ve kullanma kabiliyetini korumak maksadıyla ilgili teknolojiler ve kabiliyetleri geliştirdiğini belirtmektedir (Mallick, 2019).

2020 yılında yayımlanan Beyaz Kitap'ta ise yapay zekâ hususu ön plana çıkmaktadır. Yapay zekâyâ verilen önemden ve yapılması beklenen birtakım projelerden bahsedilmektedir. Yapılması planlanan projeler genel hatları bakımından yapay zekâ uygulamasının çeşitli sektörlerde kullanılacak olmasıyla alakalı olduğu görülmektedir. Bu sektörler; kamu, ulaşım, sağlık, konaklama, yiyecek-icecek, ticaret, oyun vb. şeklinde sıralanabilmektedir (China White Paper, 2020). Bununla birlikte kitaota, ÇHC'deki yapay zekâ teknolojisinin son yılda hemen hemen %50 civarında bir artış gösterdiği belirtilmektedir (China White Paper, 2020).

Ocak 2022 yılında “Çin'in Uzay Programı: 2021 Perspektifi” başlıklı Beyaz Kitabı yayımlanmaktadır. Genel olarak uzay endüstrisini geliştirmeye yönelik öneriler sunan kitapta Başkan Xi Jinping “geniş evreni keşfetmek, uzay endüstrisini geliştirmek ve Çin'i bir uzay gücü hâline getirmek bizim ebedi hayalimizdir” sözleriyle bu alana

verdiği önemi vurgulamaktadır. Uzay endüstrisini, genel ulusal stratejinin kritik unsuru olarak görmektedir. Bundan dolayı ÇHC, uzayın barışçıl amaçlarla keşfedilmesi ve kullanılması ilkesini desteklemektedir. Uzay endüstrisini böylesine kritik bir unsur olarak gören ÇHC, yüksek kaliteli bir uzay endüstrisi sağlamak amacıyla bazı ilkelere bağlı kalınması gerektiğini savunmaktadır. Söz konusu ilkeler; iş birliği ve paylaşım dayalı, inovasyon odaklı, koordineli, verimli ve aynı zamanda barışçıl ilerleme ilkeleri şeklinde belirtilmektedir (China White Paper, 2022a).

Kitapta, dünyaya öncülük eden en son teknolojileri hedeflediğini belirten ÇHC, büyük uzay projelerinin önde gelen ismi olarak karşımıza çıkmaktadır. Bu yönde kararlı adımlar atan ÇHC, temel teknolojilere yönelik araştırmalarını, uygulamalarını, uzay teknolojisi ve sistemlerini geliştirme çabalarını hızlandırdığını ve bunu iki katına çıkarttığını belirtmektedir. Kitapta yer alan bir diğer husus ise ÇHC'nin uzay bilimi üzerine yapmış olduğu araştırmalar için programlar başlattığını belirtmesidir. ÇHC hükûmeti uzay endüstrisini geliştirme hususunda, politika önlemleri olarak ve uzay faaliyetleri için planlar oluşturarak aktif bir tutum sergilemektedir. İyi işleyen bir pazar olursa ve hükûmet kolaylaştırıcı adımlar atarsa çok daha uyumlu olunacağı düşünülmektedir. Bu durum yüksek kaliteli bir uzay endüstrisinin büyümesi için uygun bir ortam yaratmaya çabalayarak her ikisinin de rollerine tam anlamıyla yetki vermektedir. Son olarak kitapta ÇHC, uzayın barışçıl bir şekilde keşfedilmesi, geliştirilmesi ve kullanılmasının tüm ülkeler tarafından eşit olarak kullanılacak bir hak olduğunu belirterek, uzayın gelişmesi amacıyla tüm ülkeleri ortak bir geleceğe sahip küresel bir topluluk oluşturmak adına uzayda derinlemesine iş birliği yürütmeye çağırılmaktadır (China White Paper, 2022a).

ÇHC Haziran 2022 tarihinde yapmış olduğu teknik inceleme neticesinde 1,05 milyarlık sayı ve %74,4'e ulaşan internet penetrasyon oranı ile dünyanın en büyük internet nüfusuna sahip devleti olarak karşımıza çıkmaktadır (China SCIO, 2022). İnternetin ÇHC için böylesine önem arz ettiği bu süreçte Kasım 2022 tarihinde "Siber Uzayda Ortak Bir Geleceğe Sahip Topluluk Oluşturun" başlıklı *Beyaz Kitap* yayımlanmaktadır. İnternetin, önemli bir insan başarısı ve bilgi çağının gelişinin bir simgesi olduğunun vurgusu yapılan kitapta; internetin geliştirilmesi, kullanımı, yönetimi ve insanlığa faydalı hâle getirilmesi gerektiğinin tüm insanlığın sorumluluğu olduğu ifade edilmektedir. Bu bağlamda internet gelişiminin ortak vizyonu 'paylaşım ve birlikte yönetim' olarak belirtilmektedir. Küresel bilgi teknolojisinin hızla yayıldığı bu

süreçte internette hızlı bir gelişim göstermektedir. Bundan dolayı internet, insan yaşamına ve her türlü çalışma alanına nüfuz etmektedir. Bu neticeyle, insanlığın siber uzayda ortak çabalarla ele alınması gereken kalkınma ve güvenlik problemleriyle gün geçtikçe daha çok karşı karşıya kaldığı gözlemlenmektedir (China White Paper, 2022b).

ÇHC, interneti, insanlara fayda sağlayan bir açılım ve işbirliği platformu olarak görmektedir. Yeni kalkınma dinamiği inşa eden ÇHC, gücünü siber uzay ve dijital teknolojilerde geliştirme hususunda oldukça istikrarlı bir tutum sergilemektedir. Kitapta ÇHC'nin kapsamlı istişare, ortak katkı ve ortak çıkarlar ilkesini desteklediği belirtilmektedir. Bu doğrultuda ÇHC, siber uzayda ikili, bölgesel ve uluslararası diyalog ve işbirliğini güçlendirmeye devam etmektedir. Bundan dolayı yayımlanan kitapta ÇHC, uluslararası toplumdaki taraflarla kapsamlı ortaklıklar kurma taahhüdünde bulunmakta olduğunu ifade etmektedir. İnternetin öneminin her geçen gün arttığı bu çağda ÇHC interneti insanlığın ortak evi olarak gördüğünü vurgulamaktadır. Akabinde bu evi daha temiz, daha güvenli hâle getirmenin toplumun sorumluluğu olduğu söylenmektedir. ÇHC, internetin gelişiminin faydalarından herkesin yararlanabilmesi adına siber uzayda ortak geleceğe sahip bir topluluk oluşturmak amacıyla diğer ülkelere katılacağını kitapta bildirmektedir. Bunun da her zaman olduğu gibi kendi ulusal koşulları doğrultusunda ve insan merkezli, açık ve kazan kazan işbirliği ruhuyla yapılacağı söylenmektedir (China White Paper, 2022b).

Mart 2023 tarihine gelindiğinde ise son olarak Çin Devlet Konseyi Enformasyon Bürosu tarafından “Yeni Çağda Çin’in Hukuka Dayalı Siber Uzay Yönetişimi” başlıklı teknik inceleme *Beyaz Kitabı* yayımlanmaktadır (Xinhua, 2023). Küreselleşen dünyada bilgi teknolojisinin hızla gelişimiyle beraber bu sürece uyum sağlayan ÇHC, hukuka dayalı siber uzay yönetişimini hukukun üstünlüğünü genel ulusal stratejisine entegre etmek amacıyla kendi gerçeklerinden yola çıkarak bu süreçte bilgi ve deneyim kazandığı görülmektedir. Aynı zamanda yayımlanan bu kitapta görüldüğü üzere, ÇHC'nin siber uzay yönetişimine kendine has bir yaklaşımla öncülük ettiği belirtilmektedir. Bir ülkenin iyi bir şekilde yönetilebilmesi için güçlü bir araç olarak yasaya ihtiyacı olmaktadır. Yani iyi yönetişimin ön koşulu olarak yasaların varlığı karşımıza çıkmaktadır (China White Paper, 2023).

Bunların yanı sıra internetin gelişim gösterdiği bu süreçte tüm ülkeler gibi ÇHC'nin de bu trendi takip ederek düzenlemeler yaptığı görülmektedir. Söz konusu kitapta ÇHC'nin, iyi planlanmış ve demokratik bir şekilde aynı zamanda yasalara uygun

olarak yürürlüğe giren mevzuat yoluyla siber uzay yönetişimi için yasal sistem geliştirdiği belirtilmektedir. Yapılan bu çalışmadan dolayı, siber mevzuatın sistematik, bütünsel, koordineli ve zaman açısından da verimli bir hâle geleceği vurgulanmaktadır. Kanuna dayalı Siber uzay yönetişiminin kritik bağlantısı ‘sıkı kanun yaptırımı’ olarak ifade edilmektedir. ÇHC bu doğrultuda bazı sıkı önlemler almaktadır. Bunlar şu şekilde belirtilmektedir (China White Paper, 2023):

- Siber uzayda adil ve kurallara dayalı kanun yaptırımı sağlamak,
- Kamuyu fiilen ilgilendiren kilit alanlarda yaptırımı güçlendirmek,
- Hem bireyin hem de genel olarak kamunun meşru hak ve çıkarlarını korumak.

Yayımlanan bu teknik incelemede amaç; temiz bir siber ortamda sağlam ve kurallara dayalı bir düzen oluşturmaktır. Kitapta da belirtildiği üzere ÇHC, adli adaleti sağlama ve kamu için adaleti uygulama ilkesine bağlı kalmaktadır. Bundan dolayı internet çağında adaletin ihtiyaçlarına aktif olarak cevap veren ÇHC, internet ve bilgi teknolojilerini geleneksel yargıyı güçlendirmek, siber adalet kurallarını iyileştirmek ve siber adalet modellerini yeniden düzenlemek amacıyla kullanmaktadır (China White Paper, 2023).

Yayımlanan kitapta üzerinde durulan bir diğer hususun, hukukun üstünlüğü olduğu ifade edilmektedir. Siber uzayda hukukun üstünlüğü bilgisinin yayılması noktasında halkın katılımı gerekliliği olduğu için ÇHC, yasal bilgiyi internet vasıtasıyla yaymanın içeriği, biçimi ve araçları hususunda yeni bir çığır açmak amacıyla her türlü çabayı göstermektedir. Bununla beraber, Çinli netizenlerin⁴ hukukun üstünlüğü hususundaki farkındalığının ve anlayışının genel olarak arttığı görülmektedir. Aynı zamanda çevrimiçi platformlar, yasal uyum amacıyla birincil sorumluluğu üstlenerek sektör öz disiplini benimsemektedir. Tüm insanlık için ortak faaliyet alanı olan siber uzay yönetişiminin güçlendirilmesi hususunda tüm ülkeler ile iş birliğinin artırılmasına büyük ihtiyaç duyulmaktadır. Çünkü dünyanın dört bir yanındaki tüm ülkeler, dijital ekonomiyi geliştirmek adına aynı isteği paylaşmaktadır. Aynı zamanda teknolojinin gelişimiyle beraber siber güvenlik alanında karşılaşılan risk ve tehditlerin yaratmış olduğu zararlar noktasında da eşit zorluklarla karşı karşıya kalınmaktadır. Bundan

⁴ Netizen: Ağdaş olarak da ifade edilen netizen, online topluluklarda ya da genel anlamda internette aktif olarak yer alan kişilere verilen isimdir.

dolayı tüm ülkelerin siber uzay yönetişimini güçlendirmesi açısından iş birliği olmazsa olmaz bir durum hâline gelmektedir (China White Paper, 2023).

Tüm bu anlatılanlar doğrultusunda yayımlanan teknik incelemeyle beraber Çinli yetkililer, kişisel bilgileri korumak adına 2019 yılından beri 3.22 milyon mobil uygulamanın incelendiğini belirtmektedir. Yapılan incelemeler sonucunda yasa ve düzenlemeleri ihlal eden yaklaşık 3000 civarında uygulamaya eleştiri bildirimleri gönderildiği ya da direk kaldırıldığı ifade edilmektedir. Teknik inceleme sonucunda, hedefli faaliyetler yoluyla, kişisel bilgi haklarının ihlallerinin etkin bir şekilde önlendiği açıklanmaktadır. Ayrıca ilgili düzenlemelere uyan uygulamaların sayısı da giderek artmaktadır. Aynı zamanda kamu da kişisel verilerin korunması hususunda güçlü bir farkındalık oluşmaktadır (Xinhua, 2023).

Tüm bu analizler ışığında genel bir değerlendirme yapılacak olursa; ÇHC'nin siber güvenlik politikalarını belirlerken üzerinde durduğu en önemli noktanın siber güvenlik meselesini ulusal güvenlik ile eş değer görmesi durumu olarak karşımıza çıkmaktadır. Bundan dolayı siber güvenlik adına attığı adımlarda aslında ulusal güvenlik değerlerini de göz önüne alarak hareket ettiği gözlemlenmektedir. Her ülke gibi ÇHC'de siber güvenlik alanında karşılaşılabilecek tehditlerden dolayı önlemler almaktadır. Bu bağlamda yapılan düzenlemeler, yasalar ve politikalar da temel nokta; ÇHC'ye özgü adımlar atarak hareket etmesi olmaktadır. Yani kendi siber ağlarını kullanıp diğer ağları yasaklayıp alternatifler sunarak, sansür uygulaması getirerek ya da bazı sınırlandırmalar yaparak güçlü bir savunma mekanizması geliştirdiği görülmektedir. Fakat bu noktada kamuda güvensizliğinde ortaya çıktığı görülmektedir. Peki, bu güvensizlikler nelerdir? Tamda bu nokta da siber güvensizlik hususuna da kısaca değinmenin faydalı olacağı düşünülmektedir. Genel olarak ÇHC'de oluşan ya da oluşabilecek güvensizlik problemleri şu şekilde sıralanabilmektedir:

1. Yaşanılacak herhangi bir saldırı sonrası ÇKP'ye karşı güvensizlik duygusunun oluşması riski,
2. Kritik altyapı sistemlerinin tehlikeye girme riski,
3. ABD'ye yönelik olan güvensizlik algısı.

Bununla beraber, bilişim ve teknolojinin gelişim gösterdiği süreçlerden sonra hemen hemen tüm ülkelerin birçok alanda internet kullanımını arttırdığı gözlemlenmektedir. ÇHC, diğer ülkelere göre her ne kadar interneti geç kullanmaya başlasa yine de günümüzde hızlı bir şekilde internet hususunda en çok kullanıcıya

ulaşan devletlerden biri olarak yerini almaktadır. İnterneti ilk kullandığı andan itibaren ÇHC’de, Çinli politika yapıcılar ve analistler için siber uzay, ekonomik büyüme ve iyi bir yönetim için gerekli görülse de iç istikrarı ve rejim meşrutiyetine karşı oluşabilecek bir risk veya tehdit unsuru olarak da görülmektedir (Segal, 2017: 3). Bunun yanında, bir ülkede karşılaşılabilecek herhangi bir saldırı sonrası kamuda bir güven problemi oluştuğu ifade edilmektedir. Bundan dolayı ÇHC’de karşılaşılabilecek herhangi bir saldırı dolayısıyla Çin toplumunda ÇKP’ye karşı bir güvensizlik duygusunun oluşabileceği düşünülmektedir. Bu durum da rejimin devamlılığı hususunda olumsuz etkilere sebep olacağı endişesini doğurmaktadır. Yaşanılan bu endişeden dolayı ÇHC hükûmeti kamunun internet kullanımında sert önlemler alarak bu endişeyi azaltmaya çalışmaktadır. Bu önlemlerde yukarıda sözü edilen yasalar, düzenlemeler ve politikalarla gerçekleştirilmektedir. En önemlisi de vatandaşların çevrimiçi olma durumlarının ÇHC hükûmeti tarafından sürekli denetlenmesi durumunun olması karşımıza çıkmaktadır. Aslında bakıldığında bu durum bile kamu ve devlet arasında güven problemine sebep olmaktadır (Kesgin, 2022:50-55).

Diğer yandan, devletler nezdinde, özellikle ulusal güvenliklerinin sağlanması aynı zamanda kritik altyapılarının korunması noktasında geleneksel güvenlik yöntemlerinin yetersiz kaldığını fark ederek, gelişen teknolojilerle birlikte kritik altyapının dönüşmesiyle siber güvenlik hususunda farkındalıkların arttığı görülmektedir. Ülkeler için böylesine önemli bir konu olan kritik altyapılar ÇHC içinde büyük önem arz etmektedir. ÇHC’de oluşan siber güvensizlik düşüncesinin bir diğer sebebini de, karşılaşılabilecek herhangi bir saldırı sonrası kritik altyapı sistemlerinin tehlikeye girme riski oluşturmasından kaynaklanmaktadır. Kritik altyapı denildiğinde akla ulaşım, iletişim, enerji, su, finans vs. gelse de siber güvenlik ile beraber bilgisayar sistemleri ve bilgi sistemleri de kritik altyapıyı oluşturan unsurlar olarak karşımıza çıkmaktadır. Bunlar içinde bulunduğumuz süreçte siberleşmiş enerji ve endüstriyel kontrol sistemlerinin güvenliğini içeren ülkelerin fiziki ve aynı zamanda ekonomik güçlerinin ötesinde güvenliğini nitelemektedir. Bu konuyla alakalı olarak tüm ülkelerde olduğu gibi ÇHC’de, kritik altyapıları korumak ve kamuda bilgi güvenliğini sağlamak aynı zamanda kritik altyapı sistemlerinin karşılaşılabilecek riskleri ortadan kaldırmak adına siber güvenlik stratejileri oluşturmakta ve siber güvenlik politikaları uygulamaktadır (Göçoğlu ve Aydın, 2019: 237).

Son olarak ÇHC’de siber alanda oluşan güvensizliğe sebep olan bir diğer hususun ise ABD’ye karşı olan güvensizliğin olduğu ifade edilmektedir (Raud, 2016: 7). Siber güvenlik stratejilerini geliştirme noktasında ÇHC’nin göz önüne aldığı iki unsur bulunmaktadır. Bunlar; ABD’ye karşı oluşan güvensizlik algısı ve siber uzayın kontrolsüzlüğü şeklinde belirtilmektedir. Karşılaşılan bu iki risk, ÇHC’nin ulusal güvenlik alanında problemlerin doğmasına sebep olmaktadır. ÇHC’de ulusal güvenliğin bozulması demek, ekonominin zarar görmesi, rejimin gelişiminin zayıflayıp güç kaybetmesi, toplumda güvenin azalması, bölgesel ve küresel itibarın kaybolması gibi olumsuz etkilerin ortaya çıkması demektir. Buna bağlı olarak, diğer ülkelerde yabancı kökenli Facebook, Twitter ve Google gibi sosyal medya araçları kullanılırken, ÇHC bunlara erişim yasağı getirmektedir. Bu sosyal medya araçlarına alternatif olabilecek Renren, Sina Weibo ve Baidu gibi internet platformlarını hizmete sunmaktadır. Böylece ABD’nin kontrolünde bulunan hizmetler engellenerek siber güvenlik ve siber egemenlik bir anlamda sağlanmaya çalışılmaktadır. Atılan bu adımlar sayesinde ÇHC sansür kararlarını da istediği şekilde yönetebilme fırsatı bulmaktadır. ÇHC’de, kamuya erişim engeli konulan Facebook ve Twitter uygulamaları 2020 yılına gelindiğinde politikacıların kullanımına sunulmaktadır. Çin Dış İşleri Bakanlığı sözcüsü Geng Shuang’ın dediği doğrultusunda buradaki amacın, “Pekin yönetiminin ülke dışındaki insanlarla daha iyi iletişim kurması ve ÇHC’nin politikalarının daha iyi tanıtılmasının sağlanması” sebebiyle bu platformların politikacılar tarafından kullanılmasına izin verilmektedir (NTV, 2020).

ABD’den kaynaklı oluşan bu siber güvensizlik bağlamında ÇHC, siber egemenlik isteğini uluslararası alana taşıyarak siber güvenlik stratejisi hususunda ayrı bir izleç açmaktadır. Dünyada 13 adet ana sunucu bulunmaktadır. Bu ana sunucuların 10 tanesinin ABD’ye ait olduğu belirtilmektedir. Aynı zamanda tüm sunucular ABD’nin merkezinde bulunan İnternet Tahsisli Sayılar ve İsimler Kurumu’nun (ICANN) kontrolünde yer almaktadır. ÇHC, Los Angeles merkezli kuruluş olan ICANN tarafından yönetilen internetin ABD istihbaratına ve ABD’nin çıkarlarına hizmet ettiğini düşünmektedir (Baezner, 2018: 3). Bu husus ÇHC’nin sürekli vurguladığı siber egemenlik düşüncesinin güçlenmesine yol açmaktadır (Balke, 2018: 141).

3.2.1. Siber Güvenlik Yasası

ÇHC'nin Ulusal Halk Kongresi Daimi Komitesi'nde (Standing Committee of the National People's Congress- NPC) 2015 yılında kamuoyu yoklaması yapma yoluyla halkında fikirleri göz önünde bulundurularak Siber Güvenlik Yasası tasarısı oluşturulmaktadır. 2015'te oluşturulan tasarı, Haziran 2016'da kongre tarafından ikinci kez tartışılmaya açılmaktadır. 2016 yılının Kasım ayında ise tasarının son hâli kuruluş resmi sitesinde yayımlanarak kamuoyunun ilgisine sunulmaktadır. 1 Haziran 2017 yılına gelindiğinde ise NPC'nin oluşturmuş olduğu kanun taslağı yürürlüğe girerek uygulanmaya başlanmaktadır (Göçoğlu ve Aydın, 2019: 244-245; COV, 2016). Siber Güvenlik Yasası 7 bölüm ve 79 maddeden oluşmaktadır. Bölümlere genel bir şekilde değinilecek olursa:

- **1. ve 2. Bölüm:** Genel prensipler ve hükûmetin genel siber güvenlik stratejisi hakkında bilgi verilmektedir.
- **3. Bölüm:** Çok Boyutlu Ağ Güvenliği Koruma Planı şematığı çerçevesinde ağ operatörleri için geçerli siber güvenlik yükümlülüklerini, ağ ürünleri ve hizmetleri sağlayıcılarının uyması gereken gereklilikleri ve tanımı ortaya koymaktadır.
- **4. Bölüm:** Bilgi güvenliği hususları olan; özel hayatın gizliliği, kötü amaçlı yazılımlar, siber suçlar, kanunsuz bilgi yayılımı gibi odak noktalar üzerine ele alınmaktadır.
- **5. Bölüm:** Acil durumlarda tehlikelere karşı yapılacak mücadeleler/hamleler ve yönetimi ile birlikte ağ izlemeyi kapsamaktadır.
- **6. Bölüm:** Ağ güvenliği kurallarının ihlâl edildiği durumlarda uygulanacak yaptırımları kapsamaktadır.
- **7. Bölüm:** Tanımları ve diğer ek hükûmleri içermektedir.

İnternet kullanımı ve aynı zamanda veri yönetimini düzenleyen, bunları bir araya toplayıp kapsamlı kurallar çerçevesi oluşturmak amacıyla çıkarılan yasada, ağ operatörlerinin ÇHC içerisinde bazı kişisel bilgileri depolamasına ve Çinli yetkililerin şirketlerin ağ operasyonlarına bir anda denetim yapmasına izin verilmektedir. Pekin, çıkarılan yasanın ÇHC'nin siber güvenlik için küresel en iyi uygulamalarla tertipli hâle getirmeyi hedeflediğini iddia etmektedir. Wagner'e göre yürürlüğe giren bu yasa, ÇHC'de 2010 yılında yayımlanan ve "ÇHC toprakları içinde internetin ÇHC'nin egemenliği altında olduğunu" iddia eden beyaz kitaba kadar dayanmaktadır (Wagner,

2017). Yasa ile ilgili ilk çalışmaların 2014 yılına dayandığı belirtilmektedir. 2014 yılında Ulusal Halk Kongresi ve ÇHC Halkı Siyasi Danışmanı Konferansı'nda hazırlanan raporda “siber güvenliğin korunması/sürdürülmesi” kavramı ilk kez kullanılmaktadır. 2015 yılında düzenlenen Ulusal Halk Kongresinde ise yukarıda belirtildiği üzere yasanın taslağı oluşturulmaktadır. 2016 yılına gelindiğinde ise yasanın taslağı yeniden düzenlenerek 154 evet 1 çekimser oy alarak kabul edilmektedir (KPMG, 2017: 4).

Siber güvenlik yasasının oluşturulmasında bazı hedefler ortaya konmaktadır. Bu hedefler yasanın ilk maddesinde belirtilmektedir. Söz konusu madde de belirtilen hedefler şu şekilde sıralanmaktadır (New America, 2017):

- Siber güvenliği sağlamak,
- Siber uzay/alan egemenliğini ve ulusal güvenliği, sosyal ve kamusal çıkarları korumak,
- Tüzel kişilerin, vatandaşların ve diğer kuruluşların yasal hak ve çıkarlarını korumak,
- Ekonominin ve aynı zamanda toplumun bilgilendirilmesinin sağlıklı gelişimi teşvik etmek amacıyla oluşturulmaktadır.

Oluşturulan siber güvenlik yasası, yalnızca internet güvenliğini değil aynı zamanda iletişim güvenliği, bilgisayar güvenliği, bilgi güvenliği, otomasyon ve kontrol sistemleri güvenliğini de ele almaktadır (Zhao ve Xia, 2018).

Yukarıda da kısaca bahsedildiği üzere, siber güvenlik yasası; ağ operatörleri için güvenlik gereksinimi, kişisel verilerin korunması, önemli bilgilerin altyapısı, kişisel ve deniz aşırı işletmelerin verilerinin aktarımındaki kısıtlamalar ve yükümlülük üzerine odaklanmaktadır. Kişisel bilgilerin korunması hususu üzerinde çok fazla duran yasa, bu konuda özellikle kişisel verilerin sadece bireyler mücade ettiği müddetçe toplanabileceğinin altını çizmektedir. Ulaşım, sağlık, eğitim, çevrimiçi ve çevrimdışı gibi hizmetler için bireylerin sağlamış olduğu kişisel bilgilerin ifşa edilmesi, sızdırılması ya da imha edilmesinin önüne geçmek amacıyla gerek görülen önlemlerin alınacağını vurgusu yapılmaktadır (KPMG, 2017: 8). Kısaca yasanın genel çerçevesi toparlanacak olursa şu şekilde ifade edilebilmektedir (KPMG, 2017; ReedSmith, 2018):

- Yasa bilgi altyapısının korunmasına öncelik vermektedir.
- Önemli ve hassas olan verilerin yurt içinde saklanması gerektiği ön görülmektedir.

- Yasada, şebeke işletmecilerine ve bu işletmecilerin güvenlik ihtiyaçlarına yönelik somut bir tanım sunulmaktadır.
- Kişisel bilgilerin korunmasına önem veren yasayla, bu bilgilerin toplanması ve kullanılması standartlaştırılmaktadır.
- Belirlenen kanunlara uyulmadığında bunun sonucunda verilecek cezalar yasada açıkça belirtilmektedir.
- Ticari faaliyetlerin askıya alınması konusu da yasada yer almaktadır.

7 bölüm ve 79 maddeden oluşan yasa kapsamında incelenen maddeleri genel olarak değerlendirecek olursak (KPMG,2017; Darıcılı ve Özdal, 2018: 25-26; Alioğlu, 2019: 135-136):

- ***Kişisel bilgilerin/verilerin güvenliğinin sağlanması/korunması:*** Yasa, bireysel mahremiyete ve kişisel bilgilerin/verilerin korunmasına çok fazla önem vermektedir. Kişisel bilgilerin/verilerin toplanması ve kullanılması hususunun standartlaştırıldığı yasada, işletmelerin ‘veri güvenliği’ dışında ‘bireysel mahremiyetin korunması’ gibi hususlara da odaklanması gerektiğini belirtmektedir. Yasa çerçevesinde ÇHC, vatandaşların mahremiyetinin güvenliği açısından bazı önlemler almaktadır. Bu doğrultuda özellikle ÇHC vatandaşlarının kişisel bilgilerini/verilerini elde eden yabancı küresel şirketlerin ticari faaliyetleri denetlemekte ve bu yönetmelikle beraber standartlar belirlenmektedir.
- ***Şebeke operatörlerinin güvenlik ihtiyaçları:*** Yasada şebeke operatörlerinin güvenlik ihtiyaçları net bir şekilde tanımlanmaktadır. Akabinde büyük finansal kurumların çoğunluğunun ‘ağ operatörü’ olabileceği fikri öngörülmektedir. ÇHC’de çalışan yabancı şebeke operatörlerinin yapmış oldukları ticari çalışmaları kontrol etmek ve bu şirketlerden kaynaklı oluşabilecek siber casusluk faaliyetlerine karşı mücadele etmek amacıyla mekanizmalar bulunmaktadır. Yasada bu husus ile ilgili değinilen bir diğer nokta ise kişisel bilgilerdeki/verilerdeki hataları düzeltmek amacıyla bireylere şebeke operatörlerine başvurma hakları tanınması şeklinde ifade edilmektedir. Oluşan hataları ortadan kaldırmak ya da düzeltmek için önlem almaları gerektiği söylenmektedir. Ayrıca bireylerin ya da kuruluşların kendi kullandıkları ağlardan sorumlu olduğu ve kötü amaçlarla ya da diğer yasadışı faaliyetler için web siteleri ya da

iletişim grupları kurmalarının yasak olduğunun vurgusu yapılmaktadır. Son olarak ise yasa, şebeke operatörlerine ve internet platformlarına, toplanan kişisel bilgileri/verileri koruması noktasında gerekli önlemleri alma zorunluluğu getirmektedir.

- ***Kritik bilgi altyapısı:*** Bu hususta yasa, kritik bilgi altyapısının korunmasına yönelik yaptırımlar öngörmektedir. Aynı zamanda yasa, kritik bilgi altyapısının kapsamını da belirtmektedir. Kritik alt yapının korunması ve siber savunma kapasitesini artırma amacıyla bulunan ÇHC, bu yasa ile siber güvenliği koruma hususunda önemli noktalara değinmektedir. Bu doğrultuda siber güvenliği koruma ile ilgili olarak hükûmet enerji, finans, ulaşım, kamuya açık iletişim ve bilgi hizmetleri, su kaynakları, e-devlet, kamu hizmetleri ve diğer kritik bilgi altyapısı için siber güvenlik temelinde kilit koruma uygulamaktadır. Fakat bunlar tahrip edilirse işlev kaybına uğrar ya da veri sızıntısı yaşarsa ulusal güvenliği, ulusal refahı, ulusal ekonomisi ciddi şekilde tehlikeye girebilmektedir. Bundan dolayı yasa da, kamu yararı gözetilerek kritik bilgi altyapısının korunması vurgulanmaktadır.
- ***Kişisel bilgilerin/verilerin ve ticari bilgilerin yurtdışına aktarımına ilişkin kısıtlamalar:*** Normalde yabancı şirketler ve kuruluşların ÇHC dışında bilgi aktarımı yapması gerekmektedir. Fakat yasa, hassas verilerin yurtdışında saklanması gerektiğini şart koşmaktadır.
- ***Yaptırımlar ve cezalar (yasal yükümlülükler):*** Yasaya uyulmadığı durumlarda uygulanacak cezalar açıkça belirtilmektedir. Uygulanacak olan bu cezalar ve yaptırımlar ticari faaliyetlerin askıya alınmasını da içermektedir. Uygulamaya konulan cezalar doğrultusunda, yasadışı ya da kanun kapsamına uymayan hareketler şebeke işletmelerinin kapatılmasına veya ruhsatların iptaline yol açabilmektedir. Bunun yanında bir de kanunu ihlal eden ya da siber güvenliği tehlikeye atacak faaliyetlerde bulunan işletmelerin yasadışı gelirlerine el konulabilmekte veya yasadışı gelir tutarının 10 katına kadar para cezası uygulanabilmektedir. Akabinde yasadışı geliri bulunmayan şebeke işletmeleri 5 ila 15 gün boyunca gözaltında tutulabilir ve davanın ciddiyetine bağlı olarak 100.000 RMB-1.000.000 RMB para cezası verilebileceği öngörülmektedir.

Diğer yandan, internet kontrolünün hükûmetin egemenliğinde olması gerektiğini düşünen ÇHC'nin siber güvenlik ile ilgili görüşlerini yansıtan yasanın 12. maddesine değinilmesi oldukça önemli görülmektedir. Bu maddede; ağları kullanan herhangi bir kişi ya da kuruluşun anayasa ve yasalara uyulması gerektiğini aynı zamanda kamu düzenini gözetmesi ve sosyal ahlaka uyulması gerektiğini vurgulamaktadır. Akabinde, siber güvenliğin tehlikeye atılmaması gerektiğinin altı çizilmektedir. Bu maddede ulusal güvenlik, ulusal onur ve ulusal çıkarları tehlikeye atacak, ulusal egemenliğin yıkılmasına teşvik edecek, sosyalist düzeni alt üst edecek, ayrılıkçılığı tetikleyecek, ulusal birliği bozacak, terörizm, aşırıcılık, etnik ayrımcılığı ve etnik nefreti savunacak, müstehcen ve cinsel bilgileri yayacak, ekonomik veya sosyal düzeni bozacak eylemlerden kaçınmaları gerektiği yer almaktadır (KPMG, 2017).

Son olarak yasanın 7. bölümüne değinilecek olursa bu bölümde, Çinceden çevrildiğinde anlam kayması yaşayan bazı kelimelerin tanımlarına yer verilmektedir. Bu tanımlar ise şu şekilde sıralanmaktadır (KPMG, 2017):

- “Siber” anlamına da gelen “ağ” (网络) kavramı; bilgi toplama, depolama, iletme, değişim ve işleme için belirli kural ve prosedürleri izleyen bilgisayarlardan veya diğer bilgi terminallerinden ve ilgili ekipmanlardan oluşan bir sistemi ifade etmektedir.
- “Ağ güvenliği” anlamına da gelen “Siber güvenlik” (网络安全) kavramı; ağları istikrarlı ve güvenilir bir çalışma durumuna sokmak amacıyla siber saldırıları, güvenlik ihlallerini, müdahaleleri, imhaları ve yasadışı kullanımı ve beklenmeyen kazaları önlemek için gerekli önlemleri almayı ve ağ verilerinin eksiksiz, gizli ve kullanılabilir olma kapasitesinin sağlanması şeklinde ifade edilmektedir.
- “Ağ operatörleri” (网络运营者) kavramı; ağ sahipleri, yöneticileri ve ağ servis sağlayıcıları anlamına gelmektedir.
- “Ağ verileri” (网络数据) kavramı; ağlar aracılığıyla toplanan, depolanan, iletilen, işlenen ve üretilen her türlü elektronik veri olarak tanımlanmaktadır.
- “Kişisel bilgiler” (个人信息) kavramı; elektronik olarak ya da başka yollarla kaydedilen, tek başına veya diğer bilgilerle birlikte alınan, gerçek

kişilerin tam adları, doğum tarihleri, ulusal kimlik numaraları, kişisel biyometrik bilgileri, adresleri, telefon numaraları dâhil diğer kimlik bilgilerini de içeren gerçek bir kişinin kimliğini tanımlamak için yeterli olan her türlü bilgiyi ifade ettiği belirtilmektedir.

Yasa ile ilgili anlatılanlar ışığında bakıldığında, siber güvenlik yasasının çıkmasıyla beraber ÇHC resmi makamları, internet denetimi hususunda geniş yetkiler elde etmektedir. Söz konusu yasa, bireysel kullanıcılara internet ortamında yapılacak faaliyetlerde gerçek adlarını kullanma zorunluluğu getirmektedir. Akabinde internet işletmecilerinin verdikleri hizmetlerde bu düzenlemelere uyum sağlanması adına sorumluluklar artırılmaktadır. Yasanın böylesine zorlayıcı olması birçok şirketi etkilemektedir. Bu zorlukla karşı karşıya kalan ilk küresel şirketin Apple olduğu belirtilmektedir. Bu bağlamda Temmuz 2017’de ÇHC hükûmetinin, Apple’ın ÇHC uygulama mağazasından VPN uygulamalarını kaldırması hususunda doğrudan Apple’ı uyardığı söylenmektedir. Ayrıca, dünyanın bir başka önde gelen şirketi olan Amazon’un ÇHC’li ortağının, VPN sunucusu kurmak amacıyla bulut sunucusunun kullanılmasına karşı müşterilerine bir uyarı yayımladığı görülmektedir. Yayımlanan uyarıda, müşterilerin onaylanmayan VPN’lerin kullanıldığının tespit edilmesi durumunda Amazon’un hizmet vermeyi durduracağı bilgisi verilmektedir (Yeni Medya, 2017).

3.2.2. Çin’in Siber Güvenlik Aktörleri

Siber güvenlik politikaları belirlendiğinde bu politikaların yürütülmesinde birçok aktörün aktif rol oynadığı görülmektedir. ÇHC’de siber güvenlik politikaları hususunda önemli olan noktalardan biri siber güvenlik aktörleri olarak karşımıza çıkmaktadır. ÇHC mihverinde siber güvenlik strateji yönetimindeki aktörler; sivil taraf ve askeri taraf olarak ikiye ayrılmaktadır (Köksoy, 2019: 344-345):

- **Sivil Taraf:** ÇKP, hükûmete bağlı resmi kurumlar ve çalışma grupları, telekomünikasyon, teknoloji ve bilişim şirketleri, hacker gruplar, siber milisler ve siber güvenlik enstitülerinden oluşmaktadır.
- **Askeri Taraf:** PLA içindeki birimlerden oluşmaktadır.

ÇKP, ÇHC’nin siber güvenlik stratejilerinin belirlenmesi hususunda etkin rol oynamaktadır. İçinde Devlet Başkanı ve Başbakan’ın da yer aldığı aynı zamanda

Parti'nin en önemli yedi isminden oluşan *Politbüro Daimi Komitesi*⁵, *Danıştay* ve *Merkezi Askeri Komisyon* ÇHC'nin tüm karar alma süreçlerinde olduğu gibi sivil tarafın da en üst düzey karar alma organlarını oluşturmaktadır. Söz konusu yetkililer, ÇHC'nin siber güvenlik stratejilerine ilişkin geniş çaplı girişimlerde karar alan aktörler olarak rol oynamaktadır. Burada alınan kararlar yönetim piramidi göz önünde bulundurulup yukarıdan aşağıya doğru uygulanmaktadır (Raud, 2016: 19). Ayrıca üst yapıların talimatı üzerine kurulan ve siber güvenlikle ilgili konulardan sorumlu farklı kurumlar da bulunmaktadır. Örneğin (Lindsay, 2012: 6-8; Raud, 2016: 16-19; Darıcılı, 2017: 8-18; Darıcılı, 2018: 99; Darıcılı ve Özdal, 2018: 17- 19; Pekcan, 2020: 210):

- *Sanayi ve Bilgi Teknolojileri Bakanlığı (Ministry of Industry and Information Technology- MIIT)*: 2008 yılında kurulan Bakanlık, ABD İç Güvenlik Bakanlığı ile benzer sorumluluk ve görevlere sahip olmaktadır.
- *Çin Ulusal Bilgisayar Ağı Acil Müdahale Teknik Ekibi/ Koordinasyon Merkezi (The National Computer Network Emergency Response Technical Team/Coordination Centre of China- CNCERT)*: MIIT bünyesinde 2002 yılından beri faaliyet göstermektedir. Bu sivil toplum kuruluşu, ülke ağlarında bulunan zararlı yazılımların tespit edilmesinden ve gereken önlemlerin alınıp geliştirilmesinden sorumlu tutulmaktadır. Akabinde alınan bu önlemler ve süreçler hakkında MIIT'i bilgilendirmektedir.
- *Ulusal Savunma Bilim, Teknoloji ve Sanayi Devlet İdaresi (State Administration for Science, Technology and Industry for National Defense- SASTIND)*: MIIT bünyesinde yer alan bu organ, MIIT'in ulusal savunma için bilim, endüstri ve teknolojiye ilişkin yönergelerini, yasalarını ve yönetmeliklerini hazırlamakla görevlendirilmektedir.
- *Kamu Güvenliği Bakanlığı (The Ministry of Public Security- MPS)*: Bu kuruluş siber suçları araştırmak ve kritik altyapıları gözetmeye yönelik önlemler almakla görevlendirilmektedir. Aynı zamanda karşı casuslukta önemli bir göreve sahip olan MPS bundan dolayı Çinli teknoloji firmalarını ve ihraç edilecek ürünleri denetlemekle vazifelendirilmektedir.

⁵ Ülkeyi ilgilendiren önemli hususlarda son söz sahibi olan ve hükümet yönetiminin en yetkili organı Politbüro Daimi Komitesi olduğu belirtilmektedir. ÇKP Merkez Komitesi'ne bağlı olan Politbüro Komitesi'nin Daimi Komite Başkanı Xi Jinping'dir ve 7 üyeden oluşmaktadır.

- *Devlet Güvenlik Bakanlığı (Ministry of State Security- MSS)*: Hükûmete karşı yapılan düşmanca hizmetler esasında casusluk operasyonlarından, iç istihbarat servis gereksiniminin karşılanmasından ve aynı zamanda karşı casusluk planlarından sorumlu tutulmaktadır. ÇHC'nin istihbarat yapısında önemli rol oynadığından dolayı MSS'nin görev ve yetkileri oldukça geniş tutulmaktadır. Bu bağlamda ÇKP'ye karşı gerçekleştirilen muhalefet hareketlerine direnmek ve düşman ülkelerden kaynaklanan bilgi savaşı operasyonları da MSS'nin görevleri arasında yer almaktadır.
- *Devlet Şifreleme Bürosu (State Encryption Bureau)*: Devlet Konseyi altında faaliyet göstermektedir. Bu kuruluş, devlet kurumlarının kriptoloji ihtiyaçlarını karşılamaktadır.
- *Devlet Sırları Bürosu (State Secrets Bureau)*: Gizli olan tüm ağ sistemlerini yönetmektedir.
- Sıralanan kuruluşlar haricinde birde MSS'ye bağlı olarak hizmet veren “Çin Çağdaş Uluslararası İlişkiler Enstitüsü (*Chinese Institute of Contemporary International Relations*)” ayrıca “Çin Mühendislik Akademisi (*Chinese Academy of Engineering*)” ve “Çin Bilimler Akademisi (*Chinese Academy of Sciences*)” gibi aktörler de siber uzay tabanlı teknolojilerin araştırılması noktasında aktif rol oynamaktadır.

Sivil tarafta yer alan aktörlerden bir diğeri ise *küçük çalışma grupları* olarak belirtilmektedir. Temel amaçları ÇHC'nin bilgi teknolojilerindeki gelişimi sağlamak olan bu gruplara örnek olarak; “Devlet Bilişim Öncü Grubu (*State Informatisation Leading Group- SILG*)” ve “Devlet Ağı ve Bilgi Güvenliği Koordinasyon Küçük Grubu (*State Network and Information Security Coordination Small Group- SNISCSG*)” verilmektedir. İlk önce 1993 yılında ÇKP Merkez Komitesi ve Devlet Konseyi tarafından kurulan SILG, sonrasında 2001 yılında bilişimin teşvik edilmesi ve devlet bilgi güvenliğinin sağlanması hususunda önderlik sağlamak adına yeniden kurulmaktadır. SNISCSG ise SILG'nin bir alt çalışma yapısı olarak 2003 yılında oluşturulmaktadır. Ağ ve bilgi güvenliğine odaklanan SNISCSG, bilgi güvenliği koruma sistemlerinin, yönetiminin ve operasyonunun teşvik edilmesi noktasında kolaylık sağlamaktadır. 2008'de dağılan SNISCSG, 2009'da yeniden kurulduğu söylenmektedir. Bürokratik gecikmeleri önleyen bu iki küçük çalışma grubu, strateji

belirleme süreçlerinde vakit kaybetmeden etkin kararlar alabilmektedir (Chang, 2014: 17).

Bunun yanı sıra bir diğer aktör olan Çin kökenli *telekomünikasyon, teknoloji ve bilgi teknolojisi (IT) şirketleri*, küresel boyutta faaliyet göstermektedir. Ayrıca cirolarından dolayı lider şirketler arasında yer almaktadır. Bu şirketlere verilebilecek en iyi örnekler; China Telecom, Lenova, China Unicom ve Huawei şeklinde belirtilmektedir. Yönetim kademeleri ve hissedarları ÇKP ve PLA olan bu şirketlerin bazılarının küresel faaliyetleri ÇHC ile olan bağlantıları dolayısıyla Batı dünyasında tartışılmakta ve çeşitli kısıtlamalara tabi tutulmaktadır. Çünkü şirketlerin ürün ve hizmetlerinin ÇHC tabanlı olmasından dolayı casusluk operasyonlarının kaynağı olabilmesi hususunda Batı dünyasında tehdit oluşturmaktadır (Darıcılı ve Özdal, 2018: 20).

ÇHC'nin siber güvenlik aktörleri kapsamında ele alınacak bir diğer yapı; 'Çin kökenli hacker grupları ve siber milisleri' şeklinde belirtilmektedir. Küresel ölçekte yapılan birçok siber saldırıyı gerçekleştiren hacker grupları siber uzayda bağımsız olarak faaliyet gösterdiği gibi ÇHC adına da faaliyet göstermektedir (Darıcılı, 2017: 16-18). Hacker gruplarının yapmış olduğu saldırı örnekleri çalışmanın ilerleyen kısımlarında farklı başlık altında detaylı bir şekilde ele alınmaktadır. Bununla birlikte genel olarak hacker grupları yapılacak olan siber operasyonlarda bir avantaj sağlasa da ÇHC bu durumu bu şekilde görmemektedir. Yani hacker gruplarını desteklediği takdirde bu grupların kontrolden çıkması durumunda kendilerine zarar vereceklerini düşünmektedir. Bu durumun ise yapılacak olan çeşitli muhalif hareketlerle ve düşman istihbarat ile iletişime girmeleriyle ÇKP'ye karşı olumsuz etkilerinin olacağı savunulmaktadır. ÇHC, hacker grupları tarafından yapılacak olan ve herhangi bir iç huzursuzluğa sebep olacak faaliyetler ya da manipülasyonlara yol açabilecek durumlardan dolayı endişe duymaktadır (Stevens, 2010).

ÇHC ile bağlantısı bulunmayan hacker grupları dışında ÇHC ile bağlantılı olan hacker grupları da bulunmaktadır. Yaklaşık 300.000 kişiden oluşan "*Red Hacker Alliance (Kızıl Hacker İttifakı)*" bu gruplara verilebilecek en önemli örnek olarak karşımıza çıkmaktadır. Sınırlı açık kaynak bilgisi bulunan bu grubun, açık kaynaklarda iddia edildiği gibi yurt dışında yapmış olduğu faaliyetler çerçevesinde sanayi ve teknoloji casusluğu adına yapılan operasyonlarından elde edilen önemli bilgileri ilgili ÇHC kurumlarına aktardığı söylenmektedir. ÇHC ile bağlantılı olan bu grup hükûmete

karşı memnuniyetsizlik yaşadığı durumlarda hükûmetin web sitelerini tahrif ederek bu memnuniyetsizliğe tepki göstermektedir. ÇHC hükûmeti ise bilgisayar korsanlarıyla iletişim kurmak ve yaşanan bu durumlarda faaliyetleri etkilemek ve durdurmak amacıyla çeşitli yollar geliştirmek zorunda kalmaktadır. Fakat belirlemiş olduğu yollarda kısmen başarı elde ettiği görülmektedir. Hükûmet ile grup arasında dengeleme problemi de yaşanmaktadır. Grup hükûmete karşı yaptıklarından dolayı olası bir hükûmet baskısından korkarken, hükûmette bu hacker gruplarının kışkırttığı olası bir isyana karşı endişe duymaktadır (Feakin, 2013: 4-5).

Diğer yandan internet kullanıcıları ve uzmanları arasında dünyanın en kalabalık internet topluluğuna sahip olan ÇHC'nin siber milis yapısının en birincil unsurunu bu uzmanlar oluşturmaktadır. ÇHC'nin siber milis yapısını oluşturan üyeler şu şekilde sıralanmaktadır:

- Bilişim, telekomünikasyon ve teknoloji alanlarında çalışan bilim insanları,
- Uzmanlar,
- Mühendisler,
- Ağ teknolojisine sahip vatandaşlar şeklinde sıralanmaktadır.

ÇKP ile doğrudan bağlantısı bulunmayan bu kişilerin yalnızca acil durum planlaması kapsamında ara sıra tatbikatlar yaparak ÇHC'ye yönelik gerçekleştirilecek siber saldırılara karşı eylem hatları hususunda eğitim aldıkları iddia edilmektedir. Orduyu sivil ile birleştirme fikrinin olduğu süreçlerde siber milisler sivil-askeri gelişmenin en açık ürünlerinden biri olarak görülmektedir. Milenyumun başında oluşmaya başlayan milisler, 10 milyondan fazla insanın kolektif üyeliğine dönüşmektedir (Lyll, 2018; Darıcılı ve Özdağ, 2018: 21).

ÇHC'nin siber güvenlik aktörlerinden askeri tarafta yer alan PLA ile ilgili detaylı bilgiler, ÇHC'nin siber güvenlik politikaları başlığı altında akış doğrultusunda gerekli yerlerde verilmektedir.

3.2.3. Çin ve Batı Dünyası Açısından Siber Güvenlik

Siber Güvenlik hususunu ÇHC ve Batı ekseninde siyasi boyutta ele almadan önce, terminoloji ekseninde incelemek gerekmektedir. Çünkü söz konusu terminoloji, ÇHC'de ve Batı'da farklı kullanılmaktadır. Bu durum küçük bir ayrıntı gibi görünse de aslında terminolojik eksenindeki farklılıklar ÇHC'nin ve Batı'nın siber güvenliğe yaklaşımının ilk adımı olarak değerlendirilebilmektedir. Yani bu küçük ayrıntıda dahi

ÇHC'nin kendine özgü duruşunun yine devreye girdiği görülmektedir. Akabinde ele alınan bu farklılığın ÇHC'nin siber güvenlik politikalarının daha iyi anlaşılması noktasında yardımcı olacağı düşünülmektedir.

Batı'da siber ve siber güvenlik kavramı bilinen hâliyle kullanılırken ÇHC bu kavramı yoğun olarak kullanmamaktadır. ÇHC'nin siber kavramı yerine “ağ” ya da “bilgi” kavramlarını kullandığı görülmektedir. Dolayısıyla siber güvenlik kavramı da ÇHC'de “ağ güvenliği” ya da “bilgi güvenliği” şeklinde ifade edilmektedir. Batı terminolojisinde siber güvenlik kavramı, “bilgisayarların, internet ağlarının, bilgi sistemlerinin ve süreçlerinin yazılımsal ve fiziksel güvenliği” şeklinde tanımlanırken, ÇHC siber güvenliğe karşılık gelen ağ/bilgi güvenliği kavramını, “bilgi sistemleri ve bilginin içeriği bilgi güvenliğinin ayrılmaz parçalarıdır” şeklinde ele almaktadır. Terminolojik açıdan bir diğer farklılık ise siber savaş kavramında görülmektedir. Batı'da siber savaş kavramı kullanırken, ÇHC'nin “bilgi savaşı” kavramını kullandığı belirtilmektedir. Bilgi savaşını bütünleşik ve ayrık bir disiplin olarak benimseyen ÇHC'nin aksine Batı, siber savaş daha küçük ve ayrı disiplinlere bölmektedir. ÇHC siber savaş ifadesini, sadece Batılı ülkeleri ve onların siber operasyonlarını anlatırken kullanmaktadır (Raud, 2016: 9-10, Köksoy, 2019: 345-346).

Terminolojik açıdan görülen bu farklı tanımlamaların anlamı bilindiği müddetçe, ÇHC ve Batı arasında yaşanan siber ilişkileri değerlendirmenin daha kolay olacağı düşünülmektedir. Fakat yine de farklı terminolojinin olması, ÇHC ve Batı arasındaki karmaşık olan işbirliğini geliştirmenin önündeki en zor engel olarak görülmemektedir. Bununla birlikte, ABD önderliğindeki pozisyonları benimseme hususunda isteksiz olan ÇHC, bireylere ve özel şirketlere alan tanıyan liberal bir ortam tercih eden Batı'nın tersine, siber uzayı hükûmet ve ordu aracılığıyla kontrol etmeyi tercih etmektedir (Raud, 2016: 10).

Öte yandan, teknolojinin ilerlemesiyle karşılaşılan tehdit ve riskler neticesinde siber güvenlik önlemleri alan ülkelerden biri de, dünyanın en hızlı büyüyen teknoloji devi ÇHC olmaktadır. Bu alanda yaşanan karışıklık ve zorluklarla baş etmek adına uygulamış olduğu politikalarla belirleyici rol üstlenen ÇHC'nin, siber güvenlik ile ilgili politikalarının özellikle uluslararası platforma genel anlamda kapalı olduğu ve kendine özgü farklılıkların olduğu gözlemlenmektedir. Bu durum Batılı ülkelerde ÇHC'ye karşı bir şüphe oluşmasına sebep olmaktadır. ÇHC'nin kendine özgü duruşu, biricik olma arzusu siber alanda belirlemiş olduğu politikalara da yansımaktadır. Her alanda olduğu

gibi bu alanda da lider olmak isteyen ÇHC'nin siber güvenlik politikaları, Batı ülkelerinin politikalarından ayrılan bazı hususları içermektedir. Bu doğrultuda bakıldığında, ÇHC kendi bilişim teknolojilerini geliştirme hususunda kararlı bir şekilde ilerlemektedir. Aynı zamanda bu sektörde yer alan lider ülkelerin ve şirketlerin üstünlüğünü kırmayı, kendisini uluslararası bilişim teknolojilerinden izole etmeyi ve ulusal egemenliğini siber güvenlik alanında geliştirmeyi hedefleyerek bu yönde ilerlemeyi kendisine yol bilmektedir. Siber güvenliğin, çağdaş dünyanın savaş aletlerinden biri olarak görüldüğü bu dönemde ÇHC'nin bu alana yönelik tutumunun; 'bağımsız bilişim teknolojisi olmadan siber güvenliğin, siber güvenlik olmadan da ulusal güvenliğin sağlanamayacağı' yönünde olduğu ifade edilmektedir (Gierow, 2014; Gierow, 2015: 1-2).

Başka bir yönden bakıldığında, Batı dünyası ve özellikle ABD'nin siber güvenlik alanında ÇHC'ye karşı suçlamalarda bulunduğu görülmektedir. ABD'ye yönelik yapılan siber saldırılarda ilk şüpheli olarak ÇHC'nin gösterilmesi ve bu yapılan siber saldırıların ÇHC tarafından gerçekleştirilmiş olması şüphesi sürekliliğini korumaktadır. ÇHC için sürekli olarak casusluk ve veri hırsızlığına dair iddialarda bulunulsa da bu iddialar gün yüzüne çıkarılamamaktadır. Bu duruma verilebilecek en iyi örnek; Çinli teknoloji şirketi olan Huawei ve ZTE eksenindeki siber saldırı iddiaları ve Gmail'in merkezine yönelik Çin kökenli hackerların siber saldırıda bulunduğu iddiaları verilebilmektedir (Watss, 2011; Cybermag, 2015). Huawei yayımlamış olduğu açıklamasında, ABD'li yetkililerin Huawei'nin kurum içi ağlara ve dâhili veri sistemlerine sızmak amacıyla siber saldırıda bulunduğunu iddia etse de Washington yönetimi bu iddianın tam aksi olan bir açıklama yapmaktadır. Bu açıklamada Washington yönetimi Çinli şirketlerin ahlaki değerlerini yok sayan davranışlar sergilediğini ve bu şirketlerin yönetimin işlerini bozduğunu ileri sürmektedir. Bu açıklamalara hiçbir kanıt göstermeden suçlamalarını sürdüren ABD, Huawei'nin ÇHC hükûmeti için ajanlık yaptığı fikrini ileri sürmektedir. Daha birçok ithamda bulunan ABD hükûmeti iddialarının kanıt olmamasına rağmen Huawei'ye yönelik yaptırım kararı aldığını açıklamaktadır. Hatta bu yaptırım kararlarını sadece kendisi uygulamakla kalmayıp Kanada, Avustralya ve Yeni Zelanda gibi Huawei'ye yaptırımlar uygulama yönünde adımlar atması amacıyla Avrupalı müttefiklerini ikna etmeye çalışmaktadır (Karaca, 2019).

Tüm bu anlatılanlarla beraber, küresel güçler arasında yıllardır farklı alanlarda gösterilen egemenlik mücadelelerin günümüzde siber alanda da gösterildiği gözlemlenmektedir. Siber alanın gelişmesiyle internet ortamında birtakım siber saldırı hareketlerinin yaşanması kaçınılmaz olmaktadır. Yaşanan bu siber saldırıların kaynağı her ne kadar somut olarak tespit edilemese de küresel güçler karşılıklı olarak birbirlerini suçlamakta ve çeşitli iddialar ortaya atmaktadır. Yukarıda da belirtildiği üzere bu suçlamaların hedefinde ÇHC bulunmaktadır. ÇHC'ye yönelik iddia edilen siber saldırılar ve ÇHC kaynaklı siber saldırılar farklı başlık altında ele alınmaktadır. Bundan dolayı genel çerçevede bu iddialara bakılacak olursa, ÇHC'ye yönelik suçlamalar yıllara göre şu şekilde sıralanmaktadır (Valentino ve Yadron, 2015; Köksoy, 2019: 347):

- 2009 yılında ÇHC'nin Google, diğer teknoloji şirketleri ve ABD'nin 'Ortak Saldırı' projesinin planlarına ilişkin veri hırsızlığı yapması,
- 2010 yılında İngiliz yöneticilerinin verilerine saldırı yapması,
- 2011 yılında Güney Kore internet portalına saldırı gerçekleştirmesi,
- 2013 yılında ABD kökenli medya şirketleri verilerini hacklemesi,
- 2015 yılında ABD personel yönetim sisteminin hacklenmesinden sorumlu tutulmaktadır.

Kanıtlanamayan suçlamalar dolayısıyla ÇHC birçok eleştiriye maruz kalmaktadır. Fakat tüm bu iddialar doğrultusunda ÇHC, yapılan siber saldırılar hususunda asıl mağdurun kendisi olduğunu sürekli dile getirmektedir. Siber güvenlik alanında aktif olmaya çalışan ÇHC, 2013 yılında siber istihbarat kurumu olan NSA'nın eski üyesi olan Edward Snowden'in, ABD istihbaratının ÇHC'de bulunan kişilerin ve kurumların telefon kayıtlarını ve internet kullanımını izlediğini ortaya çıkarmasıyla beraber bu alandaki aktifliğini daha fazla ön plana çıkarmaktadır (Richelson, 2013; Lindsay, 2015:7-8). ABD her ne kadar kendilerine yapılan siber saldırılarda ÇHC'yi suçlasa da Snowden'in sızdırdığı belgelerle beraber, ABD'nin ÇHC'ye karşı siber saldırı düzenlediği kamuoyuna açıkça duyurulmaktadır. Yapılan duyuru sonrasında ÇHC medyasının, "siber saldırıların kurbanı olarak uzun zamandır masummuş gibi tavır sergileyen ABD'nin, çağımızın en büyük kabadayısı olduğu ortaya çıkmıştır" sözleri oldukça dikkat çekmektedir (Singer ve Friedman, 2018: 190-191). ÇHC ve Batı dünyasının karşılıklı olarak birbirini suçlaması güven probleminin ortaya çıkmasına neden olmaktadır. Dijital altyapıların kötüleşmesiyle ilgili abartılı korkular ve bu

alandaki rekabet avantajına ilişkin artan endişeler güvensizlik sarmalını daha da şiddetlendirmektedir (Lindsay, 2015: 8).

Tüm anlatılanlar ekseninde genel anlamda ÇHC ve Batı dünyasının siber güvenlik ilişkisini değerlendirecek olursak; iki tarafında birbirine karşı söz konusu alandan dolayı şüpheli yaklaştığı görülmektedir. Bundan dolayı da çeşitli yaptırımlar uygulanmaktadır. Batı dünyasında ve özellikle ABD’de karşılaşılan herhangi bir siber saldırıda ÇHC hükûmeti suçlanmaktadır. Fakat tüm suçlamalara rağmen ÇHC bu durumu kabul etmemektedir. Aynı zamanda Batı dünyasına karşı şüpheli tutumundan dolayı Çin, herhangi bir siber saldırı girişiminde Batı dünyasını ve özellikle ABD’yi suçlamaktadır. Siber uzayın karışık yapısından dolayı saldırının kaynağı tespit edilememektedir. Bu durumda iki tarafın karşılıklı suçlamalarının süreceğinin göstergesi olarak karşımıza çıkmaktadır. Aynı zamanda ortaya atılan iddiaların siber uzayın öngörülebilir olmaması ve ÇHC’nin kapalı politikaları dolayısıyla ileride devam edeceği öngörülmektedir.

3.3. Çin Bağlamında Siber Saldırıları

Dünya’da internet kullanımının yaygınlaşmasıyla beraber ülkeler karşılaşılacak herhangi risk ve tehdide karşı önlemler olsa da yine de birçok siber saldırıyla karşı karşıya kalmaktadır. Siber uzayın öngörülmez ve karmaşık yapısından dolayı gerçekleştirilen saldırıların kaynağı bilinmemektedir. Bundan dolayı birçok devlet siber saldırının kaynağı olarak, düşman gördüğü diğer devleti suçlayarak çeşitli iddialarda bulunmaktadır. Bu çerçevede bakıldığında yukarıda belirtildiği üzere birçok devlet- özellikle ABD- karşılaştıkları herhangi bir siber saldırı durumunda siber güvenlik adına yapmış olduğu politikaları gizli tuttuğundan dolayı ÇHC’den şüphelenmektedir. Bu bağlamda, bu başlık altında ÇHC’ye yönelik yapılan siber saldırılar/iddialar ve sonrasında ÇHC’nin doğrudan yapmış olduğu siber saldırılar ele alınmaktadır.

Siber saldırı faaliyetlerini ele almadan önce siber saldırı kavramını hatırlamanın konunun anlaşılması noktasında faydalı olacağı düşünülmektedir. Bazı kaynaklarda elektronik savaş ya da bilgi savaşı olarak kullanılan siber saldırı kavramı; “bilgisayar sistemlerinin, teknolojiye bağımlı işletmelerin ve ağların kasıtlı olarak sömürülmesi” şeklinde ifade edilmektedir. Siber saldırıları gerçekleştirmek amacıyla bilgisayar kodunu, mantığı ya da verileri değiştirmek için zararlı yazılımlı kodlar kullanılmaktadır. Akabinde yapılan bu hamle ile veriler tehlikeye atılarak kimlik hırsızlığı gibi suçlara yol

açılabilir yıkıcı sonuçlar ortaya çıkmaktadır. Siber saldırılar; dolandırıcılık, kimlik sahtekârlığı, kimlik hırsızlığı, casus yazılım, yetkisiz erişim, virüsler, çalıntı donanım vs. gibi konuları kapsamaktadır (Techopedia, 2019).

1999 yılında ilk örnekleri görülen siber saldırılar internet kullanımının yaygınlaşmasıyla daha fazla artmaktadır. Bu bağlamda, Doğu Timor'un Endonezya'dan bağımsız olması için 19 Ocak 1999 yılında reklam kampanyası yapan <http://www.freedom.tp> adlı web sitesinin, Hollanda, Avusturalya, ABD ve Japonya dâhil olmak üzere 18 yerde bulunan bilgisayar korsanları tarafından siber saldırıya uğradığı görülmektedir. Site sunucusu Connect-Ireland'ın, savunması bozulduktan sonra siteyi kapatmaktan başka çaresi kalmamaktadır. Yapılan bu siber saldırı, bir hükûmet tarafından gerçekleştirilen ilk hacker saldırı olarak kabul edilmektedir. (Bellamy, 2001: 57).

Diğer yandan ÇHC'nin, her ne kadar gelişmiş istihbarat alt yapısı ve siber saldırı kapasitesi olsa da gerçek bilgi savaşı ve siber savaş yetenekleri bilinmemektedir. Siber boyutta güç ve üstünlük kazanma mücadelesi dolayısıyla ÇHC, 2050 yılına kadar "elektronik egemenliği" hedefleyen siber savaş doktrinini benimsemektedir. Bu doktrin, konvansiyonel askeri operasyonların öncesinde karşıt kuvvetlerin askeri, ekonomik ve sivil altyapıları ile iletişim kabiliyetlerini etkisiz hâle getirebilme hususunu içermektedir (Ventre, 2010; Schaap, 2009: 132). Olası bir siber savaş durumunda personel ve bilgi altyapısını güçlendirmek amacıyla bu alana büyük yatırımlar yapan ÇHC, siber saldırı kapasitesi yüksek birimler kurma ve bilişim altyapısını iyileştirme çalışmaları içine girmektedir (European Parliamentary Research Service, 2014: 5).

Bununla birlikte, Kasım 1999 yılında PLA'ya ait olan PLA Daily gazetesinde, ÇHC'nin siber saldırılarla karşılaşılması durumunda bazı hedeflerinin olduğu hususuna değinilmektedir. Gazetede, ÇHC'nin siber savaş kabiliyetinin hava, deniz ve kara gücü ile eşit öneme sahip olduğu ve ayrı bir kuvvet olarak değerlendirilmesi gerektiği vurgulanmaktadır. Aynı zamanda ÇHC'nin internetten kaynaklanan risk ve tehditlere karşı önlemler almak amacıyla gerekli yazılım teknolojilerini geliştirerek, herhangi bir tehdide karşı saldırılar ile cevap verebilme kabiliyetine sahip olabilmeyi hedeflediği belirtilmektedir. Bu bağlamda ÇHC, başta ABD olmak üzere tehdit ve risk unsuru olarak gördüğü ülkelerin ticari, askeri ve devlete ait ağlarına karşı siber saldırılarda bulunmak amacıyla detaylı planlamalar ve hazırlıklar yapmaktadır (Keith, 2007: 59).

Çalışmanın diğer kısımlarında da anlatıldığı üzere, 2011 yılında Genelkurmay bünyesinde bulunan PLA, ÇHC'nin askeri ağlarının kontrolünü sağlamak adına online bir "Mavi Ordu" kurduğunu açıklamaktadır. Batı medyası kurulan bu ordunun bilgisayar korsanı olduğundan şüphe duymaktadır. Mavi orduyla ilgili oluşan bu şüpheyi ortadan kaldırmak adına hem askeri uzman olan hem de PLA Ulusal Savunma Üniversitesi'nde bir profesör olan Zhang Shaozhong, Mavi Ordu'nun hackerlardan oluşmadığını belirtmektedir. Çoğu bilgisayar korsanı yasadışı ve uygunsuz şekilde faaliyet gösterirken Mavi Ordu'nun yasal yollarla oluşturulmuş bir birim olduğunu vurgulamaktadır. Bilgisayar korsanları bilgisayar virüsleriyle diğer bilgisayarlara gereksiz yere saldırmayı amaçlarken, Mavi Ordu ulusal internet güvenliğini korumayı hedeflemektedir (People's Daily, 2011). ÇHC'nin Mavi Ordu'yu oluşturmasının yanı sıra herhangi bir tehdit karşısında saldırıda bulunmak amacıyla siber savaş kabiliyetini geliştirmek adına yapmış olduğu bir diğer adım ise ordunun bünyesinde bulunan ve ÇHC'nin bilgi savaşı eğitiminin merkezi olan PLA Bilim ve Mühendislik Üniversitesi'ni kurmaktır. Akabinde PLA bünyesinde bilgi savaşı milis birlikleri oluşturulmaktadır. Bu birliklerin; üniversitelerden, askeriyelerden ve bilgi teknolojisi alanındaki özel şirketlerdeki kişilerin bir araya getirilmesiyle oluştuğu söylenmektedir (Carr, 2012: 257).

Bu doğrultuda ÇHC tarafından gerçekleştirildiği bilinen siber saldırılardan söz etmeden önce ÇHC'nin siber saldırılar yüzünden suçlandığı konulardan bahsetmekte fayda görülmektedir. Siber güvenlik hususunda ÇHC'nin Batı ile ilişkilerinin anlatıldığı başlıkta belirtildiği üzere, Batı ülkelerinin – özellikle ABD- siber saldırılar konusunda hedef olarak ÇHC'yi gösterdiği bilinmektedir. Fakat tüm suçlamalara rağmen ÇHC mağdurun kendisi olduğunu aynı zamanda kendisine yöneltilen siber saldırıların büyük çoğunluğunun ise ABD tarafından gerçekleştirildiğini ifade etmektedir. Bu iddialara rakamsal olarak bakıldığında doğruluk payının yüksek olduğu söylenebilmektedir. Bu hususta paylaşılan rakamlar ışığında, 10-19 milyon dolaylarında Çin bilgisayarının yabancı hackerlar tarafından yöneltildiği ileri sürülen botnetler içinde olduğu vurgulanmaktadır. ÇHC'nin lisanslı olmayan yazılım kullanması ve orijinal olan yazılımlarda bulunan güvenlik araçlarından faydalanmadığından bu saldırılara maruz kalması kaçınılmaz bir hâl almaktadır (Singer ve Friedman, 2018: 189-190). Aynı zamanda ABD her ne kadar bu saldırılarda ÇHC'yi hedef gösterse de Snowden olayıyla birçok gerçeğin gün yüzüne çıktığı görülmektedir.

Bu bağlamda belirtilen iddialar doğrultusunda ÇHC'yi işaret eden pek çok siber saldırı örneğinin olduğu tespit edilmektedir. Bunlardan birkaçı şu şekilde sıralanmaktadır:

- 2009 yılında ÇHC'nin, ABD savunma şirketi Lockheed Martin'in bilgisayarlarına eriştiği ve ABD ordusunun teknolojik olarak dünyanın en gelişmiş uçağı olan Joint Strike Fighter ile ilgili birçok veriyi topladığı iddia edilmektedir. Bunun yanı sıra yine 2009 yılında, ÇHC'nin talimatı doğrultusunda olduğu düşünülen bir kişinin, ABD'nin yeni F-35 için hazırlamış olduğu planlarını çaldığı öne sürülmektedir (Mount, 2009).
- Kasım 2012'de yapmış olduğu açıklama ile içecek devi olan Coca-Cola, 2009'da bir aydan fazla bir süredir siber saldırının kurbanı olduğunu söylemektedir. Sahte e-posta yoluyla yapılan bu saldırı, şirketin Çin Huiyuan Meyve Suyu Grubu'nu yaklaşık 2,4 milyar dolara satın almaya çalışırken gerçekleştirdiği görülmektedir. Bununla beraber devralmanın başarısız olduğu belirtilmektedir. Başarısız olunmasaydı, Çinli bir şirketin en büyük yabancı devralmasının olacağı vurgusu yapılmaktadır (BBC News, 2013).
- Google 2010 yılında yaptığı açıklama ile “Çin kaynaklı sofistike bir saldırıya” maruz kaldığını ifade etmektedir. Bu saldırıya uğrayanlar arasında bulunan insan hakları aktivistlerinin e-posta hesaplarının da ele geçirildiği belirtilmektedir. Söz konusu iddialar, Google ile ÇHC hükûmeti arasında sansür ve internet gizliliği hususunda tartışmaya sebebiyet vermektedir. Bu durumda Google'ın Çince dil operasyonlarını Hong Kong'a taşımasına neden olmaktadır. Haziran 2011'e gelindiğinde ise Google, ÇHC'nin Jinan eyaletinde bulunan bilgisayar korsanlarının yüzlerce üst düzey ABD yetkilisinin, askeri personelin ve gazetecinin kişisel e-posta hesaplarını ele geçirdiğini söylemektedir. Fakat ÇHC bu suçlamanın “kabul edilemez” olduğunu dile getirmektedir (BBC News, 2013).
- 2011 yılında, Amerikan bilgisayar güvenliği şirketi olan McAfee'nin hazırlamış olduğu raporla kamuoyunun haberdar olduğu Shady RAT saldırıları, Uluslararası Olimpiyat Komitesi, BM ve tanınmış birçok güvenlik şirketleri de dâhil olmak üzere beş yıl boyunca toplam 72 farklı

kuruluşu hedef alan ve ÇHC tarafından gerçekleştirildiği düşünülen dünyanın en geniş çaplı siber saldırı gerçekleştirilmektedir (Bates, 2011). Saldırıların 2006 yılında başladığını ve bu yılda yoğunluk gösterdiğini iddia eden McAfee, 2009-2010 yıllarında yavaşladığını belirtmektedir. 72 örgüt ve 14 ülkenin etkilendiği saldırıda, 72 örgütün 49 tanesinin ABD’de bulunduğu söylenmektedir. Böylesine geniş çaplı bir saldırıda dâhi saldırganların kimliklerinin tespit edilemediği vurgusu yapılmaktadır (Yener, 2015).

- NASA Uzay Ajansı 2011 yılında 47 siber saldırıya maruz kalmaktadır. IP adresi Çin’e kadar izlenen saldırıda NASA’nın uzaydaki robotlarını kontrol eden Jet Propulsion Laboratory’deki bilgisayarlara erişilmektedir. NASA, ABD Kongresi’ne bilgisayar korsanlarının hassas hesaplara erişim sağladığını, sistemleri ve hesapları oluşturabildiğini, silebildiğini ya da değiştirebildiğini ve bilgisayar korsanlığı yazılımı yükleyebileceğini yani bu hackerların ağlar üzerinde tam işlevsel kontrole sahip olduklarını söylemektedir (BBC News, 2013).
- ABD’nin önde gelen medya kuruluşlarından olan New York Times, 2012 yılının sonlarında ve 2013 yılının başlarında dört aylık bir süre boyunca Çin’de bulunan bilgisayar korsanlarının bilgisayar ağına ısrarla sızdığını söylemektedir. Times, yapılan saldırıların aynı üniversite bilgisayarları üzerinden yönlendirilmek de dâhil olmak üzere önceki Çin saldırılarının işaretlerini taşıdığının vurgusunu yapmaktadır (BBC News, 2013).

Tüm bunlara ek olarak yakın zamanda Avusturalya’ya düzenlenen siber saldırılarda da yine ÇHC sorumlu tutulmaktadır. Uzmanlar, Avusturalya Başbakanı Scott Morrison tarafından ortaya çıkarılan siber saldırılarda kullanılan aynı bilgisayar kodu ve taktiklerinden bazılarının Şubat 2019’da ÇHC’nin de suçlandığı Parlamento Binası’na yapılan saldırıda kullanıldığını söylemektedir. Aynı zamanda Morrison, ÇHC’nin adını doğrudan vermese de Avusturalya Stratejik Politika Enstitüsünün saldırıların yoğunluğu ve boyutu dolayısıyla ÇHC’den başlatılmış olma ihtimalinin % 95 ya da daha fazla olduğunu ifade etmektedir (The Guardian, 2020). Bu boyutta bir saldırı için gerekli olan kaynakların devlet destekli ya da büyük bir suç örgütü destekli olması gerektiği düşünülmektedir. ÇHC bu kapasiteye sahip bir ülke olduğu için saldırıların arkasında olduğu iddia edilmektedir. ÇHC dışında da bu kapasiteye sahip

devletler bulunmaktadır. Bu devletlerin Rusya, İngiltere, ABD gibi ülkeler olduğu belirtilmektedir. Bununla beraber, Avustralya Stratejik Politika Enstitüsü'nün Siber Politika Merkezi'nin kıdemli analisti Tom Uren, “ABD ve İngiltere’nin yeteneği var, ancak bunu yapacak motivasyonu yok” ifadelerini kullanmaktadır. Saldırıyı yapanın ÇHC olduğu düşünülse de kesin kanıt bulunmadan doğrudan bir ülkeyi suçlamanın doğru olmadığı ve bu suçlamanın çeşitli sonuçlar doğuracağı düşünülmektedir. Bu tip saldırılarda saldırganın bulunması zor olduğundan dolayı ülkeler doğrudan başka bir ülkeyi suçlamaktan kaçınmaktadır (Bogle, 2020).

ÇHC Dışişleri Bakanlığı Sözcüsü Zhao Lijian ÇHC’nin, Avustralyalı işletmelere ve sistemlere yönelik büyük bir siber güvenlik saldırısına karıştığı iddialarını “temelsiz” ve “saçma” ifadeleriyle reddetmektedir. Siber güvenliğin güvenilir destekçisi olduklarını belirten ÇHC, tüm iddiaların aksine siber saldırın en büyük kurbanının kendisi olduğunu sürekli dile getirmektedir (Financial Review, 2020). 2012 yılında belirtilen rakamlar doğrultusunda Savunma Bakanlığı web sitesi ve PLA askeri ağları ÇHC dışından başlatılan ayda yaklaşık 80.000 siber saldırıya maruz kaldığını belirten Siber Güvenlik Uzmanı Li Zhang, bu saldırıların özellikle ABD, Güney Kore ve Japonya’dan geldiğini ifade etmektedir (Zhang, 2012: 805).

ÇHC’nin siber saldırı yaptığı yönündeki bir diğer iddia ise ÇHC ve Hindistan arasında gerçekleşmektedir. ÇHC ve Hindistan aralarında yaşanan sınır sorunlarından dolayı siber uzayda da sürekli karşı karşıya gelmektedir. ÇHC’nin Hindistan’a yapmış olduğu siber saldırılarının arttığı yönündeki iddialar sonrasında Hindistan’ın Maharashtra Siber Güvenlik Departmanı 23 Haziran Salı günü, son 4-5 gün içinde altyapı, bilgi teknolojisi ve bankacılık ile ilgili sitelerde 40.000’den fazla şüpheli saldırıya tanık olduğunu belirten ve büyük bir kimlik avı saldırısı planlayan Çinli siber saldırganlarla ilgili uyarı yayımlamaktadır (Singh, 2020). Karşılaşılan bunca siber saldırı sonucunda Hindistan ÇHC’den tekrar gelebilecek olan siber saldırılardan dolayı tedirginlik yaşadığı için bu saldırılara karşı bir nevi nöbet tutmaktadır. Bu bağlamda karşılaşılan saldırılara tepki göstermek amacıyla Hindistan, ÇHC’ye ait 59 uygulamayı yasakladığını belirtmektedir (Sengupta ve Mankotia, 2020).

Yapılan siber saldırılarda saldırının nereden geldiği ve kim tarafından yapıldığı net olarak bilinmediği için bu durum büyük problem yaratmaktadır. Bilindiği durumlarda da ispat edilemediğinden dolayı doğrudan bir devlet suçlanamamaktadır. Örneğin, 2019 yılında APT10 adında Çin’in Devlet Güvenlik Bakanlığı adına hareket

ettiği düşünölen devlet destekli hacker grubunun Temmuz ayında ABD kamu hizmeti şirketlerini hedef alan siber saldırılar düzenlediğine yönelik suçlamalar olduđu söylenmektedir. Fakat ortaya atılan bu iddialar üzerine kanıt bulunmamaktadır. Daha önce benzer saldırılarda kullanılan taktikler doğrultusunda ÇHC suçlanmaktadır. Yani ortaya atılan iddialar ispatlanamadığı durumlarda önceden yapmış oldukları saldırıda kullandıkları taktikler göz önünde bulundurularak ya da düşman olması sebebiyle yapabileceğini düşündüğünden dolayı ölkeler birbirlerini muhtemel suçlu olarak görmektedir(Doffman, 2019; Dove, 2013).

Öte yandan, ÇHC'nin yaptığına yönelik iddia edilen siber saldırılar dışında doğrudan ÇHC tarafından gerçekleştirildiğı bilinen siber saldırılar da bulunmaktadır. Bu bağlamda ilk olarak ÇHC'nin siber saldırılarının ana hedeflerinden biri olan Tayvan hususunu ele almak gerekmektedir. Tayvan ve ÇHC arasındaki mesele, 1945-49 yıllarına dayanmaktadır. Bu dönemler arasında yaşanan iç savaş sonrasında Komünist Parti galip gelerek Çin Halk Cumhuriyeti'ni kurmaktadır. Akabinde galip olan Milliyetçi Parti ise Tayvan Adası'na kaçarak burada Çin Cumhuriyeti'ni ilan etmektedir. Çin'in temsilcisi olduğunu iddia eden iki rejim arasındaki kaos BM'nin oylama yapılarak aldığı 2758 no'lu kararla temsil hakkının Çin Cumhuriyeti yerine Çin Halk Cumhuriyetine verilmesiyle sonuçlanmaktadır. Alınan karar sonrasında ÇHC, Tayvan'ı "tek ölkö iki sistem" modeliyle yönetmek istemektedir. Aynı zamanda ilerleyen süreçle beraber barışçıl birleşimi hedeflemektedir. Fakat Tayvan bu duruma sıcak bakmayarak bunu reddetmektedir. Böylelikle ÇHC ve Tayvan arasındaki problemde günümüze kadar süregelmektedir (UN Resolution 2758, 1971; Pekcan, 2020: 216-217; Eroğlu, 2022: 67).

ÇHC ve Tayvan arasında yaşanan kaosa siber uzay boyutunda bakıldığında, ikisi arasında ilk siber savaşın 1999 yılında gerçekleştiğı görölmektedir. Tayvan'ın ÇHC'ye "devletlerarası ilişki" önermesiyle başlayan savaş sonrasında ÇHC Tayvan'ın kamusal sitelerine (hükümet, üniversite ve ticari siteler) saldırarak etkisiz hâle getirmektedir. Bu saldırıya benzer bir başka saldırı ise 2003 yılında yapılmaktadır. Çinli saldırganlar 30 Tayvan hükümet kuruluşuna siber saldırı düzenlediklerini ifade etmektedir. Bu kuruluşlar arasında Savunma Bakanlığı ve Ulusal Polis Merkezi gibi birimlerin de bulunduğu söylenmektedir (Spade, 2012: 4). Bu bağlamda, ÇHC ve Tayvan arasındaki gerginliğin siber dünyada devam ettiğı görölmektedir. İki rejim arasındaki gerginlik günümüze kadar devam etmektedir. 2022 yılında Tayvan Milli Savunma Bakanlığı

(MND), Çinli bilgisayar korsanlarının dezenformasyon oluşturmak amacıyla Tayvan'ın resmi kurum ve kuruluşlarına bir haftada 272 siber girişimde bulunduğunu duyurmaktadır (TGRT Haber, 2022). Tayvan Dışişleri Bakanlığı (MOFA) ise yaptığı açıklamada, ÇHC-Tayvan krizinde dakikada 170 milyon siber saldırıya uğradıklarını vurgulamaktadır. Aynı zamanda yapılan saldırıların asıl hedefinin Tayvan Dışişleri Bakanlığı olduğunu öğrendiklerini belirtmektedir (CNN Türk, 2022).

Bir başka yönden ise birinci sınıf araştırmacılar, analistler ve mühendislerden oluşan bir grup olan Cisco Talos, 2019 yılında Orta Tibet İdaresi (CTA) tarafından yönetilen bir posta listesini kullanarak kötü amaçlı bir Microsoft PowerPoint belgesi sunan yeni bir siber casusluk kampanyasını ortaya çıkardığını duyurmaktadır. CTA' nın web sitesinden (tibet.net) indirilen belgenin, “Tibet hiçbir zaman ÇHC'nin bir parçası olmadı” başlıklı meşru bir PDF dosyasının kopyası olduğu belirtilmektedir. Fakat indirilen bu dosya kötü amaçlı yazılım olan Uzaktan Erişim Truva Atı (Remote Access Trojan- RAT) içermektedir. E-posta, ExileRAT olarak anılan dosyaları dağıtmak amacıyla Tibet yanlısı grupları ve bireyleri hedef almaktadır. Yapılan bu saldırı, sistem ve kişisel verileri çalabilen, işlemi sonlandırabilen ya da başlatabilen ve aynı zamanda gözetim ve veri hırsızlığı yapabilen Android ve Windows tabanlı bir Truva Atı sunmaktadır. Bununla birlikte, Tibet topluluğunun 10 yıldan uzun bir süredir dijital casusluk operasyonları tarafından ısrarla hedef alındığı gözlemlenmektedir. CTA ve Tibet'teki Sivil Toplum Kuruluşları'nı (STK) hedef alan son siber casusluk girişi, ÇHC devlet destekli hackerlar tarafından gerçekleştirilen daha kapsamlı ve sofistike siber saldırıların sadece bir kısmını oluşturmaktadır. Yapılan bu saldırı girişimindeki amaç; öncelikle CTA'nın ağ sistemini giriş yapmak ve sonuç olarak faaliyetleri izlemek ve çeşitli sosyal mühendislik tekniklerini kullanarak bilgileri elde etmektir. Bu saldırı çalışmanın birinci bölümünde bahsedilen mızrak avı olarak bilinen saldırı türüyle gerçekleştirilmektedir. Son olarak belirtmek gerekir ki yapılan bu saldırının kaynağı belirlenemese de Tibetliler, bu kötü niyetli faaliyetlerin arkasında ÇHC hükûmetinin olduğuna inanmaya meyilli görünmektedir (Dalha, 2019). Bu bağlamda, Tibet bölgesinde yaşanan çatışmaların siber boyutunun yanı sıra Güney Çin Denizi'ndeki çatışmaların da siber boyutuna bakılması gerektiği düşünülmektedir. Bu noktada Filipinler ve ÇHC arasında yaşanan bir krizden söz edilebilmektedir. Filipinler Devlet Başkanı Rodrigo Duterte'nin Filipinler cephesi adına ÇHC'ye karşı net bir duruş sergilemesi beklenirken tam aksi olarak savaş veya yatıştırma arasında bir tutum

sergilediği görülmektedir. Buna rağmen ÇHC'nin Güney Çin Denizi'ne yaklaşımı, tek boyutlu ya da basitleştirilmiş stratejilere dayanmamaktadır. Kaynak açısından denizin tek taraflı denetimini sağlamak isteyen ve çevresini de güçlendirmek isteyen ÇHC, bu isteği doğrultusunda önemli ölçüde stratejik amaçlar gütmektedir. Belirlemiş olduğu stratejik amaçlarında siber saldırı olduğunu açıklamaktadır. Bu doğrultuda 2019 yılında EnSio adlı şirketin yayımladığı raporda, ÇHC'nin siber casusluk grubunun aynı yılın Nisan ayında Filipinler'deki iktidarı ve özel kuruluşları hedef alan iki zararlı yazılımı bölgede kullandığı saptanmaktadır. Birçok kez eş zamanlı olarak Filipinler'in çeşitli hükûmet web sitelerinin kaynak koduna eklenen Çince komut dosyalarının farklı sistemlerini ele geçirmeyi ve belirlemiş olduğu kullanıcılardan bilgi toplamayı amaçladığı tespit edilmektedir. Buna ek olarak, ÇHC, Güney Çin Denizi meselesinden bağımsız olarak Filipinler'e defalarca siber saldırılarda bulunduğu belirtilmektedir (Manantan, 2019).

Diğer taraftan ise 2014 yılında Hong Kong'daki ÇHC yönetimine karşı düzenlenen eylemlerde WhatsApp kullanan aktivistlerin telefonlarına protestoları rahatlıkla koordine edebilmelerini sağlayan bir program hakkında tanıtım mesajı ulaşmasıyla beraber bu tanıtım adresine, göstericilerin tıklaması sonucunda indirilen programın olasılıkla ÇHC hükûmeti tarafından geliştirilmiş olan ve kullanıcılarının telefonlarını hackleyen zararlı bir yazılım olduğu ortaya çıkmaktadır. San Francisco'da bulunan Lagoon Mobile Security şirketi, müşterilerinin ağlarında olağan dışı bir trafik gözlemlenmesiyle beraber bu sahte programı incelemeye almaktadır. Bu inceleme sonucunda ise Iphone'lardan bilgi çalabilen nadir rastlanan bir yazılım ile karşılaşilmektedir. Iphone'a yüklenen bu program, yüklendiği andan itibaren telefondaki rehber, arama kayıtları, mesajlaşma ve fotoğraflara ulaşabilmektedir. Ayrıca telefondaki kayıtları oynatma ve bilgileri başka bir adrese gönderme yeteneğine sahip olan bu program, Iphonelar'ın en hassas bölgelerinden birine uygulamalar, e-mail ve satın alma bilgilerinin bulunduğu anahtar dizinine erişebildiği tespit edilmektedir. Bununla birlikte, İOS ve Android'in zayıf noktalarının olduğu görülmektedir. Buna karşın İOS işletim sistemi ile çalışan telefonların hacklenmesi kolay değil fakat telefonlar Apple'ın koyduğu, ne tür uygulamaların çalıştırılacağına ilişkin, engelleri aşması amacıyla kırıldıysa, başka bir ifadeyle "jailbrake" sürecinden geçirildiyse hacklemenin mümkün olduğu vurgusu yapılmaktadır. Karşılaşılan bu zararlı yazılımlar

ile ilgili inceleme yapan Lagoon şirketi araştırmacıları, yazılımın ‘emir komuta’ sunucunun Çince yazıldığını gözlemlemektedir (Varlık, 2014).

Tespit edilen programla ilgili olarak şirketin CEO’su Michael Shaulov yaptığı açıklamada “ne İOS’u hedef alan böylesine sofistike bir şey ne de ÇHC izi taşıyan böyle bir şey görmemiştik” ifadelerini kullanmaktadır. Aynı zamanda Shaulov’a göre bu veriler hackerların ÇHC hükûmeti ile çalışıyor olabileceklerini işaret etmektedir. Tüm bu açıklamalara rağmen ÇHC Konsolosluğunun açıklama yapmadığı belirtilmektedir. Lagoon şirketi her ne kadar buna benzer zararlı yazılımla karşılaşmadık dese de Dallas merkezli siber istihbarat şirketi iSight Partners’tan Jhn Hultquist’e göre, program Çin istihbarat servisinin Tibetli aktivistlerin hedef alan casusluk yönetimlerine benzemektedir. 2013 yılında hackerların ÇHC’deki Uygur topluluğunun bir konferansa katılan üyelerine uygulama gibi görünen zararlı yazılım gönderdiği, programı kullananların konferansla ilgili bilgileri gördüğü ancak yazılım arka planda telefon kayıtlarını ve telefonun mikrofonu ile çevrede konuşulanları kaydettiği belirtilmektedir (Varlık, 2014).

Siber uzay hususunda ÇHC’nin dijital reformlar, geleceğe yönelik yatırımlar ve projeler dolayısıyla uluslararası alana açılan bir devlet olduğu görülmektedir. Bu doğrultuda bakıldığında ÇHC’nin küresel sistemde zıt kutbu olan ABD ile rekabet içine girmesi kaçınılmaz olmaktadır. Tıpkı diğer Batı ülkeleri gibi ABD’de ÇHC’yi ekonomik, siyasal ve teknolojik olarak önemli bir tehdit olarak algılamaktadır. ABD’nin en büyük endişelerinden biri de ÇHC’nin teknolojik altyapılarını hangi amaçla kullandığı yönünde oluşmaktadır (Eroğlu, 2022:67). Çalışmanın farklı başlığı altında ABD’nin birçok siber saldırıda ÇHC’den şüphelenmesinden söz edilmektedir. Aynı zamanda Snowden olayıyla bazı iddiaların boşa çıktığına da dikkat çekilmektedir. Bunlar dışında ÇHC’nin doğrudan ABD’ye yönelik gerçekleştirdiği bilinen siber saldırılarda bulunmaktadır. Kısaca bunlara da değinmek gerekmektedir.

2013 yılında ABD kökenli siber güvenlik şirketi olan Mandiant bir APT raporu yayımlamaktadır. Bu raporda, ÇHC kontrolünde bir siber saldırı birliği olduğundan söz edilmektedir. Aynı zamanda raporda, birliğin konumu ve kurumsal yapısı gibi spesifik bilgilerde yer almaktadır. Raporda belirtilen konumun PLA merkezine ciddi ölçüde yakın bir bölgede olması oldukça dikkat çekmektedir. Bu konum Şangay ilinin Pudong bölgesinde bulunmaktadır. 12 katlı bu binada tahmini olarak bini aşkın personel çalışmaktadır (Mandiant, 2013). ÇHC’nin bu hacker birliğine devlet elinden destek

verildiği raporda belirtilse de ÇHC bu iddiaları reddetmektedir. Bununla beraber, rapordan yaklaşık iki ay sonra (16 Nisan 2013) ÇHC Beyaz Kitap yayımlamaktadır. Bu kitapta Çin Silahlı Kuvvetleri'nin deniz, kara, hava birliğinin tüm asker ve personel sayıları verilmektedir. Daima askeri alanda gizliliğini sürdüren ÇHC, yayımladığı beyaz kitapta bu sayıları açıklayarak şeffaf ve savunmasız bir ordunun olduğunu göstermeye çalışmaktadır (Kara, 2013: 66-67). ABD, ÇHC'yi kendisine güçlü bir tehdit olarak görmesine karşın yakın temas kurarak ÇHC ile ortak çalışmalar yürütmek istemektedir. ÇHC'nin, ABD'ye karşı tutumunda kendi dış politikalarından ödün vermediği görülmektedir. Fakat bu noktada dikkat çeken asıl mesele ABD'nin ÇHC'ye karşı verdiği tavizler olmaktadır. ÇHC ve güçlü tehdit olarak görülen ülkelerin ne kadar caydırıcı bir güç olduğu bu örnekten hareketle net bir biçimde anlaşılmaktadır (Cilluffo, 2013: 4-8).

2015 yılında ABD ve ÇHC arasında yaşanan ekonomik casusluk hususuyla ilgili yapılan bir anlaşmanın olduğu gözlemlenmektedir. Bu anlaşmada, siber uzay yönetimine ve faaliyetlerine yönelik farklı yaklaşımlar bulunmaktadır. Anlaşma belirli bir noktaya kadar ABD ve ÇHC'nin yaklaşımlarını ortaya koymaktadır. ABD ve ÇHC'nin siber uzay yaklaşımına genel olarak bakıldığında ise şunların ortaya çıktığı tespit edilmektedir (Brown ve Yung, 2017);

- Siber uzayda bir ülkenin kendi kaderini kendisinin belirlemesi gerektiğine önem veren ABD, uluslararası etkileşimlerde bu özgürlükleri artırmaya yönelik hedefler belirlemektedir. Aynı zamanda internet üzerinden serbest bilgi akışının stratejik ve diplomatik başarının anahtarı olduğuna inanmaktadır.
- Ekonomik rekabeti ABD ile ilişki kurmanın bir yolu olarak gören ÇHC ise, siber uzayı ABD ile rekabet etmek amacıyla başarı ile kullanabileceği asimetrik bir araç olarak görmektedir. Aynı zamanda içeriden ya da dışarıdan gelecek fikirler için sürekli olarak duyarlı olmaya gayret göstermektedir.

ABD ve ÇHC bu anlaşmada, uluslararası toplum içinde siber uzayda uygun devlet davranışı normlarını belirleme, geliştirme ve teşvik etme hususunda siber suçlarla alakalı problemlerle mücadelede üst düzey bir ortak diyalog bağlantısı kurmaya karar vermektedir. Her ne kadar ortak bir karar söz konusu olsa da ABD'de ÇHC'nin anlaşmaya uyup uymayacağı noktasında şüpheleri olduğu görülmektedir. Sonuç olarak,

Xi Jinping'in ÇHC hükûmetinin özel şirketlere rekabet avantajı sağlamak amacıyla siber özellikli fikri mülkiyet hırsızlığına girmemesini ya da bilerek desteklememesini sağlama anlaşması, bu anlaşmanın üzerine duyulan şüpheleri haklı çıkarmaktadır (Brown ve Yung, 2017).

Bu anlatılanların yanı sıra, ÇHC'nin siber uzay noktasında ABD'den farklı bir yol izlediği hatta birçok ülkeden farklı bir yol izlediği bilinmektedir. ÇHC, gizlilik ve iletişim hakları, siber politikalarının geliştirilmesinde önemli bir rol oynamaktadır. Siber egemenliğin önemini sürekli olarak vurgulayan ÇHC, Aralık 2015 yılında Xi Jinping'in Dünya İnternet Konferansı'nda devletlerin kendi ülkelerinde siber uzay için kendi kurallarını belirlemesine izin verilmesini istemektedir. Bu doğrultuda hareket eden ÇHC hükûmetinin 2017 yılında Siber Güvenlik Yasası'nı çıkardığı bilinmektedir. Bu yasayla beraber ÇHC, internet güvenliğini sağlamanın yanı sıra birde bilgi, iletişim ve bilgisayar güvenliğini artırıcı önlemler almaktadır (Zhao ve Xia, 2018). ÇHC ve hükûmet gözetimini artırmak isteyen bazı Asya ülkeleri, bilgi güvenliğini sağlamak adına uluslararası davranış kurallarını savunmaktadır. Davranış kurallarını yararlı gören devletler, bu görüşe göre siber uzayda davranışı yönlendiren uluslararası normlar ve kurallar belirlemeye çalışmaktadır. Bu doğrultuda Brown ve Yung'a göre siber uzayın ulus-ötesi ve özerk doğası, ekonomik ve sosyal kalkınmanın yanı sıra uluslararası güvenliğe de meydan okumaktadır (Eroğlu, 2022: 68).

ÇHC ve ABD'nin siber uzay yaklaşımına kısaca değindikten sonra yeniden siber saldırılara dönülecek olursak, 2015 yılında ÇHC'nin ABD'ye yönelik gerçekleştiği siber girişimin karşımıza çıktığı görülmektedir. Bu kez ÇHC'nin hedefi, kendi ülkesindeki internette uyguladığı kısıtlamaların aşılmasına yardımcı olan bir Amerikan şirketi olmaktadır. DDoS saldırısının bu sefer daha farklı bir şekilde gerçekleştirildiği bu saldırıda, Amerikan Federal Soruşturma Bürosu'nun (FBI) şirketlere göndermiş olduğu uyarı mesajında ÇHC'den gelen saldırıların "man-in-the-middle"⁶ yöntemi ile gerçekleştirildiği belirtilmektedir. FBI mesajına göre; "ABD hükûmetinin değerlendirmesine göre, Çin dışına giden internet trafiğinin bir yerde kesilerek kullanıcıların, ABD merkezli sitelere istek göndermeleri sağlanıyor. Çin'in internet

⁶ Man-in-the-middle saldırısı: Türkçedeki karşılı 'ortadaki adam' olan bu saldırı türünde, saldırganın birbiri ile doğrudan iletişim kuran iki taraf arasındaki iletişimi gizlice lettiği ya da değiştirdiği görülmektedir. Yani bu saldırı türünde kullanıcıların bilgisayarlarına bulaştırılan küçük program aracılığıyla hedefteki sitelere birçok talep gönderilmesini sağlamak fakat kullanıcıların bu işlemlerden haberi olmamaktadır.

ağından kaynaklanan bu kasıtlı hareket, ABD merkezli internet sitelerinin hizmetlerinde aksamaya yol açtı” denilmektedir. Yapılan bu internet faaliyetlerinin, Çin Unicom ve Çin Telekom siteleri kaynaklı olarak görüldüğü belirtilmektedir. Aynı zamanda FBI, bu iki devlete ait şirketlerden kaynaklanan saldırıların Pekin’in bu işin arkasında olduğunu gösterdiğine dikkat çekmektedir. Her ne kadar güvenlik uzmanları, ÇHC’nin Google’u olarak bilinen Baidu’nun bu saldırılarda anahtar rol oynadığını vurgulasa da Baidu bu iddiaları reddetmektedir (Varlık, 2015).

Bunlara ek olarak, 2019 yılının sonlarına doğru ÇHC’nin Wuhan şehrindeki bir yabani hayvan pazarında baş göstermeye başlayan ve Covid-19 olarak adlandırılan virüsün tüm dünyayı etkisi altına aldığı bilinmektedir. Kısa süre sonra salgının hızlı bir şekilde yayılmasıyla beraber DSÖ tarafından pandemi/küresel salgın ilan edilmektedir. Haziran 2020 itibariyle ise salgından dolayı tüm dünyada toplam 9.228.526 kişinin korona virüse yakalandığı ve toplamda 475.123 kişinin ise virüsten dolayı hayatını kaybettiği kayıtlara geçmektedir (Worldometer, 2020). Böylesine büyük etki yaratan Covid-19 salgını, siber saldırıda yeni hedeflerin de ortaya çıkmasına sebep olmaktadır. Bu doğrultuda örnek verilecek olursa; Güney Koreli bilgisayar korsanlarının DTÖ’yü, Kuzey Kore’nin ise Japonya ve ABD’deki yetkilileri hedef aldığı belirtilmektedir (Sanger ve Perlroth, 2020).

Bu bağlamda, Covid-19 salgınıyla beraber ABD-ÇHC arasında hem yeni gerginlik hem de yeni siber saldırı iddiaları gündeme gelmektedir. Virüsün yayılım oranındaki artışın giderek yükselmesi ve henüz bir aşı bulunamamış olması, devletlerin virüs hususunda diğer devletlerden bilgi çalmak amacıyla siber saldırıları artırdığı görülmektedir. Karşılıklı olarak yapılan suçlamalarda, ABD Güvenlik ve İstihbarat Servisleri tarafından ÇHC’nin korona virüs için aşı çalışmalarının yapıldığı laboratuvarlara siber saldırı düzenleyip önemli bilgileri çalmaya çalıştığı duyurulmaktadır. Bu durumla alakalı olarak FBI ve ABD Siber Güvenlik Teşkilatı açıklama yaparak, Çin destekli bilgisayar korsanlarının gerçekleştirdiği siber saldırıların soruşturulduğunu belirtmektedir. Akabinde FBI ve ABD Siber Güvenlik Teşkilatı’nın bazı ilaç firmalarının da siber saldırıların hedefi olduğunu iddia ederek bu firmalara gerekli önlemleri almaları hakkında uyarılarda bulunduğu söylenmektedir. Koronavirüs vakalarında ABD, ÇHC’ye oranla kat ve kat artışla karşı karşıya kalmaktadır. Bununla beraber Trump yönetimi, ÇHC’yi birçok kez koronavirüs salgınının kaynağı hususunda

şeffaf olmamakla suçlasa da ÇHC'nin iddiaları reddettiği ifade edilmektedir (BBC News Türkçe, 2020).

Bir başka yönden ise 2020 yılında ABD'nin siber güvenlik uzmanları, FireEye'in hazırlamış olduğu bir raporda şüpheli Çinli hacker grupların siber saldırılarında ciddi oranda artış olduğunu tespit ettiklerini belirtmektedir. Birçok müşterinin hedef alındığı APT41 adı verilen bu bilgisayar hacker grupları, medya şirketleri ve kâr amacı gütmeyen kuruluşlara siber saldırılar gerçekleştirmektedir. Hazırlanan bu raporda, “son yıllarda gözlemlenen Çinli siber casuslar tarafından gerçekleştirilen en geniş çaplı siber saldırı” söylemi saldırıların şiddetini yansıtmaktadır. Ayrıca raporda, APT41'in ABD, İngiltere, Kanada ve Meksika'daki firma ağlarına girmeye çalıştığını ve bu ülkelerdeki yazılım eksikliklerini kötüye kullandığı belirtilmektedir. Bu tarz şikayetler ÇHC tarafından da meydana gelmektedir. 2020 yılının Mart ayında Çinli güvenlik şirketi Qihoo 360, havacılık, petrol ve gaz ve teknoloji de dâhil olmak üzere bir dizi Çin endüstrisini hedef alan “CIA hack grubu (APT-C-39)” tarafından 11 yıl boyunca saldırılar gerçekleştirileceği iddia edilmektedir. Söz konusu raporda, “CIA tarafından sivil havacılığın saldırıya uğrayan bilgi teknolojisi sektörlerinin sadece Çin'de değil, aynı zamanda diğer ulus devletlerde yüzlerce ticari havayolunu da kapsadığı” vurgusu yapılmaktadır. ABD'nin bu iddiaları reddetme olasılığı düşünüldüğünden raporda, hackerların CIA ile bağlantılı olduklarına dair sayısız kanıt olduğuna dair ifadeler yer almaktadır (Doffman, 2020).

Son olarak ise siber saldırıları ekonomik açıdan ele alacak olursak; yapılan saldırılar başarılı olsun ya da olmasın söz konusu saldırıların oldukça maliyetli olduğu belirtilmektedir. Çünkü saldırı sonrasında sistemi yeniden kullanılabilir hâle getirmek günler, bazen haftalar sürmektedir. ABD Savunma Bakanlığı sadece 2011 yılında siber saldırılardan dolayı 20 milyon dolar harcadığını ifade etmektedir (Dove, 2013). Siber güvenliğin geliştirilmek zorunda olduğu bu dönemde birçok devlet bu alanda yapmış olduğu iyileştirmelerden dolayı büyük bütçeler ayırmaktadır. ABD'nin 2017'de 13,75 milyar dolar olan siber güvenlik bütçesinin 2020 yılında 18,79 milyar dolara çıktığı görülmektedir (Statista, 2020). Bununla beraber, siber güvenlik harcamalarında artış isteyen ABD Başkanı Joe Biden 2024 mali yılı için bütçe teklifinde bulunmaktadır. ABD hükûmetinin siber güvenlik direncini artırmak ve ABD'nin dijital savunmasını güçlendirmek için hükûmetin bütünsel bir yaklaşımını gerektiren yakın zamanda

yayımlanan siber stratejisini uygulamak amacıyla geniş kapsamlı yatırımlar çağrısında bulunduğu tespit edilmektedir (Vasquez, 2023).

ÇHC'nin siber güvenlik harcamasının ise 2019 yılında 7,35 milyar dolar olduğu görülmektedir (Xinhua News, 2019). 2021 yılında küresel pazar araştırma şirketi olan International Data Corporation (IDC) tarafından yayımlanan sektör raporuna göre, ÇHC'nin siber güvenlik pazarına yapılan yatırımın 2021 yılında 9,78 milyar dolara, 2025 yılında ise 18,79 milyar dolara ulaşması beklenmektedir. Yayımlanan rapora göre, ülkenin siber güvenliğe yönelik harcamalarının yaklaşık yüzde 47,8'i donanım sektörüne giderken, 2021-2025 döneminde yazılım sektöründe güçlü bir büyüme yaşanacağı düşünülmektedir. Rapor, siber güvenliğe yapılan harcamalardaki yüksek artışı, ülkenin giderek artan siber güvenlik tehditleri ile karşı karşıya kalmasına bağlamaktadır. Raporda ayrıca, artan taleple birlikte ülkenin siber güvenlik sektöründe büyük bir kalkınma yaşanacağı da belirtilmektedir (Kumtepe, 2021).

2022 yılında IDC'nin yayımlamış olduğu yeni raporda, ÇHC'nin siber güvenliğe yaptığı yatırımın beş yıl içinde neredeyse üç katına çıkacağı ve ülkenin dijital ekonomisiyle birlikte hızla büyüyeceği söylenmektedir. Kasım 2022'de yayımlanan rapora göre, "ÇHC'nin siber güvenlik harcamaları, geçen yıl 31,9 milyar ABD dolarına kıyasla 2026 yılına kadar 12,2 milyar ABD dolarına ulaşacak. 4,7 milyar ABD doları donanım, 4,2 milyar ABD doları yazılım ve 3,2 milyar ABD doları güvenlik hizmetlerine gidecek" şeklinde belirtilmektedir. IDC Çin siber güvenlik analisti Wang Yiting, ÇHC'nin son yıllarda siber güvenlik düzenleme sistemini geliştirdiğini ve kurumsal gelişim ihtiyaçlarının artmaya devam ettiğini, aynı zamanda siber güvenlik pazarının pandemi ve jeopolitik sorunların etkisine rağmen istikrarlı bir büyüme sürdürmesini sağladığını söylemektedir. Wang sözlerine, "siber güvenlik endüstrisindeki şirketlerin yazılım ve hizmetlerin eğilimini kavramaları ve ürün ve hizmet yeteneklerini geliştirmeye devam etmeleri gerektiğini" de eklemektedir. Son olarak IDC raporunda, ÇHC'nin siber güvenlik harcamalarının beş yıl içinde neredeyse üç katına çıkacağının vurgusunu yapmaktadır (YICAI, 2022).

SONUÇ

1990'lı yıllar itibariyle bilişim teknolojilerinde öngörülmez bir gelişim ve dönüşüm gerçekleşmektedir. Günümüz dünyasında söz konusu bu gelişim hız kesmeden devam etmektedir. Mevzubahis gelişimin sonucunda siber uzayın önem kazanmasıyla beraber, olumlu değişimlerin ve dönüşümlerin yaşanmasının yanı sıra birtakım risk ve tehditlerle de karşılaşıldığı görülmektedir. Karşılaşılan risk ve tehditler, devletler açısından endişeye sebep olmaktadır. Nitekim bilişim teknolojilerinin gelişimi arttıkça karşılaşılan risk ve tehditlerin bıraktığı hasarın boyutu da artmaktadır. Bu noktada devletler nezdinde 'siber güvenlik' hususunun ön plana çıktığı görülmektedir. Ulusal güvenliklerini korumak adına bazı önlemler alan devletler, karşılaşılan risk ve tehditleri ortadan kaldırmanın yanı sıra siber alanda egemen olma, lider olma gibi hedefler doğrultusunda siber güvenlik politikaları geliştirmeye çalışmaktadır.

Oldukça karışık bir doğaya sahip olan siber uzayda yaşanan belirsizlik, devamlılığını korumaktadır. Siber alanın karışık ve belirsiz yapısı dolayısıyla karşılaşılan tehdidin nereden ve hangi kaynaktan geldiğini belirleme noktasında zorluklar yaşanmaktadır. Bu durum ciddi güvenlik sorunlarına sebep olmaktadır. Siber uzayın yapısından dolayı karşılaşılan bu zorluk neticesinde devletler, mevzubahis konu ile ilgili politikalarını geliştirmek ve güncellemek zorunluluğu içinde kalmaktadır. Bununla beraber başta askeri amaçla kullanılan internetin günümüzde; iletişim, eğitim, sağlık, medya, ticaret, siyaset, bilim vs. gibi her alanda farklı amaçlarla kullanıldığı görülmektedir. Hemen hemen her şeyin internetle bağlantılı olduğu ve internet aracılığıyla gerçekleştirildiği bir dönemde yaşıyor olmamız, devletlerin siber güvenliğin sağlanmasına ilişkin endişelerinin ve bu alanda karşılaşılan tehditlerin kaynağı hususundaki belirsizliğin artması ve kaynağı bulma noktasındaki zorluğun yaşanması durumunu bir kez daha kanıtlamaktadır.

1949 yılında ÇHC'nin kurulmasına önderlik eden Mao Zedong'un 1976 yılında hayatını kaybetmesinin ardından 1978 yılında Deng Xiaoping başa geldiği görülmektedir. Mao döneminde içe dönük bir dış politika izlenmektedir. Ekonomik anlamda izolasyon döneminin yaşandığı Mao döneminden sonra Deng'in başa gelmesiyle beraber, ÇHC'de dışa açık ve ekonomi odaklı politikalar takip edilmektedir. Bu doğrultuda reform programı başlatan Deng, bu program sayesinde ÇHC'nin ekonomik anlamda dışa açılımını sağlamaktadır. Yapılan çalışmalar doğrultusunda Deng döneminde ekonomide hızlı bir yükseliş gözlemlenmektedir. Hedeflenen

ekonomik büyümenin gerçekleşmesiyle beraber 1980’li yıllara gelindiğinde ise ÇHC internet ve bilgisayar teknolojilerini keşfetmeye başlamıştır. Nitekim çalışmanın üçüncü bölümünde de değinildiği üzere 1986-1987 yılları ÇHC’nin internet açısından dönüm noktasını teşkil etmektedir.

Zamanla internet teknolojilerini geliştirme yoluna giden ÇHC, mevzubahis alana daha fazla bütçe ayırma yoluna gitmiş ve aynı zamanda gelişimi açısından avantaj sağlayacağını düşündüğü için ulusal ağlar oluşturmaya başlamıştır. ÇHC diğer gelişmiş ülkelere göre internetle geç tanışsa da, internetin gelişimi ve büyümesi noktasında Pekin’in büyük katkısı bulunmaktadır. Günümüzde dünyadaki internet kullanıcısının neredeyse 2 milyonunu oluşturan ÇHC, 1999 yılında bilgi teknolojilerine daha fazla önem vermesine neden olan iki önemli olay yaşamıştır. Bu olaylar; Falun Gong protestoları ve ABD’nin Belgrad’daki Çin Büyükelçiliğini bombalamasıdır. Söz konusu olaylar sonrasında ÇHC, internet ve bilgisayar teknolojilerinin önemini daha fazla kavradığından dolayı, bu alanın gelişimi için çalışmalar başlatmaktadır. 2000’li yıllara gelindiğinde yaşanan birçok gelişme sonucunda internet teknolojilerinin gelişmesi ve kontrolünü sağlama noktasında ÇHC’nin birçok girişiminin olduğu görülmektedir.

Siber güvenlik ile ilgili olarak BM’ye bazı tasarılar sunan ÇHC’yi Batılı ülkelerden ayıran en önemli nokta ise “siber egemenlik” olgusundan kaynaklanmaktadır. ÇHC’nin sunduğu tasarılar da yer alan maddede, devletlerin internet konusunda istedikleri gibi sansür uygulayabilecekleri vurgusu yapılmaktadır. İnternet egemenliği ya da internet yönetimi devlete bağlı olan ÇHC’nin mevzubahis alanda uygulamış olduğu politikalara bakıldığında, internet hususunda özgür erişimi kısıtlayacak sansürler uyguladığı görülmektedir. CERNET, ChinaNET, ChinaGBN gibi ulusal ağları oluşturmaya başlayan ÇHC; Google, Facebook, YouTube ya da Newyork Times gibi web sitelerine erişimi yasaklayarak internet egemenliğine ket vurmaktadır. ÇHC her ne kadar sosyal medya araçlarına alternatif olarak farklı platformlar oluştursa da vatandaşların kendi kimlik bilgilerini kullanarak girmiş oldukları ilgili platformlarda sıkı denetimler yapmaktadır. Yapılan bu denetim dolayısıyla devlet her siteye, her kullanıcıya ve internette yer alan bilgilere kolaylıkla erişmektedir. Başta Hong Kong ve Tayvan gibi bölgeler açısından soruna sebep olan bu durumdan dolayı, ÇHC’nin söz konusu tutumunun insan haklarına ters düştüğü ve insan haklarını ihlal ettiği düşüncesiyle BM’ye sunduğu tasarılar çoğunluk tarafından kabul görmemektedir.

Siber güvenlik olmadan ulusal güvenliğin olamayacağını vurgulayan ÇHC hükûmeti, bu alana verdiği önemi söz konusu perspektifiyle bir kez daha göstermektedir. Bu bağlamda ÇHC mevcut siber güvenliği geliştirme noktasında ülkede bulunan en iyi üniversiteler ile siber alanda düzenli bir şekilde AR-GE faaliyetleri yürütmektedir. Bunun yanı sıra ordu yönünden güçlü olan ÇHC, teknoloji yönündeki gücünü de kullanarak; siber savaş, uzay silahları ve elektronik savaş hususunda ilgili personele bu alanda eğitimler vererek, karşılaşılan risk ve tehditler bağlamında avantajlı taraf konumuna gelme yolundaki çalışmalarını ilerletmektedir. Daima tek olma ve lider olma arzusu içinde olan ÇHC, hem siber güvenlik açısından hem de siber savaş alanında dünyanın en etkili gücü olmayı hedeflemektedir. Bundan dolayı da orduya, düşmanın bilişim teknolojilerine hasar verilmesi noktasında siber savaş üzerine eğitimler de verilmektedir.

Tez çalışmasında ortaya konan veriler ışığında birtakım bulgulara ulaşılmıştır. Bu bulgular arasında en önemli olan husus, ÇHC'nin siber güvenlik politikalarını belirlerken ulusal güvenlikle siber güvenliği eş değer görmesidir. Bundan dolayı siber güvenlik ile ilgili atılan adımlarda ulusal güvenlik değerleri göz önünde bulundurularak hareket edildiği gözlemlenmektedir. Geleneksel güvenlik anlayışından doğan siber güvenlik kavramı son zamanlarda yeni güvenlik yaklaşımı olarak görüldüğünden, popüler bir konu hâline gelmektedir. Dünya gündeminde böylesine ön plana çıkan ve popüleritesi artan bir kavram olan siber güvenliğin sağlanması konusunda birçok devlet politikalar takip etmekte ve özellikle karşılaşılabilecek risk ve tehditlere karşı önlemler almaktadır. Bu noktada ÇHC'nin diğer ülkelerden farklı olarak kendine has bir yol izlediği görülmektedir.

ÇHC genel anlamda siber güvenlik politikalarını belirlerken askeri, ekonomik ve siyasi yönden gelişmeyi hedefleyecek yollar aramaktadır. Aynı zamanda mevzu bahis alanda en etkili siber güce sahip olma hedefi doğrultusunda ilerlemektedir. Bu çerçevede yapılan düzenlemeler, yasalar ve politikalarda ortaya konan temel nokta, ÇHC'ye özgü adımlar atarak hareket edilmesi olmaktadır. Bu doğrultuda ilerleyen ÇHC hükûmetinin diğer ülkelerden farklı olarak siber bağımsızlık elde etmeye çalıştığı ve uluslararası sistemdeki mevcut bilişim teknolojilerinden izole olacak şekilde; kendi ulusal siber ağlarını/yazılımlarını kullanarak, kendi bilgi teknolojilerini geliştirerek, ulusal ve uluslararası sistemde yasaklı kabul edilen veri akışını engelleyerek, kendi ağları dışında diğer ağları yasaklayıp sansürler uygulayarak ya da birtakım

sınırlandırmalar getirerek ve onların yerine milli alternatifleri üreterek bu alternatiflerin kullanılmasıyla beraber güçlü bir savunma mekanizması geliştirdiği gözlemlenmektedir.

ÇHC'nin siber güvenlik hususuyla ilgili sergilemiş olduğu tutum her ne kadar eleştirilse de karşıt görüşlere kapalı bir şekilde bu alana ilişkin sert kurallar/denetimler uyguladığı görülmektedir. Öte yandan, siber güvenlik politikaları teoride açık ve belirgin olan ÇHC'nin uluslararası sisteme büyük oranda kapalı olduğu gözlemlenmektedir. Özellikle mevcut bilişim sistemleri endüstrisinden bağımsız olarak kendine has bilgi teknolojilerini üretmesi ve pratik boyutunun derpiş edilememesi noktasında Batılı devletlerin siber uzay hususunda ÇHC'ye karşı endişelerinin olduğu tespit edilmektedir. ÇHC'nin, kendi bilgi teknolojilerini geliştirme noktasında bilişim sektöründe önemli bir pazara sahip olması ve küresel ölçekte önemli ve etkin bir aktör olmasından dolayı, siber alanda atmış olduğu adımlar küresel sistemde bulunan diğer aktörler tarafından yakından takip edilmektedir.

Yapılan incelemeler sonucunda her ne kadar siber güvenlik hususunda en güçlü devletler sıralamasında ilk sırada ABD yer alsada ÇHC'nin politikaları bağlamında uluslararası sisteme kapalı olması, milli siber ağlarını, bilişim teknolojilerini ve alternatif sosyal ağlar üreterek yerli yazılımı/ağları teşvik etme noktasında belirli bir gelişim elde ettiğinden dolayı, ABD başta olmak üzere birçok devlet tarafından önemli bir tehdit olarak görüldüğü sonucuna ulaşılmaktadır. Son zamanlarda siber saldırılar hususunda en fazla hedef gösterilen devlet olan ÇHC'nin; siber saldırı, siber bağımsızlık ve siber savunma hususuna yönelik politikalara odaklandığı görülmektedir. Siber güvenlik politikalarının gelişimi noktasında ÇHC'nin önem verdiği bir diğer hususun ise uzay enstitüsünün ve yapay zekânın gelişimi olduğu gözlemlenmektedir. Yayımlanan beyaz kitaplarda hem yapay zekâ teknolojisinin gelişimi yönünde birtakım planlamaların yapıldığı hem de 2030'lu yıllara gelindiğinde mevzubahis alanda daha büyük bir gelişime ilişkin adımların atılacağı görülmektedir.

Tez çalışması süresinde edinilen veriler doğrultusunda ÇHC'nin her alanda lider olma arzusu olduğundan dolayı; teknoloji alanında olduğu gibi siber alanda da önemli bir güç hâline dönüşmek, ulusal güvenliği sağlamak, mevcut ekonomisini daha da güçlendirmek adına siber güvenlik politikasını geliştirmeye devam edeceği kanısına varılmaktadır. ÇHC'nin mevzubahis alanda göstermiş olduğu çaba, hem siber bağımsızlığı hem de teknolojik bağımsızlığı elde etme arzusundan kaynaklanmaktadır. Bu durumu kanıtlayan en güzel örnek, 2017 yılında yürürlüğe giren Siber Güvenlik

Yasası'dır. ÇHC'nin yürürlüğe koyduğu bu yasa; kapsam, etki ve uygulama yönünden hem ulusal hem de uluslararası sistemde büyük bir önem arz etmektedir.

Son kertede çalışma boyunca yapılan analizler doğrultusunda; Xi Jinping'in "siber güvenlik olmadan ulusal güvenlik olamaz" perspektifinden hareketle her ülke gibi ÇHC'nin de çıkarları doğrultusunda belirlemiş olduğu dış politikaların en önemli unsurunun ulusal güvenlik olduğu görülmektedir. Bununla birlikte, ulusal güvenliği sağlama noktasında geliştirilmesi gereken unsurun siber güvenlik olduğu vurgusununda sürekli olarak yapıldığı gözlemlenmektedir. Bu düşünceyle hareket eden ÇHC, bünyesinde büyük internet topluluğu barındırdığı ve bu topluluğun yapısını etkilediği için, Pekin'in siber güvenlik alanında attığı her adımın dünyanın geri kalanı tarafından izlendiği görülmektedir. Yapılan araştırmalar neticesinde kapalı politika izlemesinden ve kendine has tutumundan dolayı da diğer devletlerde endişeye sebep olduğu sonucuna ulaşılmaktadır. Öte yandan, teknoloji alanındaki avantajını kullanan ÇHC'nin siber alanda gücüne güç katmak adına, teknoloji ve orduyu birleştirerek her iki alanda da büyük bir gelişim sağlayacağı kanısına varılmaktadır. Bu doğrultuda ilerleyen ÇHC ekseninde karşılaşılabilecek herhangi bir siber savaş durumunda ordunun bu alanda geliştirilmesi, uzay silahları ve elektronik savaş hususunda personele ilgili eğitimlerin verilmesi doğrultusunda bahsi geçen iki hususun gelişimine katkı sağlayacağı düşünülmektedir. Bu durumun gerçekleşmesi hâlinde, ÇHC'nin gücüne güç katacağı yadsınamaz bir gerçek olarak karşımıza çıkmaktadır.

Diğer yandan, elde edilen bir diğer bulgu ise ÇHC'nin teknoloji alanında ulusallaşma çabasıdır. ÇHC, teknoloji alanında kendine has yazılımlar, platformlar geliştirerek ülkede yabancı yazılımları yasaklayarak, siber alanda karşılaşılabilecek riskleri en aza indirmeyi hedefleyen politikalar izlemektedir. Bu bağlamda ÇHC'nin internette hâkimiyeti sağlamak adına katı bir tutum sergilediği tespit edilmektedir. Bu durum her ne kadar halkın güvenliğini kısırsa da kontrolü sağlamak açısından ÇHC'nin kendine has olacak şekilde izlemiş olduğu en önemli yol olarak görülmektedir. Bunun yanı sıra ÇHC'nin yasalar ile internet üzerindeki hâkimiyetini koruması ve kalıcı örgütlenmeyi esas alarak olası muhalif toplumsal ve ayrılıkçı hareketleri kontrol altına almak adına gerekli durumlarda bu yasaları güçlendirmesi, ÇHC'yi siber alanda üst bir boyuta taşıyan önemli bir diğer adımı teşkil etmektedir. İnternet ile ilgili bu kontrolcü tutumunun insan haklarına aykırılığından dolayı her ne kadar Batılı ülkeler tarafından eleştirilse de ÇHC'nin kısa ve orta vadede Batı ülkeleri kaynaklı teknoloji şirketleri,

sosyal medya uygulamaları ve internet tabanlı markaların yatırımları üzerindeki kontrolünü sürdürmesi olası bir durum olarak saptanmaktadır. Sonuç olarak, elde edilen tüm bu bulgular çerçevesinde “ÇHC, siber güvenliğin sağlanması noktasında diğer büyük küresel aktörlerden farklı olarak, kendine özgü ve ulusal bir temele dayanan siber güvenlik politikası takip etmektedir” şeklinde ortaya konan ana hipotezin doğrulandığı görülmektedir.

KAYNAKLAR

- ABDUL-MUMİN, S., (2011), Detection of Man InTheMiddle Attack InIeee 802.11 Networks. KwameNkrumahUniversity Of ScienceAndTechnology: 38.
- AÇIKMEŞE, S. A., (2008), Kopenhag Okulu Ve Realist Güvenlik Çalışmalarında Aktör, Tehdit Ve Politika: Avrupa Güvenliği Üzerine Bir Değerlendirme (Yayımlanmamış Doktora Tezi), Ankara: Ankara Üniversitesi.
- ADIBELLİ, B., (2006), Çin Dış Politikasında Tayvan Sorunu , İstanbul: IQ Kültür Sanat Yayıncılık.
- ADIBELLİ, B., (2016), Pax Sinica Çin'in Dünya Düzeni, İstanbul: IQ Kültür Sanat Yayıncılık.
- AKDAĞ, Z., (2023), “Çin Dış Politikasında Süreklilik ve Değişim”, Marmara Üniversitesi Siyasi Bilimler Dergisi, C.11, S.1, ss.72-96, DOI: 10.14782marmarasbd.1206674.
- AKLEYLEK, S. ve TOK, Z. Y., (2011), “Siber Güvenlikte Kriptoloji”, Siber Güvenlik Çalıştayı, Ankara.
- AKTAŞ, M. M., (2019), Çin'in Ortadoğu Politikası ve Türkiye'nin Güvenlik Politikalarına Etkisi (1949-2018) (Yayımlanmamış Yüksek Lisans Tezi), İstanbul: Yıldız Teknik Üniversitesi, Sosyal Bilimler Enstitüsü.
- AKTAŞ, S., (2019), Bir Kuşak Bir Yol Projesi Özelinde Çin'in Yeni Süper Güç Olabilme Kapasitesi (Yayımlanmamış Yüksek Lisans Tezi), Ankara: Yıldırım Beyazıt Üniversitesi, Sosyal Bilimler Enstitüsü.
- AKYEŞİLMEN, N., (2018), Disiplinlerarası Bir Yaklaşımla: Siber Politika & Güvenlik, Ankara: Orion Kitabevi.
- ALİOĞLU, S. D., (2019), Siber Saldırıları ve Ülkelerin Siber Güvenlik Politikaları (Yayımlanmamış Yüksek Lisans Tezi), İstanbul: İstanbul Bilgi Üniversite, Lisansüstü Programlar Enstitüsü.
- Aljazeera Türk, (2014), “Ülke Profili: Çin Halk Cumhuriyeti”, <http://www.aljazeera.com.tr/ulke-profilu/ulke-profilu-cin-halk-cumhuriyeti>, (Erişim Tarihi:16.05.2023).
- ALPAR, G., (2021), “Tehdit Algısı, Güvenlik ve Strateji: Rusya Ulusal Güvenlik Strateji Belgesinin Karşılaştırmalı Analizi”, <https://www.sde.org.tr/guray-alpar/genel/tehdit-algisi-guvenlik-ve-strateji-rusya-ulusal-guvenlik-strateji-belgesinin-karsilastirmali-analizi-kose-yazisi-23026>, (Erişim Tarihi: 16.01.2023).
- ALPEREN, Ü., (2021), “Biden, Çin İçin Fırsat Mı Tehdit Mi?”, <https://fikirturu.com/jeo-strateji/biden-cin-icin-firsat-mi-tehdit-mi/>, (Erişim Tarihi:09.02.2023).
- ANDRESS, J. ve WINTERFELD, S., (2011), “Cyber Warfare:Teckniques, Tactics and Tools for Security Practitioners”, Syngress, S.1 , ss.2.
- ARAS, İ., (2018), Avrupa Birliği ve Çin Siyasi-Ekonomik İlişkiler, Ankara: Detay Yayıncılık.
- ARENDS J. F., (2012), “Homeros'dan Hobbes ve Ötekine: Avrupa Geleneğinde ‘Güvenlik’ Kavramı”, (Derleyenler: Aydın, M., Brauch, H., Günter, Ç., vd.),

- Uluslararası İlişkilerde Çatışmadan Güvenliğe, İstanbul: İstanbul Bilgi Üniversitesi Yayınları, ss.199.
- ARIMATSU, L., (2012), “A Treaty for Governing Cyber-Weapons: Potential Benefits and Practical Limitations”, 4. International Conference on Cyber Conflict.
- ARMAOĞLU, F., (2010), 20. Yüzyıl Siyasi Tarihi, İstanbul: Alkım Yayınevi, ss. 333-574.
- ARSLAN, Ö., (2021), Türkiye’nin Siber Güvenlik Politikaları Ve Siber Saldırıların Uluslararası Etkileri (Yayımlanmamış Yüksek Lisans Tezi), Düzce: Düzce Üniversitesi, Sosyal Bilimler Enstitüsü.
- ASLAN, H. K., (2014), “Yükselen Güç Çin Halk Cumhuriyeti’nin Ortadoğu Politikası”, Akademik Orta Doğu Dergisi, C.9, S.1, ss.29-55.
- ATALAY, A. H., (2012), “Kurumsal Bilgi Güvenliği”, Siber Güvenlik, Mimar ve Mühendis Dergisi, S.68, ss.42-47.
- ATAWULA, M., (2020), Çin’in Yeni Dönem Ulusal Güvenlik Politikaları Ve Küresel Rekabet Stratejisi (Yayımlanmamış Yüksek Lisans Tezi), Kahramanmaraş: Kahramanmaraş Sütçü İmam Üniversitesi, Sosyal Bilimler Enstitüsü.
- ATEŞ, D., (2013), Uluslararası Politika Dünyayı Anlamak ve Anlatmak, Bursa: Dora Yayınları.
- ATHANASSOULI, K., (2019), “Economic Implications of the Rise of Information Warfare, Cyber-War and Cyber-Security”, (Edt.: Nicholas J. Daras) inside; Cyber Security and Information Warfare, , New York: Nova Science Publishers, ss.39-57.
- AUSTIN, G., (2014), Cyber Policy in China, USA: Polity Press.
- AUSTIN, G., (2018), “How Good Are China’s Cyber Defenses?”, The Diplomat, <https://thediplomat.com/2018/07/how-good-are-chinas-cyber-defenses/>, (Erişim Tarihi:29.03.2023).
- AVRUPA KOMİSYONU, (2013), Proposal for a DIRECTIVE OF THE EUROPEAN PARLIAMENT AND OF THE COUNCIL concerning measures to ensure a high common level of network and information security across the Union, COM/2013/048 final - 2013/0027 (COD), European Commission. Brüksel: Avrupa Komisyonu, <http://eurlex.europa.eu/legalcontent/EN/TXT/PDF/?uri=CELEX:52013PC0048&from=EN>, (Erişim Tarihi:10.01.2023).
- AYDIN, M., (1996), “Uluslararası İlişkilerde Yaklaşım, Teori ve Analiz”, Uluslararası İlişkiler Dergisi, C.51, S.1.
- AYHAN, U., (2016), “Yeni Güvenlik Konsepti Ve Güvenliği Sınır Ötesinde Karşılama”, Güvenlik Çalışmaları Dergisi- Turkish Journal of Security Studies, C.18, S.8, ss. 133-143.
- AYTEKİN, E., (2023), “Çin, Azalan ve Yaşlanan Nüfus Gerçeğiyle Yüzleşiyor”, <https://www.aa.com.tr/tr/dunya/cin-azalan-ve-yaslanan-nufus-gercegiyle-yuzlesiyor/2791436>, (Erişim Tarihi:21.05.2023).
- BAEZNER, M., (2018), “Cybersecurity in Sino-American Relations”, Zürih: Center for Security Studies, ss. 224.

- BAHARÇİÇEK, A. ve İNAN, C. E., (2013), “Dış Politika’nın Belirlenmesinde Ulusal Güvenlik Algısının Rolü”, Akademik Yaklaşımlar Dergisi, C.4, S.1, ss. 101-102.
- BAİDU Baïke, (t.y.), ”Çin”, <https://baïke.baidu.com/item/%E4%B8%AD%E5%9B%BD/1122445>, (Erişim Tarihi:20.05.2023).
- BAKAN, S. ve ŞAHİN, S., (2018), “Uluslararası Güvenlik Yaklaşımlarının Tarihsel Dönüşümü Ve Yeni Tehditler”. The Journal of International Lingual Social and Educational Sciences, C.4, S.2, ss.135-152.
- BAKAN, Z. A., (2007), “Soğuk Savaş Sonrasında Yeni Güvenlik Teorileri ve Türkiye’nin Güvenlik Algılamaları”, 21. Yüzyıl Dergisi, Ekim-Kasım-Aralık 2007, Ankara, ss.35-50.
- BALKE, L., (2018), “China's New Cybersecurity Law and U.S-China Cybersecurity Issues”, Santa Clara Law Review, C.58, S.1, ss. 137-162.
- BAŞARAN, D., (2022), “Biden Yönetiminin Ulusal Güvenlik Strateji Belgesi’nde Çin”, <https://www.ankasam.org/biden-yonetiminin-ulusal-guvenlik-strateji-belgesinde-cin/>, (Erişim Tarihi:13.01.2023).
- BATES, D., (2011), “Cyber Attacks On 72 Organisations Around The World Including The UN İs The Biggest Yet Uncovered”, Mail Online, <https://www.dailymail.co.uk/sciencetech/article-2021908/Cyber-attacks-72-organisations-world-including-UN-biggest-uncovered.html>, (Erişim Tarihi:28.04.2023).
- BAYIR, Ö. E., (2013), “Uluslararası İlişkilerde Teorik Tartışmalar”, (Edt.: Hasret Ç. ve Caner S.), Soğuk Savaş Sonrasında Güvenliğe Yönelik Teorik Tartışmalar, Beta Basım, ss.171-191.
- BBC News Türkçe, (2020), “Koronavirüs: ABD İstihbaratı 'Çin'in Siber Saldırılarını' Soruşturduğunu Açıkladı”, <https://www.bbc.com/turkce/haberler-dunya52655953>, (Erişim Tarihi:01.05.2023).
- BBC News, (2013), “Cyber Attacks Blamed on China”, 31 January, <https://www.bbc.com/news/world-asia-china-21272613>, (Erişim Tarihi:28.04.2023).
- BEECH, H., (2011), “Meet China’s Newest Soldiers: An Online Blue Army”, Time, <http://world.time.com/2011/05/27/meet-chinas-newest-soldiers-an-online-blue-army/>, (Erişim Tarihi:02.04.2023).
- BELLAMY, C., (2001), “What is Information Warfare?”, (Edt: Matthews R., Treddenick J.), Managing the Revolution in Military Affairs, Londra: Palgrave Macmillan, ss. 56-75.
- BEY, M., (2018), “Great Powers in Cyberspace: The Strategic Drivers Behind US, Chinese and Russian Competition”, The Cyber Defense Review , C.3, S.3, ss.31-36.
- BGA Security, (2018), “Siber Tehdit İstihbaratı ve Kavramları”, <https://www.bgasecurity.com/2018/01/siber-tehdit-istihbarati/>, (Erişim Tarihi: 28.12.2022).
- BIÇAKÇI, S., (2014), “NATO’nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik”, Uluslararası İlişkiler Akademik Dergisi, C.10, S.40, ss.101-130.

- BIN, L. ve ZHAO, T., (2016), Understanding Chinese Nuclear Thinking, Carnegie, Washington DC, ss. 1-2.
- BİLGİÇ, A., (2011), “Güvenlik İkilemini Yeniden Düşünmek Güvenlik Çalışmalarında Yeni Bir Perspektif”, Uluslararası İlişkiler Dergisi, C.8, S.29, ss.123-124.
- BİRCAN, B., (2012), “Gelişmiş Siber Silahlar ve Tespit Yöntemleri”, TÜBİTAK BİLGEM, <http://docplayer.biz.tr/1142152-Gelismis-siber-silahlar-ve-tespit-yontemleri-bahtiyar-bircan-uzman-arastirmaci-siber-guvenlik-enstitusu.html>, (Erişim Tarihi:31.12.2022).
- BLUMENTHAL, D. ve SCİSSORS, D. M., (2016), “China’s Great Stagnation”, <https://nationalinterest.org/feature/chinas-great-stagnation18073>, (Erişim Tarihi:19.07.2023).
- BM Uluslararası Telekomünikasyon Birliği, (2008)., X.1205 : Overview of cybersecurity. ITU. <https://www.itu.int/rec/T-REC-X.1205-200804-I> (Erişim Tarihi: 22.12.2022).
- BOGLE, A., (2020), “Why China İs Being Blamed For Cyber Attacks On Australia, And What Its Hackers Might Be Looking For”, ABC News, <https://www.abc.net.au/news/2020-06-19/why-would-china-launch-cyber-attack-against-australia/12374990>, (Erişim Tarihi:28.04.2023).
- BOOTH, K., (2007), Theory of World Security, UK: Cambridge University Press.
- BOZGEYİK, A., (2018), Gaziantep’te Faaliyet Gösteren Orta ve Büyük Ölçekli İşletmelerin Siber Güvenlik Yönetim Yaklaşımlarının Analizi (Yayımlanmamış Doktora Tezi), Gaziantep: Hasan Kalyoncu Üniversitesi, Sosyal Bilimler Enstitüsü.
- BRAUCH, H. G., (2008), “Güvenliğin Yeniden Kavramsallaştırılması: Barış, Güvenlik, Kalkınma ve Çevre Kavramsal Dörtlüsü”, Uluslararası İlişkiler Dergisi, C.5, S.18, Yaz.
- BROWN, G. D. ve ANDREW O. M., (2014), “Easier Said Than Done: Legal Reviews of Cyber Weapons”, Journal of National Security Law and Policy, C.7, S.115.
- BROWN, G. ve YUNG, C. D., (2017), “Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace”, <https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/>, (Erişim Tarihi:01.05.2023).
- BRUNNER, N. ve GÖKDERE, A. Y., (1969), Çin Ekonomisi, Ankara Üniversitesi Hukuk Fakültesi Dergisi, C. 26, S. 3.
- BTK (Bilgi Teknolojileri ve İletişim Kurumu), (2009), “Siber Güvenliğin Sağlanması: Türkiye’de Mevcut Durum ve Alınması Gereken Tedbirler”, <https://www.btk.gov.tr/File/?path=ROOT%2F1%2FDocuments%2FSayfalar%2FSiberGuvenlik%2Fsg.pdf>, (Erişim Tarihi: 27.12.2022).
- BURMA, Z. A. ve ÖZDEMİR, A.A., (2024), “Ülkelerin Gelir Düzeyleri ve Ağa Hazırlık Endeksi Bileşenlerinin Dijital Göçmen Yaşlı Bireylerin İnternet ve Sosyal Medya Kullanımlarına Etkileri”, Dünya İnsan Bilimleri Dergisi, C.2024, S.1, ss.6.
- BUZAN, B. ve HANSEN, L., (2009), The Evolution of International Security Studies, New York: Cambridge University Press.

- BUZAN, B., (1983), *People, States and Fear: The National Security Problem in International Relations*. Brighton: Harvester Wheatsheaf.
- BUZAN, B., (2008), “Askeri Güvenliğin Değişen Gündemi”, *Uluslararası İlişkiler Dergisi*, C.5, S.18, ss.107.
- CARAYANNIS, G. P., (1976), “China- Tangshan Earthquake of July 28”, <https://drgeorgepc.com/Earthquake1976ChinaTangshan.html>, (Erişim Tarihi:11.06.2023).
- CARR, J., (2012), *Inside Cyber Warfare, USA: O'Reilly Media*.
- CARTWRIGHT, J. E., (2011), *Memorandum for Chiefs of the Military Servs., Commanders of the Combatant Commands, Dirs. of the Joint Staff Directories on Joint Terminology for Cyberspace Operation, Department of Defense, Washington DC*.
- CAVELTY, M. D., (2008), “Cyber- Security and Threat Politics”, *US Efforts to Ensure The Information Age*, New York: Routledge.
- CEBER, R., (2021), “Putin, Rusya’nın Yeni Ulusal Güvenlik Stratejisi’ni Onayladı”, <https://sputniknews.com.tr/20210703/putin-rusyanin-yeni-ulusal-guvenlik-stratejisini-onayladi-1044879722.html>, (Erişim Tarihi: 16.01.2023).
- CHAN, C.S., (2004), “Falun Gong in China: A Sociological Perspective”, *The China Quarterly*, C.179, ss.665-683.
- CHANG, A., (2014), *Warring State. China’s Cybersecurity Strategy: Center for a New American Security*.
- CHEN, D. ve WANG, J., (2011), *Lying Low No More? China’s New Thinking On The Tao Guang Yang Hui Strategy*, *China: An International Journal*, C.9, S.2, ss.195-216, DOI:10.1142/S021.974.7211000136.
- CHIGURH, C. E., (2006), “Çin Dış Politikasındaki Enerji Faktörü”, <https://www.docin.com/p-1662213452.html>, (Erişim Tarihi:30.06.2023).
- China Daily, (2013), “Xi Vows to Press Ahead with ‘Chinese Dream’”, https://www.chinadaily.com.cn/china/2013npc/2013-03/17/content_16314303.htm, (Erişim Tarihi:14.07.2023).
- China Daily, (2017), “Online Crime Continues To Rise In China”, https://www.chinadaily.com.cn/china/2017-10/16/content_33329294.htm, (Erişim Tarihi: 29.03.2023).
- China Daily, (2017), “Xi Jinping'in Ulusal Güvenlik Konspti/习近平的国家安全观”, https://china.chinadaily.com.cn/2017-02/22/content_28299966.htm, (Erişim Tarihi:01.11.2023).
- China Military, (2017), “China’s Militarymodernization in 2017” <https://www.uscc.gov/sites/default/files/2019-10/Chapter%202%2C%20Section%202%20-%20China%27s%20Military%20Modernization%20in%202017.pdf>, (Erişim Tarihi:05.11.2023).
- China’s Military Strategy, (2015), Ministry of National Defense, <http://eng.mod.gov.cn/xb/Publications/WhitePapers/4887928.html>, (Erişim Tarihi:04.04.2023).

- China's National Defense, (2004), "PRC: 2004 White Paper on National Defense Published", <https://fas.org/nuke/guide/china/doctrine/natdef2004.html>, (Eriřim Tarihi:01.04.2023).
- China SCIO, (2022), "White Paper: China's İnternet Population Reaches 1.05 Billion", The State Council Information Office of the People's Republic of China, http://english.scio.gov.cn/pressroom/2022-11/07/content_78506468.htm, (Eriřim Tarihi:06.04.2023).
- China White Paper, (2020), "The AI in China 2020 White Paper", Daxue Consulting, <https://daxueconsulting.com/ai-in-china-white-paper/>, (Eriřim Tarihi:06.04.2023).
- China White Paper, (2022a), "China's Space Program: A 2021 Perspective", The State Council Information Office of the People's Republic of China, http://english.scio.gov.cn/whitepapers/2022-01/28/content_78016877.htm, (Eriřim Tarihi:06.04.2023).
- China White Paper, (2022b), "Jointly Build a Community with a Shared Future in Cyberspace", The State Council Information Office of the People's Republic of China, http://english.scio.gov.cn/whitepapers/2022-11/07/content_78505694.htm, (Eriřim Tarihi:06.04.2023).
- China White Paper, (2023), "China's Law-Based Cyberspace Governance in the New Era", The State Council Information Office of the People's Republic of China, http://english.scio.gov.cn/whitepapers/2023-03/16/content_85172148.htm, (Eriřim Tarihi:06.04.2023).
- CHOUCRI, N., (2012), Cyberpolitics in International Relations, Londra: MIT Press.
- CILLUFFO, F., (2013), "Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure", <https://www.govinfo.gov/content/pkg/CHRG-113hhrg82583/html/CHRG-113hhrg82583.htm>, (Eriřim Tarihi:01.05.2023).
- CLARK, D., (2010), Characterizing Cyberspace: Past, Present and Future, MIT Csail, ss.1-3.
- CLARK, G. ve CHAN, E., (2018), "The Great Firewall of China", Bloomberg News, <https://www.bloomberg.com/quicktake/great-firewall-of-china>, (Eriřim Tarihi:14.02.2023).
- CLARKE, R. A. ve KNAKE, R. K., (2011), Siber Savaş. İstanbul: İKÜ Yayınları.
- CNN Türk, (2022), "Çin'den Tayvan'a Dakikada 170 Milyon Siber Saldırı", https://www.cnnturk.com/dunya/cinden-tayvana-dakikada-170-milyon-siber-saldiri#amp_tf=%251%24s%20adl%C4%B1%20kaynaktan&aoh=16827762600674&referrer=https%3A%2F%2Fwww.google.com&share=https%3A%2F%2Fwww.cnnturk.com%2Fdunya%2Fcinden-tayvana-dakikada-170-milyon-siber-saldiri, (Eriřim Tarihi:29.04.2023).
- CNNIC, (2012), "The Internet Timeline of China 1986~2003", China Internet Network Information Center, https://cnnic.com.cn/IDR/hlwfdzsj/201306/t20130628_40563.htm, (Eriřim Tarihi:07.02.2023).

- CONTEH, N. ve SCHMİCK, P., (2016), "Cybersecurity: Risks, Vulnerabilities And Countermeasures To Prevent Social Engineering Attacks" , International Journal of Advanced Computer Research, C.6, S.23, ss.31.
- CORDESMAN, A., (2019), "China's New 2019 Defense White Paper", <https://www.csis.org/analysis/chinas-new-2019-defense-white-paper>, (Erişim Tarihi:06.04.2023).
- CORELL, H., (2000), "The Challenge of Borderless Cyber-Crime", Symposium On The Occasion of The Signing of The United Nations Convention Against Transnational Organized Crime, Palermo, http://legal.un.org/ola/media/info_from_lc/cybercrime.Pdf, (Erişim Tarihi:01.01.2023).
- CORERA, G., (2017), "İngiltere'de Siber Güvenlik Merkezi Açıldı", BBC, <https://www.bbc.com/turkce/haberler-dunya-38967467>, (Erişim Tarihi:19.01.2023).
- COV, (2016), "China Passes New Cybersecurity Law", https://www.cov.com/-/media/files/corporate/publications/2016/11/china_passes_new_cybersecurity_law.pdf, (Erişim Tarihi:09.04.2023).
- CRIDLAND, C. (2008). "The history of the internet: the interwoven domain of enabling technologies and cultural interaction", In: Responses to Cyber Terrorism, Centre of Excellence Defence Against Terrorism, Ankara.
- CYBER CRIME STRATEGY, (March,2010), "Cyber Crime Strategy", Londra: Home Office, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228826/7842.pdf, (Erişim Tarihi:18.01.2023).
- Cyber Security Strategy of the United Kingdom, (June,2009), "Cyber Security Strategy of the United Kingdom: safety, security and resilience in cyber space", Londra: Kabine Ofisi, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/228841/7642.pdf, (Erişim Tarihi:18.01.2023).
- CyberMag, (2015), "Amerika ve Çin Siber Güvenlik Hakkında Görüşme Hâlinde", <https://www.cybermagonline.com/amerika-ve-cin-siber-guvenlik-hakkinda-gorusme-halinde>, (Erişim Tarihi:19.04.2023).
- ÇAKAN, V., (2017), Geçmişten Günümüze Çin, Asya Araştırmaları Dergisi, C.1, S.1, ss. 111-137.
- ÇAKIR, H. ve KILIÇ, M. S., (Edt.), (2014), Güncel Tehdit: Siber Suçlar, Ankara: Seçkin Kitapevi.
- ÇAKIROĞLU, D., (2008), "Çin Ülke Profili", T.C. Başbakanlık Dış Ticaret Müsteşarlığı İhracatı Geliştirme Etüd Merkezi.
- ÇAKMAK, H. ve ALTUNOK, T., (2009), Suç, Terör ve Savaş Üçgeninde Siber Dünya, Ankara: Barış Platin Kitapevi.
- ÇAKMAK, H. ve DEMİR, C. K., (2009), "Siber Dünyadaki Tehdit ve Kavramlar", (Edt.: H. Çakmak ve T. Altunok), Suç, Terör ve Savaş Üçgeninde Siber Dünya, Ankara: Barış Platin Kitabevi, ss.23-54.

- ÇALIK, Ü., (2011), “Çin Ekonomisi (Mao Ve Mao Sonrası Dönem)”, Liberal Düşünce Dergisi, S.64, ss.185-206.
- ÇALIŞKAN, E., (2022), Çin’in Tek Çin Politikası: Tayvan Ve Hong Kong (Yayımlanmamış Yüksek Lisans Tezi), Nevşehir: Hacı Bektaş Veli Üniversitesi, Sosyal Bilimler Enstitüsü.
- ÇELİKTAŞ, B. ve ÜNLÜ, N., (2018), “Cyber Security Power Ranking By Country And Its Importance On World Politics”, International Journal of Social Science, S.67, ss.469-488.
- ÇELİKTAŞ, B., (2016), Siber Güvenlik Kavramının Gelişimi ve Türkiye Özelinde Bir Değerlendirme (Yayımlanmamış Yüksek Lisans Tezi), Trabzon: Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü.
- ÇHC Devlet Konseyi Basın Ofisi, (2015), “Çin’in Askeri Stratejisi/中国的军事战略”, http://www.china.org.cn/china/2015-05/26/content_35661433.htm, (Erişim Tarihi:12.10.2023).
- ÇİFÇİ, H., (2013), Her Yönüyle Siber Savaş, İstanbul: TÜBİTAK Yayınları-Popüler Bilim Dizisi.
- DALHA, T., (2019), “The Cyber War Against Tibet”, The Diplomat, <https://thediplomat.com/2019/02/the-cyber-war-against-tibet/>, (Erişim Tarihi:29.04.2023).
- DARICILI, A. B., (2015), “NATO’nun Siber Güvenlik Stratejisi’nin Analizi. Uluslararası Sistemde Yeni Düzen Arayışları”, ss.407-417.
- DARICILI, A. B., (2017), “Demokrat Parti Hack Skandalı Bağlamında ABD ve RF’nin Siber Güvenlik Stratejilerinin Analizi”, Journal of International Studies, C.1, S.1, ss.1-24.
- DARICILI, A. B., (2017), Siber Uzay ve Siber Güvenlik: AB ve Rusya Federasyonu’nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi, Bursa: Dora Yayıncılık.
- DARICILI, A. B., (2018), Siber Uzay ve Siber Güvenlik; ABD ve Rusya Federasyonu’nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi, Bursa: Dora Yayıncılık.
- DARICILI, A.B. ve ÖZDAL, B., (2018), “Analysis of the Cyber Security Strategies of People’s Republic of China”, Güvenlik Stratejileri Dergisi, C.14, S.28, ss.1-35.
- DAZHOU, W. ve KAISHI, W., (2016), “Paradise, Panopticon, or Laboratory? A Tale of the Internet in China”, (Edt: J. L. Garcia), Pierre Musso and the Network Society: From Saint Simonianism to the Internet, Switzerland: Springer International Publishing, ss.155-187.
- DEDEOĞLU, B., (2004), “Yeniden Güvenlik Topluluğu: Benzerliklerin Karşılıklı Bağımlılığından Farklılıkların Birlikteliğine”, Uluslararası İlişkiler, C.1, S.4, ss. 2-15.
- DEMİR, E., (2020), “Xi Jinping Dönemi Çin Dış Politikası ve Kuşak Ve Yol Girişimi”, (Edt: F. Köksoy), Küresel Politikalar Ve Bölgesel Dönüşümler, Ankara: Nobel Akademik Yayıncılık, ss. 47-68.

- DEMİREL, F., (2019), Çin Halk Cumhuriyeti'nde Milliyetçilik Anlayışının Dış Politika Üzerindeki Etkileri (Yayımlanmamış Yüksek Lisans Tezi), Afyonkarahisar: Afyon Kocatepe Üniversitesi, Sosyal Bilimler Enstitüsü.
- DENG Y. ve THOMAS G. M., "China Views Globalization: Toward a New Great Power Politics?", The Washington Quarterly, C.27, S.3.
- DENG, Y., (2008), China's Struggle For Status, New York: Cambridge University Press.
- DILLON, M., (2016), Modernleşen Çin'in Tarihi, (Çev.: E. Ü. Atılğan ve A. Atılğan), İstanbul: İletişim Yayınları.
- DİNGİL, H., (2021), "Amerika'nın Avantajlarını Yenilemek: Geçici Ulusal Güvenlik Strateji Kılavuzu Mart 2021", <https://www.iramcenter.org/kitabiyat-detay/amerikanin-avantajlarini-yenilemek-gecici-ulusal-guvenlik-strateji-kilavuzu-mart-2021-7>, (Erişim Tarihi:13.01.2021).
- DOFFMAN, Z., (2019), "Chinese State Hackers Suspected Of Malicious Cyber Attack On U.S. Utilities", Forbes, <https://www.forbes.com/sites/zakdoffman/2019/08/03/chinese-state-hackers-suspected-of-malicious-cyber-attack-on-u-s-utilities/#7bd0da776758>, (Erişim Tarihi:29.04.2023).
- DOFFMAN, Z., (2020), "CIA Hackers Accused Of 11-Year Attack In New Chinese Cyber Report: This Is What's Behind It", Forbes, <https://www.forbes.com/sites/zakdoffman/2020/03/03/new-chinese-cyber-report-just-accused-cia-of-11-year-attack-this-is-whats-behind-the-report/?sh=719d691757e6>, (Erişim Tarihi:01.05.2023).
- DOVE, L. L., (2013), "Is The Chinese Army Hacking American Computers?" 22 March, HowStuffWorks.com, <https://computer.howstuffworks.com/chinese-army-hacking.htm>, (Erişim Tarihi:29.04.2023).
- DURMAZ, G., (2022), "JIANG ZEMIN: Çin'in Dönüşümünde Önemli Bir İsim", <https://www.sde.org.tr/gokberk-durmaz/genel/jiang-zemin-cinin-donusumunde-onemli-bir-isim-kose-yazisi-29292>, (Erişim Tarihi:07.07.2023).
- Dünya Ekonomik Formu, (2019), "Modern İpek Yolu: Kuşak ve Yol Girişimi nedir?", <https://tr.euronews.com/2019/04/14/video-cin-modern-ipek-yolu-nedir-kusak-ve-yol-girisimi-nedir-ipek-yolu-ne-zaman-bitecek>, (Erişim Tarihi:16.07.2023).
- EKREM, N. H., (2003), Çin Halk Cumhuriyeti Dış Politikası (1950-2000), Ankara: ASAM.
- ELMAS, M. S., (2013), "Modern Toplumun Güvenlik Çıkmazı: Tehdit, Risk ve Risk Toplumu Perspektifinden Güvenlik", Uluslararası Stratejik Araştırmalar Kurumu (USAK), Ankara: Karınca Yayınları.
- EMİR, B., (2020), Uluslararası İlişkilerin Kuramsal Çerçevesi ve Siber Güvenlik Kavramının Analizi (Yayımlanmamış Yüksek Lisans Tezi), Trabzon: Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü.
- ERALP, A., (2016), "Uluslararası İlişkiler Disiplininin Oluşumu: İdealizmRealizm Tartışması", (Edt.: Atilla Eralp), Devlet, Sistem ve Kimlik Uluslararası İlişkilerde Temel Yaklaşımlar (15.Baskı). İstanbul: İletişim Yayınları.

- ERDOĞAN, E. E., (2020), Uluslararası İlişkilerde Yeni Başat Güç Çin Halk Cumhuriyeti (Yayımlanmamış Yüksek Lisans Tezi), Ankara: Ufuk Üniversitesi, Sosyal Bilimler Enstitüsü.
- EREN, M., (2016), Avrupa Birliği'nin Siber Güvenlik Politikası (Yayımlanmamış Yüksek Lisans Tezi), İstanbul: Marmara Üniversitesi, Sosyal Bilimler Enstitüsü.
- EREN, M., (2017), "Avrupa Birliği'nin Siber Güvenlik Stratejisi İçin Kuramsal Çerçeve ve Stratejik Belgesi Öncesi AB'nin Eylemleri", Siber Politikalar Dergisi, C,2, S,3.
- EREN, M., (2017), Avrupa Birliği'nin Siber Güvenlik Politikası, İstanbul: Beta Yayınevi.
- EREN, M., (2020), "İngiltere'nin Siber Güvenlik Politikası", (Edt.: Fulya Köksoy),Yeni Küresel Tehdit Siber Saldırıları: Siber Güvenlik ve Politika Uygulamaları, Ankara: Nobel Yayıncılık.
- ERGÜL, E., (2008), Küresel Köyde Suç ve Adalet, 1. Baskı, Ankara: Adalet Yayınevi.
- EROĞLU, M. R., (2022), 21. Yüzyıl Güvenliğinde Asimetrik Bir Mücadele: Siber Uzayda Doğu Perspektifi (Yayımlanmamış Yüksek Lisans Tezi), Trabzon: Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü.
- ESEN, H., (2021), "İngiltere, Yeni Güvenlik Stratejisinde Rusya'yı 'Aktif Tehdit' Çin'i 'Sistemik Zorluk' Olarak Tanımladı", <https://www.aa.com.tr/tr/dunya/ingiltere-yeni-guvenlik-stratejisinde-rusyayi-aktif-tehdit-cini-sistemik-zorluk-olarak-tanimladi/2178149>, (Erişim Tarihi:19.01.2023).
- ESHERICH, J., PICKOWICZ, P. ve WALDER, G. A., (2006), The Chinese Cultural Revolution as History, Standford: Stanford University Press, ss. 96-120.
- Euronews, (2021), "Çin, Yüksek Kamu Borcu ve Pandemiye Rağmen 2021'de Savunmaya 210 Milyar Dolar Ayıracak", Euronews Türkiye, <https://tr.euronews.com/2021/03/05/cin-yuksekkamu-borcu-ve-pandemiye-ragmen-2021-de-savunmaya-210-milyar-dolar-ay-racak>, (Erişim Tarihi:06.04.2023).
- European Parliamentary Research Service, (2014), "Cyber defence in the EU Preparing for Cyber Warfare?", <http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf>, (Erişim Tarihi:13.01.2023).
- European Parliamentary Research Service, (2014), "Cyber defence in the EU Preparing for Cyber Warfare?", <http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf>, (Erişim Tarihi:02.04.2023).
- European Parliamentary Research Service, (2014), "Cyber Defence İn The EU Preparing For Cyber Warfare?", European Parliament, <http://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf>, (Erişim Tarihi:02.04.2023).
- Falun Dafa, (2020), "Falun Dafa'nın Kısa Tanıtımı", <https://tr.falundafa.org/index.html>, (Erişim Tarihi:09.02.2023).
- FEAKIN, T., (2013), "Enter The Cyber Dragon; Understanding Chinese Intelligence Agencies' Cyber Capabilities", Australian Strategic Policy Institute (ASPI), S.50.

- Federation Council Of The Federal Assembly Of The Russian Federation, (2014), The Concept of the Cybersecurity Strategy of the Russian Federation, <http://council.gov.ru/services/discussions/themes/38324/>, (Eriřim Tarihi:16.01.2023).
- Financial Review, (2020), “Nonsense’: China denies role in cyber attack”, 19 June, <https://www.afr.com/world/asia/nonsense-china-denies-role-in-cyber-attack-20200619-p554fw>, (Eriřim Tarihi:28.04.2023).
- GANG, W. ve SHUANG, Y., (2012), “Xi Jinping, ‘Çin Ulusunun Büyük Yenilenmesi’ Sözü Verdi”, <https://www.globaltimes.cn/content/747443.shtml>, (Eriřim Tarihi: 15.07.2023).
- GEDİK, D., (2018), Siber Güvenlik ve Terörizmin Evriliři: Türkiye Üzerine Etkileri (Yayımlanmamıř Yüksek Lisans Tezi), Düzce: Düzce Üniversitesi, Sosyal Bilimler Enstitüsü.
- GIBSON, R. ve ERLE, S., (2006), “Google Maps Hack”, Sebastopol: O’reilly Media.
- GIBSON, W., (1982), Burning Chrome, Arbor House Pub Co.
- GIBSON, W., (2016), Neuromancer, (Çev.: Sergül Oğur), İstanbul: Altıkırkbeř Yayınları.
- GIEROW, H. J., (2014), “Cyber Security in China: New Political Leadership Focuses on Boosting National Security”, Restructuring internet regulation. Placing restrictions on foreign software, Developing the PRC's own IT standards, China Monitor, S.20.
- GIEROW, H. J., (2015), “Cyber Security in China: Internet Security, Protectionism and Competitiveness: New Challenges to Western Businesses”, Marcator Institute for China Studies, https://merics.org/sites/default/files/2020-05/150407_MERICS%20China%20Monitor%2022_en.pdf, (Eriřim Tarihi:19.04.2023).
- GOLDSTEIN, J. S. ve PEVEHOUSE, J. C., (2014), Uluslararası İliřkiler, (Çev.: H. Özdemir), Ankara: BB101 Yayınları, ss. 585.
- GORDON, S. ve CHESS, D., (1999), Attitude Adjustment: Trojans and Malware on the Internet, Proceedings of the EICAR Conference, Aalborg, Denmark.
- GÖÇÖĞLU, V. ve AYDIN, M. D., (2019), “Siber Güvenlik Politikası: ABD, Rusya ve Çin Üzerine Karşılařtırılmal Bir Analiz”, Güvenlik Bilimleri Dergisi, C.8, S.2, ss. 229-252.
- GÖKTEN, K., (2013), “Büyük Ejderha ve Küresel Kapitalizm: 150 Yıllık Panorama”, 21. Yüzyılda Sosyal Bilimler Dergisi, S.5, ss.9-42.
- GRAHAM, J. ve HOWARD, R. vd., (2010), Cyber Security Essentials, Boca Raton, Auerbach Publications.
- GRIEGER, G., (2016), “One Belt, One Road (OBOR): China's Regional İntegration Initiative”, Europe: European Parliamentary Research Service.
- GRUNBERG, N., (2019), “The CCP’s Nerve Center”, <https://merics.org/en/comment/ccps-nerve-center>, (Eriřim Tarihi:15.07.2023).
- GÜÇDEMİR, Y., (2012), “Bilgisayar Ağları İnternetin Geliřimi ve Bilgi Kirlenmesi”, İstanbul Üniversitesi İletişim Fakültesi Dergisi, S.17, ss.371-378.

- GÜL, A. F., (2012), Siber Güvenlik Raporu, Çin ve ABD İncelemesi.
- GÜL, B., (2021), Amerika Birleşik Devletleri Büyük Stratejisi Çerçevesinde Çin Halk Cumhuriyeti Politikası: Barack Obama Dönemi (2009-2017) (Yayımlanmamış Yüksek Lisans Tezi), İzmir: Ege Üniversitesi, Sosyal Bilimler Enstitüsü.
- GÜLER, E. Z., (2001), “Çin Dış Politikası: Değişim ve Süreklilik”, (Hazırlayan: Deniz Ülke Arıboğan), Çin’in Gölgesinde Uzakdoğu Asya, İstanbul: Bağlam Yayınları, ss.283-296.
- GÜLEZ, G., (2014), “Çin’in Dev İnternet Sansür Sistemi Nasıl Çalışıyor?”, <https://web.archive.org/web/20160529142016/http://www.cinmacerasi.com/cini-n-dev-internet-sansur-sistemi-nasil-calisiyor/>, (Erişim Tarihi:13.02.2023).
- GÜNGÖR, M., (2015), Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma (Uzmanlık Tezi), T.C. Kalkınma Bakanlığı, Bilgi Toplumu Dairesi Başkanlığı.
- GÜNTAY, V., (2016), Uluslararası İlişkiler Temelinde Siber Güvenlik: Mikro Siber İttifak Teorisi (Micro-CAT) (Yayımlanmamış Doktora Tezi), Trabzon: Karadeniz Teknik Üniversitesi, Sosyal Bilimler Enstitüsü.
- GÜNTAY, V., (2018), “Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler”, Güvenlik Stratejileri Dergisi, C.14, S.27, ss.79-111.
- GÜNTAY, V., (2017), “Uluslararası Sistem ve Güvenlik Açısından Değişen Savaş Kurgusu: Siber Savaş Örneği”, Güvenlik Bilimleri Dergisi, C.6, S.2, ss.81-108.
- GÜRKAYNAK, M. ve İREN A. A., (2011), “Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler”, Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi, C.16, S.2, (263-279).
- GÜRSOY, E., (2015), Bilişim Yoluyla Dolandırıcılık Ve Korunma Yöntemleri (Yayımlanmamış Yüksek Lisans Tezi), Afyon: Afyon Kocatepe Üniversitesi, Sosyal Bilimler Enstitüsü.
- HAENLE, P., (2020), “What the Coronavirus Means for China’s Foreign Policy”, <https://carnegieendowment.org/2020/03/11/what-coronavirusmeans-for-china-s-foreign-policy-pub-81259>, (Erişim Tarihi:16.07.2023).
- HALO, V., (2021), “What Tech Firms Need To Know About China’s New Phase of Development”, China Internet Report Retail in Asia, <https://retailinasia.com/uncategorized/china-internet-report-2021-what-tech-firms-need-to-know-about-chinas-new-phase-of-development/>, (Erişim Tarihi:26.01.2023).
- HARRIS, S., (2014), Çin Dış Politikası, (Çev.: A. Y. Şir), Cambridge: Polity Press Ltd.
- HATHAWAY, O. ve CROTOF, R., (2012), “The Law of Cyber-Attack”, California Law Review, ss.100.
- HELMY, N., (2023), “Xi Jinping’s Vision of China’s National Security”, <https://modern diplomacy.eu/2023/08/06/xi-jinpings-vision-of-chinas-national-security/>, (Erişim Tarihi:02.10.2023).
- HENSEN, L. ve NİSSENBAUM, H., (2009), “Digital Disaster, Cyber Security and the Copenhagen School”, International Studies Quarterly, C.53, S.4, ss.1155-1175.

- HEYLIGHEN, F. ve JOSLYN, C., (2001), "Cybernetics and Second-Order Cybernetics", (Edt: R.A. Meyers), Encyclopedia of Physical Science & Technology, New York: Academic Press.
- HOLCOMBE, C., (2010), Doğu Asya Tarihi Çin Japonya Kore Medeniyetin Köklerinden 21. Yüzyıla Kadar, (Çev.: M. Özeren), İstanbul: Dergâh Yayınları.
- HONG, W., (2013), "Çin Komünist Partisi Liderlerinin Diplomatik Fikirleri ve Kültürel Kökenleri", <http://art.people.com.cn/n/2013/0328/c359841-20954374.html>, (Erişim Tarihi:08.07.2023).
- HSU, K. ve MURRAY, C., (2015), "China and International Law in Cyberspace", in; Terrorism: Commentary on Security Documents Vol 139 The Rise of China, (ed. Douglas C. Lovelace, Jr.), New York: Oxford University Press, 197-208.
- HUAQIU, L., (2004), "Deng Xiaoping'in Yeni Dönemde Çin'in Diplomatik Çalışmalarına Büyük Katkıları", https://www.gmw.cn/01gmrb/2004-08/17/content_79355.htm, (Erişim Tarihi:06.07.2023).
- HUOTARİ, M. vd., (2017), "China's Emergence As A Global Security Actor: Strategies For Europe (Rapor)", Berlin: Mercator Institute for China Studies, S.4.
- IASIELLO, E., (2014), "Is Cyber Deterrence an Illusory Course of Action?", Journal of Strategic Securit, C.7, S.1, ss.55.
- Information Security Doctrine of The Russian Federation, (2000), "The Doctrine of Information Security of the Russian Federation" <https://base.garant.ru/182535/>, (Erişim Tarihi:15.01.2023).
- ITU, (2008), Overview of Cybersecurity, ITU-T Recommendations, <https://www.itu.int/rec/T-REC-X.1205-200804-I>, (Erişim Tarihi: 10.01.2023).
- IVEZIC, M., (2017), "Cybercrime in China- A Growing Threat for the Chinese Economy", <https://society5.com/cyber-kinetic-security/chinese-cybercrime/>, (Erişim Tarihi:29.03.2023).
- JANELIUNAS, T. ve TUMKEVIČ, A., (2020), "Avoiding A Cyber World War: Rational Motives For Negative Cooperation Among The United States, China And Russia", (Edt: V. Benson and J. McAlaney), Emerging Cyber Threats and Cognitive Vulnerabilities, Londra: Elsevier Press, ss.118-146.
- JIECHI, Y., (2013), "Implementing the Chinese Dream", <https://nationalinterest.org/commentary/implementing-the-chinese-dream-9026>, (Erişim Tarihi:15.07.2023).
- JOHNSON, T. A., (2015), "Historical Reference Points in the Computer Industry and Emerging Challenges in Cybersecurity", (Edt.: Thomas A. Johnson), Cybersecurity: Protecting Critical Infrastructures from Cyber Attack and Cyber Warfare, New York: CRC Press.
- JONASSON, D. ve SIGHOLM, J., (2005), "What is Spyware?", <http://docplayer.net/8724618-What-is-spyware-daniel-jonasson-danjo620-student-liu-se-johan-sigholm-johsi264-student-liu-se-abstract-2-theory.html>, (Erişim Tarihi:31.12.2022).
- Journal of Political Sciences and Public Affairs, (2017), "New Cyber Strategy of China and the Alterations in the Field", <https://www.longdom.org/open->

- access/newcyber-strategy-of-china-and-the-alterations-in-the-field-2332-0761-1000310, (Eriřim Tarihi: 29.03.2023).
- KANWAL, G., (2009), "China's Emerging Cyber War Doctrine", *Journal of Defence Studies*, C.3, S.3, ss.14-22.
- KARA, M., (2013), *Siber Saldırıları-Siber Savaşlar ve Etkileri* (Yayımlanmamış Yüksek Lisans Tezi), İstanbul: İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü.
- KARA, O., (2023), "We Are Social Dijital 2023 Global ve Türkiye Raporu Yayımlandı!", <https://omgiletisim.com/>, (Eriřim Tarihi: 04.04.2024).
- KARABULUT, B., (2009), *Küreselleřme Sürecinde Güvenlięi Yeniden Düşünmek* (Yayımlanmamış Doktora Tezi), Ankara: Gazi Üniversitesi.
- KARACA, E., (2019), "Huawei'den ABD'ye Siber Saldırı Suçlaması", <https://www.aa.com.tr/tr/bilim-teknoloji/huaweiden-abdye-siber-saldiri-suclamasi/1573355>, (Eriřim Tarihi:19.04.2023).
- KARADAĞ, Ş., (2019), *Siber Uzayın NATO'nun Güvenlik Anlayışına Etkisi* (Yayımlanmamış Yüksek Lisans Tezi), Konya: Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü.
- KARAMANOĞLU, H., (2020), *Çin Halk Cumhuriyeti'nde Yerel Yönetimlerin Yapısı ve Dönüşüm Süreci* (Yayımlanmamış Yüksek Lisans Tezi), Konya: Necmettin Erbakan Üniversitesi, Sosyal Bilimler Enstitüsü.
- KARLUK, A. C., (2020), "Çin Rüyası Ve Küresel Hegomanya/The Chinese Dream And Global Hegemony", *Cihannüma Dergisi*, Sayı 3, 102-112.
- KAVALA, Ç. F., (2019), *Doęu Uyanıyor*, İstanbul: Doęu Kitapevi.
- KEITH, B. A., (2007), "Warfighting in Cyberspace", *Joint Force Quarterly*, S.46, 58-61.
- KELEřTEMUR, A., (2015), *Siber İstihbarat*, İstanbul: Level Kitap.
- KELLO, L., (2013), "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", *International Security*, C.38, S.2, ss.19.
- KESGİN, N., (2022), *ABD-Çin Rekabetinin Siber Güvenlik Bağlamında Ortadoęu'ya Yansımaları* (Yayımlanmamış Yüksek Lisans Tezi), Ankara: Ufuk Üniversitesi, Sosyal Bilimler Enstitüsü.
- KINIKOĞLU, B. Y., (2012, Mayıs), "Birleşik Krallık İncelemesi", İstanbul Bilgi Üniversitesi, Biliřim Ve Teknoloji Hukuku Enstitüsü, ss.30.
- KISSINGER, H., (2015), *Çin: Dünden Bugüne Yeni Çin*, (Çev.: N. I. Çeper), İstanbul: Kaknüs Yayınları.
- KLIMBURG, A., (2012), "National Cyber Security Framework Manual", Tallin: NATO CCD COE Publications, ss. 8.
- KOBIERECKA, A., (2022), *Post-Covid China: 'Vaccine Diplomacy' And The New Developments Of Chinese Foreign Policy, Place Branding and Public Diplomacy*, DOI:10.1057/s41254.022.00266-2.
- KOPUK, E. ve BAYRAÇ, H. N., (2021), "Bir Kuşak Bir Yol Projesi ve Ekonomik Etkileri", *Alanya Akademik Bakış Dergisi*, C.5, S.3, ss.1353-1374.

- KOTİK, Y. Ö., (2015), Uluslararası İlişkilerde Siber Güvenlik Algısı ve Ulus Devletin Değişen Stratejisi (Yayımlanmamış Yüksek Lisans Tezi), Adana: Çukurova Üniversitesi, Sosyal Bilimler Enstitüsü.
- KÖKSOY, F., (2019), “ Çin Halk Cumhuriyeti ve Siber Güvenlik”, Uluslararası Güvenlik Kongresi: (Kuram, Yönetim, Uygulama) Tam Metin Bildiri Kitabı, Ankara: Jandarma ve Sahil Güvenlik Akademisi, ss.337-351.
- KÖSE, F., (2021), “Rekabetçi Bir Çağda Küresel Britanya Strateji Belgesi (2021)”, <https://www.kirmizilar.com/rekabetci-bir-cagda-kuresel-britanya-strateji-belgesi-2021/>, (Erişim Tarihi:20.01.2023).
- KÖSE, T., (2007), “Psikolojik Savaşın Tehlikeli Cephanesi: Nükleer Silahlar”, <https://www.setav.org/psikolojik-tavas-in-tehlikeli-cephanesi-nukleer-silahlar/>, (Erişim Tarihi:17.07.2023).
- KPMG, (2017), “Overview of China’s Cybersecurity Law”, IT Advisory, <https://assets.kpmg.com/content/dam/kpmg/cn/pdf/en/2017/02/overview-of-cybersecurity-law.pdf>, (Erişim Tarihi:09.04.2023).
- KRAUSE, K. ve WILLIAMS, M., (1997), “From Strategy to Security: Foundations of Critical Security Studies”, Critical Security Studies: Concepts and Cases, University of Minnesota Press.
- KRAUSE, M. ve TIPTON, H., (2007), Information Security Management Handbook, CRC Press, 6th. Ed.,Akt. Ulaşanoğlu, op.cit., s. 18.
- KULA, S. ve ÇAKAR, B., (2015), “Maslow İhtiyaçlar Hiyerarşisi Bağlamında Toplumda Bireylerin Güvenlik Algısı ve Yaşam Doyumu Arasındaki İlişki”, Bartın Üniversitesi İ.İ.B.F. Dergisi, C.6, S.12, ss. 191-210.
- KUMAR, A., (2012), “New Security Security Concept Concept of China: An Analysis”, Institute of Peace and Conflict Studies (IPCS), S. May.
- KUMTEPE, D., (2021), “Çin Siber Güvenlik İçin 9,7 Milyar Dolar Harcayacak”, Haber Ortak, <https://www.stendustri.com.tr/haberortak/cin-siber-guvenlik-icin-97-milyar-dolar-harcayacak-h115041.html>, (Erişim Tarihi:01.05.2023).
- KURNAZ, İ., (2016), “Siber Güvenlik ve İlintili Kavramsal Çerçeve”, Siber Politikalar Dergisi, C.1, S.1, ss.56-77.
- LAMPTON, D. M., (2015), “Xi Jinping And The National Security Commission: Policy Coordination and Political Power”, Journal of Contemporary China, DOI: 10.1080/10670564.2015.1013366.
- LAU, F. vd., (2000), “Distributed denial of service attacks”, 2000 ieee international conference on systems, man and cybernetics.'cybernetics evolving to systems, humans, organizations, and their complex interactions', IEEE, ss. 2275-2280
- LEE, A. S., (2018), “A Century Of Humiliation: Understanding The Chinese Mindset”, <https://www.mironline.ca/century-humiliation-understanding-chinese-mindset/>, (Erişim Tarihi:20.05.2023).
- LEE, S., (2017), “An Institutional Analysis of Xi Jinping’s Centralization of Power”, Journal of Contemporary China, C. 26, S. 105, ss. 325-336.
- LEVİ, W., (1953), Modern China’s Foreign Policy, Minneapolis: University of Minnesota Press.

- LEVY, M. A., (2005), “Is The Environment a National Security Issue?”, *International Security*, C.20, S.2, Fall, ss.35-62.
- LEWIS, J. A. ve TIMLIN, K., (2011), “Cybersecurity and Cyberwarfare Preliminary Assessment of National Doctrine and Organization”, Center for Strategic and International Studies, <https://unidir.org/files/publication/pdfs/cybersecurity-and-cyberwarfare-preliminary-assessment-of-national-doctrine-and-organization-380.pdf>, (Eriřim Tarihi:01.04.2023).
- LI, H., (2015), “Genel Ulusal Gvenlik Kavramının Deęiřen zellikleri zerine/论总体国家安全观的变革性特征” , 重庆大学学 (Chongqing Daxue Xuebao), C.21, S.3, ss. 153-157.
- LI, Y. ve SCHMERER, H. J., (2017), “Trade and the New Silk Road: Opportunities, Challenges and Solutions”, *Journal of Chinese Economic and Business Studies*, C.15, S.3, ss. 205-213.
- LIBICKI, M. C., (2009), *Cyberdeterrence and Cyberwar*, RAND Corporation, Santa Monica, CA.
- LIBICKI, M., (2009), “Cyber deterrence and Cyberwar”, Santa Monica, CA: Rand Cooperation.
- LIMBA, T., PLETA, T., AGAFONOV, K., ve DAMKUS, M., (2017, June), *Cyber Security Management Model for Critical Infrastructure, Entrepreneurship and Sustainability Issues*, C.4, S.4, ss.559-573.
- LINDSAY, J., (2012), “China and Cybersecurity: Political, Economic, and Strategic Dimensions”, https://ucigcc.org/wp-content/uploads/2022/05/Lindsay_china-cybersecurity_apr-2012.pdf, (Eriřim Tarihi:15.04.2023).
- LINDSAY, J., (2015), “The Impact of China on Cybersecurity”, *International Security*, C. 39, S.3, ss. 7-47.
- LIPPIT, V., (1975), *The Great Leap Forward Reconsidered, Modern China*, C. 1, S. 1, ss. 92-115.
- LIU, Y., (2017). “Kapsamlı Ulusal Gvenlik Grř erevesinde Genel Ulusal Gvenlik Stratejisi Oluřturmak/以总体国家安全观构建国家安全总体布局”, “人民论坛” (Renmin Luntan / Halk Forumu), Aralık İlk Sayısı.
- LU, M., (2014), “Types of Cyber Attacks. Trustworthy Cyber Infrastructure For The Power Grid”, https://tcipg.org/sites/default/files/rgroup/tcipg-reading-group-fall_2014_09-12.pdf, (Eriřim Tarihi: 11.12.2022).
- LUM, T., (2001), “China and Falun Gong”, CRS Report for Congress, https://www.everycrsreport.com/files/20010803_RS20333_0fd7d966537bd6c3c83bbd9809a2db8b6e667230.pdf, (Eriřim Tarihi:10.02.2023).
- LUPOVICI, A., (2011), “Cyber Warfare and Deterrence”, *Military and Strategic Affairs*, C.3, S.3, ss.51.
- LYALL, N., (2018), “China’s Cyber Militias”, *The Diplomat*, <https://thediplomat.com/2018/03/chinas-cyber-militias/>, (Eriřim Tarihi:16.04.2023).
- LYNCH, D. C., (2015), *China’s Futures*, Stanford: Stanford University Press.

- LYYTINEN, K. ve KING, J. L., (2002), "Editorial: Around the Cradle of the Wireless Revolution: The Emergence and Evolution of Cellular Telephony", *Telecommunications Policy*, C.26, S.3-4, ss.97-100.
- MAAN, P. ve SHARMA, M., (2012), "Social Engineering: A Partial Technical Attack", *Int. J. Comput. Sci. Issues*, C.9, S.2, ss.557.
- MADDISON, A., (2007), *The World Economy Volume 1: A Millennial Perspective Volume 2: Historical Statistics*, Academic Foundation.
- MALLICK, M, G., (2019), "Vivekananda International Foundation", <https://www.readkong.com/page/china-s-defence-white-paper-vivekananda-international-2518237?p=2>, (Erişim Tarihi: 06.04.2023).
- Malware Definition, <https://techterms.com/definition/malware#:~:text=Short%20for%20%22malicious%20software%2C%22,actions%20on%20a%20computer%20system,> (Erişim Tarihi:28.12.2022).
- MANANTAN, M., (2019), "The Cyber Dimension of the South China Sea Clashes", *The Diplomat*, <https://thediplomat.com/2019/08/the-cyber-dimension-of-the-south-china-sea-clashes/>, (Erişim Tarihi:01.05.2023).
- Mandiant, (2013), "Mandiant Exposes APT1: One of China's Cyber Espionage Units & Releases 3,000 Indicators", <https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposesapt1-chinas-cyber-espionage-units.html>, (Erişim Tarihi:01.05.2023).
- MANN, I., (2008), *Hacking the Human Social Engineering Techniques and Security Countermeasures*, Gower Publishing Limited, Hampshire.
- McCarthy, N., (2018), "China Now Boasts More Than 800 Million Internet Users and 98% of Them Are Mobile", <https://www.forbes.com/sites/niallmccarthy/2018/08/23/china-now-boasts-more-than-800-million-internet-users-and-98-of-them-are-mobile-infographic/?sh=638550887092>, (Erişim Tarihi: 28.12.2023).
- MCKUNE, S., (2015), "An Analysis of the International Code of Conduct for Information Security", *The Citizen Lab*, [https://citizenlab.ca/2015/09/international-code-of-conduct/#:~:text=The%20International%20Code%20of%20Conduct%20for%20Information%20Security%20\(the%20%E2%80%9CC\).ode,Shanghai%20Cooperation%20Organization%20\(SCO\),](https://citizenlab.ca/2015/09/international-code-of-conduct/#:~:text=The%20International%20Code%20of%20Conduct%20for%20Information%20Security%20(the%20%E2%80%9CC).ode,Shanghai%20Cooperation%20Organization%20(SCO),) (Erişim Tarihi:03.04.2023).
- MELE, S., (2013), *Cyber-Weapons: Legal and Strategic Aspects*, Version 2.0, Machiavelli Editions, <http://www.strategicstudies.it/wp-content/uploads/2013/07/Machiavelli-Editions-Cyber-Weapons-Legal-and-Strategic-Aspects-V2.0.pdf>, (Erişim Tarihi: 28.12.2022).
- MFA (Ministry of Foreign Affairs of the People's Republic of China), (2013), "Xi Jinping: Let the Sense of Community of Common Destiny Take Deep Root in Neighbouring Countries", https://www.fmprc.gov.cn/mfa_eng/wjb_663304/wjbz_663308/activities_663312/t1093870.shtml, (Erişim Tarihi: 15.07.2023).
- MFA (Ministry of Foreign Affairs of the People's Republic of China), (2014), "The Central Conference on Work Relating to Foreign Affairs was Held in Beijing",

- https://www.mfa.gov.cn/eng/wjb_663304/zzjg_663340/xws_665282/xgxw_665284/201412/t20141201_600270.html, (Eriřim Tarihi:15.07.2023).
- MIANLI, Z., (2013), “Mao Zedung'un 1949'daki Ü Büyük Diplomatik Kararındaki Durum Hakkındaki Yargısı”, <http://theory.people.com.cn/n/2013/1009/c83867-23138929.html>, (Eriřim Tarihi:02.07.2023).
- MILLER, B., (2001), “The Concept Of Security: Should It Be Redefined?”, *Journal of Strategic Studies*, C.24, S.2.
- Ministry of Defense of The Russian Federation, (2011), “Conceptual Views on the Activities of the Armed Forces of the Russian Federation in the Information Space”, <https://ens.mil.ru/science/publications/more.htm?id=10845074@cmsArticle>, (Eriřim Tarihi:15.01.2023).
- MITTER, R., (2012), *Modern Çin*, Ankara: Dost Kitapevi.
- Mİř, N., (2011), “Güvenlikleřtirme Teorisi ve Siyasal Olanın Güvenlikleřtirilmesi”, *Akademik İncelemeler Dergisi*, C.6, S.2.
- MİTTER, R., (2012), *Modern Çin*, Ankara: Dost Kitapevi.
- MOKRY, S., (2016), “Is the Belt and Road Initiative Globalizing China's National Security Policy?”, <https://thedi diplomat.com/2016/10/is-the-belt-and-road-initiative-globalizing-chinas-national-security-policy/>, (Eriřim Tarihi:29.10.2023).
- MOUNT, M., (2009), “Hackers Stole Data on Pentagon's Newest Fighter Jet”, <http://edition.cnn.com/2009/US/04/21/pentagon.hacked/>, (Eriřim Tarihi:28.04.2023).
- NABIJANG, N., (2022), *Çin Halk Cumhuriyeti'nin Üüncü Dünya Politikası (Yayımlanmamıř Yüksek Lisans Tezi)*, Konya: Seluk Üniversitesi, Sosyal Bilimler Enstitüsü.
- National Cyber Security Strategy 2016-2021, (2016), “National Cyber Security Strategy 2016 to 2021”, Londra: Kabine Ofisi, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/567242/national_cyber_security_strategy_2016.pdf, (Eriřim Tarihi:19.01.2023).
- National Cyberspace Security Strategy, (2016), <https://chinacopyrightandmedia.wordpress.com/2016/12/27/national-cyberspace-security-strategy/>, (Eriřim Tarihi:05.04.2023).
- National Security Strategy, (2022), “National Security Strategy”, Washington: The White House, <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf>, (Eriřim Tarihi:13.01.2023).
- NAUGHTON, B., (2007), *The Chinese Economy Transitions and Growth*, Cambridge, Massachusetts: The MIT Press.
- NCSC, (2012), “National Strategy For The Protection Of Switzerland Against Cyber Risks”, https://www.enisa.europa.eu/topics/national-cyber-security-strategies/ncss-map/Switzerlands_Cyber_Security_strategy.pdf, (Eriřim Tarihi:12.12.2022).

- NEGRO, G., (2017), *The Internet in China: From Infrastructure to a Nascent Civil Society*, Palgrave Macmillan.
- New America, (2017), “Cybersecurity Law of the People’s Republic of China”, <https://www.newamerica.org/cybersecurity-initiative/digichina/blog/translation-cybersecurity-law-peoples-republic-china/>, (Erişim Tarihi:09.04.2023).
- NICKOLOV, E., (2008), Modern trends in the cyber attacks against the critical information infrastructure. Regional Cybersecurity Forum, 7-9.
- NTV, (2020), “Çin’de Halka Yasak Olan Sosyal Medya, Diplomatların Kullanımına Açıldı”, <https://www.ntv.com.tr/dunya/cinde-halka-yasak-olan-sosyal-medya-diplomatlarin-kullanimina-acildi,IAL-mOzrdU-ySjvnk79S4w>, (Erişim Tarihi:08.04.2023).
- NYE, J. S., (2014), *The Regime Complex for Managing Global Cyber Activities*. Chatham House, No 1.
- NYMAN, J., (2023), “Towards a global security studies: what can looking at China tell us about the concept of security?”, *European Journal of International Relations*, C.29, S.3, ss.673-697.
- O’SHEA, K., (2003), “Cyber Attack Investigative Tools and Technologies”, İç. HTCIA, Institute for Security Technology Studies, Hanover, NH: Dartmouth College.
- OĞUZ, M., (2021), *Stratejiden Yasaya Avrupa Birliği Siber Güvenlik Politikası (Yayımlanmamış Yüksek Lisans Tezi)*, İstanbul: Marmara Üniversitesi, Avrupa Araştırmaları Enstitüsü.
- OĞUZLU, H. T., (2007), “Dünya Düzenleri Ve Güvenlik: Ulus-Devlet Güvenlik Anlayışı Asılıyor Mu?”, *Güvenlik Stratejileri Dergisi*, Cilt 3, Sayı 6.
- OKTAY, F., (2017), *Çin: Ekonomi Ve Politika Yeni Büyük Güç Ve Değişen Dünya Dengeleri*. Türkiye İş Bankası Kültür Yayınları.
- OSKAY, Ü., (1967), *Çin Halk Cumhuriyetinin Kuruluşu*, Ankara Üniversitesi SBF Dergisi, C.22, S.4.
- OWNBY, D., (2008), *Falun Gong and the Future of China*, New York: Oxford University Press
- ÖCAL, A., (2022), *Uluslararası İlişkilerde Değişen Güvenlik Anlayışı Ve Türkiye’nin Siber Güvenlik Stratejileri (Yayımlanmamış Yüksek Lisans Tezi)*, Edirne: Trakya Üniversitesi, Sosyal Bilimler Enstitüsü.
- ÖĞÜN, M. N. ve KAYA, A., (2013), “Siber Güvenliğin Milli Güvenlik Açısından Önemi Ve Alınabilecek Tedbirler”, *Güvenlik Stratejileri Dergisi*, C. 9, S.18, ss. 145-181.
- ÖNAÇAN, Mehmet. B. K. ve ATAN, H., (2016), “Siber Güvenlikte Lisansüstü Eğitim: Deniz Harp Okulu Örneği”, *Trakya University Journal of Engineering Sciences*, C.17, S.1, ss.13-21.
- ÖNÜR, M. N., (2021), *Çin’in ABD’yi Dengeleme Girişimi: Yeni İpek Yolu Projesi (Yayımlanmamış Yüksek Lisans Tezi)*, Mersin: Çağ Üniversitesi, Sosyal Bilimler Enstitüsü.
- ÖZCAN, A. B., (2011), “Uluslararası Güvenlik Sorunları ve ABD’nin Güvenlik Stratejileri”, *SÜ İİBF Sosyal ve Ekonomik Araştırmalar Dergisi*, S.22.

- ÖZDAĞ, Ü., (2009), “Devlet ve İstihbarat”, Beykent Üniversitesi Stratejik Araştırmalar Dergisi, C.1, S.3, ss.34.
- ÖZDAL, B. ve UĞUR, E., (2013), “Martin C. Libicki’nin “Siber Caydırıcılık” Kavramının Nükleer Caydırıcılık Olgusu İle Karşılaştırılmalı Analizi”, 6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı.
- ÖZDEMİR, Ö., (2022), Çin Halk Cumhuriyeti’nin Türkiye’ye Yönelik Kamu Diplomasi Faaliyetleri (Yayımlanmamış Yüksek Lisans Tezi), Ankara: Hacı Bayram Veli Üniversitesi, Lisansüstü Eğitim Enstitüsü.
- ÖZSOYLU, A. F., (2006), Çin: Bir Devrin Uyanışı, Adana: Nobel Kitabevi.
- ÖZTÜRK, Z. A., (2014), “Uluslararası İlişkilerde Güvenliği Yeniden Düşünmek: Geleneksel ve Alternatif Yaklaşımlar”, (Edt.: Tayyar ARI), Uluslararası İlişkiler Teorileri-2, Bursa: Dora Yayınları, ss.149-178.
- PAJUNEN, N., (2017), Overview Of MaritimeCybersecurity, South Eastern Finland University, ss.21.
- PATTON, D. E., (2016), Evaluating U.S. and Chinese Cyber Security Strategies Within a Cultural Framework (Yayımlanmamış Yüksek Lisans Tezi), Alabama: Air Command and Staff College Air University.
- PEIRAN, W., (2012), “China's Perceptions of Cybersecurity”, Georgetown Journal of International.
- PEKCAN, C., (2020), “Çin Halk Cumhuriyeti’nin Siber Güvenlik Politikası”, (Edt: F. Köksoy), Yeni Küresel Tehdit Siber Saldırıları: Siber Güvenlik ve Politika Uygulamaları, Ankara: Nobel Akademik Yayıncılık, ss.205-225.
- People’s Daily, (2011), “Why China Established Online ‘Blue Army’?”, China.org.cn, http://www.china.org.cn/opinion/2011-06/29/content_22881772.htm, (Erişim Tarihi:27.04.2023).
- POH, A. ve Lİ, M., (2017), A China in Transition: The Rhetoric and Substance of Chinese Foreign Policy Under Xi Jinping, Asian Security, C.13, S.2, ss.84-97.
- PONNIAH, K. ve MARINKOVIC, L., (2019), “The Night The US Bombed A Chinese Embassy”, BBC News, <https://www.bbc.com/news/world-europe-48134881>, (Erişim Tarihi:13.02.2023).
- Population, (2024), “Population of People's Republic of China as of Today”, <https://populationtoday.com/cn-china/>, (Erişim Tarihi:04.04.2024).
- PRADT, T., (2016), China’s New Foreign Policy, London: Palgrave Macmillan.
- PU, G., (2015), Deng Xiaoping Çağdaş Çin’in Mimarı: Biyografisi ve Görüşleri, (Çev.: D. Kızılçeç), İstanbul: Canut Yayınevi, ss. 607.
- QIMAO, C., (2005), “Çin’in Güvenlik Anlayışı ve Politikası”, (Edt.: A. Sandıklı ve İ. Güllü), Geleceğin Süper Gücü Çin, İstanbul: Tasam Yayınları, ss. 7.
- QINGMIN, Z., (2003), “Dış Politika Analizinde Kültürel Faktörlerin Rolü ve Yeri”, Uluslararası Forumu, C.5, S.4, ss.36-38.
- QIU, J. L., (2003), The Internet in China: Data and Issues, Working Paper Prepared for Annenberg Research Seminar on International Communication conference “China and the Internet: Technology, Economy, and Society in Transition” May 30-31, held by USC, Annenberg School in Los Angeles.

- RASKA, M., (2015), "Revealed: The New Battleground in China's Future Wars", The National Interest, <http://nationalinterest.org/feature/revealed-the-battlegroundchinas-next-war-123>, (Eriřim Tarihi:02.04.2023).
- RAUD, M., (2016), "China and Cyber: Attitudes, Strategies and Organisation", Tallinn: The NATO Cooperative Cyber Defence Centre of Excellence, <https://ccdc.org/library/publications/china-and-cyber-attitudes-strategies-organisation/>, (Eriřim Tarihi:19.04.2023).
- ReedSmith, (2018), "China's Cyber Security Law", <https://www.reedsmith.com/en/perspectives/2018/01/chinas-cybersecurity-law>, (Eriřim Tarihi:05.04.2023).
- Renminwang, (2019), "Xi Jinping'in Yeni Ulusal Gvenlik Konsepti ve Asya Yeni Gvenlik Konseptinin Analizi/ 解析习近平新国家安全观 与亚洲新安全观", <http://world.people.com.cn/GB/8212/191606/385673>, (Eriřim Tarihi:11.11.2023).
- RICHELSON, J. T., (2013), "The Snowden Affair", The National Security Archive, <https://nsarchive2.gwu.edu/NSAEBB/NSAEBB436/>, (Eriřim Tarihi:19.04.2023).
- RID, T. ve PETER, M., (2012), "Cyber-Weapons", The RUSI Journal, C.157, S.1.
- ROZMAN, G., (2017), "China's Quest For Great Power Identity", (Edt.: G. Liu), Chinese Foreign Policy in Transition, New York: Routledge, ss. 119-140.
- Russian Federation, (2013), "Concept of the Foreign Policy of the Russian Federation", https://thailand.mid.ru/en/o_rossii/vneshnyaya_politika/kontseptsiya_vneshney_politiki_rf/, (Eriřim Tarihi: 16.01.2023).
- Russian Federation, (2016), "Doctrine of Information Security of the Russian Federation", http://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163, (Eriřim Tarihi:16.01.2023).
- SAĐIROĐLU, ř., (2011), "Siber Gvenlik ve Trkiye", Siber Gvenlik alıřtayı, Ankara.
- SAĐIROĐLU, ř., (2018), "Siber Gvenlik ve Savunma: nem, Tanımlar, Unsurlar ve nlemler", (Edt.: řeref S. ve Mustafa A.), Siber Gvenlik ve Savunma Farkındalık ve Caydırıcılık, Ankara: Grafiker Yayınları.
- SANCHEZ, R., (2014), "China hacking charges: the Chinese army's Unit 61398", The Telegraph, <http://www.telegraph.co.uk/news/worldnews/asia/china/10842093/China-hackingcharges-the-Chinese-armys-Unit-61398.html>, (Eriřim Tarihi:02.04.2023).
- SANDER, O., (1966), "Khrushchev'den Sonra Sovyetler BirliĐi Komnist in İliřkileri", Ankara niversitesi Sosyal Bilimler Fakltesi Dergisi, Cilt 21, Sayı 3.
- SANDER, O., (1989), "Siyasi Tarih 1918-1994", İmge Kitapevi Yayınları, C. 13.
- SANDER, O., (2013), Siyasi Tarih İlkaĐlardan 1918'e, Ankara: İmge Kitapevi.

- SANDIKLI, A. ve EMEKLİER, B., (2011), Güvenlik Yaklaşımlarında Değişim ve Dönüşüm, BİLGESAM.
- SANGER, D. ve PERLROTH, N., (2020), “U.S. to Accuse China of Trying to Hack Vaccine Data as Virus Redirects Cyberattacks”, New York Times, <https://www.nytimes.com/2020/05/10/us/politics/coronavirus-china-cyber-hacking.html>, (Erişim Tarihi:01.05.2023).
- SARAY, M. O. ve GÖKDEMİR, L., (2007), Çin Ekonomisinin Büyüme Aşamaları, Journal Of Yaşar University, C.2, S.7, ss.681-686.
- SAVÇIN, E., (2020), Devletlerin Siber Güvenlik Politikalarının Şekillendirilmesi Sürecinde Kamu-Özel Sektör İşbirliğinin Artan Önemi: İsrail Ve Yeni Zelanda Örnekleri (Yayımlanmamış Yüksek Lisans Tezi), Yalova: Yalova Üniversitesi, Sosyal Bilimler Enstitüsü.
- SAYIN, Y., (2013), “Konfüçyüs’ün Yeniden Keşfi ve Çin’in Dış Politikasında Dönüşüm”, Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi, S.29, ss.223-237.
- SCOBELL, A. vd., (2018), At the Dawn of Belt and Road: China in the Developing World, RAND, Santa Monica.
- SEGAL, A., (2015), “What to Do About China’s New Cybersecurity Regulations?”, <https://www.cfr.org/blog/what-do-about-chinas-new-cybersecurity-regulations>, (Erişim Tarihi:03.04.2023).
- SEGAL, A., (2017), “Chinese Cyber Diplomacy in a New Era of Uncertainty”, Aegis Paper Series No: 1703, Stanford: Hoover Institution.
- SENGUPTA, D. ve MANKOTIA, A.S., (2020), “India Steps Up Vigil For Cyber Attacks From China After Apps Ban”, The Economic Times, July 21, <https://telecom.economictimes.indiatimes.com/news/india-steps-up-vigil-for-cyber-attacks-from-china-after-apps-ban/76710514>, (Erişim Tarihi:29.04.2023).
- SEREN, M., (2018), “ABD Ulusal Güvenlik Strateji Belgesi: Amerikan Savunması ve Caydırıcılığı”, <https://thinktech.stm.com.tr/tr/abd-ulusal-guvenlik-strateji-belgesi-amerikan-savunmasi-ve-caydiriciligi>, (Erişim Tarihi: 16.12.2022).
- SEVDA, K., (2018), Siber Uzayda Uluslararası İlişkilerin Değişen Parametreler (Yayımlanmamış Yüksek Lisans Tezi), Konya: Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü.
- SHAMBAUGH, D., (2020), “China’s Long March To Global Power”, (Edt: D. Shamb), China and the World, New York: Oxford University Press, ss.3-24.
- SHEN, F., (2014), “Great Firewall of China”, (Edt: K. Harvey), Encyclopedia of Social Media and Politics, SAGE, C.2, ss. 599-602.
- SHIKANG, B., (2013), “Yeni Liderlik, Genel Diplomaside Yeni Bir Durum Yarattı Ve "Halk İçin Diploması" Kavramını Vurguladı”, <https://news.12371.cn/2013/07/25/ARTI1374705129819922.shtml?from=groupmessage>, (Erişim Tarihi:09.07.2023).
- SINGER, P. W. ve FRIEDMAN, A., (2018), Siber Güvenlik ve Siber Savaş, Ankara: Buzdağı.

- SINGH, N., (2020), “Rise In Cyber Attacks From China, Over 40,000 Cases In 5 Days: Maharashtra Cyber Dept”, The Logical Indian, <https://thelogicalindian.com/news/cyber-attacks-india-china-21877?infinitescroll=1>, (Eriřim Tarihi:29.04.2023).
- SİBER BÜLTEN, (2020), “İngiltere, 10 Milyon Sterlini Siber Güvenlik İçin Hibe Etti”, <https://siberbulten.com/uluslararası-iliskiler/ingiltere/ingiltere-10-milyon-sterlini-siber-guvenlik-icin-hibe-etti/>, (Eriřim Tarihi:19.01.2023).
- SİNGER, P.W. ve FRIEDMAN, A., (2014), Cybersecurity and Cyberwar, New York: Oxford University Press.
- Sizhengwang.cn, (2021), “Bağımsız bir dış politika geliştirme düşüncesi”, https://www.sizhengwang.cn/a/xbpjs_ssjjy/210421/840322.shtml, (Eriřim Tarihi:02.07.2023).
- SOLMS, V. ve NIEKERK, V., (2013), From Information security to Cyber Security, Computers & Security 38, ss.97-102.
- SÖNMEZOĞLU, F., (2002), Uluslararası İliřkilere Giriř. İstanbul: Der Yayınları.
- SPADE, C. J. M., (2012), “Information as Power: China’s Cyber Power and America’s National Security”, (Edt.: Jeffrey L. Caton), United States Army War College, ss. 4.
- Statista, (2020), “Proposed Budget Of The U.S. Government For Cyber Security İn FY 2017 To 2021(İn Billion U.S. Dollars)”, <https://www.statista.com/statistics/675399/us-government-spending-cyber-security/>, (Eriřim Tarihi:01.05.2023).
- STEVENS, T., (2010), “Breaching Protocol: The Threat of Cyberespionage”, Academia.edu, http://www.academia.edu/1158361/Breaching_Protocol_The_Threat_of_Cyberespionage, (Eriřim Tarihi:16.04.2023).
- SUYIN, H., (1995), Sabah Tufanı 2, İstanbul: Berfin Yayınları.
- SWAINE, M. D., (2013), “Chinese Views on Cybersecurity in Foreign Relations”, China Leadership Monitor, ss.1-27.
- SWEENEY, J. ve VULLIAMY, E., (1999), “Nato Bombed Chinese Deliberately”, The Guardian, <https://www.theguardian.com/world/1999/oct/17/balkans>, (Eriřim Tarihi:13.02.2023).
- ŞAHİN, B., (2020), “Değişen Dünya Düzenine Bağlı Olarak Değişen Uluslararası Güvenlik Algısı”, İmgelem Dergisi, C.4, S.6.
- ŞEN, U. B., (2021), “Rekabetçi Bir Çağda Küresel Britanya Strateji Belgesi Üzerine Değerlendirmeler”, <https://sahipkiran.org/2021/04/16/rekabetci-bir-cagda-kuresel-britanya-strateji-belgesi-uzerine-degerlendirmeler/>, (Eriřim Tarihi:19.01.2023).
- ŞENOL, M., (2018), “Hibrit Savaş Kapsamında Siber Savaş ve Siber Caydırıcılık”, (Edt.: Şeref S. ve Mustafa A.), Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık, Ankara: Grafiker Yayınları.

- TANRIVERDİ, Ç., (2020), “En Güçlü Siber Güvenliğe Sahip Ülkeler Açıklandı: Türkiye Ne Durumda?”, WebTekno, <https://www.webtekno.com/siber-guvenlik-en-guclu-ulkeler-h100650.html>, (Erişim Tarihi:04.04.2024).
- TATAR, Ü., (2011), “Sosyal Mühendislik Saldırıları”, TÜBİTAK, BİLGEM, 4. Ağ ve Bilgi Güvenliği Sempozyumu, http://www.emo.org.tr/ekler/288230da37dbf3c_ek.pdf, (Erişim Tarihi: 25.12.2022).
- TAVUKÇU, S., (2021), “ABD’nin Geçici Ulusal Güvenlik Strateji Rehberi: Kırılan Vazoyu Yapıştırmaya Çalışmak”, <https://www.sde.org.tr/sinan-tavukcu/genel/abd-nin-gecici-ulusal-guvenlik-strateji-rehberi-kirilan-vazoyu-yapistirmaya-calismak-kose-yazisi-21615>, (Erişim Tarihi:13.01.2023).
- TDK, Türk Dil Kurumu Online Sözlüğü, Caydırıcılık Nedir?, <https://sozluk.gov.tr/>, (Erişim Tarihi:02.01.2023).
- Techopedia, (2019), “Cyberattack”, <https://www.techopedia.com/definition/24748/cyberattack>, (Erişim Tarihi:26.04.2023).
- TGRT Haber, (2022), “Çin’den Tayvan’a Siber Saldırı: Resmi Kurumlar Hedef Alındı”, <https://www.tgrthaber.com.tr/dunya/cinden-tayvana-siber-saldiri-resmi-kurumlar-hedef-alindi-2841973>, (Erişim Tarihi:29.04.2023).
- The Guardian, (2020), “Mike Pompeo Blasts China's 'Coercion' Of Australia As Cyber-Attack Likened To Parliament House Hack”, <https://www.theguardian.com/world/2020/jun/20/mike-pompeo-blasts-chinas-coercion-of-australia-as-cyber-attack-likened-to-parliament-house-hack>, (Erişim Tarihi:28.04.2023).
- THE SECRETARY OF DEFENSE, (2015), “The Department of Defense Cyber Strategy”, Washington D.C.
- The UK cyber security strategy 2011-2016: Annual Report, (April,2016), Londra: Kabine Ofisi, https://assets.publishing.service.gov.uk/government/uploads/system/uploads/attachment_data/file/516331/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf, (Erişim Tarihi:19.01.2023).
- The UK Cyber Security Strategy, (2011, November), “The UK Cyber Security Strategy: Protecting and Promoting the UK in a Digital World”, Londra: Kabine Ofisi, https://www.gov.uk/government/uploads/system/uploads/attachment_data/file/60961/uk-cyber-security-strategy-final.pdf, (Erişim Tarihi:19.01.2023).
- THOMAS, T., (2004), “Russian and Chinese Information Warfare: Theory and Practice”, http://dodccrp.org/events/2004_CCRTS/CD/presentations/064.pdf, (Erişim Tarihi:28.03.2023).
- THORNBURGH, T., (2004), “Social Engineering: The “Dark Art”, Proceedings of the 1st annual conference on Information security curriculum development, Acm., Kennesaw, ss. 133-135.
- TODD, G. H., (2009), “Armed Attack in Cyberspace: Deterring Asymmetric Warfare with an Asymmetric Definition”, The Air Force Law Review, ss.65-102.

- TOKDAŞ, A., (2018), Siber Güvenlik Ve Uluslararası İlişkiler (Yayımlanmamış Yüksek Lisans Tezi), Konya: Selçuk Üniversitesi, Sosyal Bilimler Enstitüsü.
- TOKLU, V., (2004), Uluslararası İlişkiler, Ankara: İmaj Yayınevi.
- TOSUN, T. T., (2014), Çin Ekonomisinin Gelişiminin İncelenmesi Ve Çin Ekonomisinin Türk Dış Ticaretine Başlıca Etkileri (Yüksek Lisans Tezi, Sosyal Bilimler Enstitüsü), <https://acikbilim.yok.gov.tr/handle/20.500.12812/673408>, (Erişim Tarihi: 21.04.2023).
- TOSUN, T. T., (2015), Dragon'un Dönüşü: Çin, Ankara: Gece Kitaplığı.
- TURHAN, O., (2006), Bilgisayar Ağları ile İlgili Suçlar (Siber Suçlar) (Yayımlanmamış Planlama Uzmanlığı Tezi), Ankara: T.C. Başbakanlık Devlet Planlama Teşkilatı Müsteşarlığı Hukuk Müşavirliği.
- U.S. Department Of Defense, (2011), "Strategy for Operating in Cyberspace", Washington D. C.: Retrieved from, <http://csrc.nist.gov/groups/SMA/ispab/documents/DOD-Strategy-for-Operatingin-Cyberspace.pdf>, (Erişim Tarihi:12.01.2023).
- UDHB, (2016), "Ulusal Siber Güvenlik Stratejisi", T.C. Ulaştırma Denizcilik ve Haberleşme Bakanlığı, <https://hgm.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf>, (Erişim Tarihi: 11.12.2022).
- ULUTAŞ, G., (2018), "Siber Güvenlik", Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık, (Edt.: Şeref S., Mustafa A.), Ankara: Grafiker Yayınları.
- UN Resolution 2758, (1971), "Restoration of the Lawfull Rights of the People's Republic of China in the United Nations", <https://china.usc.edu/sites/default/files/article/attachments/1971-UN-China-seating.pdf>, (Erişim Tarihi:29.04.2023).
- United States Government, (2003), "The National Strategy to Secure Cyberspace", Washington D.C.: The White House Retrieved from, https://www.us-cert.gov/sites/default/files/publications/cyberspace_strategy.pdf, (Erişim Tarihi:12.01.2023).
- United States Government, (2009), "Cyberspace Policy Review: Assuring a Trusted and Resilient Information and Communications Infrastructure", Washington D.C.: The White House Retrieved from, https://www.whitehouse.gov/assets/documents/Cyberspace_Policy_Review_final.pdf, (Erişim Tarihi:12.01.2023).
- United States Government, (2011), "International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World", Washington D.C.: The White House Retrieved from, http://www.whitehouse.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf, (Erişim Tarihi:12.01.2023).
- United States Government, (2015), "National Security Strategy", Washington D.C.: The White House Retrieved from, https://www.whitehouse.gov/sites/default/files/docs/2015_national_security_strategy.pdf, (Erişim Traihi:12.01.2023).
- United Nations, (t.y.), "Comprehensive Nuclear-Test-Ban Treaty (CTBT)", <https://disarmament.unoda.org/wmd/nuclear/ctbt/>, (Erişim Tarihi:17.07.2023).

- US-DoD (2009), “Military Power of the People’s Republic of China 2009: Annual Report to Congress”, <https://www.ssri-j.com/MediaReport/DocumentUS/ChinaMilPower/MilPowerOfPRC2009.pdf>, (Erişim Tarihi:02.04.2023).
- USNI News, (2015), “China’s Military Strategy”, <https://news.usni.org/2015/05/26/document-chinas-military-strategy>, (Erişim Tarihi:04.03.2023).
- USOM (Ulusal Siber Olaylara Müdahale Merkezi), (2014), “Siber Güvenliğe İlişkin Temel Bilgiler”, <https://www.usom.gov.tr/dosya/1418807122-USOM-SGFF-001-Siber%20Guvenlige%20Giris%20ve%20Temel%20Kavramlar.pdf>, (Erişim Tarihi: 13.11.2022).
- ÜNAL, T., (2011), “Sosyal Mühendislik Saldırıları”, TÜBİTAK, BİLGEM, 4. Ağ ve Bilgi Güvenliği Sempozyumu, http://www.emo.org.tr/ekler/288230da37dbf3c_ek.pdf, (Erişim Tarihi: 22.12.2022).
- VALENTINO, J. ve YADRON, D., (2015), “Cataloging the World’s Cyberforces”, The Wall Street Journal, <https://www.wsj.com/articles/cataloging-the-worlds-cyberforces-1444610710?tesla=y>, (Erişim Tarihi:19.04.2023).
- VARLIK, E., (2014), “Çin Hong Kong Protestocularını Mobilden Vurdu!”, Siber Bülten, <https://siberbulten.com/siber-guvenlik/cin-hong-kong-protestocularini-mobilden-vurdu/>, (Erişim Tarihi:30.04.2023).
- VARLIK, E., (2015), “Çin Yeni Askeri Stratejisini Açıkladı: Stratejide Savunma, Operasyonda Saldırı”, Siber Bülten, <https://siberbulten.com/uncategorized/cin-yeni-askeri-stratejisini-acikladi-stratejide-savunma-operasyonda-saldiri/>, (Erişim Tarihi:03.04.2023).
- VARLIK, E., (2015), “Çin, ABD’li Şirketlerden İntikamını Aldı”, Siber Bülten, <https://siberbulten.com/uluslararası-iliskiler/cin-abdli-sirketlerden-intikamini-aldi/>, (Erişim Tarihi:01.05.2023).
- VASQUEZ, C., (2023), “Biden’s Budget Seeks Increase In Cybersecurity Spending”, Cyberscoop, <https://cyberscoop.com/biden-budget-2023/>, (Erişim Tarihi:01.05.2023).
- VENTRE, D., (2010), “China’s Strategy for Information Warfare: A Focus on Energy”, Journal of Energy Security, http://www.ensec.org/index.php?Itemid=361&catid=106:energysecuritycontent0510&id=241:critical-energy-infrastructure-security-and-chinese-cyber-threats&option=com_content&view=article, (Erişim Tarihi:02.04.2023).
- VERMA, A., (2012), “Internet in China: An Emergin Society”, Institute of Peace and Conflict Studies (IPCS), S. April.
- VOGEL, E., (2017), Deng Xiaoping Ve Çin’in Dönüşümü, (Çev.: M. Leliç). İstanbul: Modus Kitap.
- WAGNER, J., (2017), “China’s Cybersecurity Law: What You Need to Know”, The Diplomat, <https://thediplomat.com/2017/06/chinas-cybersecurity-law-what-you-need-to-know/>, (Erişim Tarihi:09.04.2023).

- WANG, S., (2017), "Xi Jinping's Centralisation of Chinese Foreign Policy Decision Making Power", *East Asian Policy*, C. 9, S. 2, ss. 34-42.
- WATSS, J., (2011), "Gmail Hack: Phishing Finger Pointed At China's Lanxiang Vocational School", *The Guardian*, <https://www.theguardian.com/technology/2011/jun/02/chinese-school-implicated-cyber-attacks>, (Eriřim Tarihi:19.04.2023).
- WEDERMYER, L. J., (2012), "The Changing Face of War: The Stuxnet Virus and the Need for International Regulation of Cyber Conflict", <https://www.law.msu.edu/king/2011-2012/Wedermeyer.pdf>, (Eriřim Tarihi:02.04.2023).
- WEIMANN, G., (2004), "Cyber- Terrorism, How Real Is The Treat? United States Institu of Peace, Special Report 119, Washighton D.C.
- WEIMIN, W., (2007), *The Beauty of Physics*, World Scientific Publishing.
- WELLS, H. G., (2020), *Tüm Savaşları Bitirecek Savaş*, İstanbul: İthaki Yayınları.
- WESTAD, O., (2013), *Restless Empire China And The World Since 1750*, London: Vintage Books.
- WHITTLE, B. D., (1996), *Cyberspace: The Human Dimension*, New York: W. H. Freeman & Co.
- WIENER, N., (1965), "Cybernetics, Second Edition: or the Control and Communication in Animal and the Machine", Cambridge: The MIT Press.
- WILLIAMS, P. D., (2013), *Security Studies: An Introduction 2nd Edition*, New York: Routledge,
- WILLS, D.B. ve ASHENDEN, D., (2012), "Securing Virtual Space: Cyber War, Cyber Terror, and Risk", *Space and Culture*, C.15, S.2, ss. 111.
- WOLFERS, A., (1952), "'National Security' As An Ambiguous Symbol", *Political Science Quarterly*, C.67, S.4.
- World Nuclear Association, (2023), "China: Nuclear Power", <https://www.worldnuclear.org/information-library/country-profiles/countries-a-f/china-nuclear-power.aspx>, (Eriřim Tarihi:17.07.2023).
- Worldometer, (2020), "Coronavirus Cases", <https://www.worldometers.info/coronavirus/>, (Eriřim Tarihi:01.05.2023).
- WU, B., (2001), "The Chinese Security Concept and its Historical Evolution", *Journal of Contemporary China*, C.10, S.20, ss. 275-283.
- XI, J., (2014), "New Asian Security Concept For New Progress in Security Cooperation" (Remarks at the Fourth Summit of the Conference on Interaction andConfidence Building Measures in Asia), Shanghai Expo Center, https://www.fmprc.gov.cn/mfa_eng/zxxx_662805/t1159951.shtml, (Eriřim Tarihi:03.11.2023).
- XI, J., (2014), *The Governance of China*, Beijing: Foreign Languages Press.
- XI, J., (2018), *Secure a Decisive Victory in Building a Moderately Prosperous Society in All Respects and Strive for the Great Success of Socialism with Chinese Characteristics for a New Era: Report to the 19th National Congress of the Communist Party of China*, 18 October 2017, Beijing: Foreign Languages Press.

- XIAO, R. vd., (2003), “İdeoloji ve dış politika”, Dünya Ekonomisi ve Politikası, S. 2, ss.5-7.
- XIAOPING, D., (1994)., International situations and economic problems, 3 March 1990. Selected Works of Deng Xiaoping. Cilt III. Beijing: Foreign Languages Press.
- Xi, J., (2015), “Remarks by H.E. Xi Jinping President of the People's Republic of China At the Opening Ceremony of the Second World Internet Conference”, Ministry of Foreign Affairs of the People's Republic of China, https://www.mfa.gov.cn/eng/wjdt_665385/zyjh_665391/201512/t20151224_678467.html, (Erişim Tarihi:03.04.2023).
- Xinhua Haber Ajansı, (2014), “Xi Jinping, Merkez Dış İlişkiler Çalışma Toplantısı'na Katıldı ve Önemli Bir Konuşma Yaptı/习近平出席中央外事工作会议并发表重要讲话”, http://www.xinhuanet.com/politics/2014-11/29/c_1113457723.htm, (Erişim Tarihi:12.10.2023).
- Xinhua Haber Ajansı, (2017), “Pekin'de Kuşak ve Yol Güvenliği İşbirliği Diyalogu düzenlendi ve Meng Jianzhu heyet başkanı ile bir araya geldi/“一带一路”安全合作对话会在京举行 孟建柱会见代表团团长, http://www.xinhuanet.com/politics/2017-05/04/c_1120919833.htm, (Erişim Tarihi:29.10.2023).
- Xinhua Haber Ajansı, (2018), “Xi Jinping: Kapsamlı Ulusal Güvenlik Görüşünü Geniş Bir Şekilde Uygulayarak Yeni Dönem Ulusal Güvenlik Hizmetinde Yeni Manzara Yaratalım/习近平：全面贯彻落实总体国家安全观 开创新时代国家安全工作新局面”, www.cac.gov.cn/2018-04/17/c_1122697770.htm, (Erişim Tarihi:14.11.2023).
- Xinhua News, (2019), “China to lead global cybersecurity market growth in next 5 years”, http://www.xinhuanet.com/english/2019-09/09/c_138377152.htm, (Erişim Tarihi:01.05.2023).
- Xinhua, (2023), “White Paper: China Targets Mobile Apps To Protect Personal Information”, The State Council Information Office of the People's Republic of China, http://english.scio.gov.cn/whitepapers/2023-03/16/content_85173059.htm, (Erişim Tarihi:07.04.2023).
- YALMAN, Y., (2018), “Siber Terör, Terörizm ve Mücadele”, (Edt.: Şeref S. ve Mustafa A.), Siber Güvenlik ve Savunma Farkındalık ve Caydırıcılık, Ankara: Grafiker Yayınları.
- YANG, D. L., (1996), Calamity and Reform in China: State, Rural Society, and Institutional Change Since the Great Leap Famine, Stanford: Stanford University Press.
- YANGYUE, L., (2015), “The Conceptual Underpinning of Cyber Security Studies”, Massachusetts Institute of Technology (MIT), Research Paper, S.2016-2, ss.17-18.
- YAYLA, M., (2013), “Hukuki Bir Terim Olarak ‘Siber Savaş’”, TBB Dergisi, C.2013, S.104, ss.177-202.

- YAYLA, M., (2014), “Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı”, Ankara: Hacettepe HFD, C.4, S.2.
- YAZICI, A., (2011), “Güvenli Bilgi Paylaşımı ve SAHAB ”, <https://docplayer.biz.tr/11784157-Aselsan-guvenli-bilgi-paylasimi-ve-sahab-aselsan-ali-yazici-turk-silahl-kuvvetlerini-guclendirme-vakfi-nin-bir-azerbaycan-temmuz-kurulusudur.html>, (Erişim Tarihi:11.01.2023).
- YENER, Y., (2015), “Gelmiş Geçmiş En Geniş Çaplı Siber Saldırı: Shady RAT”, Siber Bülten, <https://siberbulten.com/makale-analiz/gelmis-gecmis-en-genis-capli-siber-saldiri-shady-rat/>, (Erişim Tarihi:28.04.2023).
- YENER, Z., (2013), Siber Uzay Güvenliği: Ulusal Güvenlik ve Uluslararası Güvenliğe Etkileri (Yayımlanmamış Yüksek Lisans Tezi), Bursa: Uludağ Üniversitesi, Sosyal Bilimler Enstitüsü.
- Yeni Medya, (2017), “Çin’in Büyük Güvenlik Duvarı: Sansürde 21 Yıl”, <https://yenimedya.wordpress.com/tag/buyuk-guvenlik-duvari/>, (Erişim Tarihi:14.04.2023).
- YEŞİLYURT, H., (2015), “Ulusal Güvenlik Perspektifinde Siber Güvenlik”, (Edt.: Fatih Tombul ve diğerleri), Siber Suçlar, Tehditler, Farkındalık ve Mücadele içinde (169- 193), Ankara: Global Politika ve Strateji.
- YICAI, (2022), “China’s Spending on Cybersecurity to Nearly Triple in Five Years, IDC Says”, <https://www.yicaiglobal.com/news/china-spending-on-cybersecurity-to-nearly-triple-in-five-years-idc-says>, (Erişim Tarihi:01.05.2023).
- YIKICI, İ., (2020), Siber Teknolojilere Dayalı Yeni Uluslararası Güvenlik Konsepti Bağlamında Türkiye’nin Siber Güvenlik Stratejisi (Yayımlanmamış Yüksek Lisans Tezi), Diyarbakır: Dicle Üniversitesi, Sosyal Bilimler Enstitüsü.
- YILDIRIM, E. Y., (2018), “Bilişim Sistemlerine Yönelik Siber Saldırıları ve Siber Güvenliğin Sağlanması”, Mesleki Bilimler Dergisi, C.7, S.2, ss.24-33.
- YILDIRIM, N. E., (2017), “Çin Dış Politikasında İttifak Yapmama Prensipleri: Akademik Tartışmalar”, Savunma Bilimleri Dergisi, C.16, S.2, ss.15-35.
- YILMAZ, O., (2017), “Küreselleşme Sürecinde Dönüşen Güvenlik Algısı ve Siber Güvenlik”, Dergi Park Akademik, C.2, S.4, ss. 25-27.
- YILMAZ, O., (2020), Güvenlik Paradigmasının Değişimi; ABD ve Rusya Rekabetinin Siber Alanda Tezahürü (Yayımlanmamış Yüksek Lisans Tezi), Kocaeli: Kocaeli Üniversitesi, Sosyal Bilimler Enstitüsü.
- YILMAZ, O., (2020), Güvenlik Paradigmasının Değişimi; ABD Ve Rusya Rekabetinin Siber Alanda Tezahürü (Yayımlanmamış Yüksek Lisans Tezi), Kocaeli: Kocaeli Üniversitesi, Sosyal Bilimler Enstitüsü.
- YILMAZ, S. ve SAĞIROĞLU, Ş., (2013), “Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri”, 6. International Information Security & Cryptology Conference, Ankara.
- YILMAZ, S. ve SALCAN, O., (2008), Siber Uzay’da Güvenlik ve Türkiye, 1, İstanbul: Milenyum Yayınları.

- Yİ, G., (2004), “Yeni Dönemde Deng Xiaoping'in Diplomatik Strateji Düşünceleri Üzerine”, <http://news.sina.com.cn/c/2004-07-29/15483862728.shtml>, (Erişim Tarihi:05.07.2023).
- ZEMIN, J., (2002), “Full Text Of Jiang Zemin's Report At 16th Party Congress On Nov 8, 2002”, http://bg.china-embassy.gov.cn/eng/zgzt/zggcddslcsgdbdh/200406/t20040613_2368896.htm, (Erişim Tarihi:14.02.2023).
- ZHANG, J., (2015), “China’s New Foreign Policy under Xi Jinping: Towards ‘Peaceful Rise 2.0’?”, *Global Change, Peace & Security*, C. 27, S. 1, ss. 5-19.
- ZHANG, L., (2012), “A Chinese Perspective On Cyber War”, *International Review of the Red Cross*, C.94, S.886, ss. 801-807.
- ZHANG, Q., (2015), “Xi Jinping’in Genel Ulusal Güvenlik Konsepti Üzerine/习近平谈总体国家安全观”, “中国军网” (Zhongguo Junwang), www.81.cn/jmywyl/2015-08/04/content_6614793.htm, (Erişim Tarihi:13.05.2023).
- ZHAO, L. ve XIA, L., (2018), “China’s Cybersecurity Law: An Introduction for Foreign Businesspeople”, *China Briefing*, <https://www.china-briefing.com/news/chinas-cybersecurity-law-an-introduction-for-foreign-businesspeople/>, (Erişim Tarihi:13.04.2023).
- ZHAO, Q., (2017), “Chinese Foreign Policy In The Post-Cold War Era”, (Edt: G. Liu), *Chinese Foreign Policy in Transtion*, New York: Routledge, ss. 295-322.
- ZHAO, S., (2010), “The China Model: Can It Replace the Western Model of Modernization?”, *Journal of Contemporary China*, C. 19, S. 65.
- ZHONG, G., (2017), “Genel Sekreter Xi Jinping’in Genel Ulusal Güvenlik Konseptinin Rehberliğinde Ulusal Güvenlik Alanında Yeni Bir Sayfa Açmak/以习近平总书记总体国家安全观为指引 谱写国家安全新篇章”, “求是” (Qiuxi), http://www.qstheory.cn/dukan/qs/2017-04/15/c_1120788993.htm, (Erişim Tarihi:14.11.2023).
- ZHU, L., (2010), *China’s Foreign Policy Debates*, Paris: European Union Institute for Security Studies.
- ZHU, T., (2001), “Nationalism and Chinese Foreign Policy”, *The China Review*, S.1, ss.1-27.
- ZHU, Z., (2013), “Foreign Policy Of The People’s Republic Of China”, (Edt: R. K. Beasley v.d.), *Foreign Policy in Comprarative Perspective*, California: CQ Press, ss.118-137.
- 24 Radyo, (2024), “Çin’de İnternet Kullanıcılarının Sayısı 2023’tte 1 Milyar 90 Milyona Ulaştı”, <https://www.yirmidort.tv/dunya/cinde-internet-kullanicilarinin-sayisi-2023te-1-milyar-90-milyona-ulasti-167968>, (Erişim Tarihi:04.04.2024).

ÖZGEÇMİŞ

KİŞİSEL BİLGİLER

Adı Soyadı : Zelal ÇAĞLIN
 Uyruğu : T.C.
 Doğum Yeri ve Tarih : Mersin/11.02.1995

EĞİTİM

Derece	Adı, İl	Bitirme Yılı
Lise	: Salim Yılmaz Anadolu Lisesi- Mersin	2009-2013
Üniversite	: Batman Üniversitesi-Siyaset Bilimi ve Kamu Yönetimi	2015-2019
Yüksek Lisans:	Batman Üniversitesi-Siyaset Bilimi ve Uluslararası İlişkiler	2021-2024
	Tezli Yüksek Lisans	

İŞ DENEYİMLERİ

Yıl	Kurum	Görevi
2022-2022	Stratejik Düşünce Enstitüsü-Ankara	Stajyer Asistan
2019-2020	Piri Reis Mesleki ve Teknik Anadolu Lisesi-Batman	Stajyer Öğretmen

YABANCI DİLLER

İngilizce

YAYINLAR

ICEPHSS'22: "Bölgesel Kalkınma Politikalarındaki Dönüşümler; Türkiye Örneği"