İSTANBUL TİCARET
ÜNİVERSİTESİ

T.C

İSTANBUL TİCARET ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER

ANABİLİM DALI

SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER

YÜKSEK LİSANS PROGRAMI

21'İNCİ YÜZYILIN YÜKSELEN GÜÇ UNSURU SİBER GÜÇ VE TÜRKİYE

Yüksek Lisans Tezi

Osman GİRGİN

200007095

İstanbul, Mayıs 2020

İSTANBUL TİCARET
ÜNİVERSİTESİ

T.C

İSTANBUL TİCARET ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER

ANABİLİM DALI

SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER

YÜKSEK LİSANS PROGRAMI

21'İNCİ YÜZYILIN YÜKSELEN GÜÇ UNSURU SİBER GÜÇ VE TÜRKİYE

Yüksek Lisans Tezi

Osman GİRGİN

200007095

Danışman: Dr. Öğr. Üyesi Ayfer GENÇ YILMAZ

İstanbul, Mayıs 2020

T.C. İSTANBUL TİCARET ÜNİVERSİTESİ

T.C.
İSTANBUL TİCARET ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ

YÜKSEK LİSANS TEZİ ONAY FORMU

İstanbul Ticaret Üniversitesi Sosyal Bilimler Enstitüsü Siyaset Bilimi ve Uluslararası İlişkiler Yüksek Lisans programı öğrencisi Osman GİRGİN'in "21'inci Yüzyılın Yükselen Güç Unsuru Siber Güç ve Türkiye" başlıklı tez çalışması, Enstitümüz Yönetim Kurulu **23.06.2020** tarih ve **2020-510/02** sayılı kararıyla oluşturulan jüri tarafından oybirliği/oyçokluğu ile Yüksek Lisans Tezi olarak kabul edilmiştir.

	UNVANI, ADI SOYADI	ÜNİVERSİTE
TEZ DANIŞMANI	Dr. Öğr. Üyesi Ayfer GÖNÇ YILMAZ	İstanbul Ticaret Üniversitesi
JÜRİ ÜYESİ	Dr. Öğr. Üyesi Uğur Yasin ASAL	İstanbul Ticaret Üniversitesi
JÜRİ ÜYESİ	Dr. Öğr. Üyesi Övgü KALKAN İÇÜĞÜKSOLAK	Yalova Üniversitesi

ETİK KURALLARA UYGUNLUK

Hazırlamış olduğum tez özgün bir çalışma olup YÖK ve İTİCÜ Lisansüstü Yönetmeliklerine uygun olarak hazırlanmıştır. Ayrıca, bu çalışmayı yaparken bilimsel etik kurallarına tamamıyla uyduğumu; yararlandığım tüm kaynakları gösterdiğimi ve hiçbir kaynaktan yaptığım ayrıntılı alıntı olmadığını beyan ederim. Bu tezin ihtiva ettiği tüm hususlar şahsi görüşüm olup İstanbul Ticaret Üniversitesi'nin resmi görüşünü yansıtmamaktadır.

Osman GİRGİN

ÖZET

Teknoloji ve internet kullanımı hayatın her alanına gittikçe daha fazla nüfuz etmektedir. Günümüzde gücün değişen niteliğine paralel olarak güvenliğin içeriği ve yapısı da değişmekte, siber güç unsurları ve siber güvenlik devletlerin başlıca gündemleri arasında yer almaktadır. Güvenliğin genişleyen yapısı kapsamında konular çeşitlenmekte, aktörler devlet düzeyinden birey düzeyine doğru derinleşmekte ve söz konusu unsurlar siber uzayın amorf yapısı kapsamında artan belirsizliklere ve kırılganlıklara sebebiyet vermektedir.

Tarımdan iletişime, kanalizasyondan savunma alanına varan hemen hemen her alan artan şekilde siber teknolojilere ve siber uzaya bağlanmaktadır. Sağlamış olduğu fırsatlar bir yana, kullanıcılarının rahatlıkla kimliklerini gizleyebildikleri ve bu anlamda caydırıcı stratejilerin uygulanmasının kolay olmadığı siber uzay kapsamında risk ve tehditler daha da karmaşık bir yapıya bürünmekte ve ulusal güvenliğin korunmasını zorlaştırmaktadır. Siber uzayın karmaşık yapısı, belirsizliği ve bu alandaki politika uygulamalarının halen gelişmekte olması, siber uzay konularının uluslararası ilişkiler teorileri kapsamında açıklanmasını zorlaştırmaktadır. Bu nedenle çalışmada farklı teorilerden yararlanılarak konu Realist, Neo-liberal ve Kopenhag Ekolü'nün sunmuş olduğu yaklaşımlar çerçevesinde tartışılmaktadır.

Bu tezde, siber uzay kapsamında önemli çalışmalar yapan ve bu operasyonel alanda iddialı olan devletlerin siber güç unsurları, güvenlik politikaları ve strateji planlamaları incelenmektedir. Bu çalışma ile siber uzayın dört ana bileşeni bulunduğu, bu bileşenlerin ise; teknoloji, internet, jeopolitik uzay ve bireyler olduğu ifade edilmektedir. Siber uzayda söz sahibi olma konusunda ABD, Rusya Federasyonu, Çin Halk Cumhuriyeti ve İsrail'in söz konusu bileşenler üzerinden gerçekleştirdikleri ya da gerçekleştirmeyi planladıkları stratejiler tartışılmaktadır. Son kısımda ise, Türkiye'nin siber uzaya yönelik çalışmaları ve stratejisi ele alınmakta, mukayeseli bir yaklaşımla bu alanda yapılabilecekler konusunda öneriler getirilmektedir. Türkiye'nin uluslararası alanda söz sahibi olabilmesinde siber güvenliği bir ulusal güvenlik meselesi olarak ele almasının ve farklı sektörleri ve paydaşları içeren kapsamlı bir yaklaşımla çalışmalarına hız vermesinin elzem olduğu sonucuna varılmaktadır.

Anahtar Kelimeler: *Güç, Siber Uzay, Siber Güç, Ulusal Strateji, Güvenlik*

ABSTRACT

The usage of technology and the internet has outspread in almost every field of life. In contemporary days, the content and structure of security have been changing correspondingly to the change in the quality of security. Cyberspace security has returned to one of the important topics in the states' agenda. The subject of security has been varied because of the expansionary quality of the security, and the actors in the realm of the state have shifted into the individual realm. So-called factors caused to the uncertaiınity and fragility in the formless structure of cyberspace.

Many sectors from the agriculture to the communication, from drainage systems to defense industry have been interconnected to each other, cyberspace and cyber technologies. Aside from the opportunities the cyberspace technologies provide, it is difficult to protect national security against the threats and the risks and to establish deterrent strategies since cyberspace is a place where its users can easily hide their identity due to its complex structure. To explain cyberspace issues in terms of international relations theories is hard because of the uncertainty, complex structure, and developing policies of cyberspace. Therefore, the power and security theories of realism, neo-liberal, and Copenhagen theories were analyzed by this frame.

In this dissertation, the elements of cyberspace, security policies, and strategic plans of the states which have important efforts theoretically and practically within the scope of cyberspace are examined. By this study, it is indicated that there are four main components in cyberspace; these can be counted as technology, internet, geopolitical space, and individuals.The security policies and strategical plans of the USA, Russian Federation, Republic of Chine, and Israel which are dominating cyberspace is discussed in terms of the components of cyberspace. Then the position of Turkey is comparatively evaluated in terms of cyberspace and some offers have been done for the national and cybersecurity of Turkey. It is concluded that if Turkey wants to be a voice in the world states the policies of cyberspace should be studied carefully and accelerate the works in a comprehensive way including different sectors and stakeholders.

Keywords*:* *Power, Cyber Space, Cyber Power, National Strategy, Security.*

ÖNSÖZ

Tez çalışmam boyunca anlayış ve yardımlarını eksik etmeyen, yönlendirmeleri ve ilgisiyle çalışmamın her aşamasında bilgi ve desteğini esirgemeyen danışmanım, değerli hocam Dr. Öğretim Üyesi Ayfer Genç Yılmaz'a şükranlarımı sunarım. Tez konumu belirlemem sürecinde beni yönlendiren ve akademik anlamdaki tavsiyeleri ile çalışmama katkı sunan Prof. Dr. Gülden Ayman' a saygılarımı sunarım.

Tez sürecime teknik açıdan destek veren, yüksek lisans sürecinde her zaman desteğini hissettiğim çok değerli hocam Dr. Öğretim Üyesi Ali Burak Darıcılı'ya teşekkürü borç bilirim. Manevi desteğini esirgemeyen ve yazım aşamasında akademik yazım kurallarının neler olduğunu en ince ayrıntısına kadar öğreten, yönlendirmesi, bilgilendirmesi ile fikirlerime yön veren değerli hocam Dr. Öğretim Üyesi Övgü Kalkan Küçüksolak'a minnettarlığımı bildiririm.

Çalışmamı, hayatın her anında desteğini hissettiğim sevgili anneme ve babama ithaf ediyorum.

Osman GİRGİN

İstanbul, 2020

TABLOLAR LİSTESİ

Sayfa No.

KISALTMALAR

a.g.e.	Adı Geçen Eser
ARPA	Advanced Research Projects Agency
ABD	Amerika Birleşik Devletleri
BDT	Bağımsız Devletler Topluluğu
BM	Birleşmiş Milletler
BTK	Bilişim Teknoloji Kurumları
DDoS	Denial Of Service- Servis Hizmet Reddi
FBI	The Federal Bureau of Investigation/Federal Araştırma Bürosu
ISS	İnternet Servis Sağlayıcısı
İHA	İnsansız Hava Aracı
NATO	Kuzey Atlantik Konseyi
RF	Rusya Federasyonu
SSCB	Sovyet Sosyalist Cumhuriyetler Birliği
ŞİÖ	Şangay İşbirliği Örgütü
TÜBİTAK	Türkiye Bilimsel ve Teknolojik Araştırma Kurumu

İÇİNDEKİLER

GİRİŞ

Devletler arası güç mücadeleleri içinde bulunulan dönemin koşullarına paralel şekilde seyretmiş, güç unsurları sert güç ve özellikle de Soğuk Savaş sonrası dönemde yumuşak güç üzerinden değerlendirilmiştir. Günümüzde ise, devletler gelişen yüksek teknoloji ile internetin birleşmesi sonrası insan eliyle üretilen siber alanda üstünlük mücadelesine girişmişlerdir. Önümüzdeki dönemin güç mücadelelerinin yaşanacağı siber uzayın bileşenlerinin anlaşılması, uluslararası ilişkilerin değişen dinamiklerinin ve parametrelerinin anlaşılması açısından önem arz etmektedir. Siber uzaya ve siber güce ilişkin konular devletlerin ajandalarının üst sıralarında yer alırken, siber güvenlik ulusal güvenliğin önde gelen bileşeni olarak tanımlanmaya başlamıştır.[1] Siber uzaya ilişkin stratejilerin ve siber teknolojilerin geliştirilmesi, alanında uzman kişileri bir araya getirecek kapsamlı bir yaklaşımla mümkün olabilmektedir. Söz konusu yaklaşımların temelinde bu çalışmanın hipotezi siber uzay önümüzdeki dönemin güç mücadelelerinin yaşanacağı bir alan haline gelmektedir. Bu kapsamda, siber güç devlet politikalarının öne çıkan güç unsurudur. Bu çerçevede de ABD, Rusya, Çin, İsrail devletlerinin politikaları incelenmiş ve Türkiye' nin siber uzay politikaları ve stratejileri değerlendirilmiştir.

Realist bir yaklaşımla irdelendiğinde, devletlerin egemenlikleri ve güç maksimizasyonu konularındaki tutumlarının siber uzaya ve siber güce ilişkin konularda değişkenlik göstermediği görülmektedir. Küreselleşmenin ve karşılıklı bağımlılığın artan etkisinin neticesinde güç mücadelelerinin farklı boyutlarda ve alanlarda siber alana taşınmakta olduğunu söylemek mümkündür.[2] Bu çerçevede incelendiğinde siber araçlar, devletlerin birbirlerine yönelik operasyonları çerçevesinde devlet politikalarının bir enstrümanı haline gelmektedir.

Bu çalışmada öncelikli olarak gücün ve güvenliğin değişen nitelikleri uluslararası ilişkiler teorileri kapsamında analiz edilmiştir. Bu teorik alt yapı üzerinden devletlerin

[1] Joseph Nye, **Amerikan Gücünün Paradoksu**, Çev.: Gürol Koca, İstanbul: Literatür Yayınları, 2003, s. 10-14
[2] Manfred STEGER, **Küreselleşme**, Çev.: Abdullah Ersoy), Ankara: Dost Kitabevi Yayınları, 2006, s. 16-20

siber uzay bileşenleri kapsamında yürüttükleri politika uygulamaları ya da gerçekleştirmeyi planladıkları stratejileri açık kaynaklardan[3] edinilen belgeler, akademik araştırmalar ve incelenen ülkenin siber güvenlik raporları üzerinden değerlendirilmiştir. Üzerinde mutabık kalınan net bir güç kavramına ulaşmanın güçlüğü siber güvenlik ve siber güç kavramlarında da kendini göstermiştir. Karşılıklı bağımlılığın ciddi boyutlara vardığı günümüz ortamında son derece çok yönlü, muğlak ve tartışmalara konu olan bu kavramlar kapsamında ulusal güvenliğin ve ekonominin, siber güvenlik ile yakından ilişkili olduğu ortaya konulmuştur. Çalışmada siber uzay güvenliği kapsamında devletlerin kat ettikleri yol ve izledikleri politikalar ile siber uzayın dört ana bileşeni üzerinde yaptıkları çalışmalardan bahsedilmiştir. Anarşik bir yapıya sahip olan ve belirsizliklerin hakim olduğu siber uzayın arz ettiği risk ve tehditler karşısında küresel düzeyde işbirliklerinin, çok taraflılığın ve yönetişim anlamında bir anlayışın oluşturulmasının gerektiği, Türkiye ölçeğinde de kapsamlı stratejilerin ve AR-GE çalışmalarının hızlanarak devam etmesi gerektiği sonucuna varılmıştır.

Bu çalışmada temel olarak, siber uzayda üstünlük yarışının başat aktörleri olarak öne çıkan ABD, Rusya Federasyonu, Çin Halk Cumhuriyeti ve İsrail devletlerinin politikaları incelenmiş, aynı konu başlıkları altında Türkiye'nin siber uzay politikası ve stratejileri değerlendirilmiştir. Bu minvalde, siber güç ve siber güvenliğin ulusal güvenlik üzerindeki etkileri aşağıdaki sorunlar kapsamında tartışılmıştır:

- Siber güvenlik hangi konularda etkili olmaktadır? Siber güvenliğin temininin önemi ve amaçları nedir?
- Devletlerin siber güvenlik politikalarını etkileyen unsurlar nelerdir? Bu anlamdaki devletler arasında farklılıklar bulunmakta mıdır?
- Siber uzayda üstünlük mücadelesi veren devletlerin politika gelişimlerinde ne gibi faktörler etkili olmuştur? 2000 yılından sonra uygulanan politikalarda ne gibi değişimler yaşanmıştır?

[3] Açık Kanyak : Herkesçe rahat bir şekilde ulaşılabilecek bilgiyi kapsamaktadır. Örneğin, kuruma ait web siteleri, ulusal haber kaynakları, internet siteleri v.b.

- Siber uzaya yönelik stratejiler kapsamında sürdürülebilir çalışmaların yeri ve etkinliği nelerdir?
- Siber uzayda üstünlük yarışında olan ülkelerin hedefleri ve politika uygulamaları nelerdir?
- Türkiye'nin siber uzaya yönelik hedefleri ve politika uygulamaları nelerdir?

Tez çalışmasına siber uzay ve güç ilişkisi, özellikle devletlerin gerçekleştirdiği politikalar temeli ana literatür taramasını oluşturmuştur. Siber uzayda güç mücadelesi ne kadar gerçekleşebilir? Uluslararası ilişkiler disiplininde hangi teoriler üzerine temellendirmeler yapılmıştır? Bu ana sorulara bağlı olarak: Realizm teorisinin güç teorisinde Rusya Federasyonu ve Amerika Birleşik Devletleri'nin siber uzayda politikaları yumuşak güç üzerinden gösterilmiştir.[4] Ağ tekonolojilerinin internet ile gelişmesi bireysel kullanıcılarının sayısını artırmıştır. Bireyleri ve toplumu yeni inşa sürecine iten bu durumu açıklamak adına siber uzayın değişen koşulları tekniklerden ötürü bireyin siber uzayda güvenliği gündem oluşturmuştur. Bu bağlamda güvenlikleştirme teorisinin varlığını benimseyen Kopenhag ekolü siber uzayın merceği içerisine alınmıştır. [5] Siber uzay uluslararası ilişkilerde en çok ilişkilendirme ise neo-liberal teroisi üzerinden şekillenmiştir. Neo-liberal kuramının önemli teorisyenlerinden biri olan[6] Joseph Nye'ın çalışmaları üzerine odaklanılmıştır. Joseph Nye siber uzayı yumuşak güç üzerinden ele almıştır. Yanı sıra siber uzayı tanımlamanın zor olduğunu belirterek literatüre katkıda bulunduğu yumuşak güç ile sert gücün karışımı sonucu akıllı güç sorunsalını ön plana çıkartmıştır.[7] Türkiye üzerine yapılan çalışmaların ise çok nadir olduğu, siber uzayı domine etmesi yüksek olan devletler ile karşılaştırması ayrıntılı olarak ilk kez bu tez üzerinden yapıldığı ve literatüre katkı sağlayabileceği söylemek mümkün olabilmektedir.

[4] Ali Burak Darıcılı, **Siber Uzay ve Siber Güvenlik Nedir? Abd 'nin Siber Güvenlik Stratejisi Rusya Federasyonun Siber Güvenlik Stratejisi**, Bursa:Dora Yayınları, 2017, s.288
[5] Mehmet Eren, **Avrupa Birliği'nin Siber Güvenlik Politikası**, İstanbul: Beta, 2017, s.108
[6] Evren Çelik Wiltse, "Liberalizm, İş birliği, Kolektif Güvenlik ve Neoliberal Kurumsalcılık", ed. Evren Balta, **Küresel Siyasete Giriş Uluslararası İlişkilerde Kavramlar, Teoriler ve Süreçler**, İstanbul: İletişim Yayınları,2014, s.141
[7] Joseph Nye, **Cyber Power**, Harward Kenndy School, Cambridge:2010, s.3-7

Esasında sosyal bilimci konu başlıklarını belirlerken olabildiğince literatüre dışarıdan bakarak yorumlaması gerekmektedir. Bu tezde söz konusu eylem uygulanmak üzere birinci bölümde siber uzayı kapsadığı değerlendirilen: sert güç, yumuşak güç, bireysel güvenlik konularını kapsayan önemli teorileri açıklanmıştır. İkinci bölümde siber uzayın tanımlanması yapılırken, akademisyen ve düşünürlerin siber uzayı tanımlayamama ve uluslararası ilişkiler disiplininde bulunan teorilerde temellendirememe sorunsalı anlatılmıştır. Üçüncü bölümde ise günümüze kadar yapılan çalışmalardan ayrılmak adına siber uzayı politikaları ile domine eden ülkeler ve Türkiye'nin politikaları belirtilmiştir; bu anlamda bir domine devletler- Türkiye analiz çalışmasıdır. Bu bağlamda saha çalışmasının mümkün olmadığı, akademisyenlerce ve devletlerin resmi kaynak belgelerinin yorumlanmasına dayanmaktadır. Bu çalışmada, Türkiye'de siber güvenlik çalışmalarının öncelikli olarak hangi kurumlar tarafından nasıl yürütüldüğünün anlaşılması ve mevcut durumun diğer devletler ile karşılaştırılması konusunda bir perspektif sunulması amaçlanmıştır. Bu kapsamda gerek diğer devletlerin çalışmaları, gerekse Türkiye'nin siber güvenlik üzerine yaptığı çalışmalar ve uyguladığı politikalar yakından incelenmiştir. Siber uzayın güvenlik sorunu, uluslararası alanda bir sorun olması nedeniyle siber güvenlik üzerine çalışmaları dikkat çeken devletler kaleme almaktadır. Ele alınan Türkiye sorunsalı ilişkin bizce yeterli olabilecek kaynak ve belgelere ulaşılmış, çalışma şekillenmiştir.

1. BÖLÜM GÜCÜN DEĞİŞEN NİTELİĞİNİN İNCELENMESİ

1.1 REALİST TEORİNİN GÜÇ ve GÜVENLİK KAVRAMINA YAKLAŞIMI

1.1.1 Realist Teori

En temel amacı toprak bütünlüğünü ve ulusal güvenliğini sağlamak olan devletler, egemenlikleri çerçevesinde kendi çıkarlarını ve bu çıkarlara hangi araçlarla ulaşacaklarını belirlerler. Devlet bekası odaklı Realist yaklaşım, devletlerin güvenliklerini hangi çerçevede şekillendirdiğini ve askeri araçlar başta olmak üzere hangi araçlar üzerinden temin ettiğini açıklamaktadır.

Anarşik, yani üst otoritenin bulunmadığı, uluslararası sistemde devletlerin gücü, uluslararası alanda belirleyici olmaktadır.[8] Realist yaklaşımın önde gelen isimlerinden Morgenthau devletlerin güç mücadelesi içerisinde bulunmasının nedenini bencil ve sürekli bir çıkar çatışması içerisindeki insan doğasına dayandırmaktadır.[9] Thomas Hobbes'a referansla sürekli bir çıkar çatışması üzerinden tanımlanan ve insan insanın kurdu olduğu söz konusu güvensizlik ortamında insanın temel dayanağı kendi gücüdür. Anarşik sistem içerisinde bekasını sağlamak ve gücünü geliştirmek adına devlet, temel güç unsurlarına odaklanmaktadır. Tarih boyunca uluslararası ilişkilerde temel güç unsurunun kavramları: nüfus büyüklüğü, doğal kaynak genişliği, sahip olduğu askeri güç, ekonomik durumu ve istikrar.[10] Kendi kendine yardım prensibi çerçevesinde işleyen uluslararası düzende devletler, bekaları çerçevesinde belirledikleri stratejik planlamaları üzerinde güçlerini maksimize etmeye çalışmakta ve realizme göre söz konusu güç de askeri güç ağırlığında şekillenmektedir. Zira askeri gücü zayıflayan devletin uluslararası faaliyetler içerisinde bulunması ve çıkarları doğrultusunda diğer

[8] Tayyar Arı, **Uluslararası İlişkilere Giriş**, Bursa:MKM Yayınları, 2013, s.26
[9] Faruk Yalvaç, "Uluslararası İlişkiler Kuramında Anarşi Söylemi", **Uluslararası İlişkiler Dergisi**, C.8, S. 29 (Bahar 2011), s. 77
[10] Richard L. Armıtage, Joseph Nye, **CSIS Commıssıon On Smart Power**, The Csıs Pres, Washinton: 2007, s.6

devletleri yönlendirmesi zorlaşmaktadır.[11] Dünya politikasında söz sahibi olmak isteyen devletlerin öncelikli olarak ordularını güçlü tutma yönünde strateji izledikleri görülmektedir.[12]

Yukarıda belirtilen ana argümanlar ile devletlerin uluslararası sistem içerisinde oluşumlarını, birbirleriyle olan ilişkilerinin gözlemlemesini ve değişimlerini açıklamaya çalışan realist teori uluslararası ilişkiler disiplininin en temel teorilerinden biri olarak kabul edilmektedir. Realizmin kökeni Peloponezya Savaşları adlı eserinde eski Yunan'da şehir devletlerinin arasında geçen savaşları ele alan Thucydides, M.Ö. 3. yy' da yaşamış olan Hintli düşünür Kautilya' ya, Rönesans döneminin önemli düşünürü, 16. Yüzyılda yaşamış ve Prens kitabının yazarı Niccola Machiavelli dönemine kadar götürülebilmektedir.[13] Thucydides, Peloponez Savaşına Atina ordusunda komutan olarak katılmış ancak Trakya' da yaşamış olduğu başarısızlık nedeniyle sürgün edilmiştir. 20 yıllık sürgün hayatında meşhur eseri olan 'Poloponez Savaşları' yazmıştır. Atina' nın kaybettiği bu savaşta Thucydides ilk defa uluslararası ilişkiler argümanlarını kullandığı görülebilmektedir. Bu argümanlar içerisinde güç mücadelesi, devlet adamlarının tavırları, devletlerin şartları, diplomasi ve ittifak hareketleri, silahlanma, caydırıcılık politikaları ve en önemlisi olarak güçlü olanın yapacaklarını, yapabileceklerini, zayıf olanın ise güçlü olanın karşısında sessiz kalınabileceğini ve zayıf olanın güçlüye karşı söz sahibi olamayacağını belirtmektedir.[14] Machiavelli'nin düşüncelerinde ise işgalci devlet halinde bütün askeri güç ile saldırmasını hatta prensin alçakgönüllü değil, saldırgan, asker ruhlu, güçlü davranışları ile ideal devlet adamının rakibine karşı korkutucu olması gerektiğini belirtmektedir.[15] Peloponezya Savaşları'nda doğa durumunda haklının hukukunun geçerli olduğu ortaya konurken, Macchiavelli'nin Prens'e verdiği öğütlerde devlet adamının temel görevinin devlet bekasının sağlanması olduğunun ve ahlaki unsurların uluslararası ilişkiler çerçevesinde geri planda tutulduğunun altı çizilmektedir.

---

[11] Joseph Nye, **Amerikan Gücünün Paradoksu**, Çev: Gürol Koca, İstanbul: Literatür Yayınları, 2003, s. 12

[12] Sait Yılmaz, **Güç ve Politika**, İstanbul: Alfa Yayınları, 2008, s.48

[13] Faruk Sönmezoğlu, Hakan Güneş, Erhan Keleşoğlu, **Uluslararası İlişkilere Giriş**, İstanbul: Der Yayınları, 2011, s.41

[14] Eyüp Ersoy, "Realizm", **Uluslararası İlişkiler Teorileri**, der. Ramazan Gözen, İstanbul: İletişim Yayınları, 2019, s.166-167

[15] Niccolo Machıavellı, **Prens,** (Çev. Alev Tolga), İstanbul: Say Yayınları, 2009, s.12-25.

1929 Büyük Buhranından itibaren küresel ekonomide gözlemlenen yapısal sorunlar, Birinci Dünya Savaşı'nın kaybedenleri Almanya ve Japonya'nın revizyonist eğilimleri ve Milletler Cemiyeti'nin savaşı önlemedeki başarısızlığı, Birinci Dünya Savaşı'nın ertesinde gelişen idealist yaklaşımın işlevinin ve işleyişinin sorgulanmasına yol açmıştır.[16] İdealist düşüncenin kendi fikirlerinin test edilmediği yönündeki savunmalarına karşın E.H. Carr, Nazilerin dünyanın yarısını ve Avrupa'nın tamamını ele geçirmesiyle bir nevi test edildiğini belirtmektedir.[17] 1930'lu yıllarda gerek idealizme karşı eleştiriler yönelten, gerekse realist düşünceyi kapsamlı şekilde tartışan E.H. Carr, realizmin olgunlaşmasını sağlayan başlıca isimlerden biri olarak öne çıkmıştır.[18] Öte yandan, 2. Dünya Savaşı'nın ertesinde literatürde dominant yaklaşım haline gelen realizmin en önemli düşünürlerinden bir diğeri de 1948 tarihli Uluslararası Politika kitabının yazarı Hans J. Morgenthau'dur.[19]

Morgenthau' nun başeseri "*Uluslararası Politika'da*" realizmin altı temel ilkesini şu şekilde özetlenmektedir:[20]

- Siyaset ile insan doğasında paralellik kuran Morgenthau, siyasetin de insan doğası gibi rasyonel yasalara göre şekillendiğini savunmaktadır. Bu çerçevede realizm olguları ortaya koyarak, devlet davranışlarını bu mantık çerçevesinde anlamlandırmaktır.
- Güç üzerinden tanımlanan çıkar kavramı uluslararası siyasette realist düşüncenin temel noktasını teşkil etmektedir. Devlet yönetimi güç üzerinden tanımlanan çıkarların dikteleri kapsamında şekillenmektedir.
- İnsan doğasının bencilliğine benzer şekilde, güç ve çıkar kavramlarının temel belirleyici olduğu uluslararası siyasette devletlerin çıkarları çatışabilmektedir. Yine de

[16] Atilla Eralp, "Uluslararası İlişkilerin Oluşumu: İdealizm-Realizm Tartışması", **Devlet Sistem ve Kimlik: Uluslararası İlişkilerde Temel Yaklaşımlar**, İ.D. Dağı vd., İstanbul: İletişim Yayınları,2013, s.68-69

[17] Mustafa Aydın, "Uluslararası İlişkilerde Yaklaşım, Teori ve Analiz", **Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi**, C. 51, S.1, (Ocak 1996) s. 92

[18] Faruk Sönmezoğlu vd, **a.g.e**., s.41

[19] Mustafa Aydın, "Uluslararası İlişkilerin "Gerçekçi" Teorisi: Kökeni, Kapsamı, Kritiği", **Uluslararası İlişkiler Dergisi**, C. 1, S. 1 (Bahar 2004), s.46

[20] Hans J. Morgenthau, **Uluslararası Politika**, Ankara:Türk Siyasi İlimler Derneği Yayınları, Çev.: Ünal Aksoy, Baskın Oran, 1970,s. 2-14

Realizm ile özdeşleşen güç ve çıkar kavramı durağan bir karaktere sahip olmamakta, içinde bulunulan koşullara paralel olarak değişkenlik göstermektedir. Realizm de değişkenlik gösteren siyasi arenayı analiz eder.

- Devletlerin dış politika davranışlarında moral değerlerin varlığı sorgulanmaz. Herkes yaptığı hareketi iyi de olsa kötü de olsa haklı olarak görecektir. Çünkü kanaat getirerek geçekleştirdiği bir eylem ile gerçekçi olan ya da gerçekçi olabilecek düşüncelerini milliyetçilik ve dini duyguları ile bağlantılı hale getirip buna inanacaktır.
- Ulusların bütün düşüncelerine ket vuracak olan ise güç ve çıkar kavramı düşüncesidir. Kendi ulusumuz ve diğer ulusun arasındaki adil düzeni sağlayacak olan yine güç ve çıkar düşüncesinin ön planda olduğunu kavrayabilmekten geçecektir.
- Entelektüel açıdan Realizm, siyasal alanın hayatın diğer alanlarından ayrılarak kendine has bir alan içerisinde değerlendirildiğini savunmaktadır. Bu kendine özgü alan kendi ilkelerini ve güç üzerinden tanımlanan çıkar düşüncesini içermektedir. Görülüyor ki, realizmin diğer düşünce tarzlarından en büyük farkı, devletin gücü ne kadar etkilidir? Sorusuna cevap aranmasıdır.

Anarşik uluslararası sistemde hayatta kalmanın temel yolu güç maksimizasyonu olan realist yaklaşımda güç, temel belirleyici faktör olarak öne çıkmaktadır. Görülüyor ki, uluslararası ilişkiler disiplinin gelişimi çerçevesinde 'güç konusu' ana faktör olmasının yanı sıra uluslararası ilişkilerin varlığını belirleyen temel kavramlardan biri olarak da tartışılabilmektedir.[21] Dönemin koşullarına paralel şekilde güç unsurlarında değişim yaşanmakta ve devletler çıkarlarını ve stratejilerini belirlemektedirler.

1.1.2 Realist Teorinin Güç ve Güvenlik Anlayışı

Güç, devletler arasında kontrol ve etki unsuru olarak iki şekilde var olabilmektedir. Kontrol, bir A devletinin B devleti üzerinde yapabileceği bütün baskılar olabilir. Etki ise, kendi amaçları doğrultusunda başkalarını etkileme ya da bir aktörün yapmış olduğu davranışları kendi isteği doğrultusunda şekillendirebilme anlamına

[21] Deniz Ülke Arıboğan, **Globalleşme Senaryosunun Aktörleri**, İstanbul:Der Yayınları, 1996, s. 18

gelebilir.[22] Etki ve kontrolü sentezleyip güç tanımı yapan Robert Dahl, gücün bir devlete karşı yaptırım uygulamak ya da bir devleti herhangi bir yaptırımdan vazgeçirmek için kullanılan etkin bir araç olduğunu savunmaktadır.[23] Bu araç ile devletler diğer devletler karşısında kendi konumunu, siyasi duruşunu, kimlik olgusunu korumayı hedeflemektedirler.[24] Bir ulus devlet kendi bağımsız iradesini, duruşunu, kimliğini koruyabilmek adına caydırıcı güç politikasını uygulayabilmelidir.[25] Devletler kapasitelerini kontrol ve etki unsurlarının değerlendirilmesi ve hesaplanması[26] üzerinden tanımlarlar.

Oysa ki, kapasite, iletişim halinde olan devletler arasındaki duruma göre değişebilmektedir. Bir devlet başka bir devleti güçlü, diğer bir devleti ise güçsüz olarak algılayabilir.[27] Devletlerin birbiriyle etkileşimi doğrultusunda güç politikaları ve ulusal politikaları gelişebilir.[28] Dolayısıyla devletlerin bütün etkileşimleri her zaman siyasi olarak değerlendirilmek mümkün olmayabilir. Çeşitli sebeplerden ötürü iş birliği içerisinde olan devletlerin siyaset dışı bağlantıları olabilmektedir. Ancak bu devletlerin siyaset dışı etkileşimi sırasında devletlerin yaklaşımı içerisine güç ilişkilerinin sirayet etmesi veya güç ilişkilerinin mesele haline getirilmesi, durumu siyasal bir sorun haline getirebilir. Güç unsurunun bu merkezi konumu siyasetin ana teması olarak düşünülmesine yol açmaktadır.[29] E.H. Carr, gücün bölünemeyecek bir bütün ve aynı zamanda aktörler tarafından vazgeçilemez bir yönetim aracı olduğunu belirtmektedir.[30] Devlet bekası çerçevesinde güç maksimizasyonuna koşan devletler çerçevesinde düşünüldüğünde, devletler egemenliklerinden ve güç unsurlarından ödün vermek

---

[22] Faruk Sönmezoğlu, **Uluslararası Politika ve Dış Politika Analizi**, İstanbul: Der Yayınları, 2014, s. 265 – 266

[23] A. Raobert Dahl, The Concept of Power**, Behavioral Science**, Y.2 S.3, (Temmuz 1957), s. 202

[24] Tayyar Arı, **Uluslararası İlişkiler Teorileri Çatışma, Hegemonya, İş birliği**, Bursa: MKM Yayıncılık, 2013, s. 152 – 155

[25] Sait Yılmaz, "Uluslararası İlişkilerde Güç ve Güç Dengesinin Evrimi", **Stratejik Araştırmalar Dergisi**, C.1, S.1, (2008), s. 59

[26] Robert KAGAN, **Cennet ve Güç Yeni Dünya Düzeninde Amerika ve Avrupa**, Çev.: Selim Yeniçeri, İstanbul: Koridor Yayıncılık, 2005, s.39

[27]Salih Doğan, Şeref Kavak, Uluslararası İlişkilerde Güç Kavramı, **Uluslararası İlişkilerin Temel Kavramları**, der. Arif Behiç Özcan, Yusuf Çınar, İstanbul: Hükümdar Yayınları, 2014, s.247

[28] David A. Baldwin, Power And International Relations, **Handbook of İnternational Relations**, der. Walter Carlsnaes, Thomas Risse, Beth A. Simmons, London: Sage, 2013, s.273

[29] Edward Hallett Carr, **1919 – 1939 Yirmi Yıl Krizi**, Çev.: Can Cemgil, İstanbul: İstanbul Bilgi Üniversitesi Yayınları, 2015, s. 147

[30] Edward Hallett Carr, **a.g.e,** s.151

istememektedirler. Bu nedenle de üst bir otoritenin bulunmadığı anarşik uluslararası sistemde, devlet davranışlarının kısıtlandığı ve belki de savaşların önünün alındığı bir uluslararası sistem kurmak neredeyse imkansızdır.

Realist teorinin bakış açısıyla devlet, insan doğasına benzetilmektedir. Kendisini koruyacak otoritenin bulunmaması durumunda insan, 'güvende olmama' duygusuyla tehdit içerisinde bulunduğunu düşünebilir. Devlet düzeyinde düşünüldüğünde tehdit, bir yabancı aktörün, devletin aleyhinde gerek kendi sınırları içerisinde bulunup bir araya gelmiş kişi ve kişilerce gerekse devletin sınırları dışında bulunan kişi ve kişilerce, ülkenin çıkar ve amaçlarına zarar vermek maksadıyla faaliyet içerisinde bulunulması olarak tanımlanabilir.[31] Kendisini tehdit içerisinde gören devletler böylece çıkarları doğrultusunda en güçlü olma çabası içerisinde olabilir. Çünkü realizm mevcut güç öğelerini ön planda bulundurarak güç potansiyeli yüksek olan devletler ile olan ilişkilerinde değişim sağlayıp her zaman olduğundan daha güçlü olma düşüncesi içerisinde olabilmektedir.[32]

Güçlü olmanın güvenliği sağlayan bir araç olduğunu belirten realist teorisyenler, askeri güç argümanını savunmaktadır. Bu durumda realist düşünürler devletlerin birbirileriyle olan ilişkilerinde hiyerarşi oluşturmuşlar ve birincil politikalarına (*high politics*) devletin kalıcılığı için güç merkezini askeri güvenlik üzerine planlayıp, ikincil politika (*low politics*) olarak çevresel, kültürel, ekonomik ve sosyal konular üzerinde durmaktadır.[33] Devletlerin güvenliği sağlanmak amacıyla güç politikalarını temel faktör olarak görülebilmektedir. Dolayısıyla devlet bekasını sağlamak amacıyla askeri gücü maksimize ederek uluslararası sistem içerisinde söz sahibi olmaya çalışmaktadır.[34] Realist yaklaşım devlet merkezli düşünüp, devletin varlığı ve bütünlüğünün korunması

[31] Yılmaz Tezken, **Jeopolitikten Mili Güvenliğe**, İstanbul: Ülke Kitapları, 2005, s.205
[32] Selahaddin Bakan, Sonay Şahin, "Uluslararası Güvenlik Yaklaşımlarının Tarihsel Dönüşümü ve Yeni Tehditler", **The Journal of International Lingual, Social and Educational Sciences**, C.4, S.2, (Aralık 2018), s.18
[33] Atilla Sandıklı ve Bilgehan Emeklier "Güvenlik Yaklaşımlarında Değişim ve Döşüm", **Teoriler Işığında Güvenlik, Savaş, Barış ve Çatışma Çözümleri**, Edt. Atilla Sandıklı, İstanbul: Bilgesam Yayınları, 2012, s. 7
[34] Övgü Kalkan Küçüksolak, "Güvenlik Kavramının Realizm, Neorealizm ve Kopenhag Ekolü Çerçevesinde Tartışılması", **Turan Stratejik Araştırmalar Merkezi Dergisi**, S.14, (İlkbahar 2012), s.205

amaçlamaktadır. Bu nedenle bireyin güvenliğini, devletin güvenliği üzerinden düşündüğü değerlendirilmektedir.[35]

Realist paradigma insan doğasında bulunan kötülük, devlet yönetiminde de yansıması bulunmaktadır. İnsan, diğer insanlara göre daha güçlü olma isteği içerisinde olabilir. Çünkü içinde beslemiş olduğu kin ve nefret duyguları ile kendi gücünü göstermek adına saldırı içerisinde bulunabilir. Güvende olma duygusu içerisinde bulunan insan belli bir organizasyon içerisinde bulunan ve kendisini tehlikelerden, tehditten koruyacak ve güvenliğini sağlamak adına iradesini düzene sokacak bir devlet çatısı altına girebilir.[36] Realizm, uluslararası sistem içerisinde bir çatı altında olma düşüncesini imkânsız olduğunu savunmaktadır. Realizm, Devlet merkezli ve bencil olarak kendi güvenliğini sağlamanın doğruluğunu düşünüp, korku-merkezli düşünceyi savunmaktadır.[37] Bu durum, Realist düşünürlerin üzerinde durduğu 'güvenlik ikilemi' (*security dilemma*) olarak düşünülebilir. Güvenlik ikilemine göre devlet, sürekli kendisine karşı saldırı içerisinde olunabileceğini, egemenlik ve özgürlüğünün kısıtlanacağını düşüncesi içerisinde bulunabilir.[38] Farklı bir söyleyiş ile sürekli saldırı içerisinde olabileceğini düşünen devlet, diğer devletlere karşı güç yarışı içerisinde olabilmektedir.

Realist yaklaşıma göre uluslararası güçlerde yaygın olarak bulunan askeri güç ya da sert güç kullanımının günümüzde zor kullanımı halini aldığı söylenebilir. Güç, değişen niteliği ile devletlerin sigortaları olarak değerlendirilebilir ve yaşadığımız bu modern çağda dünya siyaseti yumuşak gücün sert güce göre önemini attıran değişimlere uğrayabilir.[39] Bu değişimler sonucu aktörler yeni unsurlara yoğunlaşarak askeri güç

[35] Selahaddin Bakan, Sonay Şahin, **a.g.m**, s.141
[36] Thomas Hobbes, **Levıathan**, Çev.: Hamiyet Ünal, İstanbul: Lıtera Yayıncılık, 2019, s.151-152
[37] Ali Bilgiç, "Güvenlik İkilemi"ni Yeniden Düşünmek Güvenlik Çalışmalarında Yeni Bir Perspektif", **Uluslararası İlişkiler**, C. 8, S. 29 (Bahar 2011), s. 131
[38] J. H. Herz, **Political Realism and Political Idealism, A Study in Theories and Realities**. Chicaho & London: The University of Chicago Press, 1950, s.157
[39] Giulio M.Gallarotti, "Soft Power: What it is, Why it's Important and the Conditions Under Which it Can Be Effectively Used", **Journal of Political Power**, (2011), C.5.S.1 s.26-28

kullanımını oluşan yeni sistem içerisinde geri plana itebilir.[40] İletişim dünyasında aktörler gücünü yumuşak güç ve akıllı güç ile sağladıkları tartışılmaktadır.

1.2 NEO-LİBERAL TEORİNİN GÜÇ ve GÜVENLİK KAVRAMINA YAKLAŞIMI

1.2.1 Neo-Liberal Teori

Devlet ve askeri güç odaklı realist teoriye eleştiri niteliğinde gelişen neo-liberal teori ekonomi, çevre gibi konuların ajanda içindeki önemini vurgulamakta ve devletlerin yanısıra diğer aktörlerin de uluslararası politikada oynadıkları rollerin önemine odaklanmaktadır.[41] Devleti tek bir yapı olarak görmeyen neo-liberal teori, devlet dışı aktörlerin, uluslararası şirketlerin, sendikaların ve sivil toplum kuruluşlarının etkili olduğunu, kompleks bağların sistemin niteliği haline gelen karşılıklı bağımlılığa yol açtığını ortaya koymaktadır. Realist teoriye benzer şekilde bireyi rasyonel aktörler olarak tanımlayan neo-liberal teori diğer taraftan ise, realist teorinin güç maksimizasyonu anlayışı yerine kazan-kazan prensibine dayalı işbirliklerini savunmaktadır. Neo-liberal teori realist yaklaşımın askeri güç odaklı anlayışı yerine ekonomi ve diğer alanlardaki işbirliklerini ve artan bağımlılıklar üzerinden demokratikleşme süreçlerini savunarak bunun rasyonel birey açısından daha karlı ve barış ortamına katkı sağlayacak bir unsur olduğunu belirtmektedir. Realist düşünce ile sistemin anarşik olması, askeri ve ekonomik güçlerin önemine yapılan vurgu ortak noktalar olmakla beraber uluslararası iş birliklerine ve kurumsallaşan çabalarına atfedilen önem iki yaklaşım arasındaki başlıca farklılıkları teşkil etmektedir.

1962 yılında meydana gelen Küba Füze Krizi sonrasında güçlü olan ABD' ye karşı güçsüz olan Vietnam'ın savaşta galip gelmesi ve 1970'lerde uluslararası alanlarda ekonomik faaliyetlerin hız kazanması nedeniyle OPEC Petrol krizinin açıklanmasında yetersiz kalan Realizm düşüncesi hızını kaybederken, yukarıda belirtilen temel

[40] Haluk Özdemir, Uluslararası ilişkilerde Güç: Çok Boyutlu Bir Değerlendirme, **Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi**, C.63 S.3, 2008, s.113-144

[41] Yücel Bozdağlıoğlu ve Çınar Özen, "Liberalizmden Neoliberalizme Güç Olgusu ve Sistemik Bağımlılık", **Uluslararası İlişkiler Dergisi**, C.1, S. 4, (Kış 2004), s.67

varsayımları kapsamında yeni – liberaller diğer bir adıyla neo-liberal yaklaşım önem kazanmaya başlamıştır.[42] Sözkonusu yaklaşımın ağırlıklı olarak uluslararası arenada meydana gelen ekonomik krizlerin etkilerini ve Realizmin yetersiz kaldığı dinamikleri açıklamak üzere geliştirildiğini söylemek mümkündür. Teorinin önemli isimlerinden Andrew Moravcsik, neoliberal teorinin savlarını şu şekilde özetlemektedir: [43]

- Devletler, ölçülü ve akla dayanan hareketler içerisinde bulunan kurumlar olmalıdır.
- Uluslararası sistemin anarşik yapısının bulunması, merkezi bir üst otoritenin bulunmamasından dolayı kendi güvenliğini sağlamak zorundadır.
- Bir topluluğun haricinde ulusal çıkar tanımlaması mümkün olmamakla beraber, toplumu oluşturan çok çeşitli yapılanmaların kabul edilmesi gerekmekte ve devletin çıkarları tek bir bütün halinde olmamalıdır.
- Devlet dış politikasında toplumun isteklerini yansıtmalıdır.
- Devlet, halkı için siyasi hedeflerini sosyal ve ekonomik alanlarda çalışmalarını en üst düzeyde tutabilir. Bu durumda askeri harcamalar yerine halkın eğitimine ve ülkenin kalkınarak refah seviyesini yükseltmek adına çalışabilir. Zira,Realist düşüncede ki gibi sadece güç politikası içerisinde bulunmayabilir.
- Devletleri uluslararası alanda birbirinden bağımsız olarak düşünmek mümkün olmayabilir. İletişim halinde bulunacak olan devletler zaman içerisinde güvenlik, sosyo-kültürel ve ekonomik politikalarında ortak noktada buluşabilirler.
- Ekonomik faaliyetler ile iletişime geçen devletlerde mutlaka bir taraf kazanacak düşüncesi olmamalıdır. Biri kazanırken diğeri de kazanabilir.
- Devlet politikasında tercih edilen düşünce zaman içerisinde çıkarı doğrultusunda değişiklik gösterebilir.
- Devletlerin arasında oluşan bağ ve karşılıklı olarak kendi çıkarlarına önemli katkılar sağlanması zaman içerisinde iletişimlerini kuvvetlendirebilir.

[42]Cemre Pekcen, "Yeni-liberal Kurumsalcılık Çerçevesinde Çin'in Komşuluk Diplomasisi: Hu Jintao ve Xi Jinping Dönemlerine Karşılaştırmalı Bir Bakış", **Uluslararası Toplum Araştırmalar Dergisi**, Y.9, C.13, S.19, (Eylül 2019), s. 2869

[43] Evren Çelik Wiltse, "Liberalizm, İş birliği, Kolektif Güvenlik ve Neoliberal Kurumsalcılık", ed. Evren Balta, **Küresel Siyasete Giriş Uluslararası İlişkilerde Kavramlar, Teoriler ve Süreçler**, İstanbul: İletişim Yayınları,2014, s.140-141

Realist yaklaşımla devletler politikalarını dışa doğru planlamaktadır. Neo-liberal anlayışta ise, politikalar içeriden dışarıya doğru hareket edebilmektedir. Dolayısıyla demokratik bir karar alma süreci çerçevesinde dış politikanın şekillenmesinde iç politika dinamikleri etkili olmaktadır. Bunun sonuçlarından biri olarak da diğer devletler ile olan karşılıklı ilişkilerde iç politik tercihler etkili olabilmekte ve devlet dışı aktörler ön plana çıkabilmektedir.

Neo-liberal yaklaşım, güç politikalarında kendi güç unsurlarını oluşturan bir devlet yerine, uluslararası kurumlar ile oluşturulmuş bir sitem için çaba göstermektedir.[44] Neo-liberal yaklaşım, güç oluşumunu devlet dışı aktörlere aktarabilmektedir. Güç kullanımı çok yönlü alanlarda, dolaylı bir şekilde kullanılmaktadır. Doğrudan sert güç yerine ekonomik gücün varlığı ya da diğer kurumlar ile birleşim sağlayarak yumuşak ve akıllı güç unsurlarını kullanabilmektedir.[45]

1.2.2 Neo-liberal Teorinin Güç ve Güvenlik Anlayışı

Neo-liberal teorinin güvenliğe yönelik yaklaşımını yumuşak güç, akıllı güç, karşılıklı bağımlılık ve işbirliği kavramları üzerinden değerlendirmek mümkündür. Neo-liberalizm gerek karşılıklı bağımlılık ilkesi gerekse işbirlikçi düşünceler doğrultusunda devletlerarası ilişkileri güven ile barışçıl bir ortamda inşa edebilmektedir.[46] 1990 sonrasında yumuşak güç kavramı, uluslararası toplum ve devlet adamları tarafından desteklenen ve üzerinde durulan bir unsur olarak ön planda tutulmuştur. Realist yaklaşım gücün askeri, coğrafi ve ekonomi gibi sert güç kapsamında maddi derinliği üzerine odaklanırken, neo-liberal yaklaşım ise gücün yumuşak güç sınırları içerisinde bulunan işbirlikçi, hukuksal, demokratik varlık, ekonomide birleşim sağlamak amaçlarını benimsemiştir.[47] Neo-liberal teorinin önde gelen isimlerinden Joseph Nye[48] da sert güç ve yumuşak güç üzerine yapmış olduğu ayrımda; askeri ve ekonomik güçler

[44] Yücel Bozdağlıoğlu ve Çınar Özen, **a.g.m**, s.76
[45] Sertif Demir, Ali Bilgin Varlık, "Realist ve Liberal Teorilerde "Güç "Anlayışı", Edt. Hasret Çomak, Caner Sancaktar, **Uluslararası İlişkilerde Teorik Tartışmalar**, İstanbul: Beta, 2013, s.80
[46] Atilla Sandıklı ve Bilgehan Emeklier "Uluslararası İlişkiler Teorileri ve Barış", **Teoriler Işığında Güvenlik, Savaş, Barış ve Çatışma Çözümleri**, Edt. Atilla Sandıklı, İstanbul: Bilgesam Yayınları, 2012, s. 140
[47] Cengiz Özel, Yumuşak Güce Bütünsel Bakış, **Güvenlik Bilimleri Dergisi**, Y.7. S.1, (Mayıs 2018), s. 3
[48] Evren Balta, **Küresel Siyasete Giriş Uluslararası İlişkilerde Kavramlar, Teoriler, Süreçler**, İstanbul: İletişim Yayınları, 2014, s.141

aracılığıyla fikirlerin kabullenilmesinin sert güç çerçevesinde geliştiğini belirtirken, bir ülkenin diğer ülkeye olan hayranlığı ve gıpta ile aynı yolda gitme isteğini ise yumuşak güç tanımlaması kapsamında değerlendirmektedir. [49]

Joseph Nye tarafından 20 yıl önce oluşturulan yumuşak güç, hem akademik hem de politik çevreler tarafından sıklıkla kullanılmaya başlanmıştır.[50] Joseph Nye, dünyanın sert güce aşina olduğunu belirterek sert güç kullanımının havuç ve sopa yöntemine dayandığını, yumuşak gücün ise tercihleri belirleme ve şekillendirmede etkili olunan bir sanat olduğunu ifade etmiştir.[51] Cezbetmenin ve ikna etmenin ön planda olduğu yumuşak güçte daimî üstünlük sağlamak için bilgiyi sürekli elde tutma, hızlı hareket etme, kolay bir şekilde fikir alışverişi sağlama, farklılaşmayı çabuklaştırma, coğrafyayı çabuk tanımlama gerekebilmektedir.[52] Sosyal ilişkiler süreci olarak tanımlanabilecek olan yumuşak güç sayesinde aktörler arasında tercihler ve hedefler arasında bir nihai etkileşim olabilmektedir. Buradaki hedefin iç duygulara hitap etmesi nedeniyle sosyal ilişkilere hızlıca ulaşım sağlanmakta ve aktörlerin uyum sağlaması gerçekleşebilmektedir. Bu durumda pazarlık eden ülkenin cezbeden aktör lehine davranış sergilemesi sağlanabilmektedir.[53]

Ülkelerin bir kısmı yumuşak güç argümanından kültürel etkileşim olarak bahsederken, diğerleri sert güç unsurlarının dışında kalan bütün alanlar olarak tanımlamaktadırlar.[54] Joseph Nye ise, sert güç-yumuşak güç karşılaştırmasında, sert gücün baskı ve para ile yapılan kabullenme olduğunu, yumuşak gücün ise herhangi bir zorlama ve beklenti oluşmadan diğer aktörün cazibesine kapılıp amaçları yönünde destekleme olduğunu belirtmektedir.[55] Farklı bir söylemde ise yumuşak güç, dış politikada bir ülkenin başka bir ülkeye bulunmuş olduğu talebi yerine getirmemesi

[49] Joseph Nye, **Amerikan Gücünün Paradoksu…**, s. 11
[50] Vuving A.L., How Soft Power Works, Paper presented at the panel "Soft Power and Smart Power," American Political Science Association Annual Meeting,2009, (Çevrimiçi) https://ssrn.com/abstract=1466220, Erişim Tarihi: 06.01.2020
[51] Joseph S.Nye, **Yumuşak Güç Dünya Siyasetinde Başarının Araçları**, Çev: Rayhan İnan Aydın, Ankara:BB101 Yayınları, 2017, s.24
[52] Sait Yılmaz, Yumuşak Güç ve Evrimi, **Turan Stratejik Araştırmalar Merkezi Dergisi**, Y.3 S.12, (Sonbahar 2011), s.34
[53] Giulio Gallarotti, "Soft Power: What it is…, s.25-26
[54] Kadir Sancak, **Uluslararası İlişkilerde Güç Kavramı ve Yumuşak Güç,** Ankara, s.69
[55] Nye,**a.g.e**. s.26-27

durumunda cezalandırma ya da baskı altına almadan ikna etme kabiliyetiyle, talebi ona cazip getirerek yani kabul edecek aktörün de kendi menfaatlerine uyması ve kendi açısından meşru görülmesini sağlayabilme kabiliyeti olabilmektedir.[56]

Soğuk savaşın bitiminden sonra dünyanın yeni bir düzene geçtiği, toplumların etkileşiminin daha fazla olacağı, demokrasinin artacağı, silahlanmanın azalacağı ve 21. Yüzyılda uluslararası sistemlerin artan entegrasyonla evrensellik içerisine girileceği tartışılmaya başlanmıştır.[57] Günümüzde teknolojinin gelişimi ve küreselleşmenin ulaşmış olduğu evre çerçevesinde düşünüldüğünde bu tartışmaların iz düşümlerini ve özellikle de siber alanda yakalanan evrenselliği görebilmekteyiz. Bilginin her an her yerde internet ve gelişen teknoloji sayesinde ulaşılabilir hale geldiğine, kültürlerin birbirileri ile anlık iletişime geçtiğine şahit olmaktayız. [58] Özellikle de siber enstrümanlar üzerinden gücün kontrol edilebilmesinde zaman ile yarışır hale gelinen günümüzde, devletler küçük yapılanmalara son derece kırılgan ve savunmasız hale gelmektedir.[59] 20. Yüzyılın sonları ve 21. Yüzyılın başlangıcında gelişen teknolojinin insanlığa sunduğu başlıca olanaklar arasında mobilite, bilgiye ulaşımda kolaylık ve hız yer almaktadır. Bilginin tekil durumdan ayrılarak bilgiler haline geldiği bilgi tarihi kuramcıları tarafından öngörülmektedir. Antropolog Peter Worsley, "Büyük B ile başlayan yekpare bir Bilgi yok, bilgiler var" söyleminde[60] teknoloji ile bilgi tekillikten ayrılarak, çoğul alanlarda toplanmaktadır. Güç, doğası gereği sürekli değişim içerisinde olmakta ve bilgi günümüzün en önemli güç unsuru haline gelmektedir. Joseph Nye içinde bulunduğumuz bilgi çağında yumuşak güç kavramı kapsamında cazibe ile ikna edici kuvvetin daha çok önem kazanacağını öngörmektedir.[61] Zira cazibenin oluşturulma amacını verilen mesajın internet, radyo – televizyon, sinema ya da eğitim uygulamaları vasıtasıyla iletilebileceğini, seçilecek olan uygun temalar ile de kısa zamanda karşı tarafın nüfuz alanında ince ayarlar sağlanabileceğini savunmaktadır.[62]

---

[56] Faruk Sönmezoğlu,**Uluslararası Politika ve Dış Politika Analizi**, Der Yayınları, İstanbul, b.6, s.265.
[57] Henry Kissenger, **Diplomasi**, Çev: İbrahim H. Kurt, İstanbul, 14. Baskı 2015, s. 781-783
[58] Emrah Aydemir, **Dış Politikada Yumuşak Güç ve Medya**, İstanbul, 2016, s.159-160
[59] Joseph Nye, **Amerikan Yüzyılı Bitti mi?**, 1.b., Çev: Burç Beşgül, Uluslararası İlişkiler Kütüphanesi, İstanbul,2016, s.105
[60] Peter Burke, **Bilgi Tarihi Nedir?,** Çev: Turgay Sivrikaya, İstanbul: Islık Yayınları, 2018, Sayfa 19-20
[61] Joseph Nye, a.g.e., s.57
[62] Josep Nye, a.g.e., s.199

Gücün bütün etki ve kontrolü düşünülerek sert güç ve yumuşak güç sentezi üzerinden, akıllı güç tanımı yapılmaktadır.[63] Bu tanımdan da anlaşılacağı üzere akıllı güç, diğerlerinden bağımsız üçüncü bir güç unsuru olarak görülmekten ziyade, sert ve yumuşak güç biçimlerinin akıllıca kullanılması kapsamında tartışılmaktadır.[64] Farklı bir söylem ile akıllı güç kavramı hem sert güç (ekonomi, askeri) hem de yumuşak güç (cezbetme, kültür, eğitim, sosyal yardım) kapsamında kompozit olarak düşünülebilir. İktidar ve bileşenleri bu iki güç unsurundan herhangi birini salt güç olarak tek başına kullanamayabilir. Bu bağlamda devletler kontrollerinde bulunan kuvvetler doğrultusunda bu iki güç unsurunun birleşimiyle akıllı bir güç oluşturabilmektedir.[65]

Günümüzde devletlerin birbirlerine karşı konvansiyonel askeri güç[66] kullanımında yıllara göre değişiklikler gözlenmektedir. Savunma harcamalarına ayrılan bütçenin oldukça yüksek olduğu veriler kapsamında anlaşılmaktadır. Dünyada, askeri harcamaların 2017 yılına göre yüzde 2,6 artış gösterdiği, 2018 yılında ise askeri harcamaların 1.822 milyar dolar olduğu tahmin edilmektedir.[67]

Tablo 1: Coğrafi Bölgelere göre Askeri Harcamaların Dağılımı

Kıta	2018 Harcama	2017-2018 Yüzde Değişimi
Afrika	**40.6**	**-8.4**
- Kuzey Afrika	- 22.2	-5.5
- Sahra Altı Africa	- 18.4	-11
Amerika	**735**	**4.4**
- Orta Amerika ve Karayipler	8.6	8.8
- Kuzey Amerika	670	4.4
- Güney Amerika	55.6	3.1
Asya ve Okyanusya	**507**	**3.3**

[63] Richard L. Armitage Joseph S. Nye, **a.g.e**, s.7
[64] Matteo Pallaver, (2011). Power and Its Forms: Hard, Soft, Smart,The London School of Economics and Political Science, s.105 (Yayınlanmış Yüksek Lisans)
[65] Tea Kılıptarı, Chine's Smart Rise, **Güvenlik Stratejileri Dergisi**, Y.9.S.18 (Bahar 2013),s.80
[66] Nükleer silahların kullanılmadığı, tank, top, tüfek gibi silah türleriyle iki ayrı devletin savaşmasıdır. Bkz: Faruk Sönmezoğlu, **Uluslararası İlişkiler Sözlüğü**, İstanbul: Der Yayınları, 2010, s.417.
[67] SIPRI, Sıprı Yearbook 2019 Armaments, Disarmament and International Security, Stockholm, 2019, s.6

- Merkez ve Güney Asya	85.9	4.2
- Doğu Asya	350	4.1
- Güney-Doğu Asya	29.1	-2.9
- Okyanusya	41.9	-0.8
Avrupa	**364**	**1.4**
- Merkez Avrupa	28.3	12
- Doğu Avrupa	69.5	-1.7
- Batı Avrupa	266	1.4
Ortadoğu	….	….
Dünya Toplam	1822	2.6
Not: Harcamalar Amerikan milyar dolar cinsinden olup, tüm veriler gerçek harcamalardan elde edilmiştir.		

Kaynak: SIPRI, 2019 Bookyears, Summary

Sert güç unsurlarına ayrılan kaynakta görülen artışa rağmen bu unsurların güvenliği sağlamada yetersiz bulunduğu ve devletlerin güvenliklerini sağlama konusunda yumuşak güç ve akıllı güç unsurlarına ciddiyetle eğildiği görülmektedir. 21. Yüzyılın gelişen dinamikleri çerçevesinde güç araçlarının farklılıklar gösterdiğini belirten Joseph Nye, askeri güç kullanımında ABD' nin tek kutup olduğunu ancak ekonomik güç kullanımında ABD, Avrupa, Japonya ve Çin gibi ülkelerin son on yıl içerisinde etken aktör olduklarını ve aynı zamanda ulus ötesi varlıkların oluşturduğu devlet dışı aktörlerin de siber uzay gibi alanlarda tehdit arz ettiğini belirtmiştir.[68] Teknolojik araçlar kitleleri mobilize etmede ve davranış biçimleri üzerinde etkili olabilmekte, anlık olarak ve çok hızlı bir şekilde yayılan enformasyon karşısında ise, müdahale etme imkanı gittikçe azalmaktadır. Örneğin Usame Bin Ladin'in 7 Ekim 2001' de el – Cezire tarafından yayınlanan video kaydına karşılık Amerikan kanalları Bin Ladin' in mesajlarını engellemeye çalışmış ancak hızlıca gelişen bilgi akışı karşısında gerek savunma hattının bulunmaması gerekse izlenen yanlış politikalar nedeniyle engel olunamamıştır.[69] Dünyanın önemli aktörlerinden biri olan ABD'nin, daha 2001 yılında TV kanalında yayınlanan video karşısında etkisiz kaldığı görülmektedir. Günümüz teknolojisinin insanüstü temposu kapsamında düşünüldüğünde, çok daha hızlı

[68] Joseph Nye, **The Future Of Power**, Public Affarias, New York, 2011, s.25
[69] Joseph Nye, **Yumuşak Güç Dünya Siyasetinde Başarının Araçları**, Çev: Rayhan İnan- Aydın, Ankara: 2017, s.154-155

sosyalleşen ve kimlik gizlemenin çok daha kolay olduğu siber uzayda, siber güç unsurları devletler için öncelikli olmaya başlamıştır. Tüm bu güç kavramsallaştırmaları ve günümüz sisteminin dinamikleri kapsamında güvenliğin ve güç bileşenlerinin çok boyutlu bir hal aldığı gözlenmektedir.

1.3 KOPENHAG EKOLÜNÜN GÜVENLİK YAKLAŞIMI

1.3.1 Kopenhag Ekolü

Realist teorinin katı, devlet ve askeri konular odaklı yaklaşımına eleştirel bir perspektifle ortaya çıkan Kopenhag Ekolü, güvenlik konularını ve aktörlerini geniş ve derin bir çerçevede ele almaktadır. Devletlerin güvenliği özellikle de içinde bulunduğumuz süreç kapsamında çok boyutlu bir yaklaşımla, karşılıklı bağımlılık çerçevesinde şekillenmektedir. Böylece, devletlerin güvenliklerinin karşılıklı bağımlılık çerçevesinde yorumlandığı çalışmalar akademik literatürde daha çok öne çıkmaktadır[70]. Kopenhag Üniversitesi bünyesinde, Avrupa Güvenliği çalışma grubu tarafından Avrupa Güvenliği' nin Askeri- Olmayan Boyutları konulu çalışması ile temeli atılmış olan Kopenhag Okulu' nun önde gelen düşünürlerini Barry Buzan ve Ole Weawer teşkil etmektedir.[71] Barry Buzan ve diğer düşünürlerin geleneksel yaklaşımda var olan aktör-tehdit-politika üçlemine karşı eleştirel savunmalar yapılmaktadır.[72] Zira, 1980 yıllarının sonunda ortaya çıkan ekol, Soğuk Savaşın bitmesi kapsamında oluşan güç boşluğu ile devletlerin kendi güvenliklerini sağlamak adına düşünceler ortaya koymaktadır. Güvenlik anlayışının geleneksel bir yaklaşımla askeri boyut odaklı düşünülmediği, güvenliğin diğer boyutlarının bireylerin güven duygusu, ekonomik refah, kültürel alanların genişlemesi gibi ikincil politikaların ön planda tutulduğu bir anlayışa işaret etmektedir.

Kopenhag Okulu çerçevesinde öne çıkan üç konu başlığı; sektörel güvenlik, bölgesel güvenlik ve güvenlikleştirme teorisidir. 1995 yıllarında Ole Weaver tarafından

[70] John Baylis, "Uluslararası İlişkilerde Güvenlik Kavramı", **Uluslararası İlişkiler Dergisi,** C.5, S.18, (Yaz 2008), s.77
[71] Evren Balta, **Küresel Siyasete Giriş Uluslararası İlişkilerde Kavramlar…,** s.251
[72] Sinem Akgül Açıkmeşe, "Algı mı? Söylem mi? Kopenhag Okulu ve Yeni Klasik Gerçekçilikte Güvenlik Tehditleri", **Uluslararası İlişkiler Dergisi**, C.8, S.30, (Yaz 2011), s.46

ortaya atılan güvenlikleştirme teorisinin, Kopenhag ekolünün temellerini oluşturduğu düşünülebilir. Güvenlik söylemi için yeni bir kavram olarak "Güvenlikleştirme süreci" tanımlamasıyla, gelenekçilerin kısıtlı alanı içerisinde yapılan tanımlamalarının dışına çıkılarak, herkes her alan içerisinde sürekli bir tehdit içerisinde konumlandırılabilmektedir.[73] Kopenhag okulunun güvenlikleştirme anlayışı, sert güç üzerinden değerlendirilen aktörlerin askeri güç dışındaki alanlara doğru genişleyerek insan yaşamının her alanını kapsayacak şekilde yorumladığı bir yapıya sahiptir.[74] Bölgesel güvenlik kavramı, Barry Buzan tarafından ilk olarak Halklar, Devletler ve Korku isimli kitabında savunulmuştur. Buzan, teoriyi Paul Huntington'un "Medeniyetler Çatışması" isimli eserinde öne sürmüş olduğu düşüncelere eleştiri olarak meydana getirmiştir. Buzan bölgesel güvenlik anlayışını iki ayrı temel üzerine oturtmaktadır. Güç dengesi oluşumunda devletlerin birbirine olan yakınlık ilişkisini ve devletlerin dostluk-düşmanlık düşüncelerini tarihsel süreçlerine bağlamaktadır.[75] Sektörel güvenlik yine Buzan tarafından açıklanmakta ve bu tezinde güvenlik konularını devlet merkezli olarak açıklamanın yetersiz ve tek merkezli kalabileceğini belirtmektedir. Kopenhag ekolünün öne sürdüğü savlar çerçevesinde, güvenliğin askeri olmayan boyutları tartışılarak devletlerin karşılaşabileceği muhtemel tehdit ve risklerin farklı alanlarda incelenmesi mümkün olabilmektedir.

1.3.2 Kopenhag Ekolünün Güç ve Güvenlik Anlayışı

Kopenhag ekolü, güç kullanımını devletlerin haklılık içerisinde bulunması, yasal yollar içerisinde olması ve kamu vicdanının meşru gördüğü faktörler üzerinden tartışmaktadır. Zira, soğuk savaş sonrası dönemde modern devletlerin güç politikaları kendi toplumsal varlığını kapsamakta ve uluslararası sistemin dinamiklerine göre zemin bulmaktadır.[76] Asimetrik bir güç ve güvenlik paradigması üzerinden şekillenen bu

[73]Evren Balta, a.g.e, s.253
[74]Övgü Kalkan Küçüksolak, "Güvenlik Kavramının Realizm, Neorealizm ve Kopenhag Ekolü Çerçevesinde Tartışılması", **Turan Stratejik Araştırmalar Merkezi Dergisi**, S.14, (İlkbahar 2012), s.205
[75] Aslan Yavuz Şir, "Bölgesel Güvenlik Kompleksi Teorisi, Enerji Güvenliği ve Rusya'', Global Strateji Enstitüsü 2.Sosyal Bilimciler Kongresi, 2003, s. 346.
[76] Barry Buzan, "Barış, Güç ve Güvenlik: Uluslararası İlişkilerde Çatışan Kavramlar", Çev: Özden S. Sarı, **Uluslararası İlişkilerde Anahtar Metinler**, der. Esra Diri, Ankara: Uluslararası İlişkiler Kütüphanesi, 2013, s.169

zeminde güçlü ve güçsüz aktörlerin bağımlılıkları ve kırılganlıkları ise, güvenliğin almış olduğu söz konusu çok boyutlu hal nedeniyle çok farklı konular bağlamında değişkenlik gösterebilmektedir.

Karşılıklı bağımlılık içerisinde iletişim ve birbirleriyle etkileşim içerisinde bulunan devletler arasında farklı güvenlik sektörleri ortaya çıkmaktadır. Kopenhag ekolü düşünürleri tehdit unsurlarının çeşitlilik içerisinde bulunabileceğini düşünmektedirler. Zira, iş birliği içerisinde bulunan devletler küreselleşme sonucunda farklı tehdit kaynakları altında kalabilmektedir.[77] Değişken bir yapıya sahip olan güç, güvenlik ortamına göre değişebilmektedir. Kopenhag ekolü, güvenlik anlayışında değişimi, bu değişimin aktör boyutlarında ise, devlet dışı kuruluşların ve bireyin öne çıkarak insan güvenliğinin üzerinde durulmasını savunmaktadır.[78] Yine aktör bazında düşünüldüğünde, ekolün önde gelen isimlerden Ole Weawer ulusa odaklanılması ile yeni güvenlik alanlarından toplumsal sektörün oluşacağını belirtmektedir.[79] Ekölün devletin yanısıra bireyi ve toplumsal grupları güvenlik çalışmalarına dahil etmesi ile yeni bir akım oluşturduğu düşünülebilmektedir. Sistemli bir şekilde uluslararası ilişkilerde güvenlik üzerine çalışma yapan Kopenhag ekolü, güvenlikleştirme, sektörel güvenlik ve bölgesel güvenlik konularıyla devletin dışında kalan aktörleri analizi dahil ederek çok daha kapsamlı bir yaklaşım sunmakta ve toplum ve bireyin içinde bulunduğu güvenlik komplekslerini açıklamaktadır.

Güvenlikleştirme, devlet içerisinde yaşanan bir olayın hangi sebepler doğrultusunda güvenlik alanına girdiğini açıklamak adına kullanılabilmektedir.[80] Bir nevi bu kavram ile toplumu ilgilendiren herhangi bir olayın güvenlik alanı içerisine dahil edilmesi ve bu çerçevede şekillendirilmesi sürecinin incelendiğini söylemek mümkündür. Gündelik bir konunun politika yapıcılar tarafından şekillendirilip, medyanın da desteğiyle, bir güvenlik konusu olarak halka sunulması ve halktan kabul görmesiyle

[77] Bekir Aydoğan, Hakan Aydın, **Güç Kavramı, Kamu Diplomasisi ve Güvenlik**, İstanbul: Ekopolitik Uluslararası İlişkiler Masası, 2011, s.39
[78] Bekir Aydoğan, Hakan Aydın, a.g.e., s.42
[79] Ole Waewer, "Toplumsal Güvenliğin Değişen Gündemi", **Uluslararası İlişkiler Dergisi**, C.5, S. 18 (Temmuz 2008), s. 153
[80] Nebi MİŞ, "Güvenlikleştirme Teorisi ve Siyasal Olanın Güvenlikleştirilmesi", **Akademik İncelemeler Dergisi**, C.6, S.2 (Temmuz 2014), s.348

güvenlikleştirilmesi, güvenliğin bir söylem olduğuna da işaret etmektedir. Bu nokta da güvenliğin farklı sektörleri kapsayan çok boyutlu yönünü, şekillendirilmesi sürecinin önemini ve süreç içerisinde rol oynayan aktörlerin etkinliğini gözler önüne sermektedir. Güvenlik alanını aktör ve konu bazında genişleten ve derinleştiren Kopenhag ekolünde güvenliğin inşa süreçleri incelenmekte, toplum ve birey güvenliğinde rol oynayan ekonomik ve refah faktörleri, çevresel faktörlerin bileşenleri, siyasi ve kültürel hakların en üst seviyeye çıkartılması gibi konular güvenlik unsurlarını etkileyen argümanlar olarak belirlenmektedir.[81]

Sektörel güvenlik, Kopenhag ekolünün ortaya çıkış amacı olarak güvenliğin askeri olmayan boyutlarının tartışılması üzerinden şekillenmektedir. Güvenlik tehditlerinin başlıklar altında tartışılmasını vurgulayan[82] Buzan, "*People, States and Fear*" kitabında güvenliği askeri güvenlik, siyasi güvenlik, ekonomik güvenlik, sosyal güvenlik ve çevresel güvenlik olmak üzere beş ayrı boyutta incelemektedir. Bu alanlar hakkında: [83]

- *Askeri güç*: kullanımı özel bir kategori içeriğinde olabilir, çünkü söz konusu askeri güç unsurunun kullanımında barışçıl durumda bulunan ilişkilerin ihlali oluşabilir. Askeri alanda oluşturulmuş bütün zorunlu şeylerin güvenlik ile ilgisi olmayabilir. [84]
- *Siyasi güvenlik:* Buzan, devletin üniter bir aktör olmadığını belirtmektedir. Devlet politikalarının uluslararası arenada uyuşması gerekmemekte ancak devletlerin iç politika sorunlarına çare bularak rejimlerini ve bağımsızlıklarını koruma altına almaları gerekmektedir.
- *Ekonomik güvenlik:* alanında devletlerin durumu riskli olabilir. Politik anlamda kendini tanımlamış bir ülkenin ekonomik sorunlar ile karşılaşması muhtemeldir. Ekonomik tehditler askeri tehditlere göre daha sınırlı olabilmektedir. Aktörlere

[81] Selim Kurt, "Toplumsal Güvenliğin Yükselişi", International Journal of Social Science, No:37, (Eylül 2015), s.465
[82]Barry Buzan, **People, States and Fear**: The National Security Problem in International Relations, BrightonWheatsheaf Book, Brighton Sussex, 1983, s.20
[83] Barry Buzan, **a.g.e**, s.25-232
[84] Barry Buzan, "Askeri Güvenliğin Değişen Gündemi", **Uluslararası İlişkiler De**rgisi, C.5, S. 18 (Yaz 2008), s. 108

uygulanacak olan ambargo, petrol tehditleri gibi bir anda şişirilen fiyatlar ile aktör kendisini bir tehdit ile karşı karşıya bulabilmektedir.

- *Sosyal güvenlik:* ekonomi ile bağlantılı olabilmektedir. Buzan, bu konu için bireylerin işsiz kalması üzerine örnek vermektedir. İşsiz kalanlar için devlet, sağlık ve sosyal güvence ile bireylerin güvenliğini sağlayabilmektedir. Ayrıca Buzan dilin çok önemli olduğunu vurgulamaktadır. Din, yerel kültür ve geleneklerin de dışarıdan gelebilecek olan tehditlere karşı korunması gerektiğini belirtmektedir.
- *Çevresel güvenlik:* ekolojik sistem içerisinde oluşan tehditleri incelemekte ve ekolojik döngü çerçevesinde devletin kurumlarının, bireylerin ve tüm canlıların süreçteki rolleri üzerinde durmaktadır. Ekolojik sistem içerisinde doğal afet olarak görünüp güvenlik için bir tehdit unsuru oluşmadığı düşünülse dahi, Buzan kuraklık, fırtına, deprem vb. olayların kitlesel göç ve çatışma olaylarında önemli rol oynayabileceğini ifade etmiştir.

Kopenhag ekolünün diğer önemli noktalarından biri de bölgesel güvenlik kompleksidir. 1990'lı yıllarda bu yaklaşımın asıl amacı, aktörlerin güvenlik açısından bölge içerisindeki etkinlik durumlarının ön planda tutulmasıdır.[85] Yaşanan son yüz yılda dünya dört büyük medeniyet olan Avrupa, Ortadoğu, Hindistan ve Çin alanlarından ayrılarak bağımsızlıklarını kazanan devletler ile farklı bölgeler oluşturmaktadır.[86] Bölgelerin farklılaşması nedeniyle zaman içerisinde ekolün yaklaşımında değişiklikler olmuştur. 1995 sonrası bölgesel güvenlik anlayışı güvenlik kompleksleri oluşturularak aktörlerin etkin dinamikleri ele alınmaktadır.[87] 2000 li yıllarda ise ekolün önemli düşünürleri, devletlerin birbirine yakın olması doğrultusunda güvenlik açısından karşılıklı bağımlılık oluşturduğunu savunmaktadır. Bu duruma en iyi örnek olarak Soğuk Savaş sonrası dönem gösterilebilmektedir. Zira, tehdidin uzaktan değil yakın bir

[85] Başar Baysal ve Çağla Lüleci, "Kopenhag Okulu ve Güvenlikleştirme Teorisi," **Güvenlik Stratejileri Dergisi**, Y.11, S.22, (Ekim 2015), s.73
[86] Barry Buzan, **İnsanlar Devletler ve Korku**, Çev: Emre Çıtak, İstanbul: Uluslararası İlişkiler Kütüphanesi (2015), s.168
[87] Başar Baysal ve Çağla Lüleci, a.g.e., s.74

coğrafi alandan gelme olasılığı daha yüksek olabilecektir.[88] Bölgesel güvenlik kompleksinin tanımının zaman içerisinde gözden geçirilerek değiştiği görülmektedir. Buzan ve diğer düşünürlerin bu değişikliğe yer vermelerinin nedeni Soğuk Savaş sonrası iki ayrı süper güce karşı bağımsız devletlerin kendi bölgelerinde daha özerk bir hal almasıdır.

Bölgesel güvenlik tanımlanması sonrası, güvenlik kompleksi daha önemli bir boyut kazanmaktadır. Zira, güvenlik kompleksi kapsamında coğrafi yakınlık önemli olabilmekte ancak hayati bir kriter teşkil etmemektedir. Avrupa Birliği örneğinde olduğu gibi coğrafi uzaklık önemli bir alan değildir. AB, güvenlik tehdidine karşılık tek bir aktör olarak davranmaktadır. Güvenlik kompleksinin tanımlamasında da devletlerin ortak bir tehdit belirlemesi bulunmaktadır. Dünya ortak sorunlara sahip olabilir. Soğuk Savaş sonrası dönemde medeniyetler arası tehditlerin oluşmasından ziyade bölgeler arası ya da bölge içi güvenlik sorunları oluşmaktadır.[89] Bu durumda tehditlerin meydana geldiği coğrafyalarda devletler iş birliği içerisinde bölge içinde ya da bölge dışında oluşan çatışmaları azaltmaya çalışmaktadırlar. Oluşan bu siyasi hareketlilik ve devletlerin işbirliği içerisinde hareket etmesi güvenlik kompleksi teorisini tanımlamaktadır. AB gibi tek vücut halinde hareket eden devletler için güvenlik kompleksi önemli bir kriter halini almaktadır. Güvenlik gündemi doğası gereği değişiklik gösterebilmektedir. Güvenlik kompleksinin oluşumunda da devletlerin birbirileri olan etkileşimi sonucu sadece sınırlarının askeri açıdan tehdit altında olması değil, güvenlik alanına giren diğer konular kapsamında değerlendirilmesi de önemli gündem maddesi halini almaktadır. Yukarıda da izah edildiği gibi Kopenhag ekolünün asıl amacı güvenlik analizini bütüncül bir şekilde ele almasıdır. Güvenliği sadece sınırlardan gelen tehditler olarak görmeyerek, ayrı ayrı vuku bulan sektörlerde güvenlik komplekslerini tanımlamaya çalışmaktadır. Günümüzde ise aktörlerin, Siber Uzay' dan gelecek olan tehditleri ortak sorun olarak kabul edip, ortak çözümler getirerek siber güvenlik kompleksini oluşturmaları gerekmektedir.

---

[88] M. Seyfettin Erol, Mehmet Şahin, "Bağımsızlıklarının 20. Yılında Orta Asya ve Kafkasya'daki Türk Cumhuriyetlerinin Entegrasyon Süreci (1991-2011), **Karadeniz Araştırmaları Dergisi**, S.137, (Bahar 2013), s.112

[89] Fikren Birdişli ve Merve Gönen, "Bölgesel Güvenlik Kompleksi Teorisi bağlamında Türkiye-İran Arasında Göç ve Sınır Güvenliği", **İran Çalışmaları Dergisi**, C.1, S.2, (2017), s. 13

2. SİBER GÜÇ ÇERÇEVESİNDE GÜVENLİK DİNAMİKLERİNİN YORUMLANMASI

2.1 Siber Uzayın Açıklanması

Siber betimlemesi üzerine ortak kabul görmüş bir tanım yapılması son derece güç olmaktadır. Siber uzay kavramını internet teknolojileri kapsamında insan eliyle üretilmiş bir alan ve insanların birbirleriyle hızlı bir şekilde dijital alanda iletişim halinde bulunmaları olarak tartışmak mümkündür.[90] Bu iletişim sayesinde bilgi sadece saklama alanı değil, teknoloji ile senkronize bir şekilde kullanılma, işlenme ve insan üstü bir hızda insan tarafından dağıtılma aracı halini almaktadır.[91] Bilginin dağıtım hızının yüksekliği ve siber uzayın sınırsızlığı güvenliğin çok farklı boyutlarını ve bu boyutların hassasiyetini gözler önüne sermektedir. Siber alanın sağladığı teknolojiler yeni ve artan haberleşme alanları, askeri platformda yeni cepheler, ekonomik sistemin kontrolünün sağlanmasında yeni erişim kaynakları ya da aktörler arasında oluşacak farklı politik alanlar açmaktadır[92].

İnternet kavramıyla özdeşleşen siber uzay alanı, William Gibson'ın 1984 yılında yayınlanan Neuromancer isimli kitabında kullanılmıştır. Gibson kitabında yirmi dört yaşında bir hırsız olan Case'in bir jak ile siber uzay içerisinde bulunan sisteme bağlandığını ve iş verenlerin vermiş olduğu önemli yazılımlar sayesinde büyük şirketlerin sistemlerine giriş yaptığından bahsetmektedir.[93] İnternetin temelinin soğuk savaş yıllarında atıldığı düşünülebilir. 4 Ekim 1957 yılında dünya yörüngesine ilk yapay uyduyu yerleştiren ve sonrasında canlı bir köpek ile Sputnik 2'yi uzaya gönderen Sovyetlere karşı teknoloji oluşturmak amacıyla ABD ARPA (Advanced Research

[90] Ali Burak Darıcılı, "Askerleştirilen ve Silahlandırılan Siber Uzay", **Sosyal ve Beşeri Bilimlere Dair Araştırma Örnekleri**, der. Ali Acavavcı, Ankara: Nobel Yayınları,2018, s.311
[91] Seda Yılmaz, Şeref Sağıroğlu, "Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri",**6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı**, Ankara: Eylül 2013, s.158
[92] Ali Burak Darıcılı, **Siber Uzay ve Siber Güvenlik Nedir? Abd 'nin Siber Güvenlik Stratejisi Rusya Federasyonun Siber Güvenlik Strate**jisi, Bursa, 2017, s.2
[93] William GIBSON, **Neuromancer**, Çev: Gonca Gülbay, İstanbul: Altıkırkbeş Yayın, (2012),s.8

Projects Agency) teknolojisinin temellerini atmıştır.[94] Ticari ve askeri alanda kullanılmaya başlanan ARPA, 1970'li yıllarda da ABD müttefikleri tarafından iletişim ağı için hızla kullanılmaya başlanmış ve FTP (File Transfer Protocol) dosyalarının aktırılmasıyla oluşturulan ARPANET sistemi ile internetin temelleri atılmıştır.[95] 1980'li yıllarda durum mesajlarına gelen ilk virüs sonucu sistemin durmasıyla beraber siber güvenlik konusu üzerinde tartışmalar başlamıştır.[96] Soğuk savaş sonrası dönemde yoğun bir kullanıma ulaşan siber uzayın güvenliği farklı sektörler ve aktörler üzerinden kapsamlı bir güvenlik yaklaşımı çerçevesinde tartışılır hale gelmiştir. Başlangıç itibariyle askeri alanda güvenlik sağlanmak amacıyla oluşturulan siber araçlar realist teori çerçevesinde değerlendirilebilecekken, geldiğimiz aşamada siber uzayın farklı aktörler ve konular üzerindeki etkileri siber güvenliğin Kopenhag ekolünün genişleyen güvenlik yaklaşımı çerçevesinde irdelenmesini zorunlu kılmaktadır.

2.2 Siber Güç Kavramsallaştırması

İnsan hayatının hemen hemen her alanına sızarak, bireyi siber alana bağımlı kılan ve onu "netizen"lere dönüştüren siber gücün dinamiklerinin anlaşılması ve bu alandaki güvenlik zafiyetlerinin azaltılması adına söz konusu gücün hangi statüde değerlendirilmesi gerektiğine dair çok çeşitli tartışmalar süregelmektedir. Siber güç kavramının uluslararası ilişkiler teorileri ve bu teorilerin belli başlı argümanları içerisinde değerlendirilmesi son derece karmaşık bir hal almaktadır. Siber alanın insan hayatına yoğun olarak girmesi ile gücün çok yönlü bir değişime uğrayacağını belirten Joseph Nye siber gücün hem sert güç hem de yumuşak güç bağlamında evrildiğini, enformasyon bakımından diğerlerini etkilememesi durumunda yumuşak güç kavramı, enformasyonun başkalarını etkilediği zaman ya da başkalarını kontrol altında tutup zarar verdiğinde ise sert güç bağlamı çerçevesinde değerlendirilebileceğini belirterek sert güç içeriğine örnek olarak Stuxnet saldırılarını göstermektedir.[97] Stuxnet virüsünün yazılımını kırarak ün kazanmış olan Ralph Langer, siber gücün kapasitesinin saldırı sonucu vuku bulan sızmanın durumuna göre belirlenebileceğini belirtmektedir. Langer

[94] Salih Bıçakcı, **21. Yüzyılda Siber Güvenlik**, İstanbul: Bilgi Üniversitesi Yayınları, (2013), s.4-5
[95] Salih Bıçakcı, a.g.e., s.7
[96] Salih Bilen, a.g.e, s.8
[97] Reyhan Güner, Joseph Nye ile Mülakat: Siber Güvenlik, Siber Güç ve Siberuzayın Geleceği Üzerine, (Çevrimiçi) https://www.academia.edu/37696368/Joseph_Nye (Erişim Tarihi: 25.10.2019), s.2

siber alanı, insanlar tarafından bir araya getirilen akıllı elektrik şebekelerinin oluşumu, siber gücü ise bir aktörün, bireyin ya da toplumun olası bir çatışma kapsamında yaptırım uygulaması üzerine oluşturulan bir dijital organizasyon olarak tanımlamaktadır.[98]

Siber uzay ve siber güç alanlarında problemleri tanımlamak adına Daniel T. Khuel' in, siber uzayın insan eliyle üretilmiş olsa dahi diğer dört alandan (hava, deniz, toprak, uzay) farklı olmadığını, bu alanlara girebilmek ve kontrol altında bulundurabilmek için insan yapımı teknolojilere ihtiyaç duyulduğunu belirtmektedir. Khuel, diğer alanlarda (hava, deniz, toprak, uzay) etkili olabilmek ve etki yaratmak için teknoloji ile birlikte operasyon yapılan bir alan olabileceğini savunmaktadır.[99] Khuel'e benzer düşünceler ifade eden John B. Sheldon da siber alan ile siber gücün birbirinden ayırt edilmesi gerektiğini belirterek, siber alanı siber teknoloji işlemlerinin gerçekleştiği ve toplumu değiştiren matbaa, telgraf, radyo, televizyon ve telefondan sonra en büyük bilgi iletme ve alma alanı olarak belirtmektedir. Siber gücü ise söz konusu alanda, teknoloji bilgileri ile gerçekleşmesi muhtemel operasyonların stratejik etki ve kontrolü olarak tanımlamaktadır. Sheldon savaşın doğasının değişmediğini betimleyerek yeni oluşum içerisinde bulunan siber alan kapsamında gerçekleştirilebilecek olan operasyonel hareketlerle karşı tarafın dijital iletişim ağının kesilebileceğini ve istihbarat birimlerinin kontrolü ele geçirilebileceğini savunmaktadır. Sheldon sert güç ve yumuşak güç unsurlarının kara, deniz, hava, uzay gibi alanlarda tek başlarına kullanılmasının yetersiz kalacağını belirterek, nispeten daha ucuz olan ve gerek barış gerekse savaş zamanında stratejik bir güç unsuru olabilecek siber gücün ulusal strateji planlamasında kullanılmasını ve güçler birleşiminin içeriğinde bulunması gerektiğini ifade etmektedir.[100]

Günümüzde siber tehdidin bireye kadar indirgenebileceğini savunan Steven Bucci, siber tehdit unsurunun basit bir ev kullanıcısından, eğitilmiş ve tam donanımlı

---

[98]Ralph Langer, Cyber Power - An Emerging Factor in National and International Security, (Çevrimiçi) https://www.cirsd.org/en/horizons/horizons-autumn-2016--issue-no-8/cyber-power-an-emerging-factor-in-national-and-international-security (Erişim Tarihi: 27.10.2019) s. 1

[99]Daniel T. Khuel, "From Cyberspace to Cyberpower: Defining the Problem", **Cyberpower and National Security**, der. Franklin D. Kamer, Stuart H. Starr ve Larry K. Went, Washington: National Defense Universıty Press, Potamac Books, 2009, s.28-29

[100]John B. Sheldon, "Toward a Theory Of Cyber Power Strategic Purpose İn Peace and War", **Cyberspace and National Security Threats, Opportunities and Power İn a Virtual World**, der. Derek S. Reveron, Washington: Georgetown University Press, 2012, s.207-211

yabancı devlet istihbarat elemanına uzanabileceğini, yöneticilerin kişisel bilgilerinin ve ulusal veri tabanlarında bulunan belgelerin ele geçirilmesine kadar uzanan geniş bir siber saldırı yelpazesinin olabileceğini, en büyük tehdit unsurunun ise gelişmiş devletler olduğunu belirtmiştir. Bucci, özellikle de gelişmiş devletlerin sahip olduğu yetenekli personelleri, ekonomik gücü ve endüstriyel anlamda tam donanımlı olabileceğinin altını çizerek, siber saldırının kalıcı ya da belirli bir süre için kontrollü bir şekilde yapılabileceğini ve bütün bu saldırılar yapılırken zorlayıcı güç halini alabileceğini, saldırdığı halkın milliyetçi duygu ve duyarlılıklarını manipüle ederek isteklerinin kabullenilmesini hızlandırabileceğini ifade etmiştir[101]. Bu düşünce ile Bucci'nin siber gücü tam olarak bir güç unsuru olarak gösterememekle beraber hem yumuşak güç hem de sert güç içeriğinde tanımladığı anlaşılmaktadır.

Joseph Nye, yaşadığımız yüz yılın diğer yüz yıllar ile karşılaştırmasının dahi yapılmaması gerektiğini belirterek, iletişim çağında bilgi çokluğu nedeniyle bilginin odak noktasının çok iyi belirlenmesini, politikanın çizgisine aykırı davranılan iletişim stratejisinin ise hiçbir işlev göremeyeceğini belirtmektedir. Yumuşak güç ve akıllı güç unsurlarının çok iyi şekilde kullanılarak bunun yanında teknoloji ile karşılıklı ağların oluştuğunu ve bu bağlamda ağ kurmanın çok önemli bir seçenek haline geldiğini söylem olarak savunurken siber alan kullanımına işaret etmektedir.[102] Zira siber alan ile tüm toplumların ağlar ile bağlantılı bir yaşam kurmaya başladığı dönemde, bir taraftan coğrafya üstü oluşan bu küreselleşme halinde sınırlar ve uzaklıklar bir tehdit unsuru olmaktan çıkabilmektedir. Yaşadığımız dünya bir ağ ile bağlantılı olmakta, terörist grupları yok eden askerler bunu bilgi aktarımı ve bir ağ vasıtasıyla yapmakta, siber diplomasinin adımları atılmakta, iş dünyasının yöneticileri dijitalleşme düşüncesiyle hareket etmekte, her zaman büyük güç unsuru olarak düşünülen medya ağlar ile anlık olarak bilgi aktarmakta, Facebook, Twitter, Instagram gibi geniş sohbet alanları sayesinde milyonlarca birey aynı anda küresel bir bağ oluşturabilmektedir.[103] Teknolojinin hızlıca gelişmesi ile ağlar ağı ile birbirine bağlı olan bütün bilgisayar

[101] Steven Bucci, "Joining Cybercrime and Cyberterrorism A Likely Scenario, **Cyberspace and National Security Threats, Opportunities and Power İn a Virtual World**, der. Derek S. Reveron, Washington: Georgetown University Press, 2012, s.57
[102] Joseph Nye, a.g.e., s.153-167
[103]Anne-Maria Slaughter, "America's Edge: Power in the Networked Century", **Foreign Affairs Dergisi,** S.88, (Ocak/Şubat 2009), s.94

kullanıcıları,[104] internet ile kullanıcıdan kullanıcıya, kullanıcıdan kullanıcılara bağlanıp çok sayıda bireyin iletişimi sağlanabilmektedir.

İletişimin gelişmesi ve hızlanmasında kuşkusuz teknolojinin büyük önemi bulunmaktadır. Teknolojilerin ve bilişimin çok yoğun olarak kullanılması neticesinde; kullanıcıların bilgisayar güvenliklerine karşı çok sayıda saldırıya maruz kalabilmektedir. [105] Bilgisayarlarda bulunan bir devlete, şirkete, kişitye ait bilgiler kritik öneme sahip olabilir. Siber uzay içeriğinde bulunan bilgilerin düşmanın ele geçirmesi ile zarara uğratabilmektedir. Bu nedenle siber uzayda bilgilerin işlem gördüğü bilgisayar ve internetin güvenliği büyük önem arz etmektedir. Sayısallaşan günümüz uluslararası ilişkilerde olan gündemini siber dünya üzerinden tekip etmeye başlayabilir. Kişilerin, şirketlerin ve devletinerin bilgi sistemleri, iletişim kaynakları, ticari faaliyetleri siber uzayın içeriğinde gelişim göstermektedir. Günümüzde bilgisayar kullanıcısın artması doğrultusunda saldırı sayılarıda doğru orantılı olarak artmaktadır. [106] Günlük hayatın içerisinde gerçekleştirilen çok sayıda işlemler elektronik ortamlarda siber dünyanın ortamlarında yapılmaya başlanmış olması, siber güvenliğin sağlanmasının zorunluluk oluşturduğu anlaşılmaktadır. Bu nedenle kullanılan internet için;

Tablo 2: Anlık olarak internet kullanıcıları ve internet ile bağlantılı olan diğer bileşenler gösterilmektedir. Bu veriler her an güncellenmektedir. Erişim tarihi dikkate alınmalıdır. (Erişim Tarihi: 27.10.2019)

Anlık olarak İnternet Kullanıcıları	*4,375,683, 375 …*
Bugüne Kadar Açılan Web Sitesi	*1,724,197,975*
Bugün Gönderilen E-Posta	*248,873,292,621*
Bugün Google İle Yapılan Arama	*6,566,640,527*
Bugün Yayınlanan Tweetter	*731,863,260*

[104] Peter Burke, **a.g.e**., s.139

[105]Gürol Canberk, Şeref Sağıroğlu, "Casus Yazılımlar: Bulaima Yöntemleri ve Önlemler", **Gazi Üniversitesi Mühendisik ve Mimarlık Fakültesi Dergis**i, C.23, S.1, 2008, s.165

[106] Gürol Canbek, Şeref Sağıroğlu, "Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme", **Erciyes Üniversitesi Fen Bilimleri Dergisi**, C.23, S.1-2, 2007, s.2

Bugün Youtube İçeriğinde İzlenen Video	*6,825,576,840*
Bugün İnstagram Yüklenen Fotoğraf Sayısı	*79,872,000*
Bugün Satılan Bilgisayar Sayısı	*677,467*
Bugün Satılan Akıllı Telefon Sayısı	*4,127,986*
Bugün Oluşan İnternet Trafiği	*6,832,743,426 GB*
Bugün İnternet İçin Kullanılan Elektrik	*3,923,676 Mega Wat*

Kaynak: https://www.internetlivestats.com/

Tabloda gösterilen veriler ışığında bu derece anlık olarak hızlı kullanımı olan siber alanın kendisinin bir yansıması olarak görülebilmektedir. Yukarıda birçok düşünürün tanımlamaları doğrultusunda, kontrolü ve üzerinde kurulabilecek bir güç kavramı için herhangi bir statü değerlendirmesi yapılmamaktadır. Bunun nedeni kavramın akademik sistemde arıtılmış olmaması, analitik bulanıklık içerisinde olup teori kapsamında yetersiz kalması olarak değerlendirilebilir.

2.3. Siber Güç Çerçevesinde Değişen Güvenlik Parametrelerinin İncelenmesi

Siber uzayın gerek çok sayıda kullanıcısı olması gerekse ihtiva ettiği işlem hacmi ve bunların kritik içeriği nedeniyle sadece iletişimin sağlandığı bir alan olmanın ötesinde güvenliğin sağlanmasının öncelikli alanı haline geldiği görülmektedir. Siber saldırılar alt yapısı yönünden çok daha yıkıcı, sistematik şekilde büyük çaplı olayların gerçekleşmesine neden olabilmektedir. Bir öncekinin gelişimi olarak ilerleyen teknolojinin gelişme süreci toplama şeklinde değil katlanarak büyüme şeklinde gerçekleşmektedir. Siber uzayın kapasitesi bu hızlı katlamalı artışlar ile daha fazla bilginin insan eline ulaşımına izin vermektedir.[107] Teknolojinin gelişimi ne kadar hızlı

[107] Ray Kuzwell, **İnsanlık 2.0 Tekilliğe Doğru Biyolojisini Aşan İnsan**, Çev. Mine Şengel, İstanbul: Alfa Yayınları, 2016, s.69

olursa insan ilişkileri ve birbirileri ile olan bağlantısı daha fazla olacaktır.[108] Günümüzde nüfus oranına göre; Asya ülkelerinin yüzde 50,7' si, Avrupa ülkelerinin yüzde 16,0'ı, Afrika ülkelerinin yüzde 11,5'i, Latin Amerika ülkelerinin yüzde 10.0'ı, Kuzey Amerika ülkelerinin yüzde 7,2'si, Ortadoğu ülkelerinin yüzde 3,9'u, Avustralya ülkelerinin ise yüzde 0,6'sı internet kullanmaktadır.[109] Dünya nüfusunun neredeyse yarısının internete bağlı olarak haberleşme, resmi işlemlerini takip etme, sosyal alan oluşturma gibi geniş bir alan oluşturuyor olması yumuşak güç argümanları doğrultusunda değerlendirildiğinde, siber uzayın devlet politikaları ve uygulanabilecek siber baskı araçlarının önemi açısından yeri daha net bir şekilde anlaşılmaktadır.

Siber uzayda birbirine bağlı kullanıcıların eğitilmesi, bütün halinde siber alanın koruma altına alınması ve koruyucu tedbirlerin uygulanması siber güvenlik olarak tanımlanabilir. Bilgisayarlar kablolu ve kablosuz ve sistematik olarak internet üzerinden birbirine bağlanmaktadır. Bilgisayar alanlarını birbirine bağlayan internetin beş farklı zafiyeti bulunmaktadır:[110]

- Taşıyıcı olarak tanımlanan ISS (İnternet Servis Sağlayıcılarının) internetin omurga sistemini oluşturmak suretiyle ilk taşıyıcı görevini görmektedir. Ev ve ofislere şirketler tarafından satılan bu ISS'ler şehirlere büyük fiber optiklerden gelerek küçük bir yapıda giriş yapmaktadır. Basit bir kullanıcı herhangi bir internet sitesine bağlandığı zaman ISS' ler üzerinden giriş yapmaktadır. Bu çerçevede, internete kablolu bağlanıldığı zaman çok daha basit ve kolay bir şekilde saldırıya maruz kalınabilmektedir. Kablosuz bağlanması durumunda ise, telsiz dalgaları arasından yine saldırıya maruz kalınabilmektedir.
- İnternetin belli bir üst yöneticisinin bulunmaması, tam anlamıyla anarşik bir sistem içerisinde bulunulduğunu göstermektedir. Teknik sistemi bulunmakta ancak herhangi bir yetkili makamı bulunmamaktadır.
- İnternetin güvenlik açısından zayıf bir yapıya sahip olması herhangi bir sisteme giriş yapmayı başarabilen bir virüse, bilgisayar üzerinde bulunan bütün

[108] Klaus Schwab, **Dördüncü Sanayi Devrimi**, Çev. Zülfü Dicleli, İstanbul: World Economic Forum, 2017, s.114
[109] Internet Usage Statıstıcs, http://www.internetworldstats.com/stats.htm (Çevrimiçi: 15.02.2020)
[110] Richard A. Clarke, Robert K.Knake, **Siber Savaş: Ulusal Güvenliğe Yönelik Yeni Tehdit**, Çev. Murat Erduran, İstanbul: İKÜ Yayınevi, 2011, s. 45-47.

programları kontrol etme şansı ve iletişim ağını kontrol edebilme gücü vermektedir.

- Malware[111] altında sıralanan kötü yazılımlar çok rahat bir şekilde bütün internet dünyasında bulunmaktadır. Malware'nin kullanım amaçları, bilgisayarın yazılımını kontrol altında tutarak yok etmek, haksız para kazanmak, kişisel bilgileri çalmaktır.
- Yapısı itibariyle incelendiğinde, İnternette ortak bir merkezin yokluğu hissedilmektedir. Kullanış biçimi kapsamında devletin kontrol altında bulunduramayacağı bir yapı arz etmektedir.

Siber uzay her geçen gün katlanarak büyümeye devam etmektedir. Küreselleşme sürecine teknoloji ile hızlı bir katkı sağlamaktadır. Bireyden topluma, toplumdan devletin önemli organlarına kadar kullanımı zorunluluk halini alan siber uzayın güvenliğinin sağlanması da gittikçe daha fazla boyutu ilgilendirmekte ve hassas bir yapıya işaret etmektedir. Gelecekte devletlerin diplomasilerini siber uzay üzerinden oluşturabilecek olmaları da siber uzayın uluslararası ilişkiler disiplininde tartışmalara konu olacak bir alan haline geleceğini göstermektedir. Bu derece önemli olan siber uzayın olumlu ve olumsuz yönlerini şu şekilde sıralamak mümkündür: [112]

Siber uzayın olumlu yönleri:

- Kolay erişebilme
- Kolay kullanım sağlama özelliği, özellikle bilgisayar donanımları ile hızlı ve kolay kullanım oluşturması
- Bilginin hızlı bir şekilde yayınlanması
- Şifreleme sistemlerinin bulunuyor olması
- Belirsiz kimlik ile siber uzayda faaliyet gösterilebilmesi
- Günün her saati ulaşılabilir olması
- Coğrafya, bölge ya da sınırı bulunmaması

Siber uzayın olumsuz yönleri:

[111] Kötü amaçlı yazılımlara verilen isimdir. Daha fazla bilgi için bkz. https://wmaraci.com/nedir/malware (Çevrimiçi:21.02.2020)

[112] Gürol Canbek, Şeref Sağıroğlu, **Bilgi ve Bilgisayar Güvenliği Casus Yazılımlar ve Koruma Yöntemleri**, Ankara, 2006, s.95

- Virüsler ile yapılan saldırılar ya da yazılımlarda bulunan açıklık nedeniyle kullanılan sistemin kolayca çökmesi
- Kötü amaçlı kullanımın çok kolay olması
- Donanım ve yazılımın saldırıya uğrama riskinin yüksek olması
- Bilginin hızlı aktarımı her ne kadar olumluysa, yanlış bilginin hızlı aktarılması da bir o kadar ciddi sonuçlara neden olabilmektedir.
- Belirsiz kimlikle faaliyet gösterilebilmesi bir yandan olumlu değerlendirilebilecekken, kötü amaçlı kullanımlarda kimlik tespitinin zorluğuna işaret etmektedir.

Siber uzayda bilgilerin sınır tanımadan, kimliksiz kişilerce hızlıca yayılabilir olması kontrolünü zorlaştırmaktadır. Dünyanın herhangi bir yerinde örneğin Müslümanlığa karşı yapılan kötü bir hareketin internet üzerinden hızlı bir şekilde yayılması neticesinde halkların oluşturduğu tepki bir baskı aracı haline gelebilmektedir. Zira kamu diplomasisinin oluşumunda halkların tepkisi ve duruşu önemli rol oynamaktadır.[113] Siber uzay, teoriler kapsamında değerlendirildiğinde neo-liberal yaklaşımın yumuşak güç perspektifi ile değerlendirmelere konu olabilmektedir.[114] Realist perspektiften bakıldığında ise, anarşik bir yapıya sahip bu yeni alanda devletlerin güç arzusu belirleyici rol oynayabilmektedir. Kopenhag ekolünün kapsamlı güvenlik yaklaşımı çerçevesinde incelendiğinde ise siber uzayın uluslararası alanda daha güvenli olması için karşılıklı olarak düzenlemeler yapılması elzemdir.

Bilgi çağı olarak adlandırılan yirmi birinci yüzyılda, bilgisayar ağları bireylerin ceplerinde bulunan ve iletişimi sağlamak adına kullandıkları telefonlara kadar inmiştir. Bu ağ, bireylerin hayatlarını kolaylaştırdığı gibi devletler için de önemli güvenlik aksiyonlarının oluşturulması anlamına gelmektedir. Günümüzde yazılımlar geliştikçe gerek birey gerekse devlet için bilgisayarlar ve siber uzay hayati öneme haiz bir bilgi alt yapısı arz etmektedir. Devletin oluşan bu alan kapsamında bireyin güvenliğini sağlayabilmesi adına hem güçlü olabilmesi hem de güvenlik politikalarını en üst seviyede tutabilmesi gerekmektedir. Kullanımı bu derece yaygın olan siber uzaya karşı

[113] Joseph S. Nye, **The Future of Power**, New York: PublicAffairs, 2011, s.109
[114] Joseph S. Nye, **a.g.e**., s.109

yapılan saldırılar silahlardan ve konvansiyonel savaşlardan daha etkili sonuçlar verebilmektedir. Gelinen noktada, kötü amaçlı bir kişinin, siber imkanları bir nevi silah haline getirerek devlete karşı çok büyük zararlar verdirebilecek kabiliyetler kazandığı görülmektedir.[115] Bu operasyonlarda bireyler, şirketler ve devletlerde kim daha iyi koda sahip ise ve bu siber uzayın gelişen kodlarını kim daha iyi kontrol altında tutabiliyor ise dünya politikasında söz sahibi olabilme ihtimali yükselmektedir.[116]

[115] Garry D. Brown, Andrew O. Metcalf, "Easier Said Than Done: Legal Reviews of Cyber Weapons", **Journal of National Security Law and Policy**, C. 7, S. 115, (2014), s. 137.
[116] Marc Goodman, **Geleceğin Suçları Dijital Dünyanın Karanlık Yüzü**, İstanbul: Timaş Yayınları, 2016, s. 67

3. BÖLÜM SİBER UZAYDA ÜSTÜNLÜK MÜCADELESİ İÇERİSİNDEKİ DEVLETLER ve TÜRKİYE

Sınırları bulunmayan, devletlerin ulusal güvenliklerini hala ne derece zarara uğratacağı tahmin dahi edilemeyen siber uzayda meydana gelebilecek tehditleri tanımlamak oldukça güçtür. Bilinen bazı saldırılar neticesinde yıllık olarak devletlerin ekonomik zararlarının bir trilyon dolardan fazla olduğu tahmin edilmektedir.[117] Son derece hızlı şekilde ilerleyen teknolojinin gelişimini takip etmenin güçleştiği günümüzde, teknolojinin ve gündelik hayatın pek çok alanının internet ile entegre olması sonucunda çok dinamik bir yapı ortaya çıkmaktadır. Bu dinamik yapı bireyden uluslararası şirketlere, buradan devletlere kadar uzanan çok düzeyli, çok aktörlü ve çok boyutlu karmaşık bir içeriğe sahiptir. Ağların güvenliğini sağlamak adına devletlerin güvenlik politikalarını siber uzayda e-sisteme taşımaları gerekmektedir. Zira, siber alanda meydana gelebilecek hasarlar hakkında birçok senaryo bulunmaktadır. Örneğin, 2000'li yıllarda yahoo, amazon gibi önemli internet sitelerinin yapısına on beş yaşında bir çocuk tarafından saldırı gerçekleştirilebilmesi kötü senaryo olarak görülürken, bugün kötü amaçlı bireylerin, şirketlerin ya da devletlerin internete bağlı olarak çalışan elektrik santrallerine yapacakları bir saldırı ile karşıdaki ülkeyi tamamen karanlıkta bırakabileceği olası kötü senaryo haline gelmiştir.[118] Türkiye örneğine baktığımızda da, Batman barajından alacağını tahsis edemeyen Alman şirketinin santralde kullanılan bilgisayarları bir şifreleme sistemi ile kilitli bırakarak şehri terk ettiği görülmüştür.[119] Neticesinde, buradan elektriği sağlanan kentlere uzun süre elektrik verilememiştir. Bu hususlar da sadece devletlerin değil, şirketlerin ve hatta bireylerin de siber imkanlardan yararlanarak ne derece kapsamlı bir güvenlik tehdidi arz edebileceğini göstermektedir. Siber alanda yapılabilecek saldırı ya da engellemeler dört ana başlık altında toplanmaktadır: [120]

---

[117] Robert K. Kane, **Internet Governance in an Age of Cyber Insecurity**, E-kitap: Council Special Report No. 56, 2010, s.5

[118] Nikola Schmidt, "Cyber Security", In R. Ondrejcsák (Ed.), **Introduction to Security Studies**, Bratislava: Cenaa, 2014, s.4

[119] Milliyet İnternet Sitesi, **Batman Barajı Şifrelendi**, https://www.milliyet.com.tr/ekonomi/batman-baraji-sifrelendi-517687, (Çevrimiçi:26.02.2020)

[120] Gürol Canbek, Şeref Sağıroğlu, **a.g.e**, s.161

Yarıda kesme: Sisteme bağlı olan yazılımların hedefine ulaştırması gereken belgelerin yerine yerleştirilememesi ya da tamamen bağlantısını erişilemez hale getirmesidir.
Gizli dinleme: Pasif bir saldırı olarak tanımlanmaktadır. Sistemin içerisine yapılan giriş ile yazılım içerisinde bulunan önemli bilgileri okuma ve ele geçirme olarak düşünülmektedir. Değer verilen verilerin başkalarınca görülmesi olarak tanımlanmaktadır.

Değiştirme: Yazılım içerisine giren başkaca tarafın hedefe ulaşması gereken belgeyi, bilgiyi değişiklik yaparak aktarmasıdır. Bu değişiklik sırasında araya giren başkaca kişi bilinmemektedir. Hedefe ulaşan bilgi ana yazılım içerisinden geliyor olarak bilinir. Bu durumda sistemin yapısı değişmektedir.
İmalat veya üretim: Hedefe ulaşan suni bilgilerin ana yazılım içerisinden geliyor gibi gösterilmesidir. Diğer taraf sahtecilik oluşturmaktadır.

Günümüzde dengelerin sağlanması adına siber uzayda sürekli güncel olan gelişmeler devletler için önem arz etmektedir. Yukarıda izah edildiği gibi siber uzay ve siber güvenlik için genel geçer bir tanım halen yapılamamaktadır. Yapılmış olan saldırıların failinin devlet mi birey mi olduğu veya devlet tarafından bireye yaptırılıp yaptırılmadığı gibi soruların tespitinin mümkün olmaması nedeniyle uluslararası hukuk çerçevesinde değerlendirilmesi mümkün olmamaktadır.[121] Ancak devletler tarafından milli yazılımlar yapılarak, içerik bilgilerini kendisi oluşturacak şekilde şifreleme sistemi üretebilmektedir. Devletlerin siber uzayda güvenliklerini sağlayabilmeleri için gerek güvenlik güçlerinin eğitimi gerekse kendi idareleri içerisinde sürekli olarak güncel kalan dinamik bir yapılanmaya gitmeleri gerekmektedir. Siber uzayda saldırı düzenleme kapasitesine ve siber güç unsurlarına haiz olan ve bu anlamda öne çıkan devletlerin sistemlerindeki düzenlemeleri ve diğer çalışmaları aşağıda incelenmektedir.

[121] Muharrem Gürkaynak ve Adem Ali İren, "Reel Dünyada Sanal Açmaz: SiberAlanda Uluslararası İlişkiler", **Süleyman Demirel Üniversitesi İktisadi ve İdariBilimler Fakültesi Dergisi**, C.16, (2011), s.265

3.1 Amerika Birleşik Devletleri (ABD)

Soğuk Savaş'ın iki büyük kutbundan biri olan ve süper güç olarak değerlendirilen ABD, inovasyon sistemlerini kamu ve özel sektör üzerinden temellendirmekte ve üniversite sistemini merkezi konumda tutarak çeşitli enstitüler ve toplumsal eğitim alanları gibi bileşenler oluşturmaktadır.[122] ABD, oluşturduğu sistemde üniversitelerin her birini teknolojinin geliştirilmesi gereken bir üs olarak görmektedir.[123] ABD, yirminci yüzyılın başından itibaren kültürel, siyasi ve ekonomik gelişimine önem vermiş ve bu gelişmelere paralel olarak teknolojide ivme yakalamıştır. Müşterek teknolojik gelişimler sonucunda ve internetin atası olarak bilinen Arpanet sisteminin kurulması kapsamında ABD devlet düzeyinde siber uzayın başat aktörlerinden biri haline gelmiştir.

1990'lı yıllar internetin sivil alanda yoğun olarak kullanılmaya başlandığı, arama motorlarının ve e-postanın dolaşıma girdiği "altın geçiş" olarak adlandırılan bir döneme işaret etmektedir. Bu dönemde siber güvenlik stratejilerinde yeni düzenlemeler yapılmış, Word Wide Web (www) sistemi ile internet üzerinden bilgisayarların bağlantısı kolaylaştırılmış ve web sayfalarının daha hızlı ziyaret edilmesi sağlanmıştır.[124] Yaygınlaşan internetin bireysel kullanıma açıldığı bu dönemde siber uzayda bireysel ve toplumsal güvenlik konuları da konuşulmaya başlanmıştır. Birbirine bu kadar hızlı ve yoğun bağlanan sanal sosyal ağlar neticesinde küreselleşme süreci çok daha farklı bir yere evirilmeye başlamıştır.

ABD, siber uzayı domine edebilmek amacıyla farklı teknolojiler geliştirmektedir. Özellikle de sivil araçların dahi silah olarak kullanılabildiği ve tehdidin ne derece belirsiz olduğunu gözler önüne seren 11 Eylül 2001 saldırılarından sonra güvenlik anlamında hem araçların hem de yaklaşımın önemli bir dönüşüm geçirdiği gözlenmektedir. Soğuk Savaşın belirgin, nereden geleceği ve niteliği belli olan ve

[122]Özlem Atay, Yasemin Hancıoğlu, "İngiltere, Amerika Birleşik Devletleri ve Türkiye'nin Ulusal İnavosyon Sistemlerinin İncelenmesi: Türkiye İçin Öneriler", **Ankara Üniversitesi SBF Dergisi**, C.74, S.2, (2019), s.522
[123] Özlem Atay, Yasemin Hancıoğlu, **a.g.m**, s.525
[124] Salih Bıçakcı, "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", **Uluslararası İlişkiler**, C.10, S.40 (Kış 2014), s. 116.

mücadele kapsamında nükleer caydırıcılık stratejisi geliştirilen tehdit unsurlarından sonra, yeni dönemin kimliği belirsiz, ne zaman ve nereden geleceği belli olmayan tehditleri yükselmektedir. 21. yüzyılın güvenlik anlayışı teknoloji ve internetin hızla geliştiği ve aktörlerin bu imkanlara ve koşullara hızla adapte olduğu bir küresel yapı çerçevesinde şekillenmektedir. Sözkonusu yapı kapsamında ABD siber alanda operasyonel birimler oluşturarak tehditlere karşı proaktif politikalar izlemekte,[125] 2.900 subay ve 27.000 personel ve timler ile siber komutanlıklar kurmaktadır. [126]

3.1.1 Amerika Birleşik Devletleri' nin Siber Uzay Çalışmaları

ABD siber uzaydan gelebilecek tehditleri küreselleşen terör kapsamında tanımlanmaktadır. Siber uzay somut bir kavram değildir. Bu nedenle diğer dört operasyonel alanda ortaya konan somut güvenlik tedbirlerinin bu alanda işlerliği bulunmamaktadır. Asimetrik bir yapıya sahip olan siber tehditler süreklilik arz etmekte ve teknolojideki gelişmelere paralel şekilde adapte olabilmektedir. ABD'nin siber uzayda geliştirdiği söylemler ve ortaya koyduğu politika uygulamaları, gerek herhangi bir devletten gelebilecek saldırıya karşı koyabilme gerekse terör saldırılarında istihbarat oluşturma ya da karşı istihbarat sağlamayı amaçlamaktadır. ABD'nin dünya nüfusunun önemli bir kısmı tarafından kullanıldığı bilinen Google, Microsoft, Apple, Youtube, Facebook gibi büyük internet siteleri üzerinden e-mail yazışmalarını takip ettiği, bu alanlarda sohbet odalarını gizli bir şekilde izlediğine yönelik iddialar mevcuttur.[127] ABD' nin siber uzayda amaçladığı politikaları özetlemek gerekirse: [128]

Politika: İnternetin gelişimi sağlanırken yenilik, iletişim ve ekonomik refah üzerine kurulu, iş birliği içerisinde çalışılabilir, güvenliği sağlanmış, gizliliğe saygısı olan, gelecek nesillerin kültürel değerler içerisinde bulunmasını sağlayan, güvenli bir internet alanı kullanımı teşvik edilmektedir. Ayrıca, siber güvenliğin sürdürülebilirliğini

[125] Sait Yılmaz, "ABD İstihbaratında Yaşanan Değişimler", **Turan Stratejik Araştırmalar Merkezi Dergisi**, C.4, S.13, (Kış 2012), s.14
[126] Sait Yılmaz, a.g.m, s.14
[127] Soner Karagül, Muhammet Fatih Özkan, "Bilgi Teknolojileri ve Uluslararası İlişkilerde Fırsat-Tehdit Paradoksu", **Bilgi Ekonomisi ve Yönetimi Dergisi**, C.10, S.1, (2015), s.124
[128] The White House Executıve Orders, "**Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure**", (Çevrimiçi), https://www.whitehouse.gov/, (Erişim Tarihi: 08.03.2020)

sağlayacak uzman kişilerce işgücü oluşturularak en üst seviyeye ulaşmak için çalışılmaktadır.

Bozulma ve Koruma: ABD'nin kritik alt yapısını bozma amaçlı ve halka karşı oluşabilecek siber tehditler hakkında Dışişleri Bakanı, Hazine Bakanı, Savunma Bakanı, Ticaret sekretaryaları, iç güvenlik sekretaryaları, adli makamlar, istihbarat direktörleri, ulusal güvenlik direktörleri ve terörle mücadele başkanlıklarının müşterek olarak sürekli rapor hazırlaması gerekmektedir.

Uluslararası İş birliği: Siber uzay faaliyetlerine ilişkin olarak ABD'nin diğer devletler ile sürekli olarak bağlantı içerisinde bulunduğu gözlenmektedir. Başta internetin küresel akışının kesilmemesi gibi konular olmak üzere diğer devletler ile çeşitli konularda birlikte çalışmaktadır. Devletin gerekli mekanizmaları ve özel şirketlerin başkanları ile gerekli fikir alışverişi sağlanmaktadır. En önemli konular arasında yer alan terör kapsamında, siber güvenlik alanlarında işbirliği için katılım stratejisi ortaya konmaktadır.

ABD' nin Uzun Süreçte Siber Uzayda İşgücü Sağlaması: Siber güvenlik çalışmalarını ve iş gücünü artırmak amacıyla konuya ilişkin çalışma alanları ilköğretimden yükseköğretime kadar müfredata eklenmektedir. Geleceğin ABD' sine ait siber güvenlik politikalarının eğitim ya da özel olarak düzenlenmiş eğitim programları kapsamında yeterliliğe ulaşması amaçlanmaktadır. Devletin önemli güvenlik ve terörle mücadele birimleri ile özel sektör arasında iş birlikleri kurulmakta ve siber güvenlik alanında iş gücünü arttırmak adına raporlar sunulmaktadır. ABD' de politikalar uzun vadeli hazırlanmakta, siber güvenlikte rekabetçiliği geliştirmek adına diğer ulusların işgücü durumu sürekli gözden geçirilmektedir.

Teknolojinin gelişmesi ile devletlerin ekonomik refah seviyeleri, araştırma ve geliştirme toplulukları gün geçtikçe artmaktadır. İnsan eliyle oluşturulan siber uzayın itici güç olarak teknolojiyi ileri boyutlara taşımasında devletlerin askeri kapasiteleri ve ağ teknolojileri etkili olmaktadır.[129] Bu doğrultuda ABD'nin siber uzay alanında yapmış olduğu çalışmalar Soğuk Savaş sonrası ve 2000'li yıllardan sonra teknolojik gelişmeler

[129]Ali Burak Darıcılı, "Amerika Birleşik Devletleri'nin Siber Kapasitesinde Rol Oynayan Kurumsal Yapılanmalarının Analizi", Edt. Tayyar Arı, Çiğdem Aydın Koyuncu, **Uludağ 9. Uluslararası İlişkiler Kongresi Dünya Politikasında Kriz ve Değişim**, Bursa: Dora Yayınları,2017, s.338

ile paralel olarak ilerlemektedir.[130] ABD'nin günümüzde siber uzayı domine etme isteğinin önde gelen unsurları arasında ekonomik refah, teknolojik üstünlük ve güvenlik sağlama kaygılarını saymak mümkündür.

3.1.2 Amerika Birleşik Devletleri'nin Siber Uzay Politikaları ve Ulusal Strateji Belgeleri

Sanayi Devrimini takip eden süreçte elektrik ve bilgi sistemlerini içeren üçüncü bir devrim ve günümüzde de siber sistemlerde yaşanan dönüşümü kapsayan dördüncü endüstri devrimi yaşanmaktadır.[131] ABD, 1940'lı yıllardan itibaren teknolojik gelişmelere öncülük etmiş, bu durum 1945 yılında Vannevar Bush tarafından hazırlanmış olan "Science The Endless Frontier" (Sonsuz Sınır Bilim) başlıklı raporda da ulusal güvenliğe önem veren üç ana içerik kapsamında vurgulanmıştır. Birincisi, mühendislik araştırmalarındaki bilimsel gelişmeler çerçevesinde yeni silahların üretiminin sağlanması; ikincisi, üretilen bu silahların ilerleyen dönemde kullanım taktiklerinde gözlemlenebilecek değişimlerin farkında olunması; son olarak ise savaşı tanımlarken askeri ve sivil unsurların aktif bir şekilde katılımı ile savaşın seyrinin değiştirilmesidir.[132]

Soğuk Savaş sonrası dönemde de teknolojik gelişmelerin güvenlik anlamındaki önemine vurgu yapan raporların hazırlandığı ve politikaların bu çerçevede oluşturulduğu görülmektedir. Bu çerçevede 22 Şubat 1993 tarihinde ABD Başkanı Wiliam J. Clinton' ın yardımcısı Albert Gore tarafından bir rapor hazırlanmıştır.[133] Rapor çerçevesinde ABD'nin daha güçlü bir ekonomiye sahip olabilmesi için kritik alanlardaki teknolojilerin gelişiminin sağlanması ve bu minvalde temel bilim, matematik ve mühendislik alanlarının gelişimine vurgu yapıldığı gözlenmektedir.

---

[130] Ali Burak Darıcılı, a.g.m, s.349

[131] Encyclopedıa Brıtannıca," The Fourth Industrial Revolution," (Çevrimiçi)https://www.britannica.com/topic/The-Fourth-Industrial-Revolution-2119734 ,Erişim Tarihi:08.03.2020

[132] National Science Foundation **Science The Endless Frontier,** (Çevrimiçi), https://www.nsf.gov/, Erişim Tarihi:08.03.2020

[133] The White House Office, **Technology for America's Economic Growth, A New Direction to Build Economic Strength,** Washıngton, 1993, s. 3

Tarihi süreçte ABD'nin içinde bulunulan dönemin güç unsurlarına yönelik kapsamlı yatırım yaptığı bilinmektedir. 1907 yılında Theodore Roosevelt deniz gücü unsurlarına yatırım yapmaktadır. Bütçenin büyük bir kısmı donanmaya aktarmış ve deniz ticaretini genişleterek, deniz gücünü yükseltmiştir.[134] Franklin Roosevelt döneminde ise Pearl Harbour ve İkinci Dünya Savaşı'nın sebepleri doğrultusunda hava ve nükleer güce yatırımlarını gerçekleştirmiştir. İkinci Dünya Savaşı'nda Almanya'nın atom bombasını revize edememiştir. Almanya'nın baskılarından kaçan Yahudiler, ABD için nükleer çalışmalara girişmiş ve nükleer bombanın gelişmesini başarmıştır. İkinci Dünya Savaşı'nda savaşı bitirmeyen Japonlara karşı kullanmıştır.[135] John F. Kennedy (1960-1963) döneminde de uzayda gerçekleşecek olan gelişmeler için gerekli planlama ve yatırım işlemlerini başlatmıştır. Soğuk Savaş sonrası Joseph Nye'ın geliştirdiği yumuşak güç ile kamu diplomasisi üzerine önem vermektedir. 2001 yılından sonra 11 Eylül olayları nedeniyle terörizmi önleyici güç unsuları üzerine çalışmıştır. ABD'nin siber güç unsurları daha çok 2006-2009 yıllarından sonra şekillenmeye başlamıştır.[136] Siber uzayda güvenlikli bir alan sağlamak adına 2011 yılında, siber güvenlik kapsamında bir rapor hazırlanmış ve söz konusu rapor dört ana başlıktan oluşmuştur: [137]

Siber Politika Oluşturma: Bu alanda sınırlar dahilindeki elektrik santrallerini kontrol eden, e-devlet sistemleri oluşturan, su barajlarını kontrol altında tutabilen ve finansal sistemin içeriğini oluşturan bilgi teknolojileri yer almaktadır. Siber politikalarla amaçlanan hedefler ekonomik gelişimenin sağlanması, araştırma topluluklarının sayılarının artması, hükümetin şeffaf olması ve daha özgür bir topluma kavuşulması şeklinde ifade edilmiştir. Uluslararası alandaki hedefler arasında da artan diyalog ile yoğunlaşan ve hızlanan ticari faaliyetler yer almıştır. Dolayısıyla ağa bağlı teknolojinin daha yaygın ve küresel bazda geniş çaplı kullanımı hedeflenmiştir. ABD, siber uzay politikaları çerçevesinde geliştireceği teknolojilerin sonucunda ekonomik alanda devrim

[134] Onur Gündüz, Volkan Göçoğlu, "Ulusal Güvenlik Anlayışından ABD'nin Güvenlik Anlayışına Kronolojik Bir Bakış, " **Uluslararası Toplum Araştırmaları Dergis**i, C.15, S.21, (Ocak 2020), s.730
[135] Burak Çınar, "İkinci Dünya Savaşı'nın Başladığı Gün Avrupa'daki Durum: Ülkelerin Savaşa Hazırlık Durumları ve Bunun Savaşa Yansıması, "**Akademik Bakış Dergisi**, C.13, S.25, (Kış 2019),s.253
[136] Joseph Nye, **Cyber Power**, Harward Kenndy School, Cambridge:2010, s.8
[137] The White House Office, Internatiomal Strategy For Cyberspace, Prosperity, Security and Openness in a Networked World, Washington, 2011, s. 3-25

yaratacağına inanmaktadır. Siber uzaya yönelik politikalarını internet kullanımının geleceği üzerine inşa etmektedir.

Siber Uzayın Geleceği: Fonksiyonları kapsamında bilgisayarlar, gerekli işlemleri tamamladıktan sonra anlık olarak iletişim sağlamaktadırlar. Milyonlarca bilgi, yeni fikirler ve zengin tartışma alanları oluşturularak dijital dillerdeki içeriklerle bir araya gelmektedir. Rapora göre, gelecek zaman diliminde bireyler ve şirketler internet üzerinden satışlar yapabilmek için yatırımlar gerçekleştireceklerdir. Bu durum ekonomik refahı gelişen bireyleri ve toplumları güçlendirecektir. ABD, bireyi güçlü olan devletin kendisinin de güçlü olacağını savunarak, uluslararası işbirliklerinin arttığı bir ortamda ticareti öncelikli tutarak siber uzayda kendine uygun koşullar hazırlamaya çalışmaktadır.

Öncelikli Politikalar: ABD, ulusların birliktelik içerisinde var olabilecekleri güvenlikli ağlar oluşturmayı hedeflemektedir. Ekonomi alanında ise, teknolojiyi teşvik eden, uluslararası standartları koruyan pazarlar oluşturmaktadır. Zira güçlü bir siber güvenlik ve ekonomik refah daha geniş anlamda önlemler almayı gerektirmektedir. Hukuk içerisinde önlemleri sağlamak adına kolluk kuvvetleri oluşturmaktadır. Siber uzayda varlık gösteren illegal içerikleri takip etmeyi amaçlamaktadır. 21. yüzyılın olası siber güvenlik sorunları karşısında, halkını ve müttefiklerini korumayı amaçlamaktadır. Bunu sağlamak adına askeri güvenlik alanları ile siber güvenlik alanlarının uyumunu sağlamak adına çalışmalar yapmaktadır. İnternetin yaygınlığına, açıklığına ve yeniliğine önem vermektedir. Siber güvenlik kapasitesi oluşturmak isteyen ülkelere gerekli bilgiyi ve eğitimi temin etmeyi amaçlamaktadır.

İlerleme: Yaklaşık otuz yıl öncesine kadar sınırlı sayıda internet kullanıcısı bulunurken, günümüzde milyonlarca insan ihtiyaçlarını internet üzerinden karşılamakta ve hatta hayatlarını ağ teknolojileri sayesinde kazanmaktadır. Ağa bağlı sözkonusu teknolojiler birkaç ülkenin ya da kendi içerisinde ayrıcalıklı olan birkaç kişinin tekelinde bulunmamalıdır. İnovasyona açık, dünya üzerinde birlikte çalışabilir siber güvenlik alanları desteklenmelidir. İnternetin nesillere karşı itici bir öğretme gücü bulunmaktadır. Zira sosyalleşmenin ana kaynaklarından birini teşkil ettiği ve içeriğinde

bilginin sınırsızlığını taşıdığı bilinmektedir. ABD'nin siber alan politikaları kapsamında oluşturduğu stratejik vizyonu hükümet kurumlarından, özel şirketlere, sivil topluma ve bireysel kullanıcıya kadar uzanmaktadır.

ABD, 2016 yılında siber güvenlik üzerine ulusal eylem planlaması yayınlanmıştır.[138] Barack Obama döneminde hazırlanan bu planlamaya göre; zorunlu olarak çevrimiçi olunan bu yeni dönemde dijital hayat günlük hayatımızı şekillendirmektedir. Ancak bu yeni dönemde teknolojinin kazancının mı yoksa kayıplarının mı daha yüksek olacağı henüz saptanamamaktadır. Bu nedenle toplum içerisinde dijital hayatın güvenliğini sağlamanın önem derecesi artmaktadır. Dijital alt yapının risk birimlerinin siber güvenlik ve kimlik sorunları doğrultusunda ele alınması ve bu sorunlar doğrultusunda açıklarının teşhis edilerek onarılması yönünde çaba harcamaktadır. ABD, 2017 yılında siber güvenlik için 19 milyar dolar bütçe ayırmıştır, 2018 yılında ise siber güvenlik ulusal strateji boyutunda ele alınmıştır.[139] Söz konusu raporda internetin temininin ve güvenliğinin kendisi tarafından sağlandığı, ağların ve buna bağlı sistemlerin içerisinde bulunan bilgilerin korunmasının da vatanı korumakla eşdeğer olduğu ifade edilmiştir. Keza ABD'nin refahı ve güvenliği siber güvenlik alanında yakalanacak olan başarılara bağlanmıştır.

ABD tarafından, 05 Mayıs 2018 yılında yayınlanan bir diğer raporda da 2018-2023 arası döneme ilişkin siber güvenlik stratejisi ortaya konmuştur.[140] Rapora göre, siber uzayda riskin çok daha kapsamlı olduğu görülmektedir. Bu anlamda devletlerin yanı sıra diğer aktörler de siber uzayın sağladığı imkanlardan yararlanmakta ve devletlerin, terör gruplarının, ulus ötesi suç örgütlerinin ve kötü niyetli bireylerin faaliyetleri dijital dünyada asimetrik bir şekilde vuku bulmaktadır. Zira internete bağlı cihaz sayısı artmakta ve bu cihazların oluşturduğu zincirlemeler dünyanın tamamını karmaşık bir şekilde sarmaktadır. Hatta 2020 yılına kadar 20 milyar cihazın birbirine bağlanması beklenmektedir. Bütün bu nedenler doğrultusunda siber güvenlik nitelikleri

[138] The White House Office, Fact Sheet: Cybersecurity National Action Plan, Washıngton:2016, www.whitehouse.gov, (Erişim Tarihi: 10.03.2020)
[139] The White House Office, National Cyber Strategy of the United States of America, Washıngton:2018, www.whitehouse.gov, (Erişim Tarihi: 12.03.2020)
[140] The White House Office, U.S Departmen Of Homeland Security Cybersecurıty Strategy, Washıngton:2018, www.whitehouse.gov, (Erişim Tarihi: 14.03.2020)

itibariyle hem küresel hem de bir iç güvenlik sorunsalı haline gelmektedir. ABD bu raporuyla iç güvenliği sağlamaya çalışmaktadır. Riskler doğrultusunda, ABD yönetiminin en önemli sorumluluğu Amerikan halkının güvenliğini sağlamaktır. Bu anlamda ABD siber güvenlik tehditlerine ve güvenlik açıklarına odaklanmaktadır. İç güvenlik kapsamında siber güvenliğe yönelik olarak yapılan yatırımlar maliyetleri artırmaktadır. Yenilikçi ve çevik olmaya öncelik verilmektedir. Zira siber uzay teknolojilerinin gelişmesine paralel şekilde risklerin de geliştiği gözlenmektedir. Siber güvenlik yetenekleri süreklilik içerisinde araştırma, geliştirme ve kullanım konusunda örnek teşkil etmeli, gelişen tehditlere ve teknolojilere ayak uydurmaya çabalamalıdır. Karmaşık yapısı olan internetin büyümesi ve gelişiminde öncelikli olarak özel sektörler, müttefik devletler ve diğer devletler ile işbirliği içerisinde olmaya çalışılmaktadır. Küresel düzeyde siber risklerin yönetilmesi, gelişmelere ve olaylara yanıt verilmesi ve ulus ötesi tehditlerin bertaraf edilmesi küresel bir yaklaşım gerektirmektedir. Siber güvenliğin bireyleri güçlendirip, refahlarını sağladığı gerçeğinden hareketle bu alanda gelişecek olan ifade özgürlüğü ve yaratıcı düşüncenin, yenilikçi hareketleri ve teknolojileri destekleyeceği düşünülmektedir. Siber güvenlik programlarının başarılı olabilmesi, yürürlükte bulunan yasalara ve politikalara uygun şekilde gizliliğe, medeni haklara ve ulusal değerlere saygı çerçevesinde değerlendirilmektedir.

ABD'nin 2019 tarihli siber güvenlik raporunda da siber uzayda sağlanacak olan güvenliğin ulusal güvenlik ve refah ile bağdaştırdığı görülmektedir.[141] Bu raporda dikkat çeken husus ise bireyleri bilgisayarları ya da bulut depolama alanlarında bulunan verilerini korumakla sorumlu tutmasıdır. Devlet yönetiminin ise siber tehditlere karşı önlemlerle yükümlü olduğu, rakiplerinin ABD'nin kritik altyapısına zarar vermesini önlemek amacıyla kararlı adımlar atıldığı belirtilmektedir.

ABD' nin resmi ve açık kaynaklarından yararlanılarak incelenmiş olan yukarıdaki raporlarda, ABD'nin siber güvenlik politikalarında öncelikli olarak güvenliğin sağlanması, ekonomik refah oluşturulması ve devlet dışı aktörler ile iş birliği içerisinde olunmasının hedeflendiği gözlenmektedir. Üst yapılanma çerçevesinde

[141] The White House Office, Presidential Proclamation on National Cybersecurity Awareness Month , Washıngton:2018, www.whitehouse.gov, (Erişim Tarihi: 14.03.2020)

Savunma Bakanlığı, İç Güvenlik Bakanlığı ve Gizli Servisler (FBI/CIA) gibi yapılanmalar öne çıkmaktadır.[142] ABD, hükümet politikaları, federal ajansları, iç güvenlik, dış güvenlik, istihbarat birimleri, özel şirketlerin kuruluş amaçları, bireylerin ortaöğrenimden yükseköğrenime kadar olan bütün süreçlerine ilişkin bilgilerin paylaşımından, koordine edilmesine ve hatta gelebilecek saldırılara, siber uzayın gelişmelerindeki güncellemeleri takip etmeye kadar güvenlik açıklarını, siber tehditlerini azaltmayı amaçlamaktadır. Dolayısıyla ABD'nin uzmanlar ile önlemler aldığı ve hazırlık içerisinde bulunduğu anlaşılmaktadır.

3.1.3 Amerika Birleşik Devletleri'ne Karşı Gerçekleşen Siber Saldırılar ve Amerika Birleşik Devletleri'nin Gerçekleştirdiği Siber Saldırıları

Siber uzayda oluşabilecek tehditler karşısında devletler, özel şirketler ve bireyler çeşitli önlemler almaktadırlar. ABD söz konusu tehditlere karşı çalışmalarını uzun zamandır planlı bir şekilde yürütmektedir. Siber uzayın tanımlaması genel olarak yapılamadığı gibi siber saldırıların tanımlaması da halen yapılamamaktadır. Genel kabul gördüğü üzere siber saldırı, iki şekilde gerçekleşmektedir. İlk durum en kötü saldırı çeşidi olarak tanımlanmaktadır. Bilgisayara yerleştirilmiş olan virüsün bilgisayar belleğindeki bütün verileri silmesidir. İkinci tanımlama ise, daha az zararlı olabileceği düşünülen virüsün dolaylı etkisiyle sistemi ve ağları kullanılamaz hale getirmesidir.[143] Siber uzayda düzenlenen saldırıların temel amaçları belirsizlik taşımaktadır. Bu amaçlar, bilgileri ele geçirerek istihbarat oluşturma, eğlence için saldırı ya da bilgisayarları ve bağlantılı olan eşyaların kontrol sistemine nüfuz etme istekleri olabilmektedir. ABD'ye karşı yapılmış ya da ABD'nin gerçekleştirmiş olduğu önemli örnek siber saldırılar aşağıda verilmiştir.

Hainan Adası Olayı: "World Wide Web War 1" olarak adlandırılmakta ve ilk siber savaş olarak kabul edilmektedir. Kendini vatansever olarak nitelendiren bazı Çinli grupların ABD'ye karşı yapmış olduğu saldırıdır. 2001 yılında meydana gelen bu

[142] Ali Burak Darıcılı, Demokrat Parti Hack Skandalı Bağlamında ABD ve RF' nın Siber Güvenlik Stratejilerinin Analizi, **Uluslararası Çalışmalar Dergisi**, C.1, S.1,2017, s.7
[143] Herbert S. Lin, "Offensive Cyber Operations and the Use of Force", **Journal of National Security Law and Policy**, C.4, S.63,2010, s.63.

saldırılar zombi ataklar olarak tanımlanmaktadır. Bu saldırıların nedeni olarak 1 Nisan 2001 yılında ABD EP-3E casus uçağı ile Çin Shenjang J-8 jet uçağının çarpışması öne sürülmektedir. Amerika'daki etkileri kapsamında Beyaz Saray'ın sitesi saatlerce kapalı kalmış, Adalet Bakanlığına ait internet sitesi tamamen kilitli duruma gelmiştir. ABD' ye ait çoğu internet sitesinde Çin bayrağı sallandırılıp, Çin marşları çalınmıştır.[144]

Titan Rain Saldırısı: İsminden anlaşılacağı üzere titan yağmuru olarak adlandırılmaktadır. Çin tarafından ABD bilgisayarlarına karşı gerçekleştirilen en yoğun saldırılar olarak bilinmektedir.[145] Saldırıları tespit eden Shawn Carpenter'a göre saldırılar kapsamında ABD'nin askeri üsleri, savunma hatları ve havacılık şirketleri hedef alınmış, saldırıların yapıldığı kurumlara ait gizli bilgilere erişildiği öne sürülmüştür.

Körfez Savaşlarında Gerçekleşen Siber Olaylar ve Siber Ağın Kullanımı: ABD'nin, Irak'a karşı iki ayrı dönemde gerçekleştirdiği savaşlardır. İlk olarak 1993 yılında bilgisayar ve ileri teknolojilerine bağlı akıllı silahlar ile gerçekleştirilmiştir.[146] İkinci olarak ise siber ağın kullanımından yararlanan ABD, 2003 tarihli Irak işgalinin öncesinde Irak'ın üst düzey komutanlarına e-posta göndererek savaşmadan teslim olma çağrısında bulunmuştur. Bu çağrıya birçok komutanın olumlu yanıt verdiği ileri sürülmektedir.[147] Körfez savaşları televizyon ve internet üzerinden takip edilebilir olması nedeniyle iletişim savaşı olarak tanımlanmaktadır.[148]

ABD'nin Askeri Bilgisayarına Saldırı: Gary McKinnon isimli hacker ABD askeri kurumlarına siber saldırı yaptığı için tutuklanmıştır. McKinnon, ABD'nin uzaylılar üzerine verileri sakladığını düşünerek yaklaşık on iki yıl sürecek saldırılar

---

[144] Craig S. Smith, "May 6-12; The First World Hacker War", (Çevrimiçi) https://www.nytimes.com/2001/05/13/weekinreview/may-6-12-the-first-world-hacker-war.html, 13 Mayıs 20012, (Erişim Tarihi: 18.03.2020)

[145] M.E.Kabay, "Industrial Espionage, Part 8: China and Titan Rain", (Çevrimiçi), https://www.networkworld.com/article/2315467/industrial-espionage--part-8--china-and-titan-rain.html, 2005, (Erişim Tarihi: 18.03.2020)

[146] Richard A. Clarke, Robert K.Knake, **Siber Savaş: Ulusal Güvenliğe Yönelik Yeni Tehdit**, Çev. Murat Erduran, İstanbul: İKÜ Yayınevi, 2011, s. 32

[147] Hasan Çiftçi, **Her Yönüyle Siber Savaş**, Ankara: Tübitak Popüler Bilim Kitapları, 2017, s.183

[148] Salih Bıçakcı, "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", **Uluslararası İlişkiler Dergisi**, C.9, S. 34, s. 207

düzenlemiştir. Sonradan fark edilen bu saldırıların 2002-2011 yılları arasında gerçekleştirildiği iddia edilmektedir. Binlerce ABD'li askerin bilgisayarlarına giriş yapıldığı ve ABD'yi yaklaşık 800.000 dolar değerinde zarara uğrattığı bilinmektedir.[149]

ABD'nin İnsansız Hava Araçlarına Saldırı: ABD'nin İnsansız Hava Araçları (İHA) olan Predator ve Reaper devre dışı bırakılarak, kontrolleri sağlanan bilgisayar tuşlarında virüslere rastlanılmıştır. Hava Kuvvetleri Komutanlığı tarafından rapor edilen bu virüslerin iyi mi kötü mü olduğu bilinmemektedir. ABD söz konusu İHA'ları Afganistan ve diğer savaş alanlarında uçurmaktadır. Tanımlanamayan bu virüs için 'keylogger' tabiri kullanılmıştır. Bilgisayarların tuş basımlarını kayıt altına aldığı bilinen virüsün kimler tarafından ve ne derece yayıldığı halen tespit edilememiştir.[150] İHA, teknolojinin savaş alanlarına sunduğu çok önemli bir istihbarat ve silah aracı olabilmektedir. Bu araçların kontrolleri siber uzaya bağlı bilgisayarlar ile sağlanmaktadır. Bu nedenle siber güvenlik her anlamda önem arz etmektedir.

ABD'li İstihbarat Servislerinin Saldırıları: Siber uzaydan gelmesi muhtemel tehditlerin hedefi devletin kilit merkezlerinde bulunan kontrol mekanizmaları olabilmektedir. Tehdidin büyüklük derecesi saldırganın siber uzayda sahip olacağı bilgiye ve ekonomiye bağlıdır. ABD'nin istihbarat birimleri Kuzey Kore, Çin, İran ve Rusya devletlerine karşı 231 siber saldırı gerçekleştirmiştir. Yüksek bütçe ile yapılan bu saldırıların asıl amacının söz konusu devletlerin nükleer devlet olması ve gizlilik derecesinde olan belgelerin ele geçirilmesi olduğu tahmin edilmektedir.[151]

ABD Başkanlık Seçimlerinde Gerçekleştirildiği İddia Edilen Siber Saldırı: Hillary Clinton Rusya Federasyo'nun(RF) siber araçlar üzerinden ABD'nin başkanlık seçimlerine müdahalede bulunduğunu iddia etmiştir.[152] Saldırıların yapıldığı dönemde

---

[149] BBC News, "Profile: Garry Mckinnon", (Çevrimiçi) https://www.bbc.com/news/uk-19946902, (Erişim Tarihi: 19.03.2020)

[150] Noah Shactman, "Exclusive: Computer Virus Hits U.S. Drone Fleet", 10.07.2011, (Çevrimiçi), https://www.wired.com/2011/10/virus-hits-drone-fleet/, (Erişim Tarihi: 19.03.2020)

[151] Barton Gelleman, Ellen Nakashima, "The Washington Post, "U.S. spy agencies mounted 231 offensive cyber-operations in 2001 documents Show", (Çevrimiçi) https://www.washingtonpost.com/world/national-security, (Erişim Tarihi: 19.03.2020)

[152] Ersin Embel, "Kronik: ABD Başkanlık Seçimleri", **Ankara Üniversitesi Siyasi Bilimler Dergisi**, S.71, C.4,2016, s.1319

ABD başkanı Obama, Rusya Devlet Başkanı Putin'i seçimlerden uzak kalması için uyarmış ve istihbarat birimlerinden iddiaların araştırılmasını istemiştir. 2016'da dünyada krize neden olan ve hala nedeni bilinmeyen 35 Rus diplomat ve Rus teknoloji firmalarına yaptırım uygulamasıyla seçimlere yönelik düzenlenen siber saldırıların bağlantılı olduğu düşünülmektedir.[153]

Edward Snowden Olayı: ABD'de casusluk olarak tanımlamaktadır. Siber olaylar kapsamında değerlendiriliyor olmasının nedeni; ABD Ulusal Güvenlik Ajansı'nın (NSA) eski çalışanı Edward Joseph Snowden The Guardian Gazetesi aracılığı ile 'Prism' isimli kitle takip programını sızdırmıştır. Söz konusu programa göre ABD'nin herhangi bir yasal izni bulunmadan, dünyadaki bütün internet kullanıcıların iletişim kayıtlarına erişebilmesini sağlamaktadır. [154] ADB, Snowden'i ulusal güvenliğe ait istihbarat çalışmalarının açık kaynaklarda paylaşılması suçlamasında bulunmuştur.[155] NSA'da 2006 yılında bilgi teknolojileri bölümünde çalışmaya başlamıştır. 2009 yılında yine NSA'ya bağlı olarak Japonya çalışmış ve NSA'nın yapmış olduğu çalışmalardan rahatsız olduğunu belirterek çok gizli belgeleri kopyalayıp kaçmıştır. İlk olarak Honk Kong' gittiğ bilinmektedir. Buradan Çin'e kaçarak The Guradian gazetesi aracılığıyla kopyaladığı bilgileri sızdırmıştır. Daha sonra ABD' nin baskıları nedeniyle RF'dan sığınma talebinde bulunmuş ve RF'de yaşamını devam ettirmektedir.[156] Yaşanan bu olay doğrultusunda internet üzerinden yapılabilen işlemlerin gizlilik içerisinde takip edilebileceği anlaşılmaktadır. Dolayısıyla yapabileceğimiz en önemli çıkarım siber uzayın kişisel hakların korunması yönünden hukuksal zeminin oluşması gerekmektedir.

ABD, bilim ve teknoloji alanlarındaki atılımını 2000'li yıllarda da artan şekilde sürdürmüştür. Siber uzayın getirdiği belirsizlikler ve devletlerin tek başlarına mücadeledeki yetersizliklerine paralel şekilde, günümüzde uluslararası şirketler ile iş

---

[153]The New York Times, "The Russian Hacking in 200 Words", (Çevrimiçi) https://www.nytimes.com/interactive/2016/12/29/us/politics/russian-hack-in-200-words.html,(Erişim Tarihi:19.03.2020)

[154] The Guardian, Edward Snowden: The Whistleblower Behind The Nsa Surveillance Revelations, 2013, (Çevrimiçi) https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance, Erişim Tarihi: 12.04.2020

[155] BBC, Edward Snowden: Leaks That Exposed Us Spy Programme, 2013, (Çevrimiçi) https://www.bbc.com/news/world-us-canada-23123964, Erişim Tarihi: 12.04.2020

[156] Biography, Edward Snowden Biography, (Çevrimiçi) https://www.biography.com/activist/edward-snowden, Erişim Tarihi: 12.04.2020

birliği sağlayarak siber uzaydaki çalışmalarını sürdürmekte ve güvenliğini sağlamaya çalışmaktadır. Siber uzaydan gelebilecek tehdit, devletlerin, uluslararası şirketlerin ve bireylerin bilgilerinin çalınması olarak ön görülmektedir. Bilginin küresel düzeyde insan üstü hızda ve kolaylıkla yayıldığı bu çağda, siber saldırılar devletlerin kontrolü dışında ve çok hızlı bir şekilde gerçekleşmektedir. Herhangi bir saldırıda devletin ifşa edilmiş bilgisi, siber uzaya bağlı kullanılan askeri aracın kontrol dışına çıkması, şirketlerin ekonomik zarara uğramış olması siber güvenlikte zayıflık olarak görülebilmektedir.

3.2 Rusya Federasyonu

Soğuk Savaş'ın diğer önemli kutbu olan Sovyet Sosyalist Cumhuriyetler Birliği (SSCB)'nin yıkılmasının ertesinde Rusya Federasyonu 25 Aralık 1991 tarihinde kurulmuştur. SSCB'nin yıkılmasıyla dünya yeni bir yapılanmaya adım atmıştır.[157] RF, büyük devlet olma politikalarını 2000'lerde uygulamaya koymuştur. Günümüzde izlemiş olduğu politikaların temellerinin 1990'lı yılların ikinci yarısında atılabildiği, 2000'lerden sonra da mümkün hale gelebildiği görülmektedir.[158]

RF, çevresinde bulunan ülkeleri çıkarları doğrultusunda kullanmaktadır. Siber güvenlik anlamında da aynı stratejiyi izleyebileceği değerlendirilmektedir. Zira civarında bulunan Estonya ve Gürcistan gibi ülkelere saldırılar gerçekleştirerek[159] domine etmektedir. Putin dönemi ile birlikte yerli yatırımlara hız veren RF'nin, siber güvenlik alanında da yerli yazılımlar geliştirdiği bilinmektedir. Diğer taraftan RF'nin siber alanda yasa dışı gruplar ile çalıştığına dair iddialar ortaya atılmaktadır. 27 Nisan 2007'de Estonya'ya yöneltmiş olduğu DDoS saldırıları kapsamında gerçekleştirilen yoğun diplomatik incelemeler neticesinde gözlemcilerin bilgisayar korsanlarının Rus devlet yöneticilerinin bilgisi dahilinde saldırı yaptığı sonucuna vardıkları görülmektedir.[160]

---

[157] Fahir Armaoğlu, **20. Yüzyıl Siyasi Tarihi 1914-1995**, Timaş Yayınevi, İstanbul:2014, s. 846
[158] Faruk Sönmezoğlu, Özgün Erler Bayır, **Dış Politika Karşılaştırmalı Bir Bakış** İstanbul: Der Yayınları, 2014, s. 473.
[159] Atalay Keleştemur, **Siber İstihbarat**, Level Kitap, İstanbul:2015, s. 187
[160] Landon J. Wedermye, "The Changing Face of War: The Stuxnet Virus and the Need for International Regulation of Cyber Conflict", Mıchgıan State Unıversıty College Of Law, 2012, (Çevrimiçi), https://digitalcommons.law.msu.edu/king/241/, (Erişim Tarihi: 25.03.2020)

3.2.1 Rusya Federasyonu'nun Siber Uzay Çalışmaları

Günümüz savaşlarının siber uzay ve teknolojik gelişmeler ile değişime uğradığı gözlemlenebilmektedir. İnsansız hava araçları ile savaşılan devletlerin coğrafyası ya da sınır bölgeleri kontrol edilebilirken, silahlı insansız hava araçları ile de saldırı gerçekleştirilebilmektedir. Bu araçların her birinin kontrolü bilgisayarlar ile uzaktan sağlanmaktadır. Bilgisayarların savaş alanlarına girmiş olduğu bu dönemden sonra devletlerin siber uzaydan bağımsız hareket etmeleri zorlaşmaktadır. Siber uzayın güvenliği ve domine edilmesi devletler açısından omurga sistemine benzetilebilmektedir. Literatürde siber savaşın ve siber silahın net bir tanımlanması yapılamamışsa da siber uzay, bilginin silahlanmış hali olarak düşünülmektedir.[161]

RF'nin bilgi güvenliğine vermiş olduğu önem 2000 yılında yayımlamış olduğu belgeden anlaşılmaktadır.[162] Söz konusu belgeye göre bilgi güvenliği, siber güvenlik ile eş değerde anlaşılmaktadır. Modern telekomünikasyon gelişmelerine önem vererek, devlete ait bilgiler koruma altına alınarak izinsiz bir şekilde erişilmesinin önüne geçilmeye çalışılmıştır. Küresel güç olmak isteyen devletlerin kendi ulusal güvenlikleri çerçevesinde diğer devletlerin bilgi alanlarını tehdit ettikleri ve çeşitli cihazların üretimi ile siber uzayı domine etmeye çalıştığı gözlemlenmektedir. Bu devletler küresel anlamda bilim ve teknolojideki gelişmeleri takip etmek amacıyla mali kaynakları yoğunlaştırmaktadırlar. RF de bilimsel ve teknoloji potansiyeli yüksek alanlarda fikri mülkiyet hakkını koruma altına alıp, araştırma ve ticaret haline getirilmesi konularında hükümet desteği sağlamaktadır.

RF, 9 Eylül 2000'de bilgi güvenliğine yönelik bir doktrin yayınlamıştır.[163] Bu doktrine göre, halkın birbiri ile olan ilişkilerinde bilgi akışını sağlayan sistemlerin

---

[161] Can Kasapoğlu, "Siber Savaş: Geleceğin Askeri Gerçekliği ve Günümüzün Bilimkurgusu Arasında", **Edam**, 2017, (Çevrimiçi) https://edam.org.tr/wp-content/uploads/2017/10/sibersavas_tr_rbs_logo.pdf (Erişim Tarihi: 25.03.2020), s.3

[162][162] The Ministry of Foreign Affairs of the Russian Federation, Natıonal Securıty Concept Of The Russıan Federatıon, 2000, (Çevrimiçi) https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768, (Erişim Tarihi: 26.03.2020)

[163] The Ministry of Foreign Affairs of the Russian Federation, Doctrine of Information Security of the Russian Federation, 2000, (Çevrimiçi) https://www.mid.ru/en/foreign_policy/official_documents , (Erişim Tarihi: 28.03.2020)

düzenlenmesi gerekmektedir. Ulusal, toplumsal ve bireysel güvenliğin sağlanması teknolojik gelişmeleri takip etmekten geçmektedir. Devletin iç ve dış politikaları oluşturulurken bilgi güvenliği alanlarında stratejik ve güncel görevler oluşturulmaktadır. Bilgi güvenliği dört ana bileşen ile ayırt edilmektedir. Bilgi alma ve edinme, Rusya'nın manevi gelişimini sağlama, toplumun ahlaki ve vatanseverlik duygularını geliştirme, bilimsel potansiyel ve gelişimini içermektedir. Bilgi güvenliğinde kişisel bilgilerin gizliliğine önem verildiği görülebilmektedir. E-posta, telgraf, telefon ve diğer iletişim araçlarının gizliliği anayasal düzenlemeler ile korunmaktadır.

RF'nin 2000 yılında yayınlamış olduğu bilgi doktrinin benzer ancak daha gelişmiş hali 5 Aralık 2016 yılında yeniden yayınlanmıştır.[164] Bu doktrinde ise bilgi alanı internetin bilgi ve telekomünikasyon ağı ile birleştirilmiş ve bunun adından 'internet' olarak bahsedilmiştir. RF'nin tamamında kullanılan web siteleri, internet ağ bileşenlerinin hepsi bilgi alt yapıları içeriğinde toplanmaktadır. İnternetin güvenli ve istikrarlı bir şekilde çalışmasını sağlamak için gerekli olan kaynakların mevcut küresel dağılımı göz önünde bulundurulduğunda hukuka uygunluğunun ve güvenliğinin sağlanamadığı ifade edilmiştir. Rusya, bunun nedenini doktrinde şu şekilde açıklamaktadır. Siber uzay güvenliği alanlarında uluslararası ilişkileri düzenleyen yasal normların bulunmaması, bunların uygulanması için bilgi teknolojilerinin özelliklerini dikkate alacak cihazların ve gerekli yasal prosedürlerin olmaması, uluslararası kapsamda siber uzay güvenliğinin sağlanamaması ve adil stratejik ortaklıkların oluşmamasından geçmektedir. Çözüm yolu olarak belirttiği politikalarda ise siber güvenliğin sağlanması için stratejik bir amaç oluşturulmalı, bu amaç kapsamında birey, toplum ve devletin hayati çıkarları doğrultusunda bilişim teknolojileri uluslararası alanlardan gelebilecek olan iç ve dış tehditlerden koruma sağlamalıdır. Bunun için uluslararası düzeyde de yasaların teşkil edilmesi gerekmektedir. RF'ye göre devletler arası ilişkilerin sürdürülebilir ve barışçıl olmasında eşit stratejik ortaklıkların oluşumu son derece önemlidir. Uluslararası sistemin ana aktörleri olan devletlerin eşit bir şekilde yer alacağı istikrarlı bir stratejik ortaklığın oluşumunda 5 itici güç bulunmaktadır:

---

[164] The Ministry of Foreign Affairs of the Russian Federation, Doctrine of Information Security of the Russian Federation, (Çevrimiçi), https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163
2000, (Erişim Tarihi: 28.03.2020)

1. Bilgi güvenliği alanlarında ulusal çıkarların sürekliliğini sağlama ve bağımsız bir politika izlemek adına RF'nin egemenliğinin korunması,

2. Uluslararası hukuka aykırı olmak üzere asker ve siyasi amaçlarla ya da terör gruplarının yanlısı olarak ve hatta diğer yasadışı amaçlar kapsamında bilgi teknolojilerinin kullanımında bulunanlara karşı uluslararası bir siber güvenlik sistemin oluşturulmasında görev alınmasının gerekliliği,

3. İnternetin, siber uzayın, bilgi teknolojilerinin kendine has olan doğasını dikkate alarak devletler arasında meydana gelebilecek savaşlar için önlemeyi ve çözmeyi amaç edinen uluslararası yasal mekanizmaların oluşturulması,

4. RF'nin siber uzay alanlarıyla ilgili olan uluslararası kuruluşlar, devletlerle ile eşitlik ilkesini korumak üzere karşılıklı iş birliği içerisinde bulunulması,

5. Rus internet sektörünün yönetimini ulusal bir şekilde geliştirilerek, siber güvenlik alanlarında milli yazılımların ortaya konmasıdır.

3.2.2 Rusya Federasyonu'nun Siber Uzay Politikaları ve Ulusal Strateji Belgeleri

RF, milli güvenliği sağlamanın çözüm yolu olarak tehditlerin zamanında tespit edilmesi ve kaynaklarının belirlenmesine önem vermektedir. Yirmi birinci yüzyılın siber alanını 'Yeni Savaş Alanı' olarak tanımlamaktadır. Bilindiği üzere RF tarih boyunca savaş alanlarına önem vermiştir. Günümüzde de savaş alanları üzerinde titizlikle hazırlıklar yapmakta ve çalışmaktadır. Çıkarlarını korumak, güvenliğini sağlamak için siber uzayda çatışmaktan çekinmeyeceği tahmin edilmektedir.[165] Siber uzayda gerçekleştirmek istediği politikaların temelini askeri alanlar teşkil etmektedir.[166] Siber uzay politikalarını geliştirmek üzere teknoloji sektörleri, akademisyenler ve Rus askeri birlikleri ile bir araya gelerek siber savaş doktrinleri geliştirmektedir.[167] Çıkarları

[165] Ali Burak Darıcılı, Rusya Federasyon'un Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi, **Bilig**, S.83, (Güz 2017), s.122

[166] Carmen-Cristina Cirlig, "Cyber defence in the EU Preparing for cyber warfare?", **European Parliamentry Research Service**, (Çevrimiçi) https://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf, (Erişim Tarihi: 28.03.2020)

[167] Charles Billo, Welton Chang, Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States**,** 2004**, Institute for Security Technology Studies**, (Çevrimiçi) https://gssd.mit.edu/search-gssd/site/cyber-warfare-analysis-means-motivations-59897-thu-12-27-2012-1242, Erişim Tarihi: 29.03.2020

doğrultusunda siber uzayı domine eden devletlerden biri olabileceği tahmin edilmektedir.[168]

RF Savunma Bakanlığı tarafından askeri birliklerin siber güvenliğin bir bileşeni olduğunu ifade eden bir belge yayımlanmıştır.[169] Söz konusu belgeye göre, silahlı kuvvetlerin siber uzay kapsamında savunmayı ve güvenliği sağlaması ve bu anlamda askeri veri kaynaklarının kullanılması gerekmektedir. Siber uzayın farklı tehdit unsurlarını barındıran karmaşık bir sistem olduğu kabul edilmektedir. Siber uzayda muhtemel operasyonların, elektronik savaşların, yaşanabilecek iletişim engellenmelerinin dost ya da düşman tarafından gelebileceği ortaya konmaktadır. Uluslararası iş birliği sağlamak adına kendisine dost olan devletler ve uluslararası örgütlerle koordineli çalışmanın önemi vurgulanmaktadır. Küresel anlamda sağlanabilecek iş birliğinin temel amacının, devletlerin siber askeri oluşumlarının uluslararası yasal bir zemine oturtulmasından geçtiği belirtilmektedir. Sınır ötesi bilgi sistemlerinde ve küresel siber güvenlik alanlarında güven duygusunun oluşturulması hedeflenmektedir. Siber uzayda çatışmayı önlemek ve caydırıcılık oluşturmak adına on kural belirlenmiştir. Bunlar şöyledir: [170]

1. Rus silahlı kuvvetlerinin siber uzay sistemlerini geliştirmek,
2. Siber güvenlik güçlerini korumak ve askeri, siyasi alanlarda gelebilecek bütün saldırılara karşı her an hazır olmak,
3. BM sözleşmesi hükümlerine ve uluslararası hukuka uygun bir şekilde uluslararası siber alan güvenliğinin güçlendirilmesi ve temel unsurlarda iş birliği geliştirmek,
4. BM himayesinde uluslararası siber güvenlik anlaşmalarının uygulanmasını sağlamak adına çaba harcamak ve genel kabul görmüş normları, uluslararası hukukun ilkelerini siber alanda uygulanabilecek ve genişletecek şekilde anlaşmalar sağlamak,

---

[168] Ali Burak Darıcılı, **Siber Uzay ve Siber Güvenlik ABD ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi**, Bursa: Dora Yayınları, 2017, s.138

[169] Ministry of Defence of the Russian Federation, Russian Federation Armed Forces' **Information Space Activities Concept,** 2011, (Çevrimiçi), https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle Erişim Tarihi: 29.03.2020

[170] Ministry of Defence of the Russian Federation, Russian Federation Armed Forces' **Information Space Activities Concept,** 2011, (Çevrimiçi), https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle Erişim Tarihi: 29.03.2020

5. Siber uzayda meydana gelebilecek askeri çatışmaların erken tespitini sağlayarak azmettiricisi ve suç ortağı/ortaklarına bulunanlara müdahalede bulunmak,

6. Çatışmanın ana nedenlerini ve tırmanmasını sağlayan faktörleri belirleyerek, acil durumlarda önleme faaliyetlerini sağlamak,

7. Çatışma olması halinde meydana gelebilecek mali problemlere karşı öncelikli olarak önlem almak,

8. Uluslararası alanlarda meydana gelmesi muhtemel yüksek maliyetli siber çatışmaları önlemek,

9. Savaşa başlamış taraflar arasında aracı olarak barışı sağlamak,

10. Muhtemel bir savaş durumunda en uygun zamanda tarafsız şekilde açıklama yapılmasıyla halkın doğru yönlendirilmesi ve saldırının diğer alanlara yayılmasının önlenmesi olarak belirtilmiştir.

Global Affairs dergisinin Rusya genel yayın yönetmeni Fedor Luyanov, 1997-2000 yılları arasında sert güvenlik politikalarında genel bir değişiklik olabileceğini belirtmektedir. Luyanov askeri ihtiyaçların halkın ihtiyaçlarına göre daha önemli olduğunu vurgulamıştır.[171] Diğer taraftan RF Genelkurmay Başkanı General Valery Gerasimov'un 2013'de kaleme aldığı makalede, modern savaşın nasıl olacağı, askerin nasıl hazırlanması ve silahlanması gerektiği sorularına cevaplar aranmaktadır. Gerasimov'un genel olarak bulmuş olduğu cevap ise, savaşların seyrinin değiştiği, modern silahlı çatışma araçların özünü etkileyen yapay zeka alanında modern otomatik askeri ekipman ve araştırma komplekslerinin değiştiği, bugün havadan kontrolü sağlanan savaşların gelecekte yürüyen robotlar sayesinde sağlanacağı, askeri birliklerde operasyonların robotize edilen birimlerce yapılacağı yönünde olmuştur.[172] RF'nin siber güvenlik politikalarını askeri birlikleri üzerine oluşturacağı görülebilmektedir. Siber güvenliğe askeri anlamda önem veren RF tarafından 29 Kasım 2013 tarihinde siber güvenlik stratejisi belgesi yayımlanmıştır.[173] Siber güvenliğe temel olarak, güvenliğini

[171] Keir Giles, Russia: National Security Strategy to 2020, **Nato Defense College**, 2009, (Çevrimiçi) https://css.ethz.ch/en/services/digital-library/publications/publication.html/154909, (Erişim Tarihi:29.03.2020)

[172] General Valery Gerasimov, The Value Of Scıence In Predıctıon, 2013, (Çevrimiçi), https://www.ies.be/files/Gerasimov%20HW%20ENG.pdf, (Erişim Tarihi: 29.03.2020)

[173] Concept Of A Cyber Securıty Strategy Russıan Federatıon, 2013, (Çevrimiçi), http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf, (Erişim Tarihi:29.03.2020)

sağlama yönetmeliğindeki mevcut boşlukları ortadan kaldırmayı, devlet organlarının, sivil toplum ve iş çevrelerinin örgütleriyle birlik içerisinde hareket etmesini sağlamayı, siber güvenlik seviyesini artırmak için ilgili tüm kurumların eylemlerini sistematik hale getirmeyi, siber güvenlik tehditleri modellerine karşı koyabilmeyi ve tedbirleri formüle etmeyi amaçlamaktadır.

Siber güvenlik stratejisinin geliştirilmesinin önemi: İnternet ve siber uzayın diğer bileşenleri Rusya'nın ekonomik kalkınmasının önemli faktörleri arasında yer almaktadır. Gelişen teknoloji, yirmi birinci yüzyılda sosyal açıdan sorumlu ve demokratik bir devletin temelini oluşturmaktadır. Bilgi teknolojilerinin kullanılması adına ulusal sektör geliştirilmeli ve sistematik devlet yapısı oluşturulmalıdır. Siber uzay bilgi teknolojilerine bağımlılığı nedeniyle halk için yeni fırsatlar yaratabilmektedir. Diğer taraftan yeni gelişen fırsatlar bireyin haklarına, çıkarlarına ve hayati işlevlerine zarar verilebilecek araçlar haline dönüşebilecek, siber suçlular ve terör gruplarınca kritik bilgi kaynaklarına saldırılar gerçekleştirilebilecek, askeri operasyonlarda siber silahların kullanılması gibi yeni tehditlerin oluşumuna sebebiyet verebilecektir.

Bilgi güvenliğinin yapısında siber güvenliğin yeri: En büyük güç unsuru olan bilginin güvenliği siber uzayda son derece kritik bir yere sahiptir. Bilgi sınırları bilinmeyen ve tahmin edilemeyen bir alan olarak düşünülmektedir. Dolayısıyla, bilginin oluşturulması, dönüştürülmesi, iletimi, kullanımı, depolanması gibi faaliyet alanlarına, bireye, topluma ve devlete siber uzaydan gelebilecek tehditlere, internet, telekomünikasyon ağlarının ve iletişim kanallarının işlevlerini sağlayabilecek teknolojik altyapısına ve kullanımına, siber uzayın tüm bileşenlerinde istenmeyen tehdit ve etkilerinden korunmasına önem verilmektedir.

Siber güvenliğin mevzuattaki yeri: Siber güvenlik stratejilerinin kendine ait özel düzenlemeleri vardır, geçerli yönetmeliklerle çelişmemektedir. Önem verilen konular hakkında; güvenliğin sağlanması için oluşabilecek hukuksal boşlukları ortadan kaldırmak, sivil toplum, özel şirketler ile birlikte devletleri siber güvenliğin sağlanması sürecine dahil edebilmek, siber güvenlik sistemlerinin seviyesini artırmak için ilgili tüm

tarafların çalışmalarını sistematik hale getirmek, tehditlere karşı koymak için gerekli tedbirleri formüle etmek üzere temel ilkelere dayandırılmaktadır.

Siber güvenliğin temel hedefi: İç ve dış politika alanlarına öncelik verilmek üzere, temel ilkelerin ve alınabilecek önlemlerin tanımlaması yapılarak RF'deki bireylerin, toplumun ve devletin siber güvenliği sağlanmaktır.

Siber güvenlik stratejisinin temel ilkeleri: Siber güvenlik alanlarında birey ve toplumun anayasal hak ve özgürlüklerini güvence altına almak, bireyin, özel şirketlerin, devletin kritik alt yapılarında bulunan sitemleri korumak, siber güvenlik alanlarında faaliyet gösteren bireylerin, toplumların, bürokraside çalışanların dijital okuryazarlığını yükselterek bu konular üzerine bilinçlendirmek, siber güvenlik gerekliliklerine uyma sorumluluğu tesis edilirken diğer taraftan aşırı kısıtlamaların uygulamalarla arasında denge ilkesinin oluşturulması, siber uzaydan gelebilecek olumsuz sonuçların boyutlarına göre risklerde öncelik oluşturulması, sürekli olarak değişim gösteren siber tehditlerine karşı koymak amacıyla siber güvenliği üst düzeyde sağlamak için bilgisayar ve araçlarının yazılım ve donanımlarını güncellemeyi benimsemektedir.

Siber güvenlik stratejisinin öncelikleri: Siber saldırı ve tehditlere karşı ulusal bir koruma sisteminin geliştirilmesi ve bu alanda milli olan özel savunma sistemlerinin oluşturulması, geliştirilmesine teşvik edilmesi, devletin kritik bilgi alt yapılarını koruyan sistemlerin zamanın gerekliklerine uygun olacak şekilde geliştirilmesi ve güncellenmesi, halkın dijital dünya kültürünün geliştirilmesi, küresel siber güvenlik seviyesinin geliştirilmesi için uluslararası anlaşmaların, mekanizmaların ve işbirliğinin artırılmasına yönelik çalışmalar yapılmasını kapsamaktadır.

Siber güvenlik faaliyetleri: Devletin ve kurumlarının kritik alanlarında siber uzaya bağlı şekilde bulunan bütün bilgi sistemlerinin korunması konusunda, tehdit kaynaklarının belirlenmesi önemli yer tutmaktadır. Bu korumayı sağlayan uzman personellerin bu sistemleri en üst seviyede kullanabilmeleri için bunların Rus diline çevrilmesini sağlamak, bilgi kaynaklarına yapılan saldırıların öncelikli olarak sonuçlarını tespit etmek, yapılabilirse yayılmasını önlemek ve ortadan kaldırmak için

devlet mekanizmasındaki sistemleri geliştirmek ve ulusal anlamda yazılımlar üretimi gerekmektedir. Faaliyet alanları devlet sırrının oluşturduğu belge, bilgi korumasında bulunan kurum ve kuruluşların herhangi bir tehditte korunması için kullanılan yabancı yazılımın kontrolü güvenli hale getirilmektedir.

Rusya Federasyonu, siber güvenlik alanlarında bireyi, özel şirketleri, kamu şirketlerini, devlet kuruluşlarını, bilimsel ve akademik kurumları ve siber güvenlik alanında kâr amacı gütmeyen kuruluşlarını stratejisinin parçalarına dahil ederek eylemlerini planlamaktadır.[174] Askeri gücünde akıllı silahlar veya siber teknoloji kullanarak güç oluşturup güvenliğini sağlamaya öncelik vermektedir. Diğer taraftan devletin kritik alt yapılarını korumayı hedeflemektedir. Silahlı gücünü son hızla geliştirmeye devam eden RF, siber unsurların askeri güç üzerindeki etkisine büyük önem atfetmektedir. Bu bağlamda Rus liderleri 2000'li yıllardan itibaren oluşturduğu resmî belgelerde siber silahlanmayı onaylamakta[175], RF siber gücünü dış politika hedefleri kapsamında kullanmaktan çekinmemektedir.[176] Estonya, Gürcistan ve Kırgızistan' a karşı yapılan ve ay ışığı olarak tabir edilen siber saldırıların failinin Rusya olduğu pek çok düzlemde dile getirilmektedir. [177]

3.2.3 Rusya Federasyonu'na Karşı Düzenlenen ve Rusya Federasyonu'nun Düzenlediği Siber Saldırıları

Devletlerarası ilişkilerde ortaya konan politika uygulamalarının şeffaflık ilkesi kapsamında sürdürülmesi uluslararası barış ve istikrarın sağlanması açısından büyük önem arz etmektedir. Belirsizliğin hâkim olduğu siber uzayda ise, tehdidin hangi aktörden geldiğinin ne zaman ve ne şekilde ortaya konduğunun taşıdığı muğlaklık devletlerin bu alanda güvenliklerini temin etme ve güçlü olma adına farklı alanlarda adımlar atmasına ve siber uzaydaki tehditlerin büyümesine yol açmaktadır. Bireyden

[174] Concept of a Cyber Security Strategy Russian Federation…, 2013, s.9-10
[175] Landon J. Wedermyer, The Changing Face of War: The Stuxnet Virus and the Need for International Regulation of Cyber Conflict, **Michigan State University College of Law** (Çevrimiçi) https://digitalcommons.law.msu.edu/cgi/viewcontent.cgi?article=1206&context=king 2012, s.13, (Erişim Tarihi:30.03.2020)
[176] Ali Burak Darıcılı, Barış Özdal, "Enformasyon Savaşı Bağlamında Rusya Federasyonu-Türkiye İlişkilerinin Analizi", **İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi,** S.4, C.19, 2017, s.25
[177] Ali Burak Darıcılı, Barış Özdal, a.g.m, s.25

topluma, devlet dışı aktörlere olmak üzere farklı düzeydeki aktörlerin çok geniş imkanlarla hareket kabiliyetine sahip olduğu siber uzayın amorf yapısı kuralların konması ve bunların denetimini zorlaştırmaktadır. İnsanüstü bir hızla işlem kabiliyetine sahip olunan bu düzlemde karşıt eylemlerin tespit edilip, önlenebilmesi için dijital bağlantıya sahip olunan altyapının güçlendirilmesi ve ilgili personelin eğitimi sürekli olarak, güncellemelere paralel şekilde sağlanmalıdır. Yukarıda yapılan Rusya'ya ait belgelerde siber güvenlik yerine enformasyon güvenliğinin kullanıldığı görülmektedir. Rusya kendi bilgilerini korumak ve özellikle çevre ülkelerini domine etmek adına da siber uzay çalışmalarına önem vermektedir. Bu anlamda Rusya'nın büyük çaplı siber saldırıların arkasında olduğu ve suç örgütleri ile bağlantılı saldırılar gerçekleştirdiği öne sürülmektedir[178]. Rusya' nın politikalarına karşı düzenlenen ve Rusya'nın dış politika hedeflerini gerçekleştirmek üzere düzenlediği bazı siber saldırılar aşağıda incelenmektedir.

Estonya Saldırısı: Estonya, interneti en fazla kullanan başlıca ülkeler arasında yer almakta ve hatta bu ülke için e-stonya tabiri kullanılmaktadır.[179] Estonya'ya karşı 2007 yılında failinin halen net olmadığı büyük bir siber saldırı gerçekleştirilmiştir. Estonya yönetimi, özellikle devlet kurumları ve birçok önemli özel şirketinin internet sitesine düzenlenen saldırıların Rusya tarafından yapıldığını iddia etmektedir.[180] Bu iddia çokça tartışılmıştır, zira Estonya NATO aracılığı ile saldırıların failinin bulunması ve tespiti yönünde yardım desteği talebinde bulunmuş da Estonya'nın bu diplomatik talebini Rusya reddetmiştir.[181] 09-10 Mayıs 2007'de başlayıp 19 Mayıs 2007' de sonra eren siber saldırılarda özellikle Estonya ekonomisi hedef alınmış, bankacılık sektörüne saldırılmıştır. Failinin kimliği bilinmemektedir.

Gürcistan Saldırısı: Gürcistan' a yönelik olarak düzenlenen saldırılar da Estonya saldırısına benzer şekilde öncelikle finans, hükümet ve medya alanlarını kilitlemeyi

[178]Siber Bülten, "Rusya Siber Alanda Neden Saldırıyor?", 2015, (Çevrimiçi) https://siberbulten.com/uluslararasi-iliskiler/rusya-siber-alanda-neden-saldiriyor/, (Erişim Tarihi: 01.04.2020)

[179] BBC Türkçe, Bir 'İnternet Cumhuriyeti' Edtonya, 2016, (Çevrimiçi) https://www.bbc.com/turkce/haberler/2016/05/160504_estonya_internet, (Erişim Tarihi:01.04.2020)

[180]BBCTurkısh, "Estonya'ya Siber Saldırı", 2007, (Çevrimiçi) http://www.bbc.co.uk/turkish/news/story/2007/05/070517_estonia_cyber.shtml, (Erişim Tarihi: 01.04.2020)

[181] Hasan Çiftçi, **Her Yönüyle Siber Savaş**, Ankara: Tübitak, 2017, s.183

amaçlamıştır.[182] Bu saldırıların Rusya tarafından gerçekleştirildiği iddia edilmektedir. Rusya, stopgeorgia.ru isimli web sitesinden birçok Rus siber saldırganını bu saldırılara davet etmiştir[183]. Gürcistan' a karşı yapılmış olan bu saldırı Rusya'nın silahlı kuvvetlerince yapılan saldırıyı da destekler niteliktedir.[184] Rus istihbarat servislerince yapıldığına dair tespitler yapılmasına rağmen, Rusya kontrolü dışında olduğunu savunmuştur. Siber saldırı kaynağı olarak DDoS kullanılmıştır.

Kırgızistan Saldırısı: ABD'nin 2009 yılından Kırgısiztan'a üs kurmak için girişimlerde bulunduğu zaman diliminde Kırgızistan'ın %80'nini kapsamak üzere internet sitelerine karşı siber saldırı gerçekleştirilmiştir.[185] Zira Rusya, Kırgızistan' a ABD üssünün yapılmasını istememektedir. 8 Ocak 2009 tarihinde Gürcistan ve Estonya' ya karşı olduğu gibi DDoS siber silahı ile Kırgızistan'a saldırı gerçekleştirildiği öne sürülmektedir.[186] Bu deliller kapsamında söz konusu saldırıların Rusya tarafından yapıldığı tahmin edilmektedir.

Litvanya Saldırısı: Yine DDoS siber silahını kullanarak, Litvanya' nın popüler olarak kabul edilen internet sitelerine çekiç ve orak simgelerini yerleştirmek suretiyle siber saldırılar gerçekleştirilmiştir.[187] Litvanya Cumhurbaşkanı Alexander Lukashenko' nun eski Sovyet yöneticiler hakkında suçlamalarda bulunması saldırıların en büyük nedeni olarak gösterilmektedir.[188] Bu nedenler kapsamında Litvanya'ya karşı saldırıların yine Rusya Federasyonu tarafından yapıldığı iddia edilmektedir. 2016 yılında ise Litvanya'da Kırım Tatarları üzerine meclis görüşmeleri yapıldığı sırada internet sitesine saldırı gerçekleştirilmiştir.[189] Rusya'nın Kırım ile tarihsel bağları ve 2014 yılında kendisine bağlanması üzerine yapılan oylama herkes tarafından bilinmektedir. Söz konusu saldırının yine Rusya tarafından gerçekleştirildiği muhtemel görülmektedir.

---

[182] Ali Burak Darıcılı, **Siber Uzay ve Siber Güvenlik…,** s.211
[183] Hasan Çiftci, **a.g.e**., s.186
[184] Ali Burak Darıcılı, Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırıların Analizi, **Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, S.2, C.7, 2014, s.7
[185] Siber Savaşlar: 5. Boyutta Savaş, (Çevrimiçi) https://www.kotuamacliyazilim.com/siber-savaslar-5-boyutta-savas/, (Erişim tarihi: 01.04.2020)
[186] Ali Burak Darıcılı, a.g.m., s.9
[187] Ali Burak Darıcılı, a.g.m.,s.
[188] Daniel McLaughlin, "Lithuania accuses Russian hackers of cyber assault after collapse of over 300 websites", 2008, (Çevrimiçi) https://www.irishtimes.com/news/lithuania-accuses-russian-hackers-of-cyber-assault-after-collapse-of-over-300-websites-1.942155, Erişim Tarihi: 01.04.2020
[189]Euronews, Litvanya Meclisi'nin İnternet Sitesine Siber Saldırı,2016 (Çevrimiçi) https://tr.euronews.com/2016/04/11/litvanya-meclisi-nin-internet-sitesine-siber-saldiri, Erişim Tarihi: 01.04.2020

Ukrayna Saldırısı: Rusya'nın, Kırım'da havaalanı ve stratejik noktaları ele geçirmesinden sonra Ukrayna parlamento üyelerinin özellikle cep telefonlarının hedef alınarak gerçekleştirilen siber saldırıdır[190]. Kırım'ın ilhakından sonra Rusya'nın Ukrayna'ya karşı bir hibrid savaş gerçekleştirdiği görülmektedir. 23 Aralık 2015' te Ukrayna'nın batı kesimi olmak üzere üç farklı bölgesinde gerçekleştirdiği siber saldırılar neticesinde 225 bin kullanıcının elektriği kesilmiştir.[191] Bilgisayar virüsünün elektrik kesintisine sebebiyet verdiği ve bütün bu saldırıların ana kaynağının Rusya Federasyonu olduğu ileri sürülmektedir. Ukrayna Cumhurbaşkanı Yardımcısı verdiği röportajda, Ukrayna'nın siber güvenlik konusuna çok önem verdiğini, çünkü sürekli olarak Rusya tarafından saldırı altında bulunduğunu, bugüne kadar yapılan saldırıların %99' unun Rusya tarafından gerçekleştirildiğini belirtmiştir.[192]

Siber saldırılar yapısı gereği karmaşık ve doğrusal olmayan düzensizliği içermektedir. Rusya, bu düzensizlikten faydalanarak yakın çevresine çok sayıda siber saldırı gerçekleştirmiştir. Rusya Federasyonu, uluslararası alanda siber suçu ve siber suçluları destekleyen bir devlet olarak algılanmaktadır. Devletin bekası odaklı ve uluslararası ilişkilerde ahlaki prensipleri göz ardı edebilen Realist yaklaşımı yansıtır şekilde Rusya'nın siber güç enstrümanlarıyla politikalarını gerçekleştirme ve gücünü maksimize etme yolunu izlediği gözlenmektedir. Yukarıda arz edilen unsurlar doğrultusunda Rusya'nın siber gücünü realpolitiğin güç mülahazaları kapsamında kullanarak etki alanını genişletmeyi ve ülkelerin politik kararlarını kendi çıkarları doğrultusunda şekillendirmeyi amaçladığını söylemek mümkündür.

---

[190] Paverl Polityuk, Jim Finkle, "Ukraine Says Communications Hit, Mps Phones Blocked", 2014, (Çevrimiçi) https://www.reuters.com/article/us-ukraine-crisis-cybersecurity/ukraine-says-communications-hit-mps-phones-blocked-idUSBREA231R220140304 , (Erişim Tarihi: 01.04.2020)

[191] Dustin Volz, "U.S. Government Concludes Cyber Attack Caused Ukraine Power Outage", Reuters, 2016, (Çevrimiçi) https://www.reuters.com/article/us-ukraine-cybersecurity/u-s-government-concludes-cyber-attack-caused-ukraine-power-outage-idUSKCN0VY30K, (Erişim Tarihi: 02.04.2020)

[192] İlya Timtchenko, "Shymkiv: Ukrainians Not Prepared for Cyber Attacks", Kyiv Post, 2017, (Çevrimiçi) https://www.kyivpost.com/business/shymkiv-ukrainians-not-prepared-cyber-attacks.html, (Erişim Tarihi: 02.04.2020)

3.3 Çin Halk Cumhuriyeti (ÇHC)

Çin Halk Cumhuriyeti, dışa kapalı ekonomi politikalarından sıyrılarak oluşturduğu stratejileri doğrultusunda dünyanın önemli ekonomik gücü olmaya başlamıştır. Sahip olduğu insan gücü ile üretimi hızla sağlamakta ve verimliliğe önem vermektedir. 1981'de Çin'de yoksulluk sayısı 634 milyon iken bu sayı 2004 yılında 128 milyona düşmüş ve ekonomik anlamda hızlı bir büyüme kaydedilmiştir. Bu büyümenin nedenleri arasında modern sektörün genişlemesini aktif olarak teşvik eden politikaları yer almaktadır.[193] Çin kademeli olarak geliştirdiği dışa açılım politikasında sahip olduğu nüfus ile yabancı yatırımcıları kendisine çekmektedir. Bir çeşit sermayeyi ithal etmektedir. ÇHC'ye ekonomik katkı ile teknoloji, kabiliyet ve ticari deneyimler sağlamaktadır.[194]

Dünya ekonomisine entegre olan ÇHC sahip olduğu işçi fazlası sayesinde dünyanın fabrikası olarak algılanmaktadır. Sahip olduğu iş gücü ekonomisine ciddi bir katkı sunmaktadır. Tarihinde matbaa, pusula, barut icatları bulunan Çin, dünyanın düzenini savaşta, edebiyatta ve seyahatlerde farklı unsurlar üzerinden değiştirebilmiştir.[195] Günümüzde ise bilim ve teknoloji alanlarında önemli değişimler sağladığı gözlemlenmektedir. Bu değişimler için geliştirmekte olduğu ileri teknoloji robotları ve uzay ile bağlantı çalışmalarına hız kazandırmaktadır. 2000' de uzay yörüngesinde 10, 2008' de 35, 1 Eylül 2015 itibariyle 142 uydusu bulunmaktadır. ABD'nin ise uzay yörüngesinde 549 aktif uydusu, RF'nin ise yaklaşık olarak 131 uydusu bulunmaktadır. Çin bu uyduların yaklaşık olarak doksan beşini Savunma Bakanlığı ve devlete ait uzay enstitülerinde kullandırmaktadır.[196] Askeri doktrinlerinde siber uzayı beşinci savaş alanı olarak kabul eden Çin, teknolojik gelişimine ve siber uzayda yaptığı çalışmalara büyük önem atfetmektedir.

---

[193] Mıcheal P. Todaro, Stephen C. Smıth, Economic Development, Boston: Peorsen, 2016, s.235

[194] Serdar Öztürk, Ali Sözdemir, Bekir Gövdere, "ÇİN: Washington Uzlaşmasından Beijing Uzlaşmasına", **C.Ü. İktisadi ve İdari Bilimler Dergisi**, C.7, S. 1, 2006, s.69

[195] New World Encyclopedia, "History of Science and Technology in China", (Çevrimiçi) http://www.newworldencyclopedia.org/entry/History_of_science_and_technology_in_China, Erişim: 03.04.2020

[196] GlobalSecurity.org,"China in Space", (Çevrimiçi) https://www.globalsecurity.org/space/world/china/index.html, Erişim Tarihi: 03.04.2020

3.3.1 Çin Halk Cumhuriyeti'nin Siber Uzay Çalışmaları

Çin, kuruluşundan yüz yıl sonra kendisini dünyanın sanayi gücü ülkesi olmayı hedeflemektedir. Çin'in büyümesini sağlayan en önemli unsuru sanayide kaydettiği gelişmeleri ile dışa açılım politikası kapsamında küreselleşmeye katılma çabası teşkil etmektedir. Siber uzay, günümüzde küreselleşmenin ana kapılarından birisi olarak gösterilmektedir. Siber uzay teknolojileri, devletlerin, toplumların ve bireylerin süreklilik içerisinde faaliyette bulunduğu, kullanımı her alana sirayet eden bir alanı oluşturmaktadır. ÇHC'nin elit düşünürleri küreselleşme çabalarında risk ve tehditlerin de önemli yer işgal ettiğini belirtmektedirler. Tehdit olarak uluslararası terör, kitle imha silahlarının yayılması, salgın hastalıklar kapsamında şiddetli akut solunum sendromları ve siber suçlar gibi örnekler gösterilmektedir.[197]

Siber uzayda ortak platform oluşturmak için uzay ile dünya üzerinde yapılan işlemlerin ilişkisini kurmak önem arz etmektedir. Gelecekte eğitim, bilim, sanat, sosyalleşme gibi hayatın hemen hemen bütün noktalarının siber alana devşirileceği düşünülmektedir. Devletler, siber uzayın güvenliğini ve kontrolünü sağlayabilirler ise, güç ve politika uygulama kabiliyetleri daha yüksek olabilecektir. Bu anlamda, öncelikli olarak askeri alanlara önem verildiği gözlenebilmektedir. Çin silahlı kuvvetleri bünyesinde 'Mavi Ordu' adında otuz kişilik personelden oluşan bir ekip oluşturmuş ve siber güvenliğin sadece toplum sorunu olmadığı, askeri bir gereksinim olduğu da iddia edilmektedir.[198] Mavi Ordu'yu ulusal güvenliği için kurduğunu belirten Çin, siber uzay kapsamında geliştirdiği politikalarında barışçıl, işbirlikçi ve kazan kazan ilkeleri ile hareket ederek ortak kader oluşturulma çabası içerisinde olduğunu vurgulamaktadır.[199] Savunma Bakanlığı'nca 2000 yılında ise, 'Altın Kalkan' adında bir internet güvenlik duvarı projesi ile gündeme gelmiştir. Söz konusu projeye göre Çin gerek duyduğu zamanlarda ve saldırı olması durumunda internet üzerinde sansürleme ve gözetleme

---

[197] Yong Deng, Thomas G. Moore, "China Views Globalization: Toward a New Great-Power Politics?", **The Washington Quarterly**, C. 27, S. 3, 2004, s. 117.

[198] Foxnews, "China Confirms Existence of Elite Cyber-Warfare Outfit the 'Blue Army'", (Çevrimiçi) http://www.foxnews.com/tech/2011/05/26/china-confirms-existence-blue-army-elite-cyber-warfare-outfit.html, 2017, Erişim Tarihi:04.04.2020

[199] China.com, "Siber Dünyada Ortak Kader Topluluğu Çağrısı", (Çevrimiçi) http://turkish.china.com/news/china/543/20170301/899556.html, Erişim Tarihi: 04.04.2020

yapabilmektedir.[200] Çin'in internet üzerindeki özel projesinin tarihinin dışa açılma politikası ile çelişkisi ironik bir durumu gözler önüne sermektedir.

3.3.2 Çin Halk Cumhuriyeti'nin Siber Uzay Politikaları ve Ulusal Strateji Belgeleri

Uluslararası ilişkiler gelişen güç araçlarına ve güç dağılımındaki değişimlere paralel şekilde mücadelelere ve çatışmalara sahne olmakta, son dönemde siber araçların gittikçe artan şekilde güç unsuruna dönüşmesi de siber alanda yükselen mücadeleleri ve bilgi savaşlarını gündeme getirmektedir. Bugünün dünyası devletler için karmaşık ve belirsizliğin rekabeti zorlaştırdığı bir dönemi içermektedir. Çin'in en büyük ekonomik güç olma yolundaki başarısında teknolojinin rolü yadsınamaz bir gerçektir. Dünyada 3,4 milyar kadar internet kullanıcısının olduğu varsayılır ise bunun 721 milyonunun Çinli kullanıcı olduğu düşünülmektedir.[201] Çin sahip olduğu güce ivme kazandırabilmek için siber uzaydaki politikalarına temel oluşturmak üzere 'Beyaz Kitap' isimli bir belge yayımlamıştır. 2004 yılında yayınlanan ilk belge savunma ve teknoloji stratejilerini açıklamaktadır.[202] Bu belgeye göre: uluslararası ilişkilerde derin ve karmaşık ilişkiler değişikliğe uğramaya devam etmektedir. Temel noktalarda istikrar devam edebilmekle beraber belirsizlik, istikrarsızlık ve güvensizlikler artmaktadır. Dünyada çoklu kutuplaşma, ekonomik küreselleşme ve dönüşümler derinlemesine değişmektedir. Çin, Beyaz Kitapta politika ve projelerini bilgi teknolojilerine teşvik, yüksek harcamalı savunma bütçesi, bilim ve teknolojileri geliştirme stratejisi izlemektedir. Temel oluşturan söz konusu rapor sonrası bilişim sistemlerinin gelişmesine önem verdiği anlaşılmaktadır. Çin, bilişim sistemlerini geliştirmek amacıyla da "2006-2020 Ulusal Bilim Stratejisi Geliştirme" adıyla altı ana başlıktan oluşan bir bildiri yayımlamıştır. Bu bildiriye göre:[203]

---

[200] Torfox, "The Great Firewall of China: Background", (Çevrimiçi) https://cs.stanford.edu/people/eroberts/cs181/projects/2010-11/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html, Erişim Tarihi: 04.04.2020

[201] Ali Burak Darıcılı, Barış Özdal, "Analysis of the Cyber Security Strategies of People's Republic of China", **Güvenlik Stratejiler Dergis**i, C.14, S. 28, 2018, s.2

[202] Çin Danıştay Bilgi Bürosu, "Beyaz Kitap Çin'in Ulusal Savunma Belgesi", Pekin, 2004, (Çevrimiçi) http://politics.people.com.cn/GB/1027/3081796.html, Erişim Tarihi: 04.04.2020

[203] Çin Komünist Partisi Merkez Komitesi, "2006-2020 Ulusal Bilişim Geliştirme Stratejisi," 2006 (Çevrimiçi) http://www.gov.cn/gongbao/content/2006/content_315999.html, Erişim Tarihi: 05.04.2020

1.*Bilişimin Küresel Temel Eğilimleri*: Bilgi teknolojilerindeki yenilikler 1990'lı yıllardan itibaren internet ağları ile yaygın bir şekilde kullanılmaya başlamaktadır. Yaşanan yüzyılda ve gelecek yıllarda bilişimin sosyo-ekonomik kalkınma üzerindeki etkisi daha derin ve büyük atılımlar ile tasarlanmaktadır. İnternet, küresel boyutta çeşitli ideolojilerin ve kültürlerin yoğun yaşandığı ortamı oluşturmaktadır. Devlet e-sisteme geçerek idari yaptırımların verimliliğini artırmakta ve demokratik gelişimlere önem kazandırmaktadır. Bu nedenle dünyadaki devletlerin ortak sorunu olarak, internetin güvenliğini sağlama sorunları artmaktadır.

2. Bilişim Gelişmelerinde Çin' in Temel Durumu: Bilişim endüstri sistemleri hızla gelişmeye devam etmektedir. Ekonomik büyümeye katkısı sürekli artmaktadır. 2005 yılında bilişim sektörünün katma değeri GSYİH'nin %7,2'si iken ekonomik büyümeye %16,6 olarak katkı sağlamaktadır. Elektronik bilgi sistemlerinin ekonomiye katkısı %30 'dan fazlasını oluşturmaktadır. Bilgi teknolojileri ile sanayileşme arasındaki ilişkiyi doğru bir şekilde ele almak ve ilerlemeye devam etmek için uzun vadeli planlar yapılmaktadır. İşletmelerin bulunduğu inovasyon sistemlerinin acilen iyileştirilmesi ve bağımsız ekipman kabiliyetlerinin acilen güçlendirilmesi gerekmektedir.

3. *Bilişim Gelişmelerinde Çin'in İdeolojik ve Stratejik Hedefleri*: Ekonomik, politik, kültürel ve askeri gelişimlerde bilişimin önemli rolünü tam olarak yerine getirmektedir. Ulusal bilişim düzeyini sürekli olarak iyileştirmektedir. Çin'in bilişimin gelişmesi konusundaki stratejik prensibi, genel planlama, kaynakları paylaşma, uygulamaları derinleştirme, pratik sonuçları arama, gerçek piyasaya dönük, yeniliğe dayalı, askeri ve sivilleri birleştiren güvenlikli bir itici güç olarak belirlenmektedir. 2020' ye kadar olan stratejik hedefleri ise temel bilgi altyapısını küresel olarak oluşturma, bağımsız yenilik yeteneğini artırma, yapısal olarak endüstri ile tamamen optimize edilmiş, güvenliği büyük ölçüde iyileştirilmiş, sanayileşme gelişim modelleri oluşturulmuş ve bilgi toplumuna geçiş için sağlam temel oluşturmayı hedeflemektedir.

4. *Bilişimin Gelişmesinde Çin'in Stratejik Odağı*: Ekonomide ulusal bilişimin teşvik edilmesi; tarımla bilişim sistemlerini entegre etmek, kentsel-kırsal bilgi hizmetleri sistemleri kurarak çiftçileri uyumlu hale getirmek, pazarlama, teknoloji, eğitim, sağlık

ve diğer internet hizmetlerini kırsalın işgücüne rasyonel desteklemeyi sağlamaktır. E-devlet sisteminin kullanımının teşvik edilmesi; kamu hizmetlerinin geliştirilmesi adına bireyleri ilgilendiren internete dayalı, kamu hizmeti kurulması ve toplumun her alanına bu kamu hizmetlerini tanıtmayı hedeflemektedir. Gelişmiş ağ kültürü oluşturmak; haber yayıncılığı, radyo, film ve edebiyat, televizyon ve sanat endüstrilerinin bilişim ile birleşmesini hızlandırmayı, kültürel ürünlerin kalitesini ve kültürel ürünlerin tedarik kapasitelerini teknoloji ile artırmayı hedeflemektedir. Sosyal bilgilendirmeyi teşvik etmek; çeşitli bilgi sistemlerinin kaynaklarını entegre etmek suretiyle, birleşmiş bir bilgi platformunu güçlendirmektedir. Milli yazılım ve donanımlara önem vererek ulusal şekilde gelişmeyi sağlamaktadır. Bilgi teknolojilerinin gelişmesini sağlamak adına eğitim alanlarına büyük önem verilmektedir.

5.*Bilişimin Gelişmesinde Çin'in Stratejik Eylemi*: Bilgi teknolojilerini temel eğitim müfredatlarında oluşturmak, öğretim içeriğini zenginleştirmek, öğreticilerin bu konuda seviyelerini geliştirmektedir. E-ticaret eylem planı oluşturmak üzere küçük ve orta büyüklükteki işletmeler e-ticaret faaliyetlerine teşvik edilmektedir.

6. *Bilişimi Koruma Önlemleri*: Bilgisayar kart devrelerinin entegrasyonunu, yazılımını, ana ürünlerin sağlanmasını ve bunlar için güvenli sanayi politikaları kapsamında yerli üretimin sağlanmasını içermektedir. Çin bilgi teknolojilerini kapsayacak hukuk sistemlerinin oluşumu için çaba harcamaktadır. İnternet ağlarının güncellenmesi takip edilmekte, bilişim sistemlerini korumakta olan ekip profesyonellerden teşkil edilmektedir.

ÇHC, 2004 ve 2006 yıllarında bilgi teknolojileri politikaları kapsamında siber uzayın güvenliği konusunda temel adımları atmıştır. Irak'ın devrik lideri Saddam Hüseyin'in, Çin ve Rusya'dan askeri teçhizat temin ederek savunma sistemini oluşturduğu bilinmektedir. Körfez savaşlarında söz konusu askeri araçların ABD tarafından siber uzay sistemleri ile kontrollü olarak bertaraf edildiği görülmektedir. ÇHC yükselen teknolojiye sahip olarak batılı devletlerin siber uzayda sahip olduğu yeteneklere sahip olmadığını fark etmiştir.[204] Bu anlamda siber uzay politikaları ulusal güvenliğin teşkil edilmesinde önemli yer oluşturmaktadır. ÇHC'nin siber uzay güvenliği kapsamında gerçekleştirmeye çalıştığı stratejik politikaları aşağıda incelenmektedir.

[204] Richard A. Clarke, Robert K.Knake, **Siber Savaş…,**s.82

Siber uzaya dair ana hatlar çalışmada ara ara belirtilmiştir. Bütün olarak betimlemek gerekirse; uzay, bilim ve teknoloji, internet ve kullanıcılar gibi temellerden oluşmaktadır. Uzayda gerçekleştirdiği faaliyetler üzerine rapor yayınlayan Çin, söz konusu raporda, amaçlarını ve vizyonunu, 2011 yılından itibaren olan gelişmeleri, gelecek beş yıl için yapılacak çalışmaları, tedbir politikalarını, uluslararası değişim ve işbirlikleri olmak üzere beş ana başlık kapsamında irdelemektedir.[205]

Amaçlar ve vizyon geliştirme: Çin uzayı barışçıl amaçlar için kullanmayı, sosyal ilerlemeyi teşvik ederek tüm insanlığa fayda sağlamayı, sosyal ilerleme için talepleri karşılamayı, halkının bilimsel ve teknolojik gelişmelere önem vermesini amaçlamaktadır. Vizyonu için ise ulusal güvenliğini temin etmeyi, Çin'i bütün alanlarda uzay gücüne sahip bir devlet haline getirmeyi, uluslararası işbirlikleri içerisinde yer almayı ve Çin halkı üzerinde uzay bileşenleri konusunda farkındalık oluşturmayı hedeflemektedir.

2011' den günümüze gelişmeler: Çin 2011 yılından 2016 yılına kadar 100'den fazla uzay aracını uzay yörüngesine göndermiştir. Televizyon, radyo ve televizyon sistemlerini siber uzay ile bağlantılı olarak geliştirmektedir. Konum bulmayı sağlayabilen uzaydan takibi mümkün olabilecek navigasyon sistemleri oluşturmaktadır. Uzayın güncel teknolojilerini takip edebilmek için Shijian-9, Shijian-10, Shijian-11 uydularını uzaya göndererek takiplerine başlamaktadır.

Gelecek beş yıl hedefleri: Uzaya gönderilecek olan araçların gelişimleri hakkında çalışmalar yaparak, pazarlamasını gerçekleştirmeyi istemektedir. Bahse konu bu araçların oluşturulmasında uzayın doğallığına uygun, maliyeti düşük, uzaktan kontrolü kolay ve güvenlikli olması yönlerinde araştırma yapmaktadır. Uydu sistemlerinin temelini oluşturan öğelerden uzaktan kontrol, iletişim ve yayıncılık ve konum belirleme gibi üç ana sistemini geliştirerek, uzay-yer entegresini sağlamaya çalışmaktadır. Sürdürülebilir kalkınmayı içeren siber uzay bilimleri uydularını kurarak, temel uygulama araştırmalarını güçlendirmek için atılımlar yapmaktadır.

Gelişim için önlem politikaları: Uzayda rasyonel gelişim sağlamak için kullanım kapasitesi, güvenliğin arttırılması ve altyapıların inşasına öncelik tanımaktadır. Uzayda

[205] The State Council Information Office The People's Republic Of China, China's Space Activities in 2016, 2016, (Çevirimiçi) http://english.scio.gov.cn/whitepapers/2017-01/10/content_40535777_2.htm, Erişim Tarihi: 08.04.2020

yenilikler büyük ölçüde artmıştır. Uzay bilimi ve teknolojilerinin gelişmesi teşvik edilmektedir. Çin uzay bilim ve teknolojisinin genel seviyelerini artırmaya öncülük etmektedir. "Çin Uzay Günü", "Dünya Uzay Haftası" ve "Bilim ve Teknoloji Haftası" gibi özel günler oluşturarak daha fazla insanı çekmeyi amaçlamaktadır.

Uluslararası işbirliği ve değişimleri: Çin uluslararası alanda geliştireceği temel politikalar ile işbirliğinin sağlanabileceği fikrini benimsemiştir. Bu politikaları maddeler halinde belirtmek gerekirse:

- Birleşmiş Milletler çerçevesinde uzayın barışçıl kullanım faaliyetlerini desteklemek,
- Uzay endüstrisinin gelişimini arzulayan devletler ve sivil toplum kuruluşlarının faaliyetlerini desteklemek,
- Ortak hedefler doğrultusunda ikili ve çok taraflı iş birliklerinin güçlendirilmesini sağlamak,
- Bölgesel uzay işbirliklerine önem vermek,
- Uluslararası yasalar ve yönetmelikler rehberliğinde düzen oluşturmak.

Çin, 2016 yılına kadar Almanya, Rusya, Avrupa, Fransa, Brezilya, ABD, Cezayir, Arjantin, Belçika, Hindistan, Endonezya, Kazakistan devletleri ile ikili uzay işbirliği anlaşmalarını imzaladığını teyit etmektedir. Günümüzde devletler uzayda faaliyetlerini geliştirmeye büyük önem vermektedirler. Geçtiğimiz her gün ise, uzay teknolojileri günlük yaşamın her alanında yaygınlaşmaktadır. Üretim ve sosyal yaşam alanlarında çok kapsamlı ve geniş etkiler yaratmaktadır. Bilişim, uzay ve siber uzay teknolojileri birbirleri ile bağlantı oluşturmaktadır. Zira siber uzay hakkında halen kesin bir tanımlama yapılamamıştır. 2008'de Pentagon'da oluşturulmuş uzman ekipler tarafından kapsayıcı olabilecek bir tanımlama yapılmaktadır. Siber uzay, internet, telekomünikasyon ağları, bilgisayar sistemleri ve gömülü işlemciler, denetleyiciler ve bu denetleyicilerin dahil olabildiği birbirine bağlı bilgi teknolojisi altyapıları ağından oluşan küresel etki alanı olarak tanımlanmaktadır.[206] Çin'in uzay ve siber uzay teknolojilerini kapsayan politikalar oluşturduğunu değerlendirmek mümkündür.

[206] P. W Singer, Allan Friedman, **Cyber Security and Cyber War : What Everyone Needs to Know**, New York: Oxford University Press, 2014, s.13

Çin siber alanı ortak kader topluluğu olarak tanımlamaktadır. Siber güvenliğe ilk defa 'siber güvenlik' tanımlamasıyla yaklaştığı 2017 yılında 'Ulusal Siber Güvenlik Stratejisi' adıyla siber güvenlik belgesi yayımlamıştır.[207]

Siber uzayın fırsatları ve zorlukları: Bilgi devrimi hızlı gelişim sağlamaktadır. İnsanlar bilgisayar sistemleri ile dijital dokümanlara çok hızlı ulaşmaktadırlar. Üretim yöntemleri ve sosyal gelişim süreci derinden etkilenmektedir. Ağ teknolojileri sayesinde, ekonomik kalkınma, kültürel etkileşim, yerel ve ulusal yönetimlerin çok daha geniş ve hızlı olacağını belirtmektedir.

Zorlukları; siber uzaydaki gelişmeler politik, ekonomik, kültürel ve bilgi kültürlerini olumsuz yönde etkileyebilmektedir. Devletin, toplumun ve bireylerin güvenliklerini ve kültürlerini korumaya ağırlıklı olarak önem verilmektedir. Terör örgütleri tarafından propagandalar çok daha yayın yapılabilecektir. Uluslararası alanda rekabet daha hızlı gelişmektedir. Sınırlarının bulunmaması nedeniyle güvenliğin çok zor sağlanabilecek bir alan olduğu belirtilmektedir.

Siber Güvenlikte amaçları: Yerli ve yabancı siber tehditleri bütün ayrıntıları ile incelemektedir. Öncelikli amacı iç ve dış politikalarında siber güvenliği sağlamaktadır. Siber silahlanmanın engellenmesinin önemli olduğunu savunmuştur. Barışçıl, güvenlikli ve açık politikalar ile siber uzayın inşa edilmesi gerekmektedir. Uluslararası alanda işbirlikçi, kazan-kazan politikalarını amaçlamaktadır.

Siber uzay ilkeleri: Çin siber uzayda devletlerin egemenliklerine saygı duymaktadır. Siber uzayda devletlerin silahlanması ya da silahlanmaması konusunda 'BM Sözleşmelerine' göre ilkeler oluşturulması gerekmektedir. Siber uzayda normlar oluşturulmalı ve hukukun üstünlüğü sağlanmalıdır.

Siber uzay stratejileri: Çin dijital alanda ulusal güvenliğini korumakta kararlıdır. Devletin sahip olduğu kritik altyapıyı korumaya önem vermektedir. Siber suç, siber terör ve siber saldırı gibi terimlerin hukuk literatüründe anlaşılır hale gelmesini planlamaktadır. Siber alanlardaki koruma yeteneklerini geliştirmeyi hedeflemektedir. Devletler ile ikili ya da çok taraflı olmak üzere siber güvenlik anlaşmalarını teşvik etmektedir.

---

[207]Lawfare, China's National Cybersecurity Strategy, 2016, (Çevrimiçi) https://www.lawfareblog.com/chinas-national-cybersecurity-strategy, Erişim Tarihi:08.04.2020

Çin, bilgi altyapı sistemlerini korumakla başlayıp, bilişim teknolojileri yönünde stratejilerini oluşturmuştur. Bu gelişim teknik bilgiye sahip kişilerce yapılabilmektedir. Siber uzay ise herkesin ortak bir paylaşımı bulunan ve kullanım kontrolü mümkün olmayan alana dönüşmektedir. Dünya çok taraflı uluslararası devlet sistemleri, sivil toplum kuruluşları ve karşılıklı bağımlılıkları ile ön plana çıkmaktadır.[208] 2017'de Dışişleri Bakanlığı ve Çin Siber Uzay İdaresi ortaklaşa olarak 'Çin Uluslararası İşbirliği Stratejisi' adıyla dört ana bölümden oluşan bir belge yayımlamıştır.[209]

Fırsatlar ve zorluklar: İnsanlık çok kutuplu, küreselleşmiş ve kültürel olarak yeni bir bilgi çağına girmektedir. İnternetin temsil ettiği bilgi ve iletişim teknolojileri yaşam biçimlerini değiştirmekte, ekonomik refahı ve sosyal gelişmeyi artırmaktadır. Siber uzay muazzam fırsatlar sunarken yeni sorun ve zorlukları da beraberinde getirmektedir. Kalkınma ve güvenlik sorunları küresel olarak endişe kaynağı oluşturmaktadır. Kritik bilgi altyapıları güvenlik açığı ve potansiyel risk taşımaktadır. Siber terörizm küresel bir kamu tehdidi haline gelmektedir. Siber alanın anarşik sistem içerisinde bulunması, siber uzayın gelişimini engellemektedir. Devletlerin siber uzayda yönetişim sistemini hayata geçirebilmesi ancak kural oluşturup, karşılıklı anlayış ve saygı içerisinde işbirliği yöntemlerinin geliştirilmesiyle mümkün olabilmektedir.

Temel prensipler: Uluslararası ilişkilerde ortak çıkarların yürütülmesi için kazan-kazan prensibini içeren bir yapının kurulması çağrısında bulunmaktadır. Siber alan devletlerin birbirine bağlı, iç içe geçtiği, menfaatlerinin bulunduğu alan olarak oluşmaktadır. Güvenli, istikrarlı, barışçıl siber alan dünya devletleri için büyük önem taşımaktadır. Devletlerin egemenlik ilkelerine saygı gösterilmesi önem arz etmektedir. BM şartında yer alan egemenlik ilkeleri siber alanda norm olarak kullanılabilir. Siber alanda hegemonya oluşturulmamalı, devletlerin içişlerine müdahale edilmemeli, ulusal güvenliğini zayıflatan siber saldırı faaliyetlerinde bulunulmamalıdır. Siber uzay sadece devletlerin bulunduğu bir alanı içermemektedir. Bireylerin, toplumların da etkileşim içinde bulunduğu platformlar oluşturmaktadır. İnsanlık için ortak faaliyet alanıdır, bu

[208] Robert O. Keohane ve Joseph S. Nye Jr., "Power and Interdependence in the Information Age", **Foreign Affairs**, C. 7 S.5, Eylül-Ekim 1998, s. 83

[209] Chinadaily, "International Strategy Of Cooperation On Cyberspace," 2017, (Çevrimiçi) https://www.chinadaily.com.cn/kindle/2017-03/02/content_28409210.htm, (Erişim Tarihi: 09.04.2020

nedenle devletlerin ortak paylaşım sistemleri oluşturması ve bu çerçevede yönetilmesi gerekmektedir.

Stratejik hedefler: Devletin siber uzayda egemenlik, güvenlik ve kalkınma çabalarını koruma adına kararlılıkla adım atılmaktadır. İnternet üzerinden bilgilerin güvenli akışını sağlamayı istemektedir. Küresel ağ bağlantılarının barış, güvenlik ve istikrar içinde sürdürülebilmesi için çabalamaktadır. Devletlerin bağımsızlıklarını korumak adına uluslararası hukukun üstünlüğünü artırmayı istemektedir. Dijital ekonomi sayesinde internet alışverişlerini, dünyanın her alanına ulaşabilecek pazar alanlarını derinleştirmektedir.

Siber uzayda eylem planlaması: Siber uzayda uluslararası barışı ve güvenliği sağlamak adına tehditleri önlemeye çalışmaktadır. Risklerin ancak bilgi teknolojilerinin kötüye kullanımını ve siber silahlanmayı azaltarak diğer devletler ile diyalog içerisinde olunabilirse başarıya ulaşacağına inanmaktadır. Önleme perspektifini uluslararası hukukun oluşturulmasına bağlamaktadır. Dünya Ekonomik Forumu altında bulunan 'İnternetin Geleceği' girişimlerinde küresel internet yönetim platformlarına, faaliyetlerine aktif olarak katılmayı ve katkıda bulunmayı planlamaktadır. Uluslararası ilişkilerde siber terörizm ve siber suçlara karşı diğer devletler ile ikili polis ve adli işbirliklerini sağlamayı planlamaktadır. Ekonomik ve kültürel değişimler hakkında ortak önlemler alınması gerekliliğini savunmaktadır.

ÇHC'nin bilgi, bilişim, siber uzay teknolojilerini birbiriyle entegre olacak şekilde düzenleme yaptığı gözlemlenmektedir. Zira uluslararası ilişkilerde siber uzayı domine etmesi muhtemel görülmektedir.[210] Çin siber uzayı domine etme amacına örnek olarak batılı devletlerin internet yönetiminin kendi tekellerinde bulunmasını göstermektedir.[211] Siber uzayı domine etme hedefi siber alanda gerçekleşen saldırılara, hatta çıkması muhtemel savaşlara neden olabilecektir.

[210] Soner Çelik, "Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşım," **ARHUSS**, C.1,S.2 ,(2018) s.118

[211] Madhulika Srikumar, "Should BRICS Rally Around China's Call For Cyber Sovereignty?", Observer Research Foundation, 2017, (Çevrimiçi) https://www.orfonline.org/expert-speak/should-brics-rally-around-china-call-for-cyber-sovereignty/, Erişim Tarihi: 08.04.2020

3.3.3 Çin Halk Cumhuriyeti'ne Karşı Düzenlenen Saldırılar ve Çin Halk Cumhuriyeti'nin Düzenlediği Siber Saldırılar

Günümüzde konvansiyonel savaş yöntemleri değişmektedir. Savaş yöntemlerinin askeri ve sosyal yapılar üzerinden ağ teknolojilerine bağlı kazanımlar sağladığı gözlemlenmektedir. Deniz, hava, kara ve uzaydan sonra beşinci boyut olan siber uzay gelişmiş teknoloji sayesinde askeri araçları kontrol edebilmekte, internet imkanları sosyal yapıyı yönlendirebilecek kapasiteye ulaşabilmektedir. Çin, teknoloji ile siyasi ve ekonomik gücünü bütüncül olarak inşa etmektedir. Siber uzaydan gelebilecek her türlü saldırıya karşı duyarlı, yapacağı saldırılarda ise çok etkili olabilmesi disiplinli bir şekilde teknoloji ve uzay bilimlerinde kaydedeceği ilerlemesine bağlanmaktadır. Bazı uzmanlar ise Çin'in internet ağları ile bağlı yapıların işlevlerini yok edebilecek teknolojiyi geliştirdiklerine inanmaktadır.[212] ÇHC, siber uzayın bir savaş alanı olabileceğini ve siber gücün hava, deniz ve kara güçlerinde olduğu gibi askeri güç unsurlarının entegre olacağını kabullenmektedir.[213] Çin'in birbirine bağlı ağlar ile gerçekleştirdiği ya da saldırıya uğradığı örnek siber saldırılar aşağıda incelenmektedir.

Çin Kızıl Korsanlar Birliği'nin ABD'ye Saldırısı: ABD, 1999'da Belgrad'da bulunan Çin konsolosluğunu yanlışlıkla bombalamış bunun akabinde ABD'nin resmi sitelerine yönelik 12 saat süren siber saldırılar düzenlenmiş, saldırıların Çinli Kızıl Korsanlar tarafından yapıldığı iddia edilmiştir.[214] Dönemin ABD yetkilileri, saldırıların üç ayrı kritik yere yapıldığını açıklamış ancak kimin yaptığını tespit edememiştir. FBI'ın yaptığı araştırmalar üzerinden saldırıların Çin kaynaklı olduğuna dair değerlendirmelerde bulunulmuştur.[215]

Joint Strike Fighter (JSF) Verilerinin Çalınması: Geliştiricilerinin arasında Türkiye'nin de bulunduğu JSF, diğer adıyla F-35 savaş uçakları ayrı ayrı kullanılması

---

[212] Altun Altun, "ABD-Çin Rekabeti Bağlamında Siber Savaş", **İnternational Journal of Academic Value Studies**, C.3, S.9, s.31

[213] Colonel Jayson M. Spade, **China's Cyber Power And America's National Security**, Pennsylvania: US Army War College, 2012, s.6

[214] Platov Vilidamir, "The USA and cyberwars", 2013, (Çevrimiçi), http://journal-neo.org/2013/10/15/rus-ssha-i-kibervojny-chast-1/, (Erişim tarihi 11.04.2020).

[215] Stephen Barr, "Anti-NATO Hackers Sabotage 3 Web Sites", 1999, (Çevrimiçi), https://www.washingtonpost.com/wp-srv/inatl/longterm/balkans/stories/hackers051299.htm, Erişim Tarihi: 11.04.2020

yerine bütün amaçlarıyla kullanılmak üzere geliştirilmiştir.[216] Edward Snowden olaylarında Çin'in siber saldırganları tarafından JSF'nin tasarımlarının çalındığı belgelenmiştir.[217] Askeri uçakların tasarım bilgilerinin çalınması gelecekte yaşanacak konvansiyonel bir savaş için çok büyük önem arz etmektedir. Askeri araçların kullanım etkisi ve diğer özelliklerinin düşman tarafından çalınması yaşanabilecek gerçek savaş içerisinde büyük bir yenilgiye sebebiyet verebilecektir.

Avusturyalı Şirketlere Siber Saldırı: 'Five Eyes' Beş Göz olarak, ABD, İngiltere, Yeni Zelanda, Avustralya ve Kanada devletleri tarafında oluşturulmuş istihbarat birimlerince tespit edilmiştir. Sydney Morning Herald tarafından siber saldırıların Çin devletinin eliyle gerçekleştirildiği iddia edilmiştir. Saldırılar yapılmadan önce Asya Pasifik İşbirliği toplantısında ABD başkan yardımcısı Çin devletine 'fikrî mülkiyet' hırsızlığı suçlamalarında bulunmuştur.[218] Söz konusu açıklamalar sonrası yapılan saldırıların tamamen siyasi çıkar amaçlı olduğu değerlendirilmektedir.

Siber uzayın kimliksiz yapısı siber alanda gerçekleştirilen saldırıların faillerinin tespitini zorlaştırmaktadır. Çin'in devlet eliyle çok sayıda siber saldırı gerçekleştirdiği iddia edilmektedir. Tahminler doğrultusunda 2020 yılında Çin'in gerçekleştirdiği ya da Çin'e karşı gerçekleştirildiği iddia edilen saldırılar şöyledir:[219]

Mart 2020: Çinli siber saldırganlar, medya, sağlık ve kâr amacı gütmeyen sektörlerde dünya çapında yetmiş beşten fazla imalat kuruluşunu hedef almıştır.

Mart 2020: Çin siber güvenlik firması Qihoo 360, Çin'in sanayi, bilimsel araştırma kuruluşlarına ve devlet kurumlarına karşı on bir yıllık bir hack kampanyasına katılmakla ABD'yi suçlamıştır,

Şubat 2020: Çinli siber gruplar uzak doğuda bulunan hükümetlerin projelerini çalmak için ilk olarak Malezya hükümetini hedef almıştır.

---

[216] Hasan Çiftci, **Siber Savaş…,** s.188

[217] Tim Brown, "Snowden Says China Stole F-35 JSF Secret Design Information, 2015", (Çevrimiçi) https://www.themanufacturer.com/articles/snowden-says-china-stole-f-35-jsf-secret-design-information/, Erişim Tarihi: 12.04.2020

[218] Saheli Roy Choudhury, "China Reportedly Steps Up Efforts To Steal Australian Company Secrets**", (Çevrimiçi)**https://www.cnbc.com/2018/11/21/cybersecurity-china-reportedly-increased-attacks-on-australian-firms.html, Erişim Tarihi: 13.04.2020

[219] CSIS, Significant Cyber Incidents, 2020, (Çevrimiçi) https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents, Erişim Tarihi: 14.04.2020

Ocak 2020: Mitsubishi şirketi, sekiz bin çalışanın verilerinin çalındığını, özel projelerinin bulunduğu bilgisayarlara saldırıldığını bildirmiştir. Söz konusu saldırıların Çinli hacker gruplarınca yapıldığını iddia etmektedir.

Siber uzay tek ulus devletinin sınırları içerisinde kullanılamamaktadır. Tek devlet tarafından domine edilmesi mümkün değildir. Realist yaklaşımda devletler anarşik sistem içerisinde güçlerini maksimize etmektedirler. Realizmin söz konusu argümanının izdüşümünü Çin'in siber uzayda gerçekleştirdiği saldırılar çerçevesinde değerlendirmek mümkündür. Zira yukarıda belirtilen saldırıların asıl amacının siyasi nitelikte olduğu ve bu olayları lehine çevirmek için yapıldığı anlaşılmaktadır.

Siber uzayda kontrolün ele geçirilmesi, başkaları tarafından siber ağlara bağlı cihazların kullanılması, devlete, şirkete ait olabilecek kritik bilgilerin çalınması siyasi, sosyal, ekonomik etkiler yaratmaktadır. Güvenlik açığının başlama nedeni siber uzaya bağlı otomasyon sistemlerinin birleşmesinden kaynaklanmaktadır. Günümüz mücadelelerinin ve savaşlarının otomasyon sistemlerinde saklanan verilerin çalınması ya da sistemlerin kilitlenmesine doğru yol aldığı görülmektedir. Çin'in gelişen teknoloji, ağlarının farklı bir boyuta taşıdığı küreselleşmeyi stratejik bir gerçeklik olarak algılayıp gelecekteki mücadelelerine soyut bir hale getirebilir. Önemle takip edilmesi gereken konu ise, Çin'in önümüzdeki dönemde ortaya koyacağı politikaları sayesinde siber alanın mağduru mu, saldırganı mı yoksa yönetişim anlamında normları takip eden bir paydaşı mı olacağı sorusu üzerinden düşünülebilecektir.

3.4 İsrail Devleti

14 Mayıs 1948 yılında kurulan İsrail Devleti, politikalarını devlet bekasının odağında şekillendirmekte ve siber politikalarını da ulusal güvenliğinin bir parçası olarak görmektedir. Güç kullanımını ulusal güvenliğine tehdit arz edebilecek konular kapsamında anlamlandıran İsrail[220], olası iç ve dış tehditler karşısında siyasi ve askeri olarak gücünü maksimize etmeyi hedeflemektedir. Hedefleri için öncelikle güvenlik politikalarını stratejik hedef olarak belirlemektedir. [221]

[220] Zafer Balpınar, "Askeri Güç Çarpanı Olarak Yahudi Yerleşim Yerleri," **Güvenlik Stratejileri Dergisi**, Y.10.S.20, (2014), s.87

[221] Abdallatif Yadak, "İsrail Güvenlik Politikası ve Güvenlik Duvarının Filistin Halkına Etkileri," **21. Yüzyılda Eğitim ve Toplum Eğitim Bilimleri ve Sosyal Araştırmalar Dergisi**, 2014, C.3, S.9, s.165

Devlet için güvenlik kavramının temelinde varoluşunu korumak ve ulusal niteliğini sürdürebilme kaygısı bulunmaktadır. Yapısında bütünlüğünü ve bağımsızlığını korumak isteyen devletler güvenlikte ihtiyaç hissettiklerini sağlamaya çalışmaktadır.[222] İsrail güçlü ve güvende olma durumu kapsamında agresif politikalar sergilemekten çekinmemektedir. İsrail'in güvenlik kaygıları sonucunda şekillenen güç inşa süreci ile birlikte politikalarının ilk sıralarında güvenliği önemli bir amaç olarak kullanmaktadır.[223] 1980'li yılların başında İsrail büyük bir ekonomik kriz yaşamıştır. Söz konusu kriz nedeniyle önemli üniversiteleri ile birlikte teknoloji ve bilim alanlarında gelişmeler sağlamak adına karar almıştır.[224] Güvenliği varoluş sebebi olarak gören İsrail Devleti'nin günümüzün teknolojik gelişmelerini yüksek oranda araştırmakta, performans seviyelerini, süreçlerini ve karmaşıklığını çözümleyebilmeyi hedefleri arasına koymaktadır.

3.4.1 İsrail Devleti'nin Siber Uzay Çalışmaları

İsrail'de Çin örneğinde olduğu gibi siber uzayın bileşenlerinde biri olan uzay üzerine yüksek teknolojili çalışmalar yapmaktadır. İsrail'in teknoloji ve bilimde diğer devletlere ayak uydurmakla kalmayıp uzayı ve siber uzayı domine etmeye çalışacağını düşünmek mümkündür. Zira İsrail'in ortaya koyduğu politikalar üzerinden hegemonyacı bir anlayışa sahip olduğu ifade edilebilmektedir.[225] ABD, Çin ve Rusya gibi dünyanın önemli ekonomik gücüne sahip devletlerden sonra Ay'a 'Beresheet' isimli uzay aracını gönderen dördüncü ülke unvanını kazanmıştır.[226] Uzayın kontrolünü sağlamak dünyanın bütününün yukarıdan gözetlenmesi şansını vermektedir.[227] Uzayda bulunan araçların kontrolü yüksek teknolojiye gereksinim duymaktadır. Teknolojide kullanılan araçlar ise siber uzayda ağlar ile birbirine bağlı bilgisayarlar sayesinde veri

---

[222] Beril Dedeoğlu, Uluslararası Güvenlik ve Strateji, **Derin Yayınları**, İstanbul:2003, s. 9
[223] Faruk Sönmezoğlu, Özgün Erler Bayır, **Dış Politika Karşılaştırmalı Bir Bakış…**, s.450
[224] Yasemin Hancıoğlu, Özlem Atay, "Türkiye, Güney Kore ve İsrail'in Ulusal İnovasyon Sistemlerinin Analizi ve Kıyaslanması," **Hacettepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**, C.36, S.2, s.33
[225] Umut Koldaş, "Azınlık İcinde Azınlık Olmak (mı?): İsrail Vatandaşı Filistinli/Arap Kadınların İsrail Anaakım Basınında Temsili", **Uluslararası İlişkiler**, C.14, S.56, 2017, s. 108
[226] Israil Global Blogs Network, "Beresheet"in Ardından – İsrailin İlk Uzay Aracı", 2019, (Çevrimiçi) https://itrade.gov.il/turkey/beresheetin-ardindan-israilin-ilk-uzay-araci/, Erişim Tarihi: 16.04.2020
[227] David E. LUPTON, **Space Warfare: A Space Power Doctrine**, Alabama: Air University Press, 1988, s.11

akışlarını sağlamaktadır. Dolayısıyla siber uzayda yapılacak olan çalışmalar sadece kendisinin bulunduğu sistemi değil, devletin bütün güvenliğine dair sistemi korumaya elverişli alanı oluşturmaktadır.

Merkeziyetçi bir yapıya sahip olan İsrail'in siber alana yönelik politikalarının oluşumu da halihazırda bu çerçevede şekillenme durumundadır. İsrail'in bu merkeziyetçi yapıda siber alanda savunmayı ilerletmeyi ve ulusal güç oluşturmayı, İsrail'in bu alanda öncülük üstlenmeyi ve bütün süreçleri ilk iki görevi destekler nitelikteki şekillendirerek üç temel stratejiyi teşvik etmektedir.[228] İsrail koruma amaçlı içine kapanık bir sistem ile internet ağı sistemlerine kendine özgü bir sistem içerisinde oluşum sağlamaktadır. Çalışmada incelemeleri yapılan devletlerin genelde 2000 sonrası dönemde, bilgi güvenliği, siber güvenlik üzerine hedef stratejilerini belirledikleri gözlemlenmiştir. İsrail'in ise 1997 yılında kurduğu şifreleme aracı halen güvenliğini korumaktadır. [229] Siber güvenlikle internet ağlarının korumaya çalışılması ile güvenliği korumaya yönelik yapılan çalışmaların asıl amacı kritik alt yapıları korumaya yönelik olmaktadır. Bu sayede ulusal güvenliği korumak amaçlanmaktadır. Zira ulusal güvenlik, devletin sahip olduğu gerek askeri gerekse bütün kaynaklara ait bütünü korumayı ifade etmektedir. İsrail'in siber güvenliği sağlamak için her yıl altı milyar dolar harcadığı belirtilmektedir. Söz konusu kaynağı siber saldırılarda kullanmak için kurmuş olduğu 'Birim 8200' ismini verdiği siber istihbarat ajanı oluşturmuştur[230]. Siber uzayı kontrol altında tutabilecek kontrol merkezlerinin işlevi kamu güvenliği açısından önem arz etmektedir.

3.4.2 İsrail Devleti'nin Siber Uzay Politikaları ve Ulusal Strateji Belgeleri

Ulusal güvenliğine büyük önem veren İsrail, siber güvenliğine de aynı şekilde önem vermektedir. Siber alanda daha çok istihbarat elde edebilmeye, yüksek teknoloji ile askeri birimler oluşturmaya çalışmaktadır. Siber güvenlik için iç politikası hariç 82

[228]Cyber Securıty Intellıgence, Israıl National Cyber Bureau (INCB), (Çevrimiçi) https://www.cybersecurityintelligence.com/israel-national-cyber-bureau-incb-2895.html, Erişim Tarihi: 17.04.2020

[229] Seda Yılmaz, Şeref Sağıroğlu, "**Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri**", …s.66

[230] Reed John, "Unit 8200: Israıl's Cyber Spy Agency", Fınancal Times, 2015, (Çevrimiçi) https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c, Erişim Tarihi: 17.04.2020

milyar dolar bütçe ayırmıştır.[231] Dış politikasında genel olarak ikili ilişkilere önem verdiği anlaşılmaktadır. 2017 yılında yapılmış olan yedinci siber güvenlik politikaları konferansında özellikle terör üzerine ABD-İsrail ikili ilişkiler doğrultusunda siber çalışma gruplarını oluşturacağını duyurmuştur.[232] Siber güvenliği geliştirmek için bütün girişimleri yaptığını, iki yüzden fazla şirketi ve çok sayıda ar-ge çalışmalarıyla ABD'den sonra Dünya'da siber güvenlik hizmetlerini ihraç eden ikinci ülke olduğunu iddia etmektedir. [233]

İsrail'in açık kaynaklarından yapılan taramalardan sonra anlaşıldığı üzere; siber güvenlik stratejilerinde belirsizlikler bulunmaktadır. Mevcut sistem içerisinde İsrail'in siber güvenliğini sağlamak üzere İsrail Savunma Kuvvetleri'ne bağlı olmak üzere dört kuruluşun varlığı bilinmektedir.[234] Söz konusu kuruluşlar: 'Birim 8200'; kamu güvenliğinde çalışmış ve emekli personellerden teşkil edilmiştir. Siber uzayda savunma sağlama, saldırı gerçekleştirme ve istihbarat toplama gibi görevlendirilmeler verilmiştir. Diğer taraftan İsrail'in Birim 8200'i oluşturmasındaki asıl amacının siber uzayda istihbarat ajanı oluşturmaya çalıştığı iddia edilmektedir.[235] İsrail, devlete ait gizli belgeler ve kritik alt yapılarını korumak için küresel internet haricinde kendine ait olan bir ağ oluşturmuştur. Kuruluşlarından ikincisi olan Shin Bet; bankacılık veri sistemlerini, hükümete ait gizli belgeleri ve ulusal altyapıyı korumak amacıyla kurulmuştur. Command, Control, Communications, Computers, Intelligence (Komuta, Kontrol, İletişim, Bilgisayar, İstihbarat); iletişim ve siber savunma yeteneklerini düzenlemektedir. İsrail Ulusal Siber Güvenlik Bürosu; politikası merkeziyetçi olan devletin siber alanda savunmayı ilerletmeyi ve ulusal güç oluşturmayı, İsrail'in öncülüğünü oluşturmayı ve bütün süreçleri ilk iki görevi destekler nitelikte ilerletme

[231] Gil Press, 6 Reasons Israel Became A Cybersecurity Powerhouse Leading The $82 Billion Industry, Forbes, 2018, (Çevrimiçi) https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/#57c4d0e8420a , Erişim Tarihi: 17.04.2020
[232] Cyber Week, Cyber Week 2017, 2017, (Çevrimiçi) https://cyberweek.tau.ac.il/2017/index.php, Erişim Tarihi: 18.04.2020
[233] Global İsrail Bloglar Ağı, "Siber Güvenlik Ulusu: İsrail Ağı Korumada Nasıl Dünya Lideri Oldu",
[234] James A. Lewis, Katrina Timlin,**Cybersecurity and Cyberwaefare Preliminary Assessment Of National Doctrine and Organization**, 2011, s.14
[235] Reed John, "Unit 8200: Israıl's Cyber Spy Agency", Fınancal Times, 2015, (Çevrimiçi) https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c, Erişim Tarihi: 17.04.2020

süreçleri olmak üzere üç temel stratejiye teşvik etmektedir.[236] İsrail'in, siber güvenlik duvarlarını oluştururken göze çarpan en önemli özelliği istihbarat üzerine yoğunlaşmasıdır. Siber güvenlik üzerine 2011 yılında bir, 2015 yılında iki ve 2015 yılına ait belgelere ek olmak üzere dört farklı belgede stratejilerini belirlemiştir. [237]

İsrail ulusal siber güvenlik yeteneklerinin geliştirilmesi başlığı altında 7 Ağustos 2011 yılında belge yayımlamıştır. Söz konusu belgeye göre; Ulusal Siber Güvenlik Bürosunun kurulması kararı alınmıştır. İsrail'in bu belge kapsamında belirlemiş olduğu stratejiler ise; siber alanda ulusal yeteneklerini geliştirmek için mevcut durumda ve gelecekte ön görülebilir tehdit ve zorlukları belirlemeyi önemli hedef olarak belirlemektedir. Siber saldırılara karşı alt yapılarını geliştirmeyi mümkün oldukça güçlendirmeyi amaçlamıştır. Diğer taraftan bilgi teknolojilerini geliştiren merkez olmayı benimsemektedir. Bunun için akademi, sanayi ve özel sektör arasında işbirliklerini teşvik etmektedir. Uluslararası alanda ise istihbarat alanı oluşturmayı, tarafları bir arada toplayarak paylaşım yapılması için siber güvenlik ile alakalı topluluğu önermektedir.

Siber güvenlikte ulusal düzenlemeleri sağlamak ve hükümetin siber güvenlik alanlarında çözümlemeler belirlemek üzere 15 Şubat 2015 tarihli belge yayımlanmıştır. 2011 tarihli belgesi esas alınmış ve burada siber tehditlerde Maliye Bakanlığı'nın görevlendirmeleri de belirlenmiştir. Söz konu görevlendirmede Maliye Bakanlığı ve Ulusal Siber Güvenlik Bürosu'nun ortaklaşa çalışmalar yapmasının gerekliliği belirtilmiştir. Türkiye'de bulunan siber güvenlik üzerine kuruluşlar için yardım ve teşvik uygulamalarını sağlamıştır. Siber tehditlere karşı oluşabilecek ekonomik krizlere karşı gerekli planlamaların yapılması gerekmektedir. Genel olarak siber güvenliğin gelişen teknoloji sonrası ulusal güvenlik ile eş değer olduğu vurgulanmaktadır. Devlete bağlı kurumlarda Bilgi Teknoloji Birimi ve Ulusal Siber Güvenlik birimleri oluşturmak üzere profesyonel yöneticiler ve personeller ile çalışmaların sağlanması

[236]Cyber Securıty Intellıgence, Israıl National Cyber Bureau (INCB), (Çevrimiçi) https://www.cybersecurityintelligence.com/israel-national-cyber-bureau-incb-2895.html, Erişim Tarihi: 17.04.2020

[237] CCDCOE, Strategy and Governance, (Çevrimiçi) https://ccdcoe.org/library/strategy-and-governance/, Erişim Tarihi: 20.04.2020

planlanmaktadır. 15 Şubat 2015 tarihli ikinci belgede, siber alanlarda savunma ve saldırı merkezlerinin güncelliğinin korunması gerektiği belirtilmektedir. Merkezlerin yönetimi Ulusal Siber Güvenlik Bürosu tarafından sağlanmaktadır. Hukuksal anlamda büronun başsavcılık makamı ile irtibatlı hareket etmeleri hakkında düzenleme yapılması gerektiği, gerekli yasal işlemleri gerçekleştirmesi özellikle vurgulanmıştır.

Ulusal Siber Güvenlik Büro'nun çalışmaları neticesinde 15 Şubat 2015 tarihli iki belgeye ek bir belge yayımlanmıştır[238]. Söz konusu belgede, siber alanın, kendi kapsamlarında benzeri olmayan çok sayıda tehdidi kapsadığı belirtilmiştir. Belirtilen tehditler banka hesaplarında bulunan paralar ile devlet sırlarında ve kritik alt yapıda bulunan bilgilerin çalınması şeklinde ifade edilmiştir. Eylemleri gerçekleştirenler ise bireyler, bilgisayar korsan grupları, organize suç örgütleri, terörist gruplar, sivil toplum kuruluşları, şirketler ve devlet olabilmektedir. Eylemlerin gerçekleşmesine neden olabilecek birçok farklı güdü hakkında: kişisel düşmanlık, ideolojik düşünce, ekonomik katkı sağlama amaçları olabileceği anlatılmaktadır. Siber uzayın sivil bir alan olduğu belirtilmiştir. Dolayısıyla dünyanın dört bir yanından gelebilecek tehditler anonim olabilmektedir. Bu nedenle savunma yapabilecek güvenlik gücünün olmaması saldırganın hedefine kolayca ulaşabilmesine olanak vermektedir. Siber saldırıların kişisel güvenlik, ekonomik güvenlik ve devletin güvenliği olmak üzere ulusal düzeyde ele alınması gerekliliği savunulmuştur.

İsrail'in açık kaynaklarda yayımlamış olduğu yukarıdaki belgeler göz önüne alındığında siber güvenliği ulusal güvenlik çerçevesinde yoğunlaştığı görülmektedir. Siber güvenlikde ulusal düzeyde mevzuat ve standardizasyonun geliştirilmesi ve ulusal siber güvenlik düzenlemesinin oluşturulmasında merkeziyetçi anlayış önemli rol oynamaktadır. Ulusal Siber Güvenlik Bürosu'nun düzenleyici organ olması ile birlikte sektörel düzenleyiciler, şirketler ve uzamanlar dünyadaki standart seviyeyi yakalamaya çalışmaktadır. Söz konusu çalışmaya 2010 yılından sonra özel sektör, üniversite ve kamu işbirliğinin siber güvenlik alanında sağlaması büyük önem arz etmektedir.[239] İsrail'in siber alanda iki hedefi bulunduğu gözlemlenmektedir. İlki savunma sağlamak

[238] CCDCOE, Strategy and Governance,…
[239] Ali Burak Darıcılı, Türkiye'nin Siber Güvenlik Politikalarının Analizi; Türkiye'nin Potansiyel Siber Güvenlik Stratejisi, TESAM Akademi Dergisi, C.6, S.2, Temmuz 2019, s.23

amacıyla kendisine ait internet ağı oluşturarak gelebilecek saldırılarda dışarı ile olan bağlantının kesilmesi ve böylelikle risklerin minimize edilebilmesidir. Diğeri de ulusal güvenliğin değişken olması nedeniyle devletin bakış açısı, hedefleri, araçları ve stratejileri ile savunma ihtiyaçlarının karşılanmasıdır.

3.4.3 İsrail Devleti'ne Karşı Düzenlenen Siber Saldırlar ve İsrail Devleti'nin Siber Saldırıları

İsrail'in güvenlik üzerine geliştirmekte olduğu stratejileri genelde jeopolitiğinin ana faktöründen kaynaklanmaktadır.[240] İsrail Ortadoğu coğrafyasında yaklaşık iki yüz yıllık Filistin devletine karşı teokratik düşünceleri ile sürekli saldırıda bulunmuştur. Gelecekte sadece kendi ulusuna ait ortak geleceğin vaatlerinde bulunarak halkını birbirine sımsıkı bağlamaktadır.[241] Yurttaşlık duygusunu oluşturarak dışarıdan gelebilecek olan tehditlere karşı ulusal kimlik üzerinden savunma sistemlerini geliştirmeye çalışmakta ve saldırılarını gerçekleştirmektedir.[242] Özellikle kimliği ile ön plana çıkan İsrail, siber alanda yine etnik yapısından ötürü saldırılara uğrayabilmektedir. Başka bir deyişle, İsrail'e karşı yapılan saldırılar ya da kendisinin düzenlendiği saldırıların temelinde ideolojik sebeplerin bulunduğu gözlemlenmektedir. Bu şartlar dahilinde İsrail'e karşı düzenlenmiş ve kendisinin gerçekleştirdiği siber saldırıların örnekleri aşağıda incelenmektedir.

Stuxnet: Siber güvenliğin önemini ve varabileceği noktaları kavramaya yarayacak olan örnek saldırılardan biridir. Saldırıdan en çok zarar gören başlıca ülke İran'da olmak üzere otuz binden fazla bilgisayara virüsün bulaştığı, en önemlisi ise İran nükleer santrallerini kontrol eden bilgisayarlarda stuxnet virüsüne rastlandığı tespit edilmiştir.[243] Kim ya da kimler tarafından yapıldığı halen tespit edilememiştir. Ancak, İsrail' de bulunan Negev Çölü'ndeki nükleer tesislerde siber saldırıların test edildiğine

[240] Lior Tabansky, Isaac Ben Israel, **Cybersecurity İn Israel**, London: Springer, 2015, s.10
[241] Çağla Gül Yasevi, İsrail İstihbaratı ve Mossad, Ed. Ümit Özdağ, **İstihbarat Örgütleri**, Ankara: Kripto Yayınları, 2014, s.217
[242] Erhan Keleşoğlu, **İsrail Yurttaşı Filistinliler Yurttaşlık, Kimlik, Siyaset**, İstanbul: İstanbul Bilgi Üniversitesi Yayınlar, 2014, s. 8
[243] Hasan ÇİFTCİ, **Siber Savaş…,** s.192

dair iddialar bulunmaktadır. İsrail, ABD, İngiltere ve Almanya'nın ortaklaşa gerçekleştirdikleri uzun zamandır iddia edilmektedir. [244]

Stuxnet'in önemli özellikleri; virüs olarak yerleştirilen bilgisayarların uzaktan kontrol edilebilmesidir. Herkes tarafından kullanılan internet ağları üzerinden çalışması mümkün görünmemektedir. USB olarak tabir edilen bilgisayarlara aracı olarak bilgi aktarılması gereken cihazlar ile virüs yerleştirilmektedir.[245] Bilgisayarın arkasında hayalet isimleri ortadan kaldırmaktadır. Failinin virüsün yayılmasını isteyen kişilere yardımcı olan biri/birileri tarafından yerleştirildiği değerlendirilmektedir. Diğer taraftan özellikle nükleer santrallere yerleştirilmesi ile Hollandalı bilim adamlarınca çalışma evreleri tespit edilmiştir. Bulaştığı bilgisayarların kontrolünde bulunan endüstriyel motorlara aylarca kısa aralıklarla değişimler sağlamaktadır. Motor hızının düşük ya da değişik seviyelerde seyir etmesi nükleer üretiminin normal çalışmasını sabote etmektedir.[246] Stuxnet saldırıların ortak bir saldırı olması ile birlikte Negev Çölü'nde (Birim 8200'ün bulunduğu alan) benzer kopyalama işlemi yaptığını inkâr etmemesi, bilgisayarlarında oluşturdukları kanıtların tespit edilememesi nedeniyle oluşturan kişinin İsrail'de olabileceği iddia edilmiştir.[247]

Orchard Operasyonu: Suriye topraklarında nükleer silah üretimi yapıldığına dair oluşan şüpheli durumlar neticesinde, İsrail Suriye' de bulunan bir takım tesisi İHA'lar ile yok etmiştir. Söz konusu saldırıda İsrail, İHA'yı kullandığı teknoloji sayesinde görünmez hale getirmiştir.[248] Askeri teknoloji üreticileri İsrail'in geliştirdiği bu olayın savaş stratejisi olmasından ziyade elektronik bir savaş olayı olduğunu vurgulamaktadırlar. Bu varsayım neticesinde; İsrail'in Birim 8200 tarafından Suriye'ye ait radar sistemlerine giriş yaparak operasyonun gerçekleştiği sırada radarı kör hale

---

[244] The New York Times, "Israeli Test on Worm Called Crucial in Iran Nuclear Delay", 2011, (Çevrimiçi) https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html, Erişim Tarihi: 22.04.2020

[245] James P. Farwell, Rafal Rohozinski, "Stuxnet and The Future of Cyber War", **Survival**, C.53, S.1, 2011, s.24.

[246]Braodcom, "Stuxnet: A Breakthrough", 2010, (Çevrimiçi) https://community.broadcom.com/symantecenterprise/communities, Erişim Tarihi: 22.04.2020

[247] The Guardian, "Stuxnet Worm İs The 'Work Of A National Government Agency", 2010, (Çevrimiçi) https://www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency, Erişim Tarihi: 22.04.2020

[248]The New York Times, "A Silent Attack, but Not a Subtle One", 2010, (Çevrimiçi) https://www.nytimes.com/2010/09/27/technology/27virus.html?_r=1, Erişim Tarihi: 22.04.2020

getirdikleri iddia edilmektedir[249]. Zira yukarıda da incelemesi yapılmış olması nedeniyle Birim 8200 İsrail'in sinyalleri çözen ve karmaşık hale getirebilen personellerden oluşmaktadır.

Cast Lead Harakatı: İsrail kara kuvvetleri ile birlikte 27 Aralık 2008 tarihinde 22 günlük sürecek Gazze'ye karşı bir saldırı başlatmıştır.[250] İsrail'in bu saldırısı üzerine Filistinli siber gruplar gerek kamuoyu oluşturmak gerekse yapılan operasyonun haksızlığını belirtmek üzere siber saldırılar başlatarak on binin üzerinde internet sitesine İsrail aleyhinde ilanlar yerleştirmişlerdir.[251] Söz konusu saldırılara karşılık İsrail Devleti kendisi ile birlikte gönüllü siber gruplar oluşturarak karşılık vermiştir. [252]

Mavi Marmara Olayı: İsrail'in Cast Lead operasyonu sonrası Filistin halkına çok sayıda kayıplar yaşatmıştır. Türkiye, insani yardım kuruluşları aracılığıyla Filistin halkına deniz yolu üzerinden yardım ulaştırmaya çalışmıştır. Ancak İsrail askerleri tarafından yardım gemisine saldırı yapılmış ve çok sayıda sivilin ölümüne neden olmuştur. [253] Bu nedenle Türk siber gruplarınca Tel Aviv Belediyesi'nin resmî web sitesi başta olmak üzere İsrail Kamu Güvenlik Bakanlığı'na siber saldırılar gerçekleştirerek, İsrail Devleti üç milyon dolar zarara uğratılmıştır. [254]

İsrail hakkında dikkat çekici noktalar arasında ulusalcı, merkezi yapı sistemi, maksimize edilmiş güç, saldırgan, yüksek derece güvenlikli bir yapıya sahip olduğu bulunmaktadır. Güvenlik hakkında bu kadar etkin alan oluşturmaya çalışan sistem hayatın ayrılmaz parçası haline gelen siber güvenlik için faaliyetlerini sürekli yerine getirmektedir. İsrail'in güvenlik için istihbarat ve bileşenlerine önem verdiği gözlemlenmektedir. Diğer taraftan İsrail, güvenliğine karşı gelebilecek tehditlerde, diğer

[249]IEEE Spectrum, "The Hunt for the Kill Switch", 2008, (Çevrimiçi) https://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch, Erişim Tarihi: 22.04.2020
[250] Israel Defense Forces, "Operation Cast Lead", 2008, (Çevrimiçi) https://www.idf.il/en/minisites/wars-and-operations/operation-cast-lead-2008-09/, Erişim Tarihi: 22.04.2020
[251] Jeffery Carr, **Cyber Watfare**, USA: O'Reılly, 2012, s.19
[252] Hasan Çiftci, Siber Savaş…, s.187
[253] Time Turk, "5 Yıl Önce Mavi Marmara'da Ne Oldu?", 2015, (Çevrimiçi) https://www.timeturk.com/5-yil-once-mavi-marmara-da-ne-oldu/haber-108512, Erişim Tarihi: 23.04.2020
[254]Milliyet, Türk Hackerlardan Mavi Marmara İntikamı, 2014, (Çevrimiçi) https://www.milliyet.com.tr/yerel-haberler/istanbul/turk-hackerlardan-mavi-marmara-intikami-10368356, Erişim Tarihi: 23.04.2020

devletlerin istihbarat birimleri ile iletişime geçmektedir.[255] Siber güvenlik için itici gücü her zaman hazırlamaya çalışmaktadır. Zira, İsrail'in banka sistemleri, su, elektrik şebekeleri, trafik bilgisi, ulaşımı bilgisayarlar üzerinden siber alana bağlanmaktadır. [256] İsrail, kurmuş olduğu birimler ile milli müdahale sistemi oluşturmaktadır. Söz konusu sitem Savunma Bakanlığına bağlı olarak yürütülmektedir.

3.5 Türkiye'nin Siber Uzaya Yönelik Çalışmaları ve Stratejileri

Artan internet kullanımı, teknolojiye olan bağımlılık, siber alanın verdiği iletişim, bilgi saklama kolaylığı ve ekonomik faaliyetler; devletler, bireyler ve toplumlar tarafından siber uzayın son derece yoğun bir şekilde, hayatın hemen hemen her alanında kullanıldığına işaret etmektedir. Dijital ortamlarda yaşanan ekonomik, toplumsal ve askeri dönüşümler, dijital kaynaklarda meydana gelen ve gelmesi muhtemel tehditlerin klasik kaynaklara kıyasla ne denli farklılık arz ettiğini sergilemektedir.[257] Dolayısıyla devletler açısından önemli bir güç unsuru teşkil eden siber gücün oluşturulabilmesi için siber uzayın faaliyet alanlarının ve bu alanlara ilişkin güncel gelişmelerin göz önünde bulundurulması gerekmektedir. Siber gücün kazanımı ve devamlılığı konusunda dikkat edilecek başlıca hususlar arasında; internet kullanımının gözden geçirilmesi, teknolojinin geliştirilmesi, jeopolitik uzaya hâkim olunması, bilgilerin saklandığı belleklerin korunaklı ve güvenli hale getirilmesi ve bellekleri birbirine bağlayan ağların güvenliğinin sağlanması yer almaktadır.

İnternet kullanımı hakkında bazı tespitler yapılmıştır. Türkiye'de 2019 yılında 3,48 Milyon internet kullanıcısı ile %49 oranında iken, 2020 yılında ise internet kullanıcısı 4,4 milyon kullanıcı olarak %54'e kullanıcıya yükselmiştir. [258] İnternet kullanımı ve iletişim uzayda bulunan uydular sayesinde gerçekleşmektedir. Türkiye'nin uzay üzerine yaptığı çalışmalar değişik tarihlerde gelişmeler göstermiştir. 1979 yılında ilk uydu

---

[255] Çağla Gül Yesevi, İsrail ve ABD'nin Askeri ve İstihbari İttifakının Değerlendirilmesi ve Pollard Olayı, 2015, (Çevrimiçi) https://21yyte.org/tr/merkezler/israil-ve-abdnin-askeri-ve-istihbari-ittifakinin-degerlendirilmesi-ve-pollard-olayi, Erişim Tarihi: 24.04.2020

[256] NTV, "İsrail Siber Savaşa Hazırlanıyor", 2011, (Çevrimiçi) https://www.ntv.com.tr/turkiye/israil-siber-savasa-hazirlaniyor,ja4MNACLtE2_vKAMwGW4GQ, Erişim Tarihi: 24.04.2020

[257] P.W Singer, Allan Friedman, **Siber Güvenlik ve Siber Savaş**, Çev. Ali Atav,Ankara: Buzdağı, 2018, s. 29

[258]Slideshare, Dijital 2020 Turkey (January 2020), 2020, (Çevrimiçi) https://www.slideshare.net/DataReportal/digital-2020-turkey-january-2020-v01?from_action=save, Erişim Tarihi: 24.04.2020

istasyonu kurulmuş, 1980'li ve 1990'lı yıllarda Türksat uyduları TÜBİTAK tarafından uzaya gönderilmiştir[259]. 13 Temmuz 2009 yılında gönderilen Göktürk-1 uydu aracı ile dünyanın herhangi bir coğrafyasında gerek askeri, gerekse sivil istihbarat sağlamak amacıyla çok yüksek çözünürlükte görüntülerin elde edilebilmesi sağlanmaktadır.[260] 2012 Göktürk-2, 2019 yılında ise Göktürk-3 uyduları uzay yörüngesine gönderilmiştir. Genel olarak yüksek çözünürlük ile yer küreden görüntü alınması amaçlanmakta, Millî Savunma Bakanlığı'na bağlı birimlerce kullanılmaktadır.[261] Haberleşme uydusu olarak ise Tüksat 6A uydusu bulunmaktadır. [262] Uzay yörüngesinde askeri olarak kullanılan yüksek teknolojiler aynı zamanda sivil alanlarda GPRS, internet, iletişim gibi alanlarda da kullanılmaktadır. Söz konusu kullanımlar, toplumun refahı ve yaşam kalitesini geliştirmede önem arz etmektedir.[263]

Siber uzay ve güvenlik alanında yaşanan gelişmeler savaşların ve araçların doğasında da çeşitli dönüşümlere yol açmakta, yüksek teknoloji üretimi akıllı silahlar ve siber uzayın güdümünde kullanılabilen silahlar öne çıkmaktadır. Söz konusu hareketlenmelerde riskleri minimize etmek için ortak aklın sunacağı tek fikir bulunmaktadır. Yerli üretime önem vermek ve yerli yazılımları teşvik etmek gerekmektedir. 1963 yılında TÜBİTAK'ın kurulması ile birlikte bilimsel çalışmaların teşviki açısından önemli bir adım atılmış[264], teknolojinin gelişmesi 1990'lı yıllarda hız kazanarak devam ederken[265], 2000'li yıllarda bilim ve teknolojide yeni stratejiler belirlemek üzere "Vizyon 2023: Bilim ve Teknoloji Stratejileri" temelinde amaç ve hedef portföyü belirlenmiştir. [266]

---

[259] Gökbilim, Türkiye'nin Uzay Çalışmaları, 2020, (Çevrimiçi) https://gokbilimi.net/turkiyenin-uzay-calismalari/, Erişim Tarihi: 25.04.2020

[260] Türk Havacılık Uzay Sanayi, Uzay Göktürk-1, 2009, (Çevrimiçi) https://www.tai.com.tr/urun/gokturk-1, Erişim Tarihi: 25.04.2020

[261] Türk Havacılık Uzay Sanayi, Uzay Göktürk-2, 2012, (Çevrimiçi), https://www.tusas.com/urun/gokturk-2 Erişim Tarihi: 25.04.2020

[262] Türk Havacılık Uzay Sanayi, Uzay Ürünleri, 2020, (Çevrimiçi), https://www.tusas.com/urunler/uzay, Erişim Tarihi: 25.04.2020

[263] Sait Yılmaz, **Uzay Güvenliği**, İstanbul: Milenyum Yayınları, 2013, s. 253

[264] Erhan Aslanoğlu, "Ulusal Yenilenme Sistemleri Çerçevesinde Türkiye' de Teknoloji Politikaları," **Mülkiye Dergisi**, C.25, s. 230, s.53

[265] Erhan Aslanoğlu, a.g.m, s.70

[266] Cem Saatçioğlu, "Ulusal Yenilik Sistemi Çerçevesinde Uygulanan Bilim ve Teknoloji Politikaları: İsrail, AB ve Türkiye Örneği," Sosyal Bilimler Dergisi, S. 1, 2005, s.195

3.5.1 Türkiye'nin Siber Güvenlik Stratejisi ve Siber Güç Kapsamında Çalışmaları

Siber uzay güvenliğinde alt yapı çalışmaları devam eden Türkiye'de, politikaların şekillenmesiyle birlikte askeri, sivil ve hukuk alanlarında siber uzaya yönelik zeminin hazırlanabilmesi için hazırlıklara başlanmıştır. Siber güvenlikte ilk müdahale stratejisi olarak 2009 yılında Bilgi Teknolojileri ve İletişim Kurumu (BTK) tarafından "Ulusal Sanal Ortam Güvenlik Politikası" isimli belge yayınlanmıştır[267]. Söz konusu raporda, siber alandan gelen tehditlere karşı stratejilerin belirlenmesi, herhangi bir saldırı gerçekleşmesi sonrası öncelikle faillerinin tespit edilmesi ve bu şahıslara karşı yasal işlemlerin en hızlı şekilde gerçekleştirilmesi için hukuksal zeminin oluşturulması, bütün bu alanlarda başarılı olunabilmesi için öncelikle kolluk güçlerinin gereksinimlerini sağlayacak personelin ve yargıda konuya hâkim yetkililerin bulunması konusundaki planlamanın gerekliliği vurgulanmıştır. [268]

Siber güvenliğin gerek politikasının belirlenmesi, gerekse yasal zemininin oluşturulmasına yönelik olarak 20 Ekim 2012'de 28447 no ile Resmî Gazetede yayınlanan kararda siber güvenlik çalışmalarının yürütülmesi, koordinasyonu ve yönetilmesi ifade edilmiştir. Söz konusu kararlar kapsamında Ulaştırma, Denizcilik ve Haberleşme Bakanlığına bağlı olarak BTK aracığıyla Ulusal Siber Güvenlik birimi kapsamında siber güvenlik stratejilerinin oluşturulacağı belirlenmiştir. Söz konusu karara göre; Siber Güvenlik Kurulunun görev ve yetkileri: [269]

- Siber güvenliği sağlamak adına stratejileri, politikaları ve harekât planlamalarını hazırlamak,
- Kamuya ait bilgi alt yapılarının korunmasını ve güvenliğine esas ve usulleri oluşturmak,

---

[267] Salih Bıçakcı, Doruk Ergün, Mitat Çelikpala, Türkiye' de Siber Güvenlik ve Nükleer Enerji, Edam, s.36 (Çevrimiçi) https://edam.org.tr/document/CyberNuclear/SiberKitapTR/edam_siber_guvenlik_b2.pdf, Erişim Tarihi: 30.04.2020

[268] Ünal Tatar, **Siber Savaş ve Sanal Ortam Güvenlik Politikası**, Ankara: Tubitak, 2009

[269] Resmi Gazete, Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar, 2012, (Çevrimiçi) https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf, Erişim Tarihi: 30.04.2020

- Bilgi teknolojileri ve iletişime dair alt yapıların sistemlerini kontrol altında tutmak,
- Milli çözümlere önem vermek ve siber risklerin savunma sistemini milli üretim üzerinden sağlamak,
- Siber güvenliği sağlarken uzman personeli temin etmek,
- Siber güvenliğin bilinçlendirilmesi için eğitim alanlarında gerekli koordinasyonu sağlamak,
- Bilgi güvenliğini önemsemek ve özellikle bilgi üretiminde çalışanlara gerekli eğitimi vererek siber güvenliklilerini sağlamak.

Siber uzay üzerine Türkiye' de gerekli politikaların belirlenmesi konusunda ulusal siber güvenlik organizasyonu şu şekilde şekillenmiştir; Ulaştırma ve Altyapı Bakanlığı'na bağlı olmak üzere Siber Güvenlik Kurulu, Haberleşme Genel Müdürlüğü, Ulusal Siber Olaylara Müdahale Merkezi (BTK-USOM), Kurumsal Siber Olaylara Müdahale Ekibi (SOME), Sektörel SOME olmak üzere siber güvenliği sağlayacak olan kurum ve kuruluşlar belirlenmiştir.[270] 2013 – 2014 yılı için Siber Güvenlik Eylem Planlama belgesi yayımlanmıştır.[271] Söz konusu belgeye göre; siber güvenliğin risklerinin tanımlaması yapılmış, ilkesel stratejiler belirlenmiştir. Eylem planlaması kapsamında; siber güvenliğin yasal alanda düzenlemelerini gerçekleştirmek, yargılanma sürecinde sisteme yardım edecek çalışmaların oluşturulması, ulusal siber güvenlik altyapılarının güçlenmeleri üzerine çalışmalar yapılması, milli teknolojiler ve yerel yazılımlar ile insan kaynağının yine Türkiye içerisinden oluşturulması, siber güvenliğin sağlanması için oluşturulan mekanizmaların güçlü hale getirilmesi hedeflenmiştir. Söz konusu belge siber güvenliğe dair ilk eylem planlaması olarak görülmektedir.

2016-2019 Ulusal Siber Güvenlik Stratejisi'nde siber suçlarla mücadele etmenin farkındalığı üzerinde durulmuş, siber alana ait savunmaların güçlendirilmesinin ve kritik altyapıların güvenliği vurgulanmıştır.[272] Söz konusu belgeye göre, 2012 yılında resmî

[270] T.C Ulaştırma ve Altyapı Bakanlığı, Siber Güvenlik, 2020, (Çevrimiçi) https://www.uab.gov.tr/siber-guvenlik, Erişim Tarihi: 01.05.2020
[271] BTK, Eylem Planlaması, 2013, (Çevrimiçi) https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf, Erişim Tarihi: 01.05.2020
[272] T.C Ulaştırma ve Altyapı Bakanlığı, Siber Güvenlik, 2020, (Çevrimiçi) https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf
Erişim Tarihi: 01.05.2020

gazetede yayımlanan kanunun çerçevesi genel hatları ile çizilmiş, eylem stratejisi beş ana başlık içerisinde özetlemiştir:

Siber Güvenliğin Güçlendirilmesi ve Kritik Altyapıların Korunması: Öncelikle devletin ve ulusal ekonominin varlığını oluşturan kritik altyapıları korumanın önemi vurgulanmıştır. Siber alanın risklerinden bahsedilmiş, toplumu etkileyecek eylemlere engel olunması planlanmıştır.

Siber Suçlarla Mücadele: Özellikle ekonomik olarak etkisi olan siber saldırıların önlenmesi hedeflenmiştir.

Farkındalık Oluşturma: Siber uzaya dahil olan ve bileşenlerinden birisi olan bireylerde eğitim ve konferanslar ile farkındalığın oluşturulması amaçlanmıştır.

Siber Güvenlik İşbirliğinin Geliştirilmesi: Özel şirketler, Sivil Toplum Kuruluşları (STK), kamu kuruluşları ve diğer paydaşlarının işbirliği içerisinde teknoloji ve mevzuat gereksinimlerinin oluşturulması ön plana çıkartılmıştır.

Milli Güvenlik Kapsamında Siber Güvenlik: Devletin varlığını ve bütünlüğünü, ulusal ekonominin istikrarını, kritik altyapıların mevcut durumunu ve toplumu etkileyen siber tehditlerin verebileceği zararları minimize etmeye yönelik planlamalar yapılmıştır.

Diğer devletlerin siber güvenlik üzerine gerçekleştirmeye çalıştığı politikalar ile Türkiye'nin hedef stratejilerinde bazı benzerlikler olduğu görülmektedir. Türkiye, siber güç unsurlarını politik anlamda şekillendirmekte ve geliştirmeye çalışmaktadır. Türkiye'nin bu alandaki yapılanması üst birimlerden alta doğru ilerlemektedir. Farklı bir ifadeyle siber uzay güvenliği üst birimlerden alt birimlere doğru geniş bir yelpaze gücüyle sağlanmaktadır. Dolayısıyla gerek kamu görevlisi anlamında gerekse özel şirketler kapsamında yetiştirilmiş personel ihtiyacının oluşacağını söylemek mümkündür. Siber uzayın karmaşık ve anonim yapısını çözebilecek kişilere ihtiyaç duyulmaktadır. Ayrıca devletler analitik zekâsı ile belirli yazılımların içeriğinde bulunan açıkları tespit etmektedir.[273] Bu nedenle personel atılımları siber güç sağlamada önemli adımlar oluşturabilmektedir. Son dönemde Türkiye'nin bu yönde sürdürdüğü çalışmalar kapsamında Hazine ve Maliye Bakanlığınca hazırlanan '1 Milyon Yazılımcı

[273] Vahap Eren, Siber Güvenlik Alanında Gelecek Hedeflerimiz, S.1, **Siber Güvenlik Dergisi**, 2017, s.32

Projesi' kapsamında herhangi bir şart aranmadan gençlerden oluşan bir grup oluşturulması planlanmıştır. [274]

Siber güvenlik ulusal güvenlik açısından önemli kriterler taşımaktadır. Uluslararası alanda stratejik hedeflere güç, ekonomi dengelerinde oyun değiştirici rollere sahip olma özelliğini katabilmektedir. Siber uzayın bu anlamdaki güç ve ekonomik faydaları kapsamında ele alınması gerekmektedir. Bu nedenle Türkiye'nin öncelikle teknoloji alanında gelişme sağlaması ve siber güvenlik yönetişimi oluşturması elzem görülmektedir. Zira ABD'de siber silahların kullanımı yoğun bir şekilde gerçekleşirken, İsrail'de başbakanlığa bağlı olarak 'Siber Güvenlik Bürosu' oluşturulmuştur. Diğer taraftan siber uzayı domine etmeye çalışan devletlerde göze çarpan önemli özellikler STK, akademisyenler ve özel şirketler ile yapılan çalışmalar kapsamında düzenlenmektedir. Türkiye' de özel üniversiteler hariç bu konuda herhangi bir atılım yaptığı görülmemektedir.

3.5.2 Türkiye'ye Karşı Düzenlenen Saldırılar ve Türkiye'nin Siber Uzay Operasyonları

Siber saldırıların etkileri zaman zaman değişim göstermektedir. Sebebiyet verdiği zararları maddi tarafların en önemli ölçütü olarak kabul edilmektedir. Diğer taraftan devletlere, şirketlere ve bireylere ait kritik bilgiler dijital olarak siber uzay içeriğinde saklanmaktadır. Devletler tarafından siber operasyonlar, siber uzaya ait uluslararası normların bulunmaması nedeniyle gizlilik içerisinde yürütülmektedir. Özel şirketler, diğer şirketlere ait kritik bilgileri çalmak için saldırı gerçekleştirirken, bireyler de sahip oldukları teknik bilgiler kapsamında devletlere, şirketlere, bireylere kadar farklı düzeydeki aktörlere saldırılar düzenleyebilmektedirler. Joseph Nye, söz konusu saldırıları, siber savaş ve ekonomik casusluk alanlarını devletler ile ilişkilendirirken, siber suç ve siber terörizm eylemlerini devlet dışı aktörler ile ilişkilendirmektedir. [275] İnternete bağlı olarak kullanımda olan bilgisayarların her daim tehdit altında olabileceği

[274] T.C. Hazine ve Maliye Bakanlığı, 1 Milyon İstihdam Kullanıcı Klavuzu, 2020 (Çevrimiçi) https://1milyonistihdam.hmb.gov.tr/kilavuz/kilavuzKullanici.pdf, Erişim Tarihi: 01.05.2020

[275] Joseph S Nye, "Nuclear Lessons for Cyber Security?" **Strategic Studies Quarterly** C.5, S.4, 2011, s.20

görülmektedir. Türkiye'ye karşı düzenlenmiş ya da Türkiye'nin düzenlediği iddia edilen siber saldırılardan örnekler aşağıda anlatılmaktadır.

Devlet Kurumlarının Web Sitelerine Saldırı: 'Anonymous' hacker gruplarınca[276] 2015 yılında Türkiye'deki kamuya ait internet sitelerine uzun süreli siber saldırılar düzenlenmiştir. [277] Siber saldırılar Türkiye'yi uzun süreli olarak etki altında tutmuştur ve uluslararası literatüre geçecek şekilde tanımlanmıştır[278]. 'Tr' uzantılı internet saldırılarının düzenlenmesinin nedeni olarak 25 Kasım 2015 tarihinde sınırlarımızı ihlal eden uçağın Türk Hava Kuvvetleri tarafından düşürülmesi iddia edilmiştir. [279] Bu bağlamda saldırıların kaynağı olarak RF'nin değerlendirilmesi mümkün görülmektedir.

HummingBad Virüsü: Cep telefonlarının yazılım programı olan Androidlerin içeriğinde 2016 yılında Hummingbad isimli virüse rastlanmıştır. Söz konusu virüs on milyon telefon kullanıcısına bulaşmıştır. Yaklaşık olarak zararın üç yüz bin dolar olduğu tespit edilmiştir. 2016 yılında Türkiye' de de görülmüştür[280]. HummingBad Virüsü nün tespiti Check Point isimli siber güvenlik firması tarafından yapılmıştır. Çinli siber saldırganlar tarafından oluşturulan virüsle birlikte telefonlardaki kişisel veriler ele geçirilmiş ve banka şifreleri çalınmıştır[281].

Gümrük Sitemlerine Saldırı: Gümrük Müsteşarlığı'nda bulunan Bilişim Sistemlerine karşı saldırılar düzenlenmiştir. Gümrük işlemlerinin 19 saat boyunca gerçekleşememesi nedeniyle bir milyar dolar zarar oluşmuştur[282]. Siber olayların

---

[276] Devlet ya da büyük şirketlerin arkasında durduğu gruplar olarak bilinmektedir. Daha fazla bilgi için bakınız: (Çevrimiçi) https://onedio.com/haber/cagin-en-guclu-silahi-onlar-dunyanin-en-etkili-hacker-gruplariyla-tanisin-869341, Erişim Tarihi: 02.05.2020

[277] Sabah, "Kamuya Siber Saldırı", 2015, (Çevrimiçi) https://www.sabah.com.tr/ekonomi/2015/12/25/kamuya-siber-saldiri, ErişimTarihi: 02.05.2020

[278] Webrazzi, "Türkiye Siber Saldırılar Altında: Bilmeniz Gerekenler", 2015, (Çevrimiçi) https://webrazzi.com/2015/12/25/turkiye-siber-saldiri-altinda-bilmeniz-gerekenler/, Erişim Tarihi: 02.05.2020

[279] DW, "Türkiye'ye Siber Saldırı", 2015, (Çevrimiçi) https://www.dw.com/tr/t%C3%BCrkiyeye-siber-sald%C4%B1r%C4%B1/a-18942536, Erişim Tarihi: 02.05.2020

[280] Shiftdelete.net, Zararlı Android Uygulamalarının Listesi, 2017, (Çevrimiçi) https://shiftdelete.net/zararli-android-uygulamalarinin-listesi-78856, Erişim Tarihi: 02.05.2020

[281] The Guardina, HummingBad Android malware: who did it, why, and is your device infected?, 2017, (Çevrimiçi) https://www.theguardian.com/technology/2016/jul/06/what-is-hummingbad-malware-android-devices-checkpoint, Erişim Tarihi: 02.05.2020

[282] Hürriyet, "Gümrükte Sistem Çöktü Bir Milyar Dolar Zarar Oluştu", 2011, (Çevrimiçi) https://www.hurriyet.com.tr/ekonomi/gumrukte-sistem-coktu-1-milyar-dolarlik-ticaret-durdu-16920642, Erişim Tarihi: 03.05.2020

ekonomi ile birebir bağlantısı örneklenmiştir. Bu kapsamda çok cüzi rakamlar ile oluşturulabilen bilgisayar virüsü, milyarlar değerinde zarar verdirebilmektedir.

Türkiye'ye karşı RF ve Almanya'nın özel şirketleri tarafından siber saldırılar gerçekleştirildiği yukarıda anlatılmıştır. Türkiye'ye karşı yapılan saldırıların genel olarak kamu kurumlarına ve ekonominin işlev aldığı noktalara yönelik olması siber savunmada uzman personele ihtiyaç bulunduğunu göstermektedir. Yakın gelecekte dünyada siber uzayın askeri alanlar haline gelebileceği değerlendirilmektedir. Dolayısıyla özellikle Türk Silahlı Kuvvetleri'nin bu yönde çalışmaları olması gerekmektedir. Türkiye'de siber uzay konusunda farkındalığın arttığı ve yürütmenin sürekli güncelleme içerisinde bulunduğu yukarıda incelenmiştir. Ayrıca siber güvenlik milli güvenlik ile eş değer tutulmaktadır [283].

Siber alandan gelecek olan saldırının zamanını belirlemek çok zordur. Bu duruma bağlı olarak siber saldırılara karşı profesyonelce ve hızlı karşılık verilmesi gerekmektedir. Cumhurbaşkanlığı tarafından yapılan çalışmalarda tek çatı altında siber savunma sistemlerinin oluşturulması hedeflenmiştir.[284] Yukarıda Haberleşme ve Altyapı Bakanlığı'nın alt birimlerinde olan siber savunma kadrolarının tek çatı altında toplanarak yapacakları çalışmalar ise; siber güvenliğe dair altyapıların oluşturulması, risk durum analizlerinin belirlenmesi, tedbirler hakkında stratejileri amaçlanmaktadır. Diğer taraftan istihbarat birimlerinde özel olarak elektronik daire başkanlıkları kurulduğu görülmektedir. [285] Son dönemlerde ise 'Türkiye Siber Güvenlik Kümelenmesi' kurulmuştur. Cumhurbaşkanlığı seviyesinde olan söz konusu kuruluş, Savunma Sanayii Başkanlığı önderliğinde kamu, özel şirket ve akademik temsilcilerden oluşturularak Türkiye'de siber güvenliğin geliştirilmesi amacıyla kurulmuştur. [286]

---

[283] Haberler, "8. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı", 2015, (Çevrimiçi) https://www.haberler.com/8-uluslararasi-bilgi-guvenligi-ve-kriptoloji-7829357-haberi/, Erişim Tarihi: 04.05

[284] STM, "**2017 Ocak-Mart Dönemi Türkiye Siber Tehdit Durum Raporu**", İstanbul, 2017, s.15

[285] Mit, "Organızatıonal Chart Of The National Intelligence Organization,", 2020, (Çevrimiçi) https://www.mit.gov.tr/eng/teskilat.html#, Erişim Tarihi: 04.05.2020

[286] Türkiye Siber Güvenlik Kümelenmesi, Siber Güvenlik Kümelenmenin Kurulma Amacı, 2020, (Çevrimiçi) https://www.siberkume.org.tr/Index#close, Erişim Tarihi: 04.05.2020

SONUÇ

Uluslararası ilişkiler disiplininde güç ve güvenlik önemli yer kapsamaktadır. Gelinen nokta itibariyle güvenlik, konvansiyonel araçların ve klasik yapının ötesine geçerek yenilikçi ve yüksek teknolojiler çerçevesinde çok yönlü bir hal almaktadır. Özellikle de siber uzayda yaşanan teknolojik gelişmelerin yansıması olarak konular çeşitlenmekte, devlet düzeyinden birey düzeyine uzanan bir düzlemde çok farklı aktörler güvenlik tehdidi arz edebilecek kapasiteye ulaşmaktadırlar. Dijital dünyadan gittikçe artan bir ivmeyle yöneltilen tehditler, bilinmeyen zamanda ve anonim saldırganlar tarafından gerçekleştirilmektedir. Artan belirsizliklere ve küreselleşme çerçevesinde güçlenen karşılıklı bağımlılığa paralel şekilde kırılganlıklar da yükseliş göstermekte ve bu durum devletleri güvenliklerini temin etmek üzere farklı çerçevede düşünmeye, planlar oluşturmaya ve stratejiler geliştirmeye itmektedir.

21. yüzyılda yükselen güç unsuru siber güç ve Türkiye'nin ele alındığı bu tezde güç kavramının ve unsurlarının açıklanması konusunda Realist ve Neo-liberal teorilerden yararlanılmış, güvenlik kavramının genişleyen içeriğinin analiz edilmesinde de Kopenhag Okulu'ndan yararlanılmıştır. Güç maksimizasyonu amacını vurgulayan Realist yaklaşım bu çerçevede her türlü aracın kullanılabileceğini ve etik prensiplerin devlet bekası kapsamında göz ardı edilebileceğini öne sürmekte, askeri unsurlar üzerinden sert güç kullanımı odaklı analizler ortaya koymaktadır. Realist yaklaşımın güç kavramını sert güç kapsamında ele alması karşısında, Neo-liberal yaklaşım güce daha geniş bir çerçeveden bakarak yumuşak güç kavramını ele almaktadır.

Beşinci operasyonel alan olarak gelişen siber uzay, gücün ve güvenliğin çok daha farklı bir boyutunu ortaya koymakta ve bu boyutta varlık gösteren aktörlerin ve araçların ne derece çeşitlendiğini sergilemektedir. Kopenhag Okulu'nun genişletilmiş güvenlik perspektifi ve güvenlikleştirme kavramı bu gelişmelerin açıklanması konusunda kapsamlı bir yaklaşım ortaya koymaktadır. Egemen devletler arasındaki çatışma ve rekabet siber uzay boyutuna taşınmakta, teknoloji ve internet etkili araçlar halini almaktadır. Günümüz gelişmeleri devlet ve askeri güç odaklı anlayışın ötesine

geçmekte, devlet dışı aktörler internet ve teknolojinin sunmuş olduğu imkanlardan yararlanarak asimetrik güç elde etmektedirler. Söz konusu yapı da klasik realist yaklaşımın gelişmeleri açıklamada yetersiz kaldığını göstermekte ve Kopenhag Okulu'nun genişletilmiş güvenlik anlayışı kapsamlı bir analiz için perspektif sunmaktadır.

Siber uzay, bilgisayarlar, internet ağları ve teknoloji ile kullanıcıları birbirine bağlamaktadır. Düşük fiyatlar ve kolay erişim sayesinde internet ve teknoloji kullanımı birey düzeyinde ciddi bir seviyeye erişmiş, günlük hayatın neredeyse hemen hemen her alanına yayılan kullanım alanlarıyla küresel ekonominin güçlü bir cephesi haline gelmiştir. Siber uzay düzleminde vukuu bulan devletlerarası mücadelelerde propaganda, politika ve ekonomik unsurlar önemli araçlar arasında yerlerini almaya başlamıştır. Bu kapsamda yakın gelecekte şirketler, bireyler ve devletlerin internet üzerinden ticaretlerini geliştirmek üzere yatırımlarını ve bu alandaki çalışmalarını hızlandıracakları aşikardır. Yatırımcıların ekonomik refahı geliştikçe uluslar yani toplumlar da güçlenecektir. Bireyi, şirketleri güçlü olan devletlerin uluslararası alanda güçlü olacağı savı kapsamında, siber uzay düzlemindeki işbirliklerinin geliştirilmesinin ve bu alanda normların ve kuralların oluşturulmasının faydalı olacağı değerlendirilmektedir. Mevcut durumda üzerinde evrensel anlamda mutabık olunan ve uygulama gücü bulunan net kuralların ve normların bulunmaması, siber uzaydaki belirsizliği derinleştirmekte ve bu alanın önümüzdeki dönemde daha yoğun mücadelelere sahne olabileceğinin güçlü işaretlerini vermektedir.

Siber savaş alanlarını cazip hale getiren çeşitli avantajlar bulunmaktadır. Yapısı gereği çok ucuza silah 'virüs' elde edilebilmektedir. Ucuz maliyetli bu silahlar ile karşı tarafın ekonomisine ciddi zararlar verilebilmektedir. Ani ve beklenmedik bir zamanda hedefi hazırlıksız ve savunmasız yakalamak mümkündür. Siber uzaydaki muğlaklık, saldırganların kimliğini kolaylıkla gizlemelerine olanak tanıyarak tespit edilip cezalandırılmalarını zorlaştırmaktadır.

Siber alan üzerinden finans, elektrik, ulaşım, sağlık v.b gibi temel hizmetlerin sağlanıyor olması yeni güvenlik anlayışını gündeme getirmekte ve özellikle de kritik

altyapıların güvenliği önemli gündem maddelerinden biri haline gelmektedir. Kritik altyapılara sadece devletler değil, bireylerin de saldırılar düzenleyebildiği görülmekte bu unsur da siber uzayın sağladığı imkanların ve asimetrik gücün ulaşmış olduğu noktayı göstermektedir. Siber uzaya ve teknolojilere son derece ucuz maliyetle ulaşılabilmesi ve siber uzayın yapısı kapsamında kimliğin rahatlıkla gizlenebilir olması karşısında devletlerin kırılganlıklarının arttığı, ciddi bütçelere mal olan enerji sistemleri, uzay sistemleri ya da finans sistemleri gibi yapıların tehdit edilebildiği görülmektedir. Siber uzayın söz konusu unsurları devletlerin güvenlik tehditleri karşısında her aşamada kapsamlı önlemler almasına neden olmakta ve bu anlamda artan şekilde mühendise, yazılımcıya, programcıya, sosyal medya uzmanına ve geliştiricilere ihtiyaç duyulmaktadır. Tüm bu unsurların sonucunda siber alanın güvenli ve düzenli şekilde korunması devletler için bir ulusal güvenlik meselesi haline gelmiştir.

Bu çalışmada, siber uzayı domine etme yönünde stratejiler geliştirildiğinden hareketle ABD, RF, ÇHC ve İsrail Devleti'nin siber uzay ve bileşenleri üzerine yaptıkları çalışmalar incelenmiştir. Aynı konu başlıkları doğrultusunda Türkiye'nin siber uzay stratejilerine ışık tutularak mevcut durum analiz edilmiştir. ABD'de özel şirketler ve kamu kurumlarının işbirliği içerisinde ve akademisyenlerin fikirleri doğrultusunda siber güvenlik politikaları izlemektedir. ABD'de eğitim müfredatlarında siber güvenlik farkındalığının oluşturulması için programlar oluşturulmuştur. Siber güvenliği teminin en önemli bileşenlerinden biri olarak eğitimin üzerinde durulmaktadır. Siber uzay askeri çarpan olarak görülmekte, ekonominin güçlü olması için teknoloji ve siber uzayın güvenliği ulusal stratejinin ana unsurları arasında yer almaktadır. İstihbarat anlamında da siber uzay CIA'nın uzman birimlerince aktif ve yaygın olarak kullanılmaktadır.

RF Soğuk Savaş döneminden itibaren teknolojide büyük ilerleme kaydetmiştir. RF'nin siber uzayda öne çıkan çalışmalarının ulusal yazılım, donanım ve uzay araçları kapsamında olduğu görülmektedir. İnternetin halk üzerinde oluşturabileceği etkiye karşı hassasiyet göstermekte ve bilgi güvenliği konusunda önlemler almaya çalışmaktadır. Herhangi bir saldırı ya da risk döneminde etkilerin minimum düzeye indirilmesi ve özellikle yerli yazılımların geliştirilmesinde AR-GE faaliyetlilerine destek verildiği

resmi belgelerde görülmektedir. ÇHC, siber alanda güvenlik sağlanması konusunda devletler arasında işbirliğini teşvik etmektedir. Siber kalkınma için ulusal strateji izlemektedir. Uluslararası işbirlikleri çerçevesinde ise, kazan-kazan yaklaşımını yansıtmakta ve etkili olmaya çalışmaktadır. ÇHC iletişimi güçlendirmek, karşılıklı işbirliğini derinleştirmek, ortaklık kurmak ve siber uzayı insanlık için ortak bir alan haline getirmeye çalıştığını vurgulamaktadır. ÇHC'nin siber uzay politikaları temel itibariyle iki unsur üzerine bina edilmektedir. Birincisi teknolojiye atfedilen büyük önem, ikincisi de uzayda yer edinme kapsamında yaptığı çalışmalardır. ÇHC 1990'lı yıllarda, 'Altın Geçiş' olarak tanımladığı büyük bilişim uygulama projeleri başlatmış ve sanayileşmeyi teşvik etmiştir. ÇHC için bu dönemi siber uzay adına stratejik gelişmeler dönemi olarak tanımlamak mümkündür. İsrail Devleti'nin siber uzayda yaptığı çalışmaların kapsamına ulaşmak kolay olmamakla beraber açık kaynaklarda siber uzayı daha çok istihbarat anlamında kullandığına dair iddialar bulunmaktadır. Söz konusu amaç doğrultusunda istihbarat birimleri kurulmuş, kritik hükümet sistemlerinin herhangi bir siber tehditten etkilenmemesi için internet gibi ancak internetten bağımsız olarak çalışabilen ve genelde gizli belgelerin içeriğinin bulunduğu ağlar oluşturulmuştur. Böylece dışarından gelebilecek saldırılara nispeten engel olunabilmektedir.

Türkiye'nin siber uzay kapsamında hazırlamış olduğu stratejiler değerlendirildiğinde siber uzayda iddialı diğer devletlere paralel bir yaklaşım sergilediği görülmektedir. İstihbarat kuruluşlarında birimler oluşturulmakta, teknoloji ve uzay alanında daha hızlı çalışılmasının altı çizilmektedir. AR-GE çalışmaları için geç kalınmadığını düşünmek mümkünse de gelişmelerin takip edilebilmesi için akademisyenler ile fikir alışverişine hız verilmesi gerektiğini söylemek mümkündür. Stratejilerin genel olarak ilgili birimlerde çalışan kişilerin uzmanlık alanları üzerinden geliştirildiği görülmektedir. Söz konusu tezlere bu çalışmada yer verilmemekle beraber akademi dünyasında siber uzay ve ilgili alanlardaki çalışmalar son derece sınırlı kalmaktadır. Daha geniş bir perspektifle değerlendirildiğinde, yumuşak gücü literatüre katan Joseph Nye'ın ABD'nin Savunma Bakanlığında siber güvenlik üzerine bir dönem etkin görev alması, siber güvenliğin uzmanlık alanından uluslararası strateji alanına nasıl evrildiğini ispatlar niteliktedir. Türkiye'nin yaptığı çalışmalar değerlendirildiğinde, bu alanda ulusal yeteneklerin geliştirilmesinde eğitim faktörünün önemi ortaya

çıkmaktadır. Gelecek dönemde risklerin yönetilebilmesi için çalışılmasının, siber uzayın bileşenleri olarak internetin kontrolünün sağlanmasının, yüksek teknoloji için sanayileşmeye önem verilmesinin, jeopolitik uzayda bulunan Göktürk uydularının sayısının arttırılmasının, siber alanın kullanıcılarının farkındalığının eğitimler ile arttırılmasının gerekliliğini vurgulamak mümkündür. Türkiye'nin söz konusu dört alanı koordineli olarak faaliyete geçirmesi, siber uzayda ciddi bir etkinlik sağlanmasına katkı sağlayacaktır.

Gelinen noktada siber uzayda güvenlik, kritik sistemlerin korunması, gelişen teknolojiye ayak uydurulması- hatta önüne geçilmesi- bireylerin eğitimi ve farkındalık oluşturulması gibi bireyden devlet düzeyine varan pek çok konuyu içeren bir alan haline gelmiştir. Bugünün güvenlik anlayışı klasik askeri güç tanımlamasının ötesine geçerek akıllı güç, siber güç gibi unsurlara bağımlı hale gelmektedir. Güçlü devletler mücadelelerini siber uzaya taşımışlar, teknolojide ciddi gelişmeler kaydetmişlerdir. Uzaya amaçları belirli uydular göndermişlerdir. Bu devletler söz konusu gelişmelere paralel politikalar inşa etmişler ve bu politikaların başarılı olabilmesi için başta eğitim alanı olmak üzere pek çok alanda politika geliştirmişler, vatandaşlarının farkındalığını hedeflemişlerdir. Türkiye'nin alandaki çalışmalarına bakıldığında ise, bir yandan güçlü olan devletlere paralel politikalar uygulama çabası içerisinde olduğu görülmüştür. Diğer yandan ise, uzaya dahil olmaya başlayan Türkiye'nin çalışmalarını hızlandırması gerektiği zira teknolojik gelişmelerde geride kaldığı gözlemlenmiştir. Siber güvenlik, siber uzay, siber güç kapsamında akademik anlamda önemli eksiklikler olduğu, pek çok devletin ilkokul seviyelerine kadar siber güvenlik üzerine eğitimler verdiği bir düzende Türkiye'de yüksek eğitim seviyesinde dahi araştırmaların çok zayıf olduğu değerlendirilmiştir.

İçerisinde bulunduğumuz dijital çağ bir taraftan bilgiye hızlı ulaşım, telekomünikasyon gibi pek çok alanda yeni imkanlar sunarken, siber uzayın belirsizliğinin ve kuralsızlığının getirdiği risk ve tehditler bireyden devlet güvenliğine kadar farklı düzeylerde olumsuz etkiler yaratabilmektedir. Söz konusu risk ve tehditler karşısında devletlerin çok taraflı politikalar üretmesinin ve işbirliklerine girmesinin önem kazandığı, tek taraflı politikaların artan kırılganlıklar karşısında yetersiz kalacağı değerlendirilmektedir. Arz edilen çerçevede Türkiye'nin gelişmeleri yakından takip

etmesi, teknoloji altyapısını geliştirerek kırılganlıklarını minimize etmeye çalışması ve bütüncül bir yaklaşımla sürecin farklı paydaşlarını bir araya getireceği çabalar içerisinde olması ulusal güvenliğin temini açısından büyük önem arz etmektedir.

İlerleyen süreçte siber uzayın güç mücadelelerine konu olacağı ve ulusal güvenliğin en önemli unsurlarından biri olacağını söylemek mümkündür. Hayatın hemen hemen her alanına nüfuz eden siber uzayın Türkiye ölçeğinde bir ulusal güvenlik meselesi olarak değerlendirilmesi gerekmektedir. Bu alanda yapılan çalışmalara hız verilmesi, farklı sektörleri ve paydaşları içeren kapsamlı bir yaklaşımla ele alınması ulusal güvenliğin korunmasında büyük önem arz etmektedir.

KAYNAKÇA

Açıkmeşe, Sinem Akgül "Algı mı? Söylem mi? Kopenhag Okulu ve Yeni Klasik Gerçekçilikte Güvenlik Tehditleri", **Uluslararası İlişkiler Dergisi**, C.8, S.30, (Yaz 2011), Ss.43-73

Altun, Altun. "ABD-Çin Rekabeti Bağlamında Siber Savaş". **İnternational Journal of Academic Value Studies**. C.3, S.9, ss.24-34

Arı, Tayyar. **Uluslararası İlişkilere Giriş**. Bursa:MKM Yayınları. 2013.

Arı, Tayyar. **Uluslararası İlişkiler Teorileri Çatışma, Hegemonya, İş birliği**. Bursa: MKM Yayıncılık. 2013.

Arıboğan, Deniz Ülke. **Globalleşme Senaryosunun Aktörleri**. İstanbul:Der Yayınları. 1996.

Armaoğlu, Fahir. **20. Yüzyıl Siyasi Tarihi 1914-1995**. Timaş Yayınevi. İstanbul:2014.

Armıtage, Richard, L. Joseph Nye. **CSIS Commıssıon On Smart Power**. The Csıs Pres,
Washinton: 2007.

Aslanoğlu, Erhan. "Ulusal Yenilenme Sistemleri Çerçevesinde Türkiye' de Teknoloji Politikaları". **Mülkiye Dergisi**. C.25. S. 230. ss.119-152

Atay, Özlem Yasemin Hancıoğlu. "İngiltere, Amerika Birleşik Devletleri ve Türkiye'nin Ulusal İnavosyon Sistemlerinin İncelenmesi: Türkiye İçin Öneriler". **Ankara Üniversitesi SBF Dergisi**. C.74. S.2.2019. ss.511-547.

Aydın, Mustafa. "Uluslararası İlişkilerin "Gerçekçi" Teorisi: Kökeni, Kapsamı, Kritiği". **Uluslararası İlişkiler Dergisi**, C. 1, S. 1 (Bahar 2004).ss.33-60.

Aydın, Mustafa. "Uluslararası İlişkilerde Yaklaşım, Teori ve Analiz". **Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi**. C. 51, S.1. (Ocak 1996).

Aydoğan, Bekir Hakan Aydın. **Güç Kavramı, Kamu Diplomasisi ve Güvenlik**. İstanbul: Ekopolitik Uluslararası İlişkiler Masası. 2011.

Bakan, Selahaddin Sonay Şahin. "Uluslararası Güvenlik Yaklaşımlarının Tarihsel Dönüşümü ve Yeni Tehditler". **The Journal of International Lingual, Social and Educational Sciences**. C.4, S.2, (Aralık 2018). ss.135-152

Balta, Evren. **Küresel Siyasete Giriş Uluslararası İlişkilerde Kavramlar, Teoriler, Süreçler**. İstanbul: İletişim Yayınları. 2014.

Baldwin, David A. Power And International Relations. **Handbook of İnternational Relations**. der. Walter Carlsnaes, Thomas Risse, Beth A. Simmons. London: Sage. 2013.

Balpınar, Zafer. "Askeri Güç Çarpanı Olarak Yahudi Yerleşim Yerleri". **Güvenlik Stratejileri Dergisi**. Y.10.S.20. (2014), ss.85-117

Barr, Stephen. "Anti-NATO Hackers Sabotage 3 Web Sites". 1999. (Çevrimiçi**),** https://www.washingtonpost.com/wp-srv/inatl/longterm/balkans/stories/hackers051299.htm. Erişim Tarihi: 11.04.2020

Baylis, John "Uluslararası İlişkilerde Güvenlik Kavramı", **Uluslararası İlişkiler Dergisi,** C.5, S.18, (Yaz 2008), s.77

Baysal, Başar ve Çağla Lüleci. "Kopenhag Okulu ve Güvenlikleştirme Teorisi". **Güvenlik Stratejileri Dergisi**. Y.11, S.22. (Ekim 2015). ss.61-96

BBC News. "Profile: Garry Mckinnon". (Çevrimiçi) https://www.bbc.com/news/uk-19946902. (Erişim Tarihi: 19.03.2020)

BBC Türkçe. Bir 'İnternet Cumhuriyeti' Edtonya. 2016. (Çevrimiçi) https://www.bbc.com/turkce/haberler/2016/05/160504_estonya_internet. (Erişim Tarihi:01.04.2020)

BBC. "Edward Snowden: Leaks That Exposed Us Spy Programme". 2013. (Çevrimiçi) https://www.bbc.com/news/world-us-canada-23123964. Erişim Tarihi: 12.04.2020

BBC Turkısh. "Estonya'ya Siber Saldırı". 2007. (Çevrimiçi) http://www.bbc.co.uk/turkish/news/story/2007/05/070517_estonia_cyber.shtml. (Erişim Tarihi: 01.04.2020)

Bıçakcı, Salih. "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik". **Uluslararası İlişkiler Dergisi**. C.10. S.40. (Kış 2014). ss. 101-130.

Bıçakcı, Salih. Doruk Ergün, Mitat Çelikpala, Türkiye' de Siber Güvenlik ve Nükleer Enerji. **Edam**. s.36 (Çevrimiçi) https://edam.org.tr/document/CyberNuclear/SiberKitapTR/edam_siber_guvenlik_b2.pdf, Erişim Tarihi: 30.04.2020

Biography. "Edward Snowden Biography". (Çevrimiçi) https://www.biography.com/activist/edward-snowden. Erişim Tarihi: 12.04.2020

Bıçakcı, Salih. "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu". **Uluslararası İlişkiler Dergisi**. C.9. S. 34. s. 205-226

Bilgiç, Ali. "Güvenlik İkilemi"ni Yeniden Düşünmek Güvenlik Çalışmalarında Yeni Bir Perspektif". **Uluslararası İlişkiler**. C. 8, S. 29 (Bahar 2011). s. 123-142

Bozdağlıoğlu, Yücel ve Çınar Özen. "Liberalizmden Neoliberalizme Güç Olgusu ve Sistemik Bağımlılık". **Uluslararası İlişkiler Dergisi**. C.1, S. 4. (Kış 2004). s.59-79.

Bucci, Steven "Joining Cybercrime and Cyberterrorism A Likely Scenario. **Cyberspace and National Security Threats, Opportunities and Power İn a Virtual World**. der. Derek S. Reveron, Washington: Georgetown University Press. 2012.

Burke, Peter. **Bilgi Tarihi Nedir?.** Çev: Turgay Sivrikaya. İstanbul: Islık Yayınları. 2018.

Buzan, Barry. **People, States and Fear**: The National Security Problem in International Relations. BrightonWheatsheaf Book. Brighton Sussex. 1983.

Buzan, Barry. "Askeri Güvenliğin Değişen Gündemi". **Uluslararası İlişkiler Dergisi**. C.5, S. 18 (Yaz 2008). ss. 107-123

Buzan, Barry. **İnsanlar Devletler ve Korku**. Çev: Emre Çıtak. İstanbul: Uluslararası İlişkiler Kütüphanesi. 2015.

Buzan, Barry "Barış, Güç ve Güvenlik: Uluslararası İlişkilerde Çatışan Kavramlar". Çev: Özden S. Sarı. **Uluslararası İlişkilerde Anahtar Metinler**. der. Esra Diri. Ankara: Uluslararası İlişkiler Kütüphanesi.

Bıçakcı, Salih. **21. Yüzyılda Siber Güvenlik**. İstanbul: Bilgi Üniversitesi Yayınları. 2013

Birdişli, Fikren ve Merve Gönen. "Bölgesel Güvenlik Kompleksi Teorisi bağlamında Türkiye-İran Arasında Göç ve Sınır Güvenliği". **İran Çalışmaları Dergisi**. C.1, S.2. (2017). ss. 11-38.

Billo, Charles Welton Chang. "Cyber Warfare: An Analysis of the Means and Motivations of Selected Nation States" 2004**. Institute for Security Technology Studies**. (Çevrimiçi) https://gssd.mit.edu/search-gssd/site/cyber-warfare-analysis-means-motivations-59897-thu-12-27-2012-1242, Erişim Tarihi: 29.03.2020

Brown, Garry D. Andrew O. Metcalf. "Easier Said Than Done: Legal Reviews of Cyber Weapons". **Journal of National Security Law and Policy**. C. 7. S. 115. 2014. s. 115-138.

Brown, Tim "Snowden Says China Stole F-35 JSF Secret Design Information, 2015". (Çevrimiçi) https://www.themanufacturer.com/articles/snowden-says-china-stole-f-35-jsf-secret-design-information/. Erişim Tarihi: 12.04.2020

Braodcom. "Stuxnet: A Breakthrough". 2010. (Çevrimiçi) https://community.broadcom.com/symantecenterprise/communities. Erişim Tarihi: 22.04.2020

BTK. Eylem Planlaması. 2013. (Çevrimiçi) https://www.btk.gov.tr/uploads/pages/2-1-strateji-eylem-plani-2013-2014-5a3412cf8f45a.pdf. Erişim Tarihi: 01.05.2020

Carr, Edward Hallett. **1919 – 1939 Yirmi Yıl Krizi**. Çev.: Can Cemgil. İstanbul: İstanbul Bilgi Üniversitesi Yayınları. 2015.

Carr, Jeffery. **Cyber Watfare**. USA: O'Reılly. 2012.

Canberk, Gürol ve Şeref Sağıroğlu. "Casus Yazılımlar: Bulaima Yöntemleri ve Önlemler". **Gazi Üniversitesi Mühendisik ve Mimarlık Fakültesi Dergis**i. C.23. S.1. 2008. s.165-180

Canbek, Gürol Şeref Sağıroğlu. "Bilgisayar Sistemlerine Yapılan Saldırılar ve Türleri: Bir İnceleme". **Erciyes Üniversitesi Fen Bilimleri Dergisi**. C.23. S.1-2. 2007. s.1-12

China.com. "Siber Dünyada Ortak Kader Topluluğu Çağrısı". (Çevrimiçi) http://turkish.china.com/news/china/543/20170301/899556.html. Erişim Tarihi: 04.04.2020

Chinadaily. "International Strategy Of Cooperation On Cyberspace". 2017. (Çevrimiçi) https://www.chinadaily.com.cn/kindle/2017-03/02/content_28409210.htm. (Erişim Tarihi: 09.04.2020

Choudhury, Saheli Roy "China Reportedly Steps Up Efforts To Steal Australian Company Secrets**", (Çevrimiçi)**https://www.cnbc.com/2018/11/21/cybersecurity-china-reportedly-increased-attacks-on-australian-firms.html, Erişim Tarihi: 13.04.2020

Cirlig, Carmen-Cristina. "Cyber defence in the EU Preparing for cyber warfare?". **European Parliamentry Research Service**. (Çevrimiçi) https://www.europarl.europa.eu/EPRS/EPRS-Briefing-542143-Cyber-defence-in-the-EU-FINAL.pdf. (Erişim Tarihi: 28.03.2020)

Clarke, Richard A. Robert K.Knake. **Siber Savaş: Ulusal Güvenliğe Yönelik Yeni Tehdit**. Çev. Murat Erduran. İstanbul: İKÜ Yayınevi. 2011.

CSIS "Significant Cyber Incidents". 2020. (Çevrimiçi) https://www.csis.org/programs/technology-policy-program/significant-cyber-incidents. Erişim Tarihi: 14.04.2020

Concept Of A Cyber Securıty Strategy Russıan Federatıon. 2013. (Çevrimiçi), http://council.gov.ru/media/files/41d4b3dfbdb25cea8a73.pdf. (Erişim Tarihi:29.03.2020)

Cyber Securıty Intellıgence. Israıl National Cyber Bureau (INCB). (Çevrimiçi) https://www.cybersecurityintelligence.com/israel-national-cyber-bureau-incb-2895.html. Erişim Tarihi: 17.04.2020

Cyber Week. Cyber Week 2017. 2017. (Çevrimiçi) https://cyberweek.tau.ac.il/2017/index.php. Erişim Tarihi: 18.04.2020

CCDCOE. Strategy and Governance. (Çevrimiçi) https://ccdcoe.org/library/strategy-and-governance/. Erişim Tarihi: 20.04.2020

Çelik, Soner. "Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşim". **ARHUSS**. C.1.S.2.(2018), ss.110-119

Çınar, Burak. "İkinci Dünya Savaşı'nın Başladığı Gün Avrupa'daki Durum: Ülkelerin Savaşa Hazırlık Durumları ve Bunun Savaşa Yansıması". **Akademik Bakış Dergisi**. C.13. S.25. (Kış 2019). s.239-266

Çin Danıştay Bilgi Bürosu. "Beyaz Kitap Çin'in Ulusal Savunma Belgesi". Pekin. 2004. (Çevrimiçi) http://politics.people.com.cn/GB/1027/3081796.html. Erişim Tarihi: 04.04.2020

Çiftçi, Hasan. **Her Yönüyle Siber Savaş**. Ankara: Tübitak Popüler Bilim Kitapları. 2017.

Çin Komünist Partisi Merkez Komitesi. "2006-2020 Ulusal Bilişim Geliştirme Stratejisi".2006 (Çevrimiçi) http://www.gov.cn/gongbao/content/2006/content_315999.html. Erişim Tarihi: 05.04.2020

Darıcılı, Ali Burak. "Türkiye'nin Siber Güvenlik Politikalarının Analizi; Türkiye'nin Potansiyel Siber Güvenlik Stratejisi". **TESAM Akademi Dergisi**. C.6. S.2. Temmuz 2019. ss.11-33

Darıcılı, Ali Burak Barış Özdal. "Analysis of the Cyber Security Strategies of People's Republic of China". **Güvenlik Stratejiler Dergisi**. C.14. S. 28. 2018.

Darıcılı, Ali Burak Barış Özdal. "Enformasyon Savaşı Bağlamında Rusya Federasyonu-Türkiye İlişkilerinin Analizi". **İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi.** S.4. C.19. 2017. ss.18-40

Darıcılı, Ali Burak. "Askerleştirilen ve Silahlandırılan Siber Uzay". **Sosyal ve Beşeri Bilimlere Dair Araştırma Örnekleri**. der. Ali Acavavcı, Ankara: Nobel Yayınları.2018.

Darıcılı, Ali Burak. **Siber Uzay ve Siber Güvenlik Nedir? Abd 'nin Siber Güvenlik Stratejisi Rusya Federasyonun Siber Güvenlik Stratejilerinin Karşılaştırılmalı Analizi**. Bursa: Dora Yayınları, 2017.

Darıcılı, Ali Burak. "Amerika Birleşik Devletleri'nin Siber Kapasitesinde Rol Oynayan Kurumsal Yapılanmalarının Analizi". Edt. Tayyar Arı. Çiğdem Aydın Koyuncu. **Uludağ 9. Uluslararası İlişkiler Kongresi Dünya Politikasında Kriz ve Değişim**. Bursa: Dora Yayınları.2017.

Darıcılı, Ali Burak. Demokrat Parti Hack Skandalı Bağlamında ABD ve RF' nın Siber Güvenlik Stratejilerinin Analizi. **Uluslararası Çalışmalar Dergisi**. C.1. S.1.2017. ss.1-24

Darıcılı, Ali Burak. "Rusya Federasyon'un Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi". **Bilig**. S.83. (Güz 2017). ss.121-146

Darıcılı, Ali Burak. Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırıların Analizi. **Uludağ Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**. S.2. C.7. 2014. ss.1-16

Dahl, A. Raobert. ***The Concept of Power,*** **Behavioral Science**. Y.2 S.3. (Temmuz 1957). ss. 201-215.

Demir, Sertif Ali Bilgin Varlık. "Realist ve Liberal Teorilerde "Güç "Anlayışı". Edt. Hasret Çomak, Caner Sancaktar. **Uluslararası İlişkilerde Teorik Tartışmalar**. İstanbul: Beta. 2013.

Deng, Yong Thomas G. Moore. "China Views Globalization: Toward a New Great-Power Politics?". **The Washington Quarterly**. C. 27. S. 3. 2004.

Doğan, Salih Şeref Kavak. Uluslararası İlişkilerde Güç Kavramı. **Uluslararası İlişkilerin Temel Kavramları**. der. Arif Behiç Özcan, Yusuf Çınar. İstanbul: Hükümdar Yayınları. 2014.

DW. "Türkiye'ye Siber Saldırı". 2015, (Çevrimiçi). https://www.dw.com/tr/t%C3%BCrkiyeye-siber-sald%C4%B1r%C4%B1/a-18942536. Erişim Tarihi: 02.05.2020

Ersoy, Eyüp. "Realizm". **Uluslararası İlişkiler Teorileri**. der. Ramazan Gözen. İstanbul: İletişim Yayınları. 2019.

Eralp, Atilla. "Uluslararası İlişkilerin Oluşumu: İdealizm-Realizm Tartışması". **Devlet Sistem ve Kimlik: Uluslararası İlişkilerde Temel Yaklaşımlar**. İ.D. Dağı vd., İstanbul: İletişim Yayınları. 2013.

Erol, M. Seyfettin Mehmet Şahin. "Bağımsızlıklarının 20. Yılında Orta Asya ve Kafkasya'daki Türk Cumhuriyetlerinin Entegrasyon Süreci (1991-2011). **Karadeniz Araştırmaları Dergisi**. S.137. (Bahar 2013). ss.111-136

Eren,Vahap. “Siber Güvenlik Alanında Gelecek Hedeflerimiz”. S.1. **Siber Güvenlik Dergisi**. 2017. ss.32-33

Encyclopedıa Brıtannıca,” The Fourth Industrial Revolution,” (Çevrimiçi)https://www.britannica.com/topic/The-Fourth-Industrial-Revolution-2119734,Erişim Tarihi:08.03.2020

Embel, Ersin. “Kronik: ABD Başkanlık Seçimleri”. **Ankara Üniversitesi Siyasi Bilimler Dergisi**. S.71. C.4,2016. s.1319

Euronews. Litvanya Meclisi'nin İnternet Sitesine Siber Saldırı,2016 (Çevrimiçi) https://tr.euronews.com/2016/04/11/litvanya-meclisi-nin-internet-sitesine-siber-saldiri. Erişim Tarihi: 01.04.2020

Farwell,James P. Rafal Rohozinski. “Stuxnet and The Future of Cyber War”. **Survival**. C.53. S.1. 2011. ss.23-40.

Foxnews. “China Confirms Existence of Elite Cyber-Warfare Outfit the 'Blue Army'”. (Çevrimiçi) http://www.foxnews.com/tech/2011/05/26/china-confirms-existence-blue-army-elite-cyber-warfare-outfit.html. 2017. Erişim Tarihi:04.04.2020

Gallarotti, Giulio. “Soft Power: What it is, Why it’s Important and the Conditions Under Which it Can Be Effectively Used”. **Journal of Political Power**. (2011). C.4. S.1.25-47.

Gelleman, Barton Ellen Nakashima. “The Washington Post, “U.S. spy agencies mounted 231 offensive cyber-operations in 2001 documents Show”. (Çevrimiçi) https://www.washingtonpost.com/world/national-security. (Erişim Tarihi: 19.03.2020)

Gerasimov, Valery The Value Of Scıence In Predıctıon. 2013. (Çevrimiçi). https://www.ies.be/files/Gerasimov%20HW%20ENG.pdf. (Erişim Tarihi: 29.03.2020)

Gıbson,William. **Neuromancer**. Çev.: Gonca Gülbay. İstanbul: Altıkırkbeş Yayın. 2012.

Giles, Keir. Russia: National Security Strategy to 2020, **Nato Defense College**. 2009. (Çevrimiçi) https://css.ethz.ch/en/services/digital-library/publications/publication.html/154909. (Erişim Tarihi:29.03.2020)

Güner, Reyhan. Joseph Nye ile Mülakat: Siber Güvenlik, Siber Güç ve Siberuzayın Geleceği Üzerine. (Çevrimiçi) https://www.academia.edu/37696368/Joseph_Nye. (Erişim Tarihi: 25.10.2019).

Gürkaynak, Muharrem ve Adem Ali İren, "Reel Dünyada Sanal Açmaz: SiberAlanda Uluslararası İlişkiler", **Süleyman Demirel Üniversitesi İktisadi ve İdariBilimler Fakültesi Dergisi**, C.16, 2011, ss.263-279

Goodman, Marc. **Geleceğin Suçları Dijital Dünyanın Karanlık Yüzü**. İstanbul: Timaş Yayınları. 2016.

Gore, Albert. **Technology for America's Economic Growth, A New Direction to Build Economic Strength.** Washıngton: The White House Office Of The Press Secretary. 1993.

Gökbilim. Türkiye'nin Uzay Çalışmaları. 2020. (Çevrimiçi) https://gokbilimi.net/turkiyenin-uzay-calismalari/. Erişim Tarihi: 25.04.2020

Gündüz, Onur Volkan Göçoğlu. "Ulusal Güvenlik Anlayışından ABD'nin Güvenlik Anlayışına Kronolojik Bir Bakış. "**Uluslararası Toplum Araştırmaları Dergisi**. C.15. S.21. (Ocak 2020). ss.725-755

Global Security.org. "China in Space". (Çevrimiçi) https://www.globalsecurity.org/space/world/china/index.html. Erişim Tarihi: 03.04.2020

Global İsrail Bloglar Ağı. "Siber Güvenlik Ulusu: İsrail Ağı Korumada Nasıl Dünya Lideri Oldu". 2020. (Çevrimiçi) https://itrade.gov.il/turkey/siber-guvenlik-ulusu-israil-agi-korumada-nasil-dunya-lideri-oldu/. Erişim Tarihi: 17.04.2020

Haberler. "8. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı". 2015, (Çevrimiçi) https://www.haberler.com/8-uluslararasi-bilgi-guvenligi-ve-kriptoloji-7829357-haberi/. Erişim Tarihi: 04.05

Hancıoğlu, Yasemin Özlem Atay. "Türkiye, Güney Kore ve İsrail'in Ulusal İnovasyon Sistemlerinin Analizi ve Kıyaslanması". **Hacettepe Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi**. C.36. S.2. ss. 21-50

Herz, J. H. **Political Realism and Political Idealism, A Study in Theories and Realities**. Chicaho & London: The University of Chicago Press. 1950.

Hobbes, Thomas. **Levıathan**. Çev.: Hamiyet Ünal. İstanbul: Lıtera Yayıncılık. 2019.

Hürriyet. "Gümrükte Sistem Çöktü Bir Milyar Dolar Zarar Oluştu". 2011. (Çevrimiçi) https://www.hurriyet.com.tr/ekonomi/gumrukte-sistem-coktu-1-milyar-dolarlik-ticaret-durdu-16920642. Erişim Tarihi: 03.05.2020

Internet Usage Statıstıcs. http://www.internetworldstats.com/stats.htm. (Çevrimiçi: 15.02.2020)

Israil Global Blogs Network. "Beresheet"in Ardından – İsrailin İlk Uzay Aracı". 2019. (Çevrimiçi) https://itrade.gov.il/turkey/beresheetin-ardindan-israilin-ilk-uzay-araci/. Erişim Tarihi: 16.04.2020

IEEE Spectrum. "The Hunt for the Kill Switch". 2008. (Çevrimiçi) https://spectrum.ieee.org/semiconductors/design/the-hunt-for-the-kill-switch. Erişim Tarihi: 22.04.2020

Israel Defense Forces. "Operation Cast Lead". 2008. (Çevrimiçi) https://www.idf.il/en/minisites/wars-and-operations/operation-cast-lead-2008-09/. Erişim Tarihi: 22.04.2020

John, Reed. "Unit 8200: Israıl's Cyber Spy Agency". Fınancal Times. 2015. (Çevrimiçi) https://www.ft.com/content/69f150da-25b8-11e5-bd83-71cb60e8f08c. Erişim Tarihi: 17.04.2020

Kabay, M.E. "Industrial Espionage, Part 8: China and Titan Rain". (Çevrimiçi), https://www.networkworld.com/article/2315467/industrial-espionage--part-8--china-and-titan-rain.html. 2005ş (Erişim Tarihi: 18.03.2020)

Karagül, Soner Muhammet Fatih Özkan. "Bilgi Teknolojileri ve Uluslararası İlişkilerde Fırsat-Tehdit Paradoksu". **Bilgi Ekonomisi ve Yönetimi Dergisi**. C.10. S.1. (2015) s.115-127

Kagan, Robert. **Cennet ve Güç Yeni Dünya Düzeninde Amerika ve Avrupa**. Çev.: Selim Yeniçeri. İstanbul: Koridor Yayıncılık. 2005.

Kane, Robert K. **Internet Governance in an Age of Cyber Insecurity**. Council Special Report No. 56. 2010.

Kasapoğlu, Can. "Siber Savaş: Geleceğin Askeri Gerçekliği ve Günümüzün Bilimkurgusu Arasında". **Edam**. 2017. (Çevrimiçi) https://edam.org.tr/wp-content/uploads/2017/10/sibersavas_tr_rbs_logo.pdf (Erişim Tarihi: 25.03.2020), s.3

Keleşoğlu, Erhan. **İsrail Yurttaşı Filistinliler Yurttaşlık, Kimlik, Siyaset**. İstanbul: İstanbul Bilgi Üniversitesi Yayınlar. 2014.

Keleştemur, Atalay. **Siber İstihbarat**. Level Kitap. İstanbul:2015.

Keohane Robert O. ve Joseph S. Nye Jr. "Power and Interdependence in the Information Age". **Foreign Affairs**. C. 7. S.5. Eylül-Ekim 1998. Ss.81-94

Khuel, Daniel T. "From Cyberspace to Cyberpower: Defining the Problem". **Cyberpower and National Security**, der. Franklin D. Kamer, Stuart H. Starr ve Larry K. Went, Washington: National Defense Universıty Press, Potamac Books. 2009.

Kılıptarı, Tea "Chine's Smart Rise," **Güvenlik Stratejileri Dergisi**, Y.9.S.18 (Bahar 2013). Ss. 77-102

Kissenger, Henry. **Diplomasi**. Çev.: İbrahim H. Kurt. İstanbul: Türkiye İş Bankası. 2015.

Kurt, Selim. "Toplumsal Güvenliğin Yükselişi". International Journal of Social Science. S.37. (Eylül 2015). ss. 459-476

Kuzwell, Ray. **İnsanlık 2.0 Tekilliğe Doğru Biyolojisini Aşan İnsan**. Çev.: Mine Şengel. İstanbul: Alfa Yayınları. 2016.

Küçüksolak, Övgü Kalkan. "Güvenlik Kavramının Realizm, Neorealizm ve Kopenhag Ekolü Çerçevesinde Tartışılması". **Turan Stratejik Araştırmalar Merkezi Dergisi**. S.14, (İlkbahar 2012). s.202-208

Koldaş, Umut. "Azınlık İcinde Azınlık Olmak (mı?): İsrail Vatandaşı Filistinli/Arap Kadınların İsrail Anaakım Basınında Temsili". **Uluslararası İlişkiler Dergisi**. C.14. S.56. 2017. ss. 105-120

Kötü Amaçlı Yazılım. Siber Savaşlar: 5. Boyutta Savaş. (Çevrimiçi) https://www.kotuamacliyazilim.com/siber-savaslar-5-boyutta-savas/. (Erişim tarihi: 01.04.2020)

Langer, Ralph Cyber Power - An Emerging Factor in National and International Security. (Çevrimiçi) https://www.cirsd.org/en/horizons/horizons-autumn-2016--issue-no-8/cyber-power-an-emerging-factor-in-national-and-international-security (Erişim Tarihi: 27.10.2019)

Lawfare, China's National Cybersecurity Strategy. 2016. (Çevrimiçi) https://www.lawfareblog.com/chinas-national-cybersecurity-strategy. Erişim Tarihi:08.04.2020

Lewis, James A. Katrina Timlin. **Cybersecurity and Cyberwaefare Preliminary Assessment Of National Doctrine and Organization**. Unıder Resources. 2011. s.14

Lin, Herbert S. "Offensive Cyber Operations and the Use of Force". **Journal of National Security Law and Policy**. C.4. S.63.2010. s.63-86

Lupton,David E. **Space Warfare: A Space Power Doctrine**. Alabama: Air University Press. 1988.

Machıavellı, Niccolo. **Prens.** (Çev. Alev Tolga). İstanbul: Say Yayınları. 2009.

Mclaughlin, Daniel "Lithuania accuses Russian hackers of cyber assault after collapse of over 300 websites". 2008. (Çevrimiçi)

https://www.irishtimes.com/news/lithuania-accuses-russian-hackers-of-cyber-assault-after-collapse-of-over-300-websites-1.942155. Erişim Tarihi: 01.04.2020

Morgenthau, Hans J. **Uluslararası Politika**. Ankara: Türk Siyasi İlimler Derneği Yayınları. Çev.: Ünal Aksoy. Baskın Oran. 1970.

Miş, Nebi. "Güvenlikleştirme Teorisi ve Siyasal Olanın Güvenlikleştirilmesi". **Akademik İncelemeler Dergisi**. C.6, S.2 (Temmuz 2014). ss.345-381

Milliyet İnternet Sitesi, **Batman Barajı Şifrelendi**, (Çevrimiçi) https://www.milliyet.com.tr/ekonomi/batman-baraji-sifrelendi-517687, (Erişim Tarihi:26.02.2020)

Milliyet. Türk Hackerlardan Mavi Marmara İntikamı. 2014. (Çevrimiçi) https://www.milliyet.com.tr/yerel-haberler/istanbul/turk-hackerlardan-mavi-marmara-intikami-10368356. Erişim Tarihi: 23.04.2020

Ministry of Defence of the Russian Federation. 'Russian Federation Armed Forces'. **Information Space Activities Concept.** 2011. (Çevrimiçi).https://eng.mil.ru/en/science/publications/more.htm?id=10845074@cmsArticle. Erişim Tarihi: 29.03.2020

Mit. "Organızatıonal Chart Of The National Intelligence Organization,". 2020. (Çevrimiçi) https://www.mit.gov.tr/eng/teskilat.html#. Erişim Tarihi: 04.05.2020

National Science Foundation. **Science The Endless Frontier,** (Çevrimiçi). https://www.nsf.gov/. Erişim Tarihi:08.03.2020

New World Encyclopedia. "History of Science and Technology in China". (Çevrimiçi) http://www.newworldencyclopedia.org/entry/History_of_science_and_technology_in_China. Erişim: 03.04.2020

NTV. "İsrail Siber Savaşa Hazırlanıyor". 2011. (Çevrimiçi) https://www.ntv.com.tr/turkiye/israil-siber-savasa-hazirlaniyor,ja4MNACLtE2_vKAMwGW4GQ. Erişim Tarihi: 24.04.2020

Nye, Joseph. **Amerikan Yüzyılı Bitti mi?**. Çev.: Burç Beşgül. İstanbul: Uluslararası İlişkiler Kütüphanesi. 2016.

Nye, Joseph. **Amerikan Gücünün Paradoksu**. Çev: Gürol Koca. İstanbul: Literatür Yayınları. 2003.

Nye, S Joseph. **Yumuşak Güç Dünya Siyasetinde Başarının Araçları**. Çev: Rayhan İnan Aydın. Ankara:BB101 Yayınları. 2017.

Nye, Joseph. **The Future Of Power**. New York: Public Affarias. 2011.

Nye, Joseph. **Cyber Power**. Cambridge:Harward Kenndy School. 2010.

Nye Joseph. “Nuclear Lessons for Cyber Security?”. **Strategic Studies Quarterly** C.5, S.4, 2011, ss.18-38

Resmi Gazete. Ulusal Siber Güvenlik Çalışmalarının Yürütülmesi, Yönetilmesi ve Koordinasyonuna İlişkin Karar. 2012. (Çevrimiçi) https://www.resmigazete.gov.tr/eskiler/2012/10/20121020-18-1.pdf. Erişim Tarihi: 30.04.2020

Özdemir, Haluk. Uluslararası ilişkilerde Güç: Çok Boyutlu Bir Değerlendirme. **Ankara Üniversitesi Siyasal Bilgiler Fakültesi Dergisi**. C.63 S.3. 2008. s.113-144

Özel, Cengiz. Yumuşak Güce Bütünsel Bakış. **Güvenlik Bilimleri Dergisi**. Y.7. S.1. 2018, ss.1-27.

Öztürk, Serdar Ali Sözdemir. Bekir Gövdere. “ÇİN: Washington Uzlaşmasından Beijing Uzlaşmasına”. **C.Ü. İktisadi ve İdari Bilimler Dergisi**. C.7. S. 1. 2006. Ss.61-73

Pallaver, Matteo. “Power and Its Forms: Hard, Soft, Smart”. (The London School of Economics and Political Science Yayınlanmış Yüksek Lisans Tezi). London. 2011.

Polityuk,Paverl Jim Finkle. “Ukraine Says Communications Hit, Mps Phones Blocked”. 2014. (Çevrimiçi) https://www.reuters.com/article/us-ukraine-crisis-cybersecurity/ukraine-says-communications-hit-mps-phones-blocked-idUSBREA231R220140304 . (Erişim Tarihi: 01.04.2020)

Pekcen, Cemre. “Yeni-liberal Kurumsalcılık Çerçevesinde Çin’in Komşuluk Diplomasisi: Hu Jintao ve Xi Jinping Dönemlerine Karşılaştırmalı Bir Bakış”. **Uluslararası Toplum Araştırmalar Dergisi**. Y.9, C.13, S.19, (Eylül 2019), ss. 2866-2892

Press, Gil. 6 Reasons Israel Became A Cybersecurity Powerhouse Leading The $82 Billion Türkiye Siber Güvenlik Kümelenmesi, Siber Güvenlik Kümelenmenin Kurulma Amacı, 2020, (Çevrimiçi) https://www.siberkume.org.tr/Index#close, Erişim Tarihi: 04.05.2020Industry. Forbes. 2018. (Çevrimiçi) https://www.forbes.com/sites/gilpress/2017/07/18/6-reasons-israel-became-a-cybersecurity-powerhouse-leading-the-82-billion-industry/#57c4d0e8420a. Erişim Tarihi: 17.04.2020

Saatçioğlu, Cem. “Ulusal Yenilik Sistemi Çerçevesinde Uygulanan Bilim ve Teknoloji Politikaları: İsrail, AB ve Türkiye Örneği”. **Sosyal Bilimler Dergisi**. S. 1. 2005. ss.179-198

Sabah. “Kamuya Siber Saldırı”. 2015. (Çevrimiçi) https://www.sabah.com.tr/ekonomi/2015/12/25/kamuya-siber-saldiri. ErişimTarihi: 02.05.2020

Sandıklı, Atilla ve Bilgehan Emeklier. "Güvenlik Yaklaşımlarında Değişim ve Döşüm". ***Teoriler Işığında Güvenlik, Savaş, Barış ve Çatışma Çözümleri***. Edt. Atilla Sandıklı. İstanbul: Bilgesam Yayınları. 2012.

Sancak, Kadir. **Uluslararası İlişkilerde Güç Kavramı ve Yumuşak Güç.** Ankara: Nobel Yayınları. 2016.

Schwab, Klaus. **Dördüncü Sanayi Devrimi**. Çev.: Zülfü Dicleli, İstanbul: World Economic Forum. 2017.

Schmidt, Nikola. "Cyber Security", In R. Ondrejcsák (Ed.). **Introduction to Security Studies**. Bratislava: Cenaa. 2014.

Sheldon, John B. "Toward a Theory Of Cyber Power Strategic Purpose İn Peace and War". **Cyberspace and National Security Threats, Opportunities and Power İn a Virtual World**. der. Derek S. Reveron, Washington: Georgetown University Press. 2012.

Shactman, Noah. "Exclusive: Computer Virus Hits U.S. Drone Fleet".2011. (Çevrimiçi). https://www.wired.com/2011/10/virus-hits-drone-fleet/. (Erişim Tarihi: 19.03.2020)

Shiftdelete.net. Zararlı Android Uygulamalarının Listesi, 2017. (Çevrimiçi) https://shiftdelete.net/zararli-android-uygulamalarinin-listesi-78856. Erişim Tarihi: 02.05.2020

Slaughter, Anne-Maria. "America's Edge: Power in the Networked Century". **Foreign Affairs Dergisi.** S.88, (Ocak/Şubat 2009), ss.94-113

Slideshare. Dijital 2020 Turkey (January 2020). 2020. (Çevrimiçi) https://www.slideshare.net/DataReportal/digital-2020-turkey-january-2020-v01?from_action=save. Erişim Tarihi: 24.04.2020

SIPRI. Sıprı Yearbook 2019 Armaments, Disarmament and International Security. Stockholm.2019.

Singer, P. W Allan Friedman. **Cyber Security and Cyber War : What Everyone Needs to Know**. New York: Oxford University Press. 2014.

Singer, P.W Allan Friedman. **Siber Güvenlik ve Siber Savaş**. Çev.: Ali Atav. Ankara: Buzdağı. 2018.

Smith, Craig S. "May 6-12; The First World Hacker War". (Çevrimiçi) https://www.nytimes.com/2001/05/13/weekinreview/may-6-12-the-first-world-hacker-war.html. 13 Mayıs 20012. (Erişim Tarihi: 18.03.2020)

Sönmezoğlu, Faruk. **Uluslararası Politika ve Dış Politika Analizi**. İstanbul: Der Yayınları. 2014.

Sönmezoğlu, Faruk Hakan Güneş, Erhan Keleşoğlu. **Uluslararası İlişkilere Giriş**, İstanbul: Der Yayınları. 2011.

Sönmezoğlu, Faruk. **Uluslararası İlişkiler Sözlüğü**. İstanbul: Der Yayınları. 2010.

Sönmezoğlu, Faruk Özgün Erler Bayır. **Dış Politika Karşılaştırmalı Bir Bakış** İstanbul: Der Yayınları. 2014.

Siber Bülten. "Rusya Siber Alanda Neden Saldırıyor?". 2015. (Çevrimiçi) https://siberbulten.com/uluslararasi-iliskiler/rusya-siber-alanda-neden-saldiriyor/. (Erişim Tarihi: 01.04.2020)

Spade, Colonel Jayson M. **China's Cyber Power And America's National Security**. Pennsylvania: US Army War College. 2012.

Srikumar, Madhulika. "Should BRICS Rally Around China's Call For Cyber Sovereignty?". Observer Research Foundation. 2017. (Çevrimiçi). https://www.orfonline.org/expert-speak/should-brics-rally-around-china-call-for-cyber-sovereignty/. Erişim Tarihi: 08.04.2020

STM. "**2017 Ocak-Mart Dönemi Türkiye Siber Tehdit Durum Raporu**". İstanbul, 2017.

STEGER, Manfred, B.; Küreselleşme (Çev. Abdullah Ersoy). Dost Kitabevi Yay. Ankara. 2006.

Şir, Aslan Yavuz. "Bölgesel Güvenlik Kompleksi Teorisi, Enerji Güvenliği ve Rusya''. **Global Strateji Enstitüsü 2.Sosyal Bilimciler Kongresi**. 2003.

Tatar, Ünal. **Siber Savaş ve Sanal Ortam Güvenlik Politikası**. Ankara: Tubitak. 2009.

Tabansky, Lior. Isaac Ben Israel. **Cybersecurity İn Israel**. London: Springer. 2015.

T.C Ulaştırma ve Altyapı Bakanlığı. Siber Güvenlik. 2020. (Çevrimiçi) https://www.uab.gov.tr/siber-guvenlik, Erişim Tarihi: 01.05.2020

T.C Ulaştırma ve Altyapı Bakanlığı. Siber Güvenlik. 2020. (Çevrimiçi) https://www.uab.gov.tr/uploads/pages/siber-guvenlik/2016-2019guvenlik.pdf Erişim Tarihi: 01.05.2020

T.C. Hazine ve Maliye Bakanlığı. 1 Milyon İstihdam Kullanıcı Klavuzu. 2020 (Çevrimiçi) https://1milyonistihdam.hmb.gov.tr/kilavuz/kilavuzKullanici.pdf. Erişim Tarihi: 01.05.2020

Tezken, Yılmaz. **Jeopolitikten Mili Güvenliğe**. İstanbul: Ülke Kitapları. 2005.

Timtchenko, İlya. “Shymkiv: Ukrainians Not Prepared for Cyber Attacks”. Kyiv Post. 2017. (Çevrimiçi) https://www.kyivpost.com/business/shymkiv-ukrainians-not-prepared-cyber-attacks.html. (Erişim Tarihi: 02.04.2020)

The New York Times. “Israeli Test on Worm Called Crucial in Iran Nuclear Delay”. 2011. (Çevrimiçi) https://www.nytimes.com/2011/01/16/world/middleeast/16stuxnet.html. Erişim Tarihi: 22.04.2020

The Ministry of Foreign Affairs of the Russian Federation. Natıonal Securıty Concept Of The Russıan Federatıon. 2000. (Çevrimiçi) https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/589768. (Erişim Tarihi: 26.03.2020)

The Ministry of Foreign Affairs of the Russian Federation. Doctrine of Information Security of the Russian Federation. 2000 (Çevrimiçi) https://www.mid.ru/en/foreign_policy/official_documents. (Erişim Tarihi: 28.03.2020)

The Ministry of Foreign Affairs of the Russian Federation, Doctrine of Information Security of the Russian Federation. (Çevrimiçi). https://www.mid.ru/en/foreign_policy/official_documents/-/asset_publisher/CptICkB6BZ29/content/id/2563163
2000. (Erişim Tarihi: 28.03.2020)

The White House Executıve Orders. “**Presidential Executive Order on Strengthening the Cybersecurity of Federal Networks and Critical Infrastructure**”. (Çevrimiçi). https://www.whitehouse.gov/, Erişim Tarihi: 08.03.2020.

The White House Office. Internatiomal Strategy For Cyberspace, Prosperity. Security and Openness in a Networked World. Washington. 2011.

The White House Office. Fact Sheet: Cybersecurity National Action Plan. Washıngton:2016. www.whitehouse.gov. (Erişim Tarihi: 10.03.2020).

The White House Office. National Cyber Strategy of the United States of America, Washıngton:2018. www.whitehouse.gov. (Erişim Tarihi: 12.03.2020).

The White House Office. U.S Departmen Of Homeland Security Cybersecurıty Strategy. Washıngton:2018. www.whitehouse.gov. (Erişim Tarihi: 14.03.2020)

The White House Office. Presidential Proclamation on National Cybersecurity Awareness Month. Washıngton:2018. www.whitehouse.gov. (Erişim Tarihi: 14.03.2020)

The New York Times. “The Russian Hacking in 200 Words”. (Çevrimiçi) https://www.nytimes.com/interactive/2016/12/29/us/politics/russian-hack-in-200-words.html. (Erişim Tarihi:19.03.2020)

The Guardian. Edward Snowden: The Whistleblower Behind The Nsa Surveillance Revelations. 2013, (Çevrimiçi) https://www.theguardian.com/world/2013/jun/09/edward-snowden-nsa-whistleblower-surveillance. Erişim Tarihi: 12.04.2020

The State Council Information Office The People’s Republic Of China. China’s Space Activities in 2016.(Çevirimiçi) http://english.scio.gov.cn/whitepapers/2017-01/10/content_40535777_2.htm. Erişim Tarihi: 08.04.2020

The Guardian. “Stuxnet Worm İs The 'Work Of A National Government Agency”. 2010. (Çevrimiçi) https://www.theguardian.com/technology/2010/sep/24/stuxnet-worm-national-agency. Erişim Tarihi: 22.04.2020

The Guardina. HummingBad Android malware: who did it, why, and is your device infected?. 2017. (Çevrimiçi) https://www.theguardian.com/technology/2016/jul/06/what-is-hummingbad-malware-android-devices-checkpoint. Erişim Tarihi: 02.05.2020

The New York Times. “A Silent Attack, but Not a Subtle One”. 2010, (Çevrimiçi) https://www.nytimes.com/2010/09/27/technology/27virus.html?_r=1. Erişim Tarihi: 22.04.2020

Time Turk. “5 Yıl Önce Mavi Marmara’da Ne Oldu?”. 2015. (Çevrimiçi) https://www.timeturk.com/5-yil-once-mavi-marmara-da-ne-oldu/haber-108512. Erişim Tarihi: 23.04.2020

Todaro, Mıcheal P. **Stephen C. Smıth, Economic Development**. Boston: Peorsen. 2016.

Torfox. “The Great Firewall of China: Background”. (Çevrimiçi) https://cs.stanford.edu/people/eroberts/cs181/projects/201011/FreedomOfInformationChina/the-great-firewall-of-china-background/index.html. Erişim Tarihi: 04.04.2020

Türk Havacılık Uzay Sanayi. Uzay Göktürk-1. 2009. (Çevrimiçi) https://www.tai.com.tr/urun/gokturk-1. Erişim Tarihi: 25.04.2020

Türk Havacılık Uzay Sanayi. Uzay Göktürk-2. 2012. (Çevrimiçi). https://www.tusas.com/urun/gokturk-2. Erişim Tarihi: 25.04.2020

Türk Havacılık Uzay Sanayi. Uzay Ürünleri. 2020. (Çevrimiçi). https://www.tusas.com/urunler/uzay. Erişim Tarihi: 25.04.2020

Türkiye Siber Güvenlik Kümelenmesi, Siber Güvenlik Kümelenmenin Kurulma Amacı, 2020, (Çevrimiçi) https://www.siberkume.org.tr/Index#close, Erişim Tarihi: 04.05.2020

Vuving, A.L. How Soft Power Works, Paper presented at the panel "Soft Power and Smart Power".American Political Science Association Annual Meeting.2009. (Çevrimiçi) https://ssrn.com/abstract=1466220.(Erişim Tarihi: 06.01.2020)

Vilidamir, Platov. "The USA and cyberwars". 2013. (Çevrimiçi). http://journal-neo.org/2013/10/15/rus-ssha-i-kibervojny-chast-1/. (Erişim tarihi 11.04.2020).

Volz, Dustin. "U.S. Government Concludes Cyber Attack Caused Ukraine Power Outage". Reuters, 2016, (Çevrimiçi) https://www.reuters.com/article/us-ukraine-cybersecurity/u-s-government-concludes-cyber-attack-caused-ukraine-power-outage-idUSKCN0VY30K. (Erişim Tarihi: 02.04.2020)

Yadak, Abdallatif. "İsrail Güvenlik Politikası ve Güvenlik Duvarının Filistin Halkına Etkileri". **21. Yüzyılda Eğitim ve Toplum Eğitim Bilimleri ve Sosyal Araştırmalar Dergisi**. 2014. C.3. S.9. ss. 163-175

Yesevi, Çağla Gül. İsrail ve ABD'nin Askeri ve İstihbari İttifakının Değerlendirilmesi ve Pollard Olayı. 2015. (Çevrimiçi) https://21yyte.org/tr/merkezler/israil-ve-abdnin-askeri-ve-istihbari-ittifakinin-degerlendirilmesi-ve-pollard-olayi. Erişim Tarihi: 24.04.2020

Yasevi, Çağla Gül. İsrail İstihbaratı ve Mossad, Ed. Ümit Özdağ. **İstihbarat Örgütleri**. Ankara: Kripto Yayınları. 2014.

Yalvaç, Faruk. "Uluslararası İlişkiler Kuramında Anarşi Söylemi". **Uluslararası İlişkiler Dergisi**, C.8, S. 29 (Bahar 2011), ss. 71-99.

Yılmaz, Sait. **Uzay Güvenliği**. İstanbul: Milenyum Yayınları. 2013.

Yılmaz, Sait. **Güç ve Politika**. İstanbul: Alfa Yayınları. 2008.

Yılmaz, Sait "Uluslararası İlişkilerde Güç ve Güç Dengesinin Evrimi". **Stratejik Araştırmalar Dergisi**. C.1, S.1. (2008). ss. 27-65

Yılmaz, Sait Yumuşak Güç ve Evrimi. **Turan Stratejik Araştırmalar Merkezi Dergisi**. Y.3 S.12. (2011). Ss.27-65

Yılmaz, Sait "ABD İstihbaratında Yaşanan Değişimler". **Turan Stratejik Araştırmalar Merkezi Dergisi**. C.4. S.13. (Kış 2012). ss.10-16

Yılmaz, Seda Şeref Sağıroğlu. "Siber Güvenlik Risk Analizi, Tehdit ve Hazırlık Seviyeleri". **6. Uluslararası Bilgi Güvenliği ve Kriptoloji Konferansı**. Ankara: Eylül. 2013.

Wedermye, Landon J. “The Changing Face of War: The Stuxnet Virus and the Need for International Regulation of Cyber Conflict”. Mıchgıan State Unıversıty College Of Law. 2012. (Çevrimiçi). https://digitalcommons.law.msu.edu/king/241/. (Erişim Tarihi: 25.03.2020)

Webrazzi. “Türkiye Siber Saldırılar Altında: Bilmeniz Gerekenler”. 2015. (Çevrimiçi) https://webrazzi.com/2015/12/25/turkiye-siber-saldiri-altinda-bilmeniz-gerekenler/. Erişim Tarihi: 02.05.2020

Wiltse, Evren Çelik. “Liberalizm, İş birliği, Kolektif Güvenlik ve Neoliberal Kurumsalcılık”. ed. Evren Balta. **Küresel Siyasete Giriş Uluslararası İlişkilerde Kavramlar, Teoriler ve Süreçler**. İstanbul: İletişim Yayınları.2014.

Waewer, Ole. “Toplumsal Güvenliğin Değişen Gündemi”. **Uluslararası İlişkiler Dergisi**. C.5, S. 18 (Temmuz 2008). ss. 151-178.