KARADENİZ TEKNİK ÜNİVERSİTESİ * SOSYAL BİLİMLER ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER ANABİLİM DALI

ULUSLARARASI İLİŞKİLER PROGRAMI

21. YÜZYIL GÜVENLİĞİNDE ASİMETRİK BİR MÜCADELE: SİBER UZAYDA DOĞU PERSPEKTİFİ

YÜKSEK LİSANS TEZİ

Muhammed Resul EROĞLU

OCAK - 2022

TRABZON

KARADENİZ TEKNİK ÜNİVERSİTESİ * SOSYAL BİLİMLER ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER ANABİLİM DALI

ULUSLARARASI İLİŞKİLER PROGRAMI

21. YÜZYIL GÜVENLİĞİNDE ASİMETRİK BİR MÜCADELE: SİBER UZAYDA DOĞU PERSPEKTİFİ

YÜKSEK LİSANS TEZİ

Muhammed Resul EROĞLU

Tez Danışmanı: Doç. Dr. Vahit GÜNTAY

OCAK - 2022

TRABZON

BİLDİRİM

Tez içindeki bütün bilgilerin etik davranış ve akademik kurallar çerçevesinde elde edilerek sunulduğunu, ayrıca KTÜ – Sosyal Bilimler Enstitüsü Tez Yazım Kılavuzu'na uygun olarak hazırlanan bu Çalışmada yararlanılan kaynakların tümüne eksiksiz atıf yapıldığını, aksinin ortaya çıkması durumunda her tür yasal sonucu kabul edeceğimi beyan ederim.

Muhammed Resul EROĞLU
10.01.2022

ÖNSÖZ

Günümüzde güvenlik ihtiyacının en önemli dinamiklerinden biri olarak görülen siber uzay, içinde bulunan aktör çeşitliliğinin artmasıyla birlikte güvenlik çalışmalarında tehdit algısını şekillendirerek terör kavramının da yeniden yorumlanmasına ışık tutmuştur. Teknolojik imkanlara erişen ve bu doğrultuda altyapı ve kurumlarını dijitalleştiren devletler, siber uzaya bağımlılıkları istikametinde kapasite ve yeteneklerini geliştirme yoluna gitmiştir. Çalışmanın ana dinamikleri, siber uzayın güvenlik ile ilişkilendirilmesi çerçevesinde oluşturulmuştur. Ayrıca siber uzayda kapasite ve güç artırımına giderek saldırı ve savunma mekanizmalarında önemli bir ivme kazanan Asya devletlerinin kurumsal mekanizmaları ve uygulamaları incelenecektir.

Bu tezde bilgi ve tecrübelerinden yararlandığım ve katkılarını esirgemeyerek tezin her aşamasında beni yönlendiren değerli danışmanım Doç. Dr. Vahit GÜNTAY'a, öğrenim hayatımda akademik düşünce yapımın şekillenmesine katkıda bulunan başta Doç. Dr. İsmail KÖSE olmak üzere Doç. Dr. Bülent ŞENER ve Doç. Dr. Özgür TÜFEKÇİ'ye teşekkür ederim.

Ocak, 2022 Muhammed Resul EROĞLU

İÇİNDEKİLER

ÜÇÜNCÜ BÖLÜM

ÖZET

Güvenlik ve terör kavramları, içerisinde bulunulan döneme göre şekil alan ve değişimler gösteren dinamik kavramlar olarak değerlendirilmektedir. Özellikle teknoloji ve sanayinin gelişimiyle birlikte bu kavramlar değişime uğrayarak zamanla yeni boyutlara ve yeni tanımlara kavuşmuştur. Savaşta konvansiyonel silahlar, güvenlikte de geleneksel anlayış yerini nükleer silahlar ve uluslararası güvenlik kavramlarına bırakarak caydırıcılık unsurunu da ortaya çıkarmıştır. Aynı zamanda geleneksel terörizm paradigmasına da yeni bir boyut olarak giren ve bu paradigmayı değiştirme potansiyeli taşıyan "siber terör" kavramı da önemli bir dinamik olarak karşılanmaktadır.

Soğuk Savaş'ın sona ermesiyle birlikte uluslararası sistemde çok kutuplu düzenin ortaya çıkması, Doğu devletlerinin bu sistemde kendilerini göstermesine ve Batı hegemonyasına karşı bir tutum sergilemesine olanak sağlamıştır. Bu bağlamda literatürde yeni bir kavram olarak giren siber uzay, devletlerin önemli bir mücadele alanı olarak değerlendirilmektedir. Aktör kavramının devlet-dışı veya devlet destekli aktörler olarak çeşitlenmesi sebebiyle asimetrik bir ortam olarak görülen siber uzayda gerçekleşen mücadele Asya devletlerinin güvenlik yaklaşımları ve saldırgan tutumlarını ileri bir boyuta sürüklemiştir.

Bu çalışmada nitel yöntem kullanılacak olup ilk olarak güvenlik ve teröre kavramsal çerçeveden bakılacaktır. Ardından 21. yüzyıl gerçeği olarak görülen siber uzay kavramının güvenlik ve terörle ilişkilendirilmesine değinilecektir. Batı ile aynı kampta bulunmayan Asya devletlerinin, başta Batı olmak üzere yakın çevresine yönelik saldırgan tutumları; devletlerin demokratik yapısı, rejim tipi ve yönetim şekilleriyle ilişkilendirilmiştir. Bu bağlamda siber güvenlik sınıflandırmasında yer alan Asya devletlerinin analiz edilerek alana katkı verilmesi amaçlanmaktadır.

Anahtar Kelimeler: Uluslararası Güvenlik, Siber Uzay, Siber Terör, Siber Güvenlik

ABSTRACT

The concepts of security and terrorism are evaluated as dynamic concepts that take shape and show changes according to the current period. Especially with the development of technology and industry, these concepts have changed and gained new dimensions and new definitions over time. Conventional weapons in war and traditional understanding in security have been replaced by nuclear weapons and international security concepts, revealing the deterrence factor. At the same time, the concept of "cyber terrorism" which has entered the traditional terrorism paradigm as a new dimension and has the potential to change this paradigm, is also evaluated as an important dynamic.

The emergence of a multipolar order in the international system with the end of the Cold War allowed the Eastern states to show themselves in this system and to display an attitude against the Western hegemony. In this context, cyberspace, which is a new concept in the literature, is considered as an important struggle area of states. The struggle in cyberspace, which is seen as an asymmetrical environment due to the diversification of the actor concept as non-state/supported actors, has advanced the security approaches and aggressive attitudes of Asian states.

In this study, the qualitative method will be used and firstly, security and terrorism will be looked at from a conceptual framework. Then, it will be mentioned that the concept of cyberspace, which is seen as a 21st century reality, is associated with security and terrorism. The aggressive attitudes of Asian states, which are not in the same camp with the West, towards their immediate surroundings, especially the West; The democratic structure of the states has been associated with the regime type and management styles. In this context, it is aimed to contribute to the field by analyzing the Asian states in the cyber security classification.

Keywords: International Security, Cyberspace, Cyber Terror, Cyber Security

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR LİSTESİ

AB	:	Avrupa Birliği
ABD	:	Amerika Birleşik Devletleri
AGİT	:	Avrupa Güvenlik ve İşbirliği Teşkilatı
APT	:	Advanced Persistent Threats
ARF	:	ASEAN Regional Forum
ARPA	:	Advanced Research Projects Agency
ASEAN	:	Güneydoğu Asya Ülkeleri Birliği
BARC	:	Bhaba Atom Araştırma Merkezi
BDT	:	Bağımsız Devletler Topluluğu
BM	:	Birleşmiş Milletler
CEC	:	China Electronics Corporation
CERT-EU	:	European Union Computer Emergency Response Team
CETC	:	China Electronics Technology Group
CIA	:	Central Intelligence Agency
CISA	:	ABD Siber Güvenlik ve Altyapı Güvenlik Ajansı
COURAGE	:	Cybercrime and Cyberterrorism European Research Agenda
Covid19	:	Koronavirüs
CTA	:	Merkezi Tibet Yönetimi
DAİŞ	:	Irak Şam İslam Devleti
DDOS	:	Distributed Denial of Service
DHS	:	İç Güvenlik Bakanlığı
ENISA	:	European Union Agency for Network and Information Security
e-posta	:	Elektronik Posta
ETA	:	Bask Yurdu ve Özgürlük
FBI	:	Federal Soruşturma Bürosu
FSB	:	Rusya Federal Güvenlik Servisi
FSO	:	Federal Koruma Servisi
FSTEC	:	Teknik ve İhracat Kontrollü Federal Servisi
GRU	:	Ana İstihbarat Direktörlüğü
IDDS	:	Brookings Institution, Institute for Defense and Disarmament Studies
IISS	:	Internationel Institute for Strategic Studies
IMPACT	:	The International Multilateral Partnership Against Cyber Threats
IoT	:	Internet Of Things

IRA	:	İrlanda Cumhuriyet Ordusu
IRC	:	Internet Relay Chat
ISP	:	Internet Service Provider
ITU	:	International Telecommunication Union
KGAÖ	:	Kolektif Güvenlik Antlaşması Örgütü
KII	:	Korea Information Infrastructure
KPA	:	Kore Halk Ordusu
MÖ	:	Milattan Önce
MS	:	Milattan Sonra
NATO	:	Kuzey Atlantik Antlaşması Örgütü
NCIRC	:	NATO Computer Incident Response Capability
NSA	:	Ulusal Güvenlik Ajansı
PLA	:	People's Liberation Army
PLASSF	:	People's Liberation Army Strategic Support Force
RAND	:	Research and Development
RGB	:	Genel Keşif Bürosu
RMA	:	Askeri İşlerde Devrim
RSAIH	:	Rus Sivil ve Askeri İstihbarat Hizmetleri
SIPRI	:	Stockholm International Peace Research Institute
SSCB	:	Sovyet Sosyalist Cumhuriyetler Birliği
SVR	:	Dış İstihbarat Servisi
SWIFT	:	Bankalar Arası Finansal Telekomünikasyon Derneği
ŞİÖ	:	Şangay İşbirliği Örgütü
T.C.	:	Türkiye Cumhuriyeti
TCP/IP	:	Transmission Control Protocol/Internet Protocol
TERENA	:	Trans-European Research and Educational Networking Association
UAB	:	Ulaştırma Denizcilik ve Haberleşme Bakanlığı

GİRİŞ

Devletler nezdinde güvenlik algısının şekillenmesi, 17. yüzyılın ortalarından itibaren ulus-devlet anlayışının oluşmasıyla birlikte modern güvenlik sisteminin başlangıcına tekabül etmektedir. Bu dönemden itibaren güvenlik anlayışı, dünya siyaseti üzerinde her geçen dönem şekillenerek değişimler göstermiş ve farklı yorumların da oluşmasıyla birlikte literatürde daima tartışılan bir konu olmuştur. 20. yüzyılın başlarından itibaren teknolojik imkanların artması nezdinde küreselleşen dünya, modern hayata geçişi hızlandırarak endüstrileşmenin yeni boyutlar kazanmasına ışık tutmuştur.

Soğuk Savaş'ın sonlarına doğru teknolojik alanda çok daha kapsamlı yeniliklerin ortaya çıkması, devletlerin bilgiye erişimini mümkün kılmıştır. Öyle ki siber yetenekler noktasına vurgu yapan ve bu alanda kapasite artırma çabasında olan çoğu hükümet, başta devletler olmak üzere siber uzayda yer alan devlet-dışı aktörleri tehdit çemberine almıştır. Siber uzayda devlet destekli ve/veya devlet-dışı aktörlerin oluşturduğu çatışma ortamı, siber terör kavramının literatürde tartışılmasına gerekçe olmuş ve siber uzayı, uluslararası örgütlerin de dahil olduğu çok denklemli bir ortam haline getirmiştir. Siber kapasitelerini geliştiren pek çok devlet, sorun yaşadığı devletlere yönelik saldırgan tutumlar göstermektedir. Bilgiye erişimin siber uzay çerçevesinde mümkün olması, henüz kapsamlı bir yasal düzenlemenin gerçekleşmemesi ve saldırıyı gerçekleştiren kişi(ler)in kimliklerinin kesin olarak tespit edilmesinin zorluğu, siber uzayda devletlerin saldırı motivasyonunu artırmaktadır.

Bu çalışmanın temel araştırma soruları şu şekilde oluşturulmuştur: Siber uzaydaki aktör çeşitliliği, geleneksel güvenlik ve terör anlayışını nasıl etkilemiştir? Çalışmada incelenen Asya devletlerinin saldırganlık nedenleri ve devletlerin saldırganlık tutumlarının demokratik yapısı, rejim tipi ve yönetim şekilleriyle olan ilişkileri nelerdir? Bu araştırma soruları üzerinden şekillenen çalışmanın temel hipotezi Batı karşıtı devletlerin siber uzayda daha saldırgan olduğu üzerine oluşturulmuştur. Bu hipotezi kanıtlamak için Asya devletleri, incelenmiştir. Çalışmanın amacı "Siber uzay kavramını analiz etmek ve literatürde yapılan çalışmalara değinmek, siber uzaydaki aktörleri, amaçlarını ve araçlarını incelemek ve Asya devletlerinin güvenlik yaklaşımlarını ve saldırgan tutumlarını analiz etmek" olarak belirlenmiştir. Yapılan literatür taramasında realist paradigmadaki geleneksel güvenlik ve terör anlayışının 1990'larla birlikte eleştirel güvenlik çerçevesinde tartışılmaya başlandığı görülmüştür. Eleştirel güvenlikle birlikte devlet dışı aktörlerin de referans nesnesi olarak kabul edilmesi, siber güvenlik olgusunun disiplin içerisinde inşacı çerçeveden tartışılmasını mümkün kılmıştır.

Eleştirel kaynak incelemesi ve nitel araştırma yönteminin kullanıldığı bu çalışmada açık kaynaklardan elde edilen makaleler, kitaplar, tezler ve bağımsız kuruluşların raporlarından yararlanılmıştır. Aynı zamanda hipotezi desteklemek adına çok sayıda veri, tablo ve şekillere aktarılmıştır. Literatürde siber uzaya yönelik yapılan önemli katkılar ayrıntılı bir şekilde verilmeye çalışılmıştır. Ayrıca tezde incelenecek olan Asya devletlerinin siber güvenlik perspektifleri ve kurumsal mekanizmalarına yönelik yoğunlaştırılmış çalışmalar yeterince bulunmadığı için literatürde bir eksiklik mevcuttur. Bundan dolayı eksikliğin giderilmesi ve özgün bir çalışma oluşturulması için çalışmanın odak noktası bu alan üzerine belirlenmiş ve çoğunlukla devletlerin resmî belge ve raporlarına başvurulmuştur.

Üç bölümden oluşan çalışmanın *Kavramsal Çerçevede Uluslararası Güvenlik ve Terör* adlı ilk bölümünde güvenlik ve terör çalışmalarının kapsamıyla bu kavramların siber uzaya taşınması aktarılmıştır. Aynı zamanda güvenlik teröre yönelik yapılan tanımlar, kavramların yeniden yorumlanmasını ve tartışılmasını mümkün kıldığı için bu kavramların teorik tahlili yapılarak günümüze kadar geldiği süreç ve 21. yüzyıldaki halinin teknolojiyle bağlantısı kapsamlı olarak analiz edilmiştir.

Çalışmanın *Uluslararası Güvenlikte Yeni Bir Alan: Siber Uzay* isimli ikinci bölümünde 21. yüzyılda güvenlik algısının değişmesi ve terör kavramının yeniden yorumlanması iki farklı olay çerçevesinde incelenmiş ve dönüm noktası niteliğinde olduğu yorumu yapılmıştır. Bununla birlikte siber uzay kavramının tanımı ve alana yapılan katkılar aktarılarak siber uzayda yer alan aktörler, kullandıkları silahlar ve uluslararası aktörlerin siber güvenliğe bakış açısı analiz edilmiştir.

Uluslararası Güvenlikte Yeni Bir Alan: Siber Uzay adındaki üçüncü bölümde ise siber uzayda doğu perspektifi yansıtılmaya çalışılmış ve siber uzayda saldırganlık unsuruyla paralellik kurulmuştur. Siber uzayda saldırgan devletlerin büyük bir kısmının Asya bölgesinde yer aldığı hipotezinden yola çıkılarak çalışmanın üçüncü ve son bölümünde detaylı olarak bu bölgeden bahsedilmiş ve devletlerin neden saldırgan olduğu analiz edilmiştir. Ardından siber güvenlik sınıflandırmasına yer alan Asya devletlerinin (sırasıyla Çin, İran, Rusya, Kuzey Kore, Hindistan, Güney Kore ve Japonya), mevcut konjonktürdeki durumları, kurumsal mekanizmaları ve uygulamaları incelenerek sonuca gidilmiştir.

BİRİNCİ BÖLÜM

1. KAVRAMSAL ÇERÇEVEDE ULUSLARARASI GÜVENLİK VE TERÖR

Devletler için olmazsa olmaz bir kavram olan güvenlik, ulus-devletin ortaya çıkışından itibaren güncelliğini ve önemini koruyarak ilerlemiştir. Tarih boyunca her bir aktörün güvenlik algısı bulunduğu coğrafya içerisinde karşılaştığı tehditler nezdinde değişiklikler göstermiştir Her devlet için hem iç hem de dış güvenlik açısından benzer kaygılar var olmaktadır. 20. yüzyılın ilk yarısından itibaren siyasi olaylar, küreselleşmeden etkilenerek uluslararası ilişkiler literatürüne güvenlik nezdinde yeni yaklaşımları beraberinde getirmiştir. Nitekim *Uluslararası Güvenlik* kavramı ilk olarak 20. yüzyılın ilk yarısından itibaren ortaya çıkmış olup, bu kavramı tetikleyen yegâne unsur, dönemin mevcut konjonktüründe kendisini iyiden iyiye gösteren ve uluslararası bir boyut kazanan terör olmuştur.

1.1. Uluslararası İlişkiler ve Güvenlik

Uluslararası sistemin bir denge içerisinde bütünlüğünü koruyabilmesi için güvenlik, devletler açısından süreklilik arz eden bir ihtiyaçtır. Şüphesiz devletlerin birbirleriyle ilişki içerisinde bulunduğu zamanlarda en çok dikkat ettikleri husus, kendi güvenlikleri olmuştur. Kendini sürekli bir şekilde yenileyen bu durum, uluslararası ilişkiler disiplininin tarih boyunca devamlı olarak güvenlik eksenli ilerlemesine ışık tutmaktadır. Yüzyıllar boyunca süregelen güç mücadelelerinde değişen güvenlik algılarının tarihsel olaylara direkt veya dolaylı yoldan etkisi, disiplin içerisinde belirgin bir şekilde gözlemlenmektedir.

1.1.1. Uluslararası Güvenlik Kavramının Tarihsel Gelişimi

Epistemolojik açıdan zengin tanımları içerisinde barındıran güvenlik kavramı, doğal ve beşerî etkileriyle birlikte evrimleşerek mevcudiyetini sürdüren ve bilimsel olarak tartışılan bir dinamik olarak değerlendirilmektedir. Akademik anlamda güvenlik çalışmalarının adından en çok söz ettirdiği dönemler, dünya siyasetinde güvensizlik ikileminin yüksek olduğu dönemler olarak adlandırılmaktadır. Walt (1991), Soğuk Savaş yıllarını güvenlik çalışmalarının zirve yaptığı bir dönem olarak nitelendirmektedir.

Güvenlik kavramının akademik çerçevede incelenmesinin Soğuk Savaş dönemi itibariyle başlaması, güvenliğin çeşitlenmesine zemin hazırlamıştır. 1950'li yıllardan günümüze çehresi ve

kapsamı genişleyen güvenlik, farklı tanımlarda incelenerek içerik ve nitelik olarak da zenginlik kazanmıştır. Bunlara örnek olarak insani güvenlik, bölgesel güvenlik, eleştirel güvenlik, çevre güvenliği ve konstrüktivist güvenlik gibi çeşitli alanlarda incelenmektedir. Ancak güvenlik kavramının tarihsel gelişimi hakkında yapılan antropolojik çalışmalar, diğer çalışmalara oranla biraz da kısıtlı kalmıştır. Birdişli (2020: 238)'ye göre bu alanda yapılan az sayıda çalışma daha çok kimlik, ırk ve etnik gibi sadece antropolojik temelde incelendiğinden dolayı uluslararası ilişkiler çerçevesinde güvenliğin tarihsel gelişimine akademik ilgi sınırlı seviyede kalmıştır. Güvenliğin tarihsel gelişimi hakkında çalışmalarda önde gelen isimler[1] Soğuk Savaş dönemi sınırlarından geriye gitmek yerine, bu yıllar çerçevesinde gelişen olayları incelemişlerdir.

17. yüzyılda ulus-devlet anlayışının oluşması, modern güvenlik sisteminde bir milat olarak değerlendirilmekte ve literatürde kabul görmektedir. Fakat ilk çağlardan 17. yüzyıla kadar güvenlik kavramının ne gibi aşamalardan geçtiğine dair örnekler, akademik çerçevede oldukça kısıtlı kalmıştır. Heywood (2018: 116), insanlığın başlangıcı olarak kabul edilen Milattan Öncesi (MÖ) dönemden, 17. yüzyıla kadar geçen süreyi *Primitif Güvenlik Dönemi* olarak adlandırmıştır. Kolektif bilinç oluşana kadar insan hayatını fizyolojik ihtiyaçlar ve güdüler şekillendirmiştir. Bu ihtiyaçlar, insanlarda var oluş, beslenme, üretim gibi temel çıkarlara dayalı tehdit ve güvenlik sorularına zemin hazırlamıştır. Bu dönem ayrıca kendi içerisinde *Pre-Teolojik ve Proto-Teolojik Güvenlik Dönemi* olarak ikiye ayrılmaktadır (Heywood, 2018: 117). 1648 Westfalya Anlaşması'ndan Soğuk Savaş dönemi sonlarına kadar süren dönem *Modern/Sistemik Güvenlik Dönemi,* (bu dönem de kendi içerisinde *Güç Koalisyonları Dönemi ve Güç İttifakları Dönemi* olarak ikiye ayrılır.*)* 1990'dan günümüze kadar gelen dönem ise *Post-Modern Dönem* olarak belirtilmektedir (Birdişli, 2020a: 239).

Tablo 1: Güvenliğin Tarihsel Gelişimi

I. Primitif Güvenlik Dönemi (MÖ-MS 1648)
I.I. Pre-Teolojik Güvenlik Dönemi
I.II. Proto-Teolojik Güvenlik Dönemi
II. Modern/Sistemik Güvenlik Dönemi (1648-1990)
II.I. Güç/Güvenlik Koalisyonları Dönemi (1815-1945)
II.II. Güç İttifakları Dönemi (1945-1990)
III. Post Modern Güvenlik Dönemi (1990 ve sonrası)

Kaynak: Birdişli, 2020

Pre-Teolojik Güvenlik Dönemi, insanların çevresinde gerçekleşen tüm eylemlerin kudretini algılanan her şeye atfetmekle açıklanmaktadır. Bunlar da toplumun, gözle görülen kavramlara daha kutsal anlamlar yüklemesine olanak sağlamıştır. Üreterek geçim sağlama temelinde doğayla iç içe

[1] Güvenliğin tarihsel gelişimi noktasında literatürde önemli yere sahip olan Barry Buzan, Ole Waever, Stephen M. Walt gibi isimler, disiplin içerisinde yaptığı çalışmalarla güvenlik kavramının anlaşılmasına ve yorumlanmasına önemli katkılarda bulunmuştur. Ayrıntı için bkz, (Birdişli, 2020a: 239).

geçen bu dönemin en belirgin özelliği, kişisel veya kitlesel çaba ile elde edilen hane, toprak, gıda gibi özel mülklerin korunmaya çalışılması olmuştur. Bu unsurların korunduğu ölçüde bir üst otoriteye ihtiyaç duyulmuştur (Şenel, 2017). *Proto-Teolojik Güvenlik Dönemi*, yerleşik hayattaki nüfusun artması dolayısıyla güvenlik ihtiyacının daha da genişleyerek boyut kazandığı ve devletin ilk olarak ortaya çıktığı dönem olmuştur. *Proto-teolojik* dönemin üretim biçimine dayalı olarak iki farklı yapıyı içerisinde barındırdığı görüşü savunulmuştur. Bu görüşe göre, neolitik çiftçiler ve neolitik çobanlar olarak iki farklı tabaka ortaya çıkmıştır. Çiftçi tabakası için toprak, ekilip biçilerek faydalanılan bir yerin yanında sosyokültürel yaşamın da üstünde geçtiği bir yapıdır ve tehdit gördüğü zaman, koşullar neyi gerektiriyorsa onu yapmayı öncüller. Çiftçi tabakaya göre ana amaç, "vatan" olarak görülen toprağın korunması, mümkün olduğu çerçevede de genişletilmesidir (Şenel, 2017). Neolitik çoban tabakası, üretim kolunda olmadıklarından dolayı ticaret vasıtasıyla elde ettiği deneyimler sayesinde varlıklarını birbirlerine bağlı bir şekilde, aidiyet çerçevesinde sürdürmeye gayret göstermişlerdir. Çünkü bu tabakadaki dayanışma, çiftçi toplumlara nazaran daha kuvvetli olduğundan dolayı *Asabiyet*[2] kavramıyla ilişkilendirilmektedir.

İnsanlığın tarih boyunca yaşam alanları, faaliyetleri ve tercihleri genişledikçe, ihtiyaçları da o orantıda değişim göstermiştir. Özellikle belirli yaşam alanlarının oluşmasından sonra sosyal ve etnik kimliklerin oluşması kabile tipi yaşam tarzını meydana getirmiş, bu da doğal olarak güvenlik ihtiyacını doğurmuştur. Mülkiyet, bireysel ve kitlesel güvenliğin sağlanma arzusu, güvenlik organizasyonu açığını doğurmuş ve bu sorumluluğu *Proto-teolojik* dönemde devlete üstlenmiştir. Heywood (1997), somut anlamda güvenlik örgütlenmesini ilk olarak devletin oluşturduğunu söylemiştir. Geleneksel anlamda devlet, güvenliği tesis etmek adına sorumlu tek mercii olarak değerlendirilmiş, güvenliğini sağlamak için de yetkilerinin sınırsız olduğu vurgusu yapılmıştır. Devletin yetkilerinin sınırsızlığı, kendisine atfedilen anlam genişliğini de zenginleştirmiştir. Özellikle *Proto-teolojik* dönemde devlet, kutsal bir yapı olarak görülerek Tanrı ile arasında ilişki kurulmuştur. Böylece devlet yapısı, dini otoriteler tarafından korunmaya çalışılmıştır (Birdişli, 2020a: 242).

Güvenlik kavramı, 17. yüzyıl öncesi dönemlere bakıldığında başat aktörün ve referans nesnesinin devlet olmasıyla ilişkilendirilmektedir. Modern sistem olarak kabul edilen 1648 Westfalya Anlaşması'yla birlikte güç kazanan ulus-devlet algısı, ulusal zemini garanti altına almayı ve siyasetin kaynağını din gibi toplum dışı bir varlık yerine direkt topluma adayarak ulus olma bilincini öncelemiştir. 1789'daki Fransız Devrimi, devletlere ulus olma bilincinin yanında ulusal iradeyi gerçekleştirmeyi de mümkün kılmıştır. Bu çerçevede devlet, dini veya herhangi farklı bir dış

[2] Asabiyet *(Asabiyye)*, İbn-i Haldun tarafından tasvir edilen, birlikte yaşayan bir grup içindeki aidiyet ve yardımlaşma duygusunun yüksek olmasından ötürü grup dayanışmasının da öteki olana karşı mücadelede bir ilham kaynağı oluşturduğu olarak yorumlanmaktadır. *İbn Haldûn'a göre asabiyet, en iptidai şekliyle, beşerin tabiatında bulunan zulüm ve düşmanlık temayüllerine karşı yine aynı tabiattan gelen akraba gibi yakınlara acıma duygusunun doğurduğu yardımlaşma ve dayanışma eğilimidir.* Ayrıntı için bkz, (İslam Ansiklopedisi, 1991).

etmenin etkisi altında kalmaksızın hür iradesiyle kararlar alabilecek, ulusal çıkarları gereği işbirlikleri kurabilecektir (Waltz, 1988). Nitekim dönemin düşünürleri de bu algının şekillenmesinde önemli role sahiptir. Hobbes, Machiavelli gibi realist düşünürler, devletlerarası ilişkileri güç mücadelesiyle açıklamaktadır ve devletler arasında daimî bir barışın sağlanmasına olanak vermemektedir. Bu çerçevede realistler, Kant'ın vurguladığı barışçıl çizgiden uzak bir perspektif çizmişlerdir.

Güvenlikte modern dönem, 1990 sonlarına doğru süren ve kendinden sonraki dönemlerin sebebi olarak nitelendirilen uzun bir dönemdir. Şüphesiz bu dönem; devletler arasında yaşanan sayısız savaş ve siyasi gerilimi, sosyoekonomik ve sosyokültürel devrimleri, tüm dünyayı ilgilendiren iki büyük savaş ve Soğuk Savaş'ı içerisinde barındırdığından dolayı akademik disiplin içerisindeki zenginliğin de yegâne kaynağı olmuştur. Napolyon Savaşları ve II. Dünya Savaşı yılları arasındaki dönem, *Güç/Güvenlik Koalisyonları Dönemi* olarak adlandırılmaktadır (Birdişli, 2020a: 244). Bu dönemde ilk göze çarpan husus, uluslararası hukukun ve devletlerarası işbirliğinin oluşturulmaya çalışılmasıdır. Nitekim devletlerarası güvenliği ve işbirliğini tesis etmek amacıyla 1815 yılında gerçekleştirilen Viyana Kongresi ve I. Dünya Savaşı sonrasında yapılan Paris Barış Konferansı önemli doneler sunmaktadır. Bu zirvelerden çıkarılacak sonuç, devletlerin savaşa son vermek amacıyla çeşitli işbirliklerine başvurarak kolektif güvenlik oluşturmaya çalışmasıdır (Üçarol, 2015).

Modern/Sistemik Güvenlik Dönemi içerisinde II. Dünya Savaşı'ndan Soğuk Savaş dönemi sonuna kadar süren dönem, *Güç İttifakları Dönemi* olarak tanımlanmaktadır (Birdişli, 2020a: 246). Bu dönemde uluslararası güvenlik, iki zıt kutbun çehresinde gerçekleşmiş ve bölgesel ittifakları da beraberinde getirmiştir. Kuzey Atlantik Antlaşması Örgütü (NATO) ve Varşova Paktı'na dahil olmayan devletler, ciddi güvenlik riskleri yaşayacağından taraf seçmeye zorlanmıştır. Üçüncü bir seçeneğin 1961'e kadar[3] dile getirilmediği ve Arıboğan (2017)'ın da gri olarak nitelendirdiği bu konjonktürde siyasi kamplaşmaya yönelik eğilim giderek artmıştır. Anarşik bir düzlemde giden uluslararası sistem, devletlerin birbirlerine beslediği güven duygusunu minimize etmiştir. Güvenlik ikileminin şiddetinin yoğun olduğu bir siyasal ortamda devletler, birbiriyle işbirliği yerine çatışmaya ve çözümsüzlüğe daha yatkın bir karakter ortaya koymuşlardır. Keza Soğuk Savaş dönemi de bu ortamdan nasibini fazlasıyla almıştır. Bu dönemde güvenlik, devlet politikalarının ana ekseninde yer almıştır. Öyle ki 1947 yılında Amerika Birleşik Devletleri (ABD)'de yürürlüğe konulan Ulusal Güvenlik Yasası, ilerleyen yıllarda Sovyet Sosyalist Cumhuriyetler Birliği (SSCB)'ne yönelik güvenlik kaygılarının artacak olmasına karşın bir hukuksal mekanizma niteliğindedir. Bu durum, Soğuk Savaş döneminin NATO ve Varşova Paktı arasındaki mücadele döneminin güvenlik

[3] Yugoslavya, Endonezya, Hindistan, Mısır, Gana ülkelerinin öncülüğünü yaptığı ve bu ülkeler haricinde 115 ülkenin üye olduğu Bağlantısızlar Hareketi, iki bloka da dahil olmak istemeyip, üçüncü bir yol arayışına giden ülkelerin; *üye ülkelerin millî bağımsızlığını, egemenliğini, toprak bütünlüğünü ve güvenliğini, sömürgecilikten, yayılmacılıktan, ırkçılıktan ve her türlü dış baskı, istila, işgal ve dış müdahaleden* korumayı amaçladığı bir girişimdir. Ayrıntı için bkz, (Brown, 1966).

anlayışının temellerini oluşturmuştur (Birdişli, 2010: 223). İki kutuplu sistem, devletleri sürekli güvensizliğe yönelterek dönemin hâkim ideolojisi olan realizm ile paralel ilerlemiştir.

20. yüzyılın ortalarında çağdaş realistler olarak adlandırılan Mearsheimer ve Waltz gibi düşünürler, klasik yaklaşımdan farklı olarak devletlerin birbirleriyle güvenliği sağlamak adına çeşitli amaçlarla bir araya gelebileceğini, ilişkilerin kurulabileceğini ve işbirliklerinin karşılıklı fayda çerçevesinde sınırlı bir şekilde yapılabileceğini vurgulamışlardır (Mearsheimer, 1994: 19-22). Nitekim bu anlayış, 20. yüzyılın sonlarına doğru kendisini iyiden iyiye hissettirerek güvenlik kavramının tartışılmasına ve yapılan tartışmalar ışığında yaşanan tarihi olaylarla birlikte kavramın boyut değiştirmesine katkı sağlamıştır. Örneğin Buzan, 20. yüzyılın sonuna doğru güvenlik kavramının tanımını genişletmiş ve içerisine siyasi, ekonomik, sosyal, çevresel ve askeri boyutları da katmıştır (Baylis 2008: 73). Klasik güvenlik anlayışının giderek azaldığı bu dönemde güvenlik kavramı, Soğuk Savaş'ın sona ermesiyle birlikte kendisini yeni kalıplar, yeni yorumlar içerisinde bulmuştur. 1990 ve sonrası dönem, *Post-Modern Güvenlik Dönemi* veya *Yeni Güvenlik Stratejileri Dönemi* olarak adlandırılmaktadır. Bu döneme post-modern denilmesinin sebebi, uluslararası sistemde yaşanan güç boşluğunun, kimlik arayışlarının ve güvenlik bunalımlarının yarattığı muğlaklık olarak görülmektedir. Muğlaklık kavramı, uluslararası ilişkiler disiplini içerisinde ilk olarak Arnold Wolfers tarafından kullanılmıştır. Wolfers (1952), algılanan tehditlere karşı savunma mekanizması geliştirmek için tehditlerin, araçların, değerlerin ve maliyetlerin ne olduğunun belirlenmesi gerektiğini savunmuştur (Birdişli, 2020b: 247). 1990 sonrası dönemde devletlerin içerisinde bulunduğu belirsizlik ortamı, dönem konjonktürünün post-modern güvenlik çerçevesinde değerlendirilmesine ışık tutmuştur. Birey temelli güvenlik kaygısının sıklıkla dile getirilmesi, güvenliğin sınıflandırılmasında aktör sayısını ve çeşitliliğini de arttırmakla birlikte çalışmanın ana konusu olan uluslararası güvenlik kavramını daha görünür kılmıştır.

1.1.1.1. Klasik Güvenlik Yaklaşımı

Klasik, diğer bir deyişle geleneksel güvenlik olarak adlandırılan bu yaklaşımda ana aktör devlet olmuştur. Westfalya sürecinden başlayıp Soğuk Savaş döneminin sonuna kadar kendisinden daha yoğun bir şekilde bahsedilen klasik güvenlik yaklaşımı, ulusal güvenlik kaygılarının yoğun olduğu, çözümsüzlük halinde savaşa başvurulduğu ve bu savaşlarda konvansiyonel silahların kullanıldığı bir ortamla ilişkilendirilmektedir. Ulus-devlet örgütlenmesinin oluşturduğu güvenlik ikileminde devletler, kendi ulusal çıkarlarını maksimize etmek için mücadele etmektedir. Bu anlayış içerisinde sürekli olarak devletler işbirliğinden uzak, anarşik bir ortamda varlıklarını sürdürmek zorunda kalmaktadır. Şüphesiz bu ortam, dönemin hâkim ideolojisi olan klasik realizmin bir tezahürü niteliğindedir.

I. Dünya Savaşı'ndan sonra meydana gelen ekonomik, siyasal ve sosyal sıkıntıları gidermek için atılan barışçıl adımlar, kısa süre sonra II. Dünya Savaşı'nın patlak vermesiyle sonuçsuz

kalmıştır. İki savaş arası uluslararası sistem, literatürde daha çok kendisinden sonra gelecek dönemin ne olacağına dair öngörülerin tartışıldığı bir dönem olarak bilinir. Bu dönemin I. Dünya Savaşı'nın sonucu mu yoksa II. Dünya Savaşı'nın sebebi mi olduğu disiplin içerisinde tartışılan bir olgu olmuştur. İki savaş arası dönem şüphesiz kendinden bir önceki ve bir sonraki dönemi birbirine bağlayan köprüdür. Bu dönem, I. Dünya Savaşı sonrası sistemi barışçıl temellere ve işbirliğine dayandıran idealizmin izinin yavaş yavaş silindiği ve güvensizliğin hiç olmadığı kadar yoğun yaşanacağı yeni bir döneme geçişin temellerinin atıldığı bir dönem olarak da nitelendirilebilir. Neorealist düşünür olan Edward Hallett Carr, iki savaş arası dönemde yazdığı "The Twenty Years Crisis" kitabı ile idealist yaklaşıma kapsamlı eleştiriler getirmiştir. Düşünsel altyapısını Machiavelli ve Hobbes'tan alan Carr, devletlerin güçlerinin daha da çok artırmasını isteyeceğini vurgulayarak böyle bir ortamda barışın sağlanmasının imkânsız olduğuna değinerek daha çok savaşın analiz konusu olması gerektiğini vurgulamıştır (Bakan ve Şahin, 2018: 140).

Neorealist yaklaşıma göre devletlerin sınıflandırılmasında temel kıstas, askeri yeterliliktir. Bir diğer deyişle bir devlet askeri alanda ne kadar güçlüyse, kendisini o kadar güvende hissetmektedir. Bu çerçevede koşullar dahilinde Mearsheimer (1995) ve Jervis (1978)'e göre devletler, saldırgan ve savunmacı olarak sınıflandırılmaktadır. Jervis (1978)'e göre bir devletin savunmacı olması, savaş çıkma ihtimalini minimize etmektedir ve devletleri iletişime sevk etmektedir. Mearsheimer (1995)'a göre ise devletler, saldırgan çizgide çıkarlarını maksimize etmek için karşı devletin kazanımlarını minimize etmelidir. Nitekim uluslararası sistem gereği ittifakların da kalıcı olmayacağı savunulmaktadır. Keza aynı şekilde Morgenthau (1970)'ya göre insanın özünde çıkar olması, devletlerin karakterleriyle örtüşmektedir ve bu da sürekli çatışmayı doğurmaktadır. Bundan kaçınmanın yolu ise üst otoriteye başvurmakla açıklanmaktadır (Haser, 2018: 16).

Soğuk Savaş döneminde oluşan iki kutup, güç dengesi üzerine inşa edilerek birey ve toplum temelli güvenlik kaygılarını ikinci plana atmıştır. 20. yüzyılın sonuna doğru devletlerin güvenlik temelinde işbirliği yapabileceğine yönelik tartışmalar, birey temelli güvenliğin oluşturulmasına zemin hazırlamıştır. Özellikle Soğuk Savaş'ın sona ermesi, eleştirel güvenlik anlayışının daha somut bir çerçevede dile getirilmesine olanak sağlamıştır.

1.1.1.2. Eleştirel Güvenlik Yaklaşımı

Soğuk Savaş dönemi sonrası güvenlik çalışmalarının ilgi noktası, ulusal güvenlikten uluslararası güvenliğe doğru dönüşüm gerçekleştirmiştir. Güvenlik çalışmalarında 20. yüzyılın sonuna doğru kimlik, şiddet, risk ve korkuların nedenleri de incelenmiş ve güvenlik anlayışı çeşitlenmiştir. Bu çerçevede geleneksel güvenlik, yerini teorik altyapısını idealizmden alan eleştirel yaklaşıma bırakmıştır. Ayrıca bu dönemden itibaren uluslararası güvenlik çalışmalarında sadece sonuçların değil, nedenlerin de konuşulduğu bir alan meydana gelmiş ve böylece savaşla birlikte savaşın ardında bıraktığı sosyal ve kültürel sonuçlar da incelenmeye başlamıştır. 1970'li yıllardan

itibaren yeni bir boyut kazanan güvenlik çalışmaları önemli siyasal olaylardan etkilenmiştir. Walt (1991), 1970'lerde Vietnam Savaşı'nın bitişiyle birlikte Ford Vakfı'nın birçok akademik çalışmaya öncülük edip ekonomik destek vermesinin yeni güvenlik yaklaşımında dönüm noktası olduğunu belirterek eleştirel güvenlik çalışmalarını uluslararası ilişkilerde bir rönesans olarak nitelendirmiştir. Ayrıca Walt (1991)'a göre eleştirel güvenlik çalışmaları, askeri gücün rolü hakkında kümülatif bilgiye ulaşmayı hedeflemektedir (Birdişli, 2010: 234).

Walt (1991), Soğuk Savaş'ın sonlarına doğru; devletlerarası güven ilişkilerine, işbirliklerinin niteliğine, caydırıcılık ilkesi ve nükleer stratejilerin uygulanabilirliğine, konvansiyonel savaşın dönüşümüne, ABD'nin askeri ve diplomatik anlamda oluşturduğu "büyük strateji" teorisine[4], uluslararası ilişkiler teorilerinin realizm ve liberalizm çerçevesinde güvenlik çalışmalarına etkisine değinmiştir. Bu çerçevede Research and Development (RAND)'ın güvenlik çalışmalarının akademik perspektiften incelenerek alanının genişlemesi ve Internationel Institute for Strategic Studies (IISS), Brookings Institution, Institute for Defense and Disarmament Studies (IDDS), Stockholm International Peace Research Institute (SIPRI) gibi yeni düşünce kuruluşlarının da ortaya çıkmasının güvenlik yaklaşımlarının dönüşümüne katkı sağladığı şeklinde yorumlamıştır (Walt, 1991: 215-222).

Eleştirel güvenlikte analiz seviyesi olarak birey, toplum ve kültürlerarası etkileşim referans alınmıştır. Bu doğrultuda Özgün ve Özgürleştirici Güvenlik Yaklaşımları, eleştirel güvenliğin sınıflandırılmasına önemli bir rol oynamıştır. Özgün Güvenlik Yaklaşımı John Galtung'un başını çektiği Yapısal Şiddet anlayışı ve Feminist Güvenlik Teorilerinden meydana gelirken, Özgürleştirici Güvenlik Yaklaşımı ise Galler (Frankfurt) Ekolü ve Paris Ekolü tarafından temsil edilmektedir. Klasik ve eleştirel güvenliğin her ikisini de içerisinde barından konstrüktivist güvenlik (Kopenhag Ekolü); birey, toplum ve devleti aynı anda analiz merkezine tabi tutmaktadır. Konstrüktivist güvenlik yaklaşımının önemli temsilcileri Buzan ve Hansen (2009: 209-215), bu güvenlik anlayışını düzensiz (discursive) olarak adlandırmıştır. Konstrüktivist güvenlik bu yönüyle diğer güvenlik yaklaşımlarından ayrılmaktadır (Birdişli, 2010: 245-251).

Soğuk Savaş sonrası dönemi kavramsallaştırma çabalarına bakıldığında üç farklı teoriden bahsedilmektedir. Bunlardan ilki *Güç Geçişi Teorisi*'dir. Organski'nin geliştirdiği bu teori, güç hiyerarşisini önceleyerek Soğuk Savaş döneminin başat iki aktörü olan ABD ve SSCB'nin güç kaybına uğraması sonucu çok kutuplu sistemde bir veya birden fazla süper gücün varlığının sorgulandığı bir teori olmuştur (Organski, 1958). İkincisi, Soğuk Savaş sonrası terörizm tehlikesine

[4] İngilizce adıyla "Grand Strategy" olarak adlandırılan bu durum, ABD'nin dış politikada çıkarları çerçevesinde belirleyeceği planlar bütünü olarak açıklanmaktadır. Bu doğrultuda ABD, dış politika kararlarını ve araçlarını nasıl ortaya koyacağını belirleyerek belirli dönemler aralığında uygulanmaktadır. Ayrıntı için bkz, (Özdemir, 2018).

karşı ABD'nin "önleyici savaş (preventive war), ön alıcı vuruş (pre-emptive strike)[5]" gibi tek taraflı müdahalelerine yönelik diğer devletlerin davranışlarını inceleyen *Yumuşak Dengeleme Teorisi'*dir. Üçüncü teori ise, askeri gücün uygulanması olarak açıklanan Sert Güç (Hard Power) ve ekonomik, siyasi veya kültürel amaçlarla diplomatik kanalların kullanılması olarak açıklanan Yumuşak Güç (Soft Power) kavramlarının bir stratejik unsur olarak kullanılıp, hedef ülkenin siyasi sistemini etkilemek ve zayıflatmak için her türlü aracın kullanıldığı manipüle edici diplomatik politikalar bütününe verilen isim olan *Keskin Güç (Sharp Power)* teorisidir (Ludwig ve Walker, 2017). Bu teori, ülke içerisinde ifade özgürlüğünü kısıtlayıp, uluslararası kamuoyunda hakkındaki olumsuz düşünceleri manipülatif hareketlerle önlemeyi amaçlayan Rusya ve Çin gibi otoriter ülkelere atfedilmiştir (Birdişli, 2020b: 249). Bunun yanında Joseph Nye (2009)'ın ortaya koyduğu *"Akıllı Güç (Smart Power)"* kavramı, Soğuk Savaş sonrası dönemi açıklamak için bir diğer önemli örnek olarak değerlendirilmektedir. Yumuşak Güç ve Sert Güç kavramlarının her ikisini de içerisinde barındıran ve koşullara göre değişiklik gösteren bu kavram, günümüzde birçok devletin aktif olarak kullandığı bir durum olarak nitelendirilmektedir.

Netice itibariyle eleştirel güvenlik anlayışı, özgürleşme ekseniyle birlikte alanını ve analiz düzeyini genişletmiştir. Güvenliği sağlamaktan daha çok güvensizliğin nedenlerini araştıran ve birçok alanda bu olgunun nedenselliğini tartışan eleştirel güvenlik yaklaşımları, günümüzdeki güvenlik çalışmalarına ilham kaynağı olmakla birlikte güvenlik anlayışının gelişiminde kilit bir rol oynamıştır.

1.1.1.3. 21. Yüzyılda Güvenlik

Uluslararası sistemde aktör sayısındaki çeşitlilik, küreselleşme ile ilişkili bir biçimde yıllar geçtikçe artış göstermiştir. Özellikle terörizmin bu dönemde ulus-aşırı bir nitelik kazanması sebebiyle, devletlerin uluslararası alanda var olan her türlü aktörle teması söz konusu olmuştur. Çok kutuplu sistemin karmaşasında devletler, uyguladıkları/uygulayacakları şiddeti meşru kılmak için terörizmi kullanmaktadır. Uluslararası örgütlerden ve uluslararası kamuoyundan destek alan/almayan pek çok devlet, iç ve dış yetki sınırını genişletmeyi amaçlamaktadır. Dolayısıyla terör kavramı, Soğuk Savaş sonrası dönemi anlamak açısından bir mihenk taşı olarak Schmid (2004)'in ilerde değinilecek olan görece meşruluk düşüncesini haklı çıkarmaktadır.

Güvenlik algısının şekillenmesi ve küreselleşmeye bağlı olarak zamanla olgunlaşması önemli tarihsel olaylarla açıklanmaktadır. 21. yüzyıla geçiş aşaması ve özellikle 2000'li yılların başlarında güvenlik algısı yeni formlar kazanarak yeni aktörleri, tehditleri, şiddet enstrümanlarını ve güvenlik

[5] Bush Doktrini temel ilkesi olan önleyici savaş **(preventive war),** ön alıcı vuruş **(pre-emptive strike)** kavramları, terörizme karşı savaş bağlamında, devletlere karşı direkt olarak kuvvet kullanması şeklinde açıklanmaktadır. Ayrıntı için bkz, (Değdaş, 2018).

anlayışlarını beraberinde getirmiştir. Soğuk Savaş sonrası dönem, akademik çerçevede sistem tartışmalarının sıklıkla yaşandığı bir dönem olmuştur. Uluslararası sistemdeki değişim, güvenlik ve terör kavramının ulus-aşırı bir nitelik kazanmasına direkt olarak neden olmuştur. Sistemin değişmesi, terörün yeniden yorumlanması ve teknolojik devrimle ilişkilendirilmesi iki farklı olayla özetlenmektedir. Güvenlik algısının yeniden yorumlanmasında bir dönüm noktası olarak yorumlanan iki ana gelişme: 1991'de SSCB'nin dağılması ve 11 Eylül 2001 saldırılarıdır. Ayrıca güvenliğin ulus-aşırı boyut kazanmasının yanında teknolojik unsurları da içinde barındırması, siber güvenlik kavramını tartışmaya açmıştır. Özellikle 2008 yılındaki Estonya saldırıları, ciddi bir farkındalık oluşturarak devletlerin bu alana yönelik ilgilerini artırmıştır.

SSCB'nin dağılmasıyla dünyanın çok kutuplu sisteme geçişi ve 11 Eylül 2001 saldırıları, güvenlik anlayışında ciddi değişimlerin gerçekleşmesine gerekçe olmuştur. Nitekim bu dönemden itibaren uluslararası terörizm uluslararası ilişkiler disiplininde kendine yer edinmiştir. Günümüzde asimetrik tehditlerin en başında olan terörizm, ilerleyen yıllarda çeşitli alanlarda varlığını sürdürerek genişlemiştir ve bu dönemde küreselleşme olgusuyla birlikte teknolojinin devrimsel ilerleyişi, terör unsurlarının siber uzayda daha da büyüyerek genişlemesine ışık tutmuştur.

SSCB'nin dağılmasıyla birlikte Soğuk Savaş'ın sona ermesi, uluslararası ilişkiler disiplininde bir güç dengesi/dengesizliği oluşturmuş, sistem tartışmalarına yol açmıştır. Neorealist düşünürlere göre iki kutuplu sistem, çok kutuplu sisteme nazaran daha barışçıl bir profil çizmiştir. Waltz, Carr gibi Neorealist düşünürler çok kutuplu sistemi bir kaos ve karmaşadan ibaret olarak nitelendirmektedir. Neorealistlere göre bu karmaşa, mutlak istikrarsızlık getirecektir (Kim, 2011: 351). Aynı zamanda Neorealistler, tek kutuplu sistemi sürdürülebilir bir sistem olarak görmemektedir. Nitekim ABD karşısında bir oluşumun ABD'nin gücünü dengeleyeceği olası bir düşünce olarak değerlendirilmemiştir.

Neorealist düşünürlere karşılık olarak hegemonik istikrar teorisyenleri tek kutuplu sistemin daha sürdürülebilir olduğunu savunmaktadır. Wohlforth (1999: 8)'a göre, uluslararası sistemdeki büyük güçler, eşit güce sahip oldukları takdirde, savaş kaçınılmaz bir sonuç olmaktadır. Ancak mevcut sistemde yer alan aktörlerden biri diğer aktörlerden daha güçlü konuma geldiği takdirde daha sürdürülebilir bir sistemden bahsedilmektedir (Kim, 2011: 355). Bu tanım hegemonik istikrar teorisyenleri tarafından yapılmaktadır. İki kutuplu sistemin istikrarı noktasında Neorealistlere karşı yapılan en kapsamlı eleştiri Copeland (1996)'dan gelmiştir. Copeland (1996: 32)'a göre Soğuk Savaş'ta istikrarı iki kutuplu yapı değil, nükleer silahlar sağlamaktadır. Nükleer silahların olmadığı dönemlerde istikrarsız bir yapının olduğu gözlemlenmektedir ve bu da istikrarın iki kutuplu sistemden ibaret olmadığını anlatmaktadır. Sistem tartışmalarından hareketle gücün dağılımının nasıl, ne ölçüde/şekilde, kim/kimlere dağıtıldığı sorusu cevaplandırıldığı takdirde analiz daha belirgin bir boyut kazanacaktır. Nitekim gücün dağıtımı devletleri farklı davranışlara yöneltmektedir (Yalçın, 2015: 214-218).

11 Eylül 2001 saldırıları güvenlik yaklaşımlarında şüphesiz yeni bir dönemin kapılarını açmıştır. Tek kutuplu sistemin hâkim olduğu bir dünyada ABD, devletleri (özellikle NATO bünyesindeki) denetimi ve gözetimi altında tutmak için 2000'li yıllardan itibaren terörizme karşı birlikte mücadele mesajları vermiştir. Bu noktada kendisine düşman olarak tanımladığı devletleri, askeri, ekonomik ve birçok alanda destek vermek ile suçlamıştır. ABD, bu devletleri kendisine düşman olarak görmekle kalmayıp, onları "haydut devlet (rogue state)" sıfatıyla adlandırmış ve uluslararası alanda kendisine destek sağlayarak gücünü test etmiştir.

Küresel çapta güvenlik yaklaşımının çeşitlik kazandığı bir olay olarak nitelendirilen Rusya'nın Estonya'ya siber saldırıları sonrası devletler, siber alanda ciddi bir farkındalık yaşayarak odak noktalarını siber alana taşımıştır. SSCB'nin dağılması sonrası bağımsızlığını kazanan Estonya, telekomünikasyon ve internet altyapılarına ciddi yatırımlar yaparak teknoloji alanında önemli adımlar atmıştır. 2007 yılında özellikle banka hesaplarına yönelik ciddi ölçüde bir siber saldırı gerçekleşmiş ve ülke bundan ağır bir yara almıştır. Nitekim iletişim altyapısının da hacklenmesi sonucu haberleşmenin uzun bir süre sağlanamaması, saldırıyı algılama süresini de uzun tuttuğu için alınan yaranın boyutu daha da derinleşmiştir. Saldırının Rusya-Estonya arasında yaşanan siyasi gerilimin hemen akabinde olması ve saldırganların Rus blog sayfalarında organize olduğunu tespit eden Estonya hükümeti, bu saldırının Rusya'dan geldiği iddiasında bulunmuştur ve literatürde de bu şekilde değerlendirilmiştir (Yener, 2015).

21. yüzyılın güvenliğinde yeni bir alan açılmakta ve bu alanın taşıdığı hayati önem, gerçekleşen her saldırıdan sonra deneyimlenmektedir. Bununla birlikte NATO'nun alan genişletme hususunda bu saldırıların payı büyüktür. Özellikle NATO üyesi olan Estonya'ya saldırı gerçekleşmesi, 2002'deki Prag Zirvesinde dile getirilen dijital felaket (dijital 9/11) senaryosunu tartışmaya açmıştır. NATO, 2006 yılında terörizmi ilişkilendirerek raporladığı güvenlik belgesine[6], saldırı sonrası İngiliz raportör Lord Jopling (2007)'in ilave raporuyla siber güvenlik eklenmiştir (Bıçakcı, 2012: 217). NATO bu saldırı sonrası Estonya'ya ciddi yardımlarda bulunmuş, ilerleyen dönemlerde bir siber güvenlik stratejisi belirleyerek bu yaklaşımını kurumsallaştırmıştır. Bu stratejiyi Bükreş Zirvesi (2008)'nde detaylı bir şekilde ele alan NATO, üye devletlerin siber uzayda gelişim kat etmesini sağlamak için kaynak yaratacağını belirterek ittifak üyelerinin siber savunma konusunda birbirlerine yardım etmesi gerektiğini vurgulamıştır.

[6] 19. Bölüm, "İttifak'ın Terörizmle Mücadele ve Kitle İmha Silahlarının Yayılmasına Karşı Rolü" (Chapter 19, *The Alliance's Role In The Fight Against Terrorism And Proliferation Of Weapons Of Mass Destruction*) adlı başlıkta NATO'nun terör stratejisine yer verilmiştir. Ayrıntı için bkz, (NATO, 2006a: 167).

1.1.2. Güvenlik ve Strateji

Dedeoğlu (2003: 21)'na göre güvenlik kavramı, varlığını koruma ve sürdürme kaygısı olarak tanımlanmaktadır. Güvenlik, tehdidin boyutuna ve şiddetine göre çeşitlilik göstermektedir. Güvenlik kavramı devlet, sistem, bölge, toplum, birey gibi pek çok değişkeni içerisinde barındırmaktadır. Var olan tehditlerin ortadan kaldırılarak oluşabilecek yeni tehditlere karşı önlemlerin alınması, devletlerin bağımsızlıklarını devam ettirebilmesi adına yegâne bir gereklilik olarak karşımıza çıkmaktadır (Brauch, 2008: 24). Güvenlik yaklaşımlarında strateji belirleme noktasında farklı görüşler bulunmaktadır ve bunlar; barışçıl ve çatışmacı güvenlik stratejileri olarak adlandırılmaktadır.

1.1.2.1. Barışçıl Güvenlik Stratejileri

Tehdidin algılanması ve aktörlerin yaklaşımı, güvenlik stratejisinin belirlenmesinde kilit bir rol oynamaktadır. İdealist temellere dayandırılan barışçıl stratejide savaşın yokluğu, güvenliğin sağlanması ve antlaşmalarla daimî korunması olarak açıklanmaktadır. İdealist düşünürlere göre uluslararası işbirliğinin kurulması, statükonun devamı ve sürdürülebilirliği açısından önemlidir ve ayrıca uluslararası işbirliği, barışı da tesis etmelidir. Karl Deutsch'un "güvenlik topluluğu" kavramı, güvenliğin birlikler vasıtasıyla demokratik bir zemin üzerinden inşa edilmesi noktasında önemli bir anekdot olarak değerlendirilmektedir (İşyar, 2008: 8). Nitekim Avrupa Birliği (AB) ve NATO içerisindeki devletler güvenlik stratejilerini belirlerken askeri güce başvurmaktan kaçınarak daha az maliyetli bir yolu tercih etmektedir. Plüralist yaklaşıma göre savaşın kolektif bilinç ve örgütler vasıtasıyla engellenmesi mümkündür. Barışçıl stratejileriler bağlamında kolektif vurgu, devletlerin işbirliği ve bağımlılık seviyelerini de dolaylı olarak artırmaktadır (İşyar, 2008: 8).

Kolektif bilinç ve barışçıl strateji noktasında demokrasinin önemini vurgulayan Kant (2020), devletlerin savaştan uzak durması için demokrasiyi gerekli görerek ve demokratik devletlerin birbirleriyle savaşmak yerine diyaloğu tercih edeceğini belirterek ilerleyen dönemlerde literatürde, "demokratik barış teorisi" olarak adlandırılan kuramın, düşünsel zeminini hazırlamıştır. II. Dünya Savaşı'yla beraber uluslararası sistemin değişmesi, devletlerarası düzenin iki kutuplu sistem üzerinden açıklanmasına sebebiyet vermiştir. Aktör tutumlarının da mevcut dönemdeki değişimi sebebiyle idealist yaklaşım, yerini realizme bırakmış ve Soğuk Savaş yılları boyunca iki güç arasında çıkar çatışmaları meydana gelmiştir. Dolayısıyla bu dönemde çatışmacı güvenlik, uygulanması kaçınılmaz bir strateji olmuştur.

1.1.2.2. Çatışmacı Güvenlik Stratejileri

Uluslararası sistemin anarşik oluşu, realistler tarafından sıklıkla üzerinde durulan bir vurgudur. Özellikle iki kutuplu sistem döneminde güvenliğin merkezinde devlet olduğu için askeri alanlara

yatırım yapılması güvenliği sağlamanın temel prensiplerinden birisi olmuştur. Kimi aktörler direkt olarak, kimi aktörler de dolaylı olarak çatışmacı stratejiye başvurmaktadır. Yapısı gereği herhangi bir aktör, tehdit algısını belirlediği andan itibaren atak yapmanın yollarını aramaktadır. Başka bir aktör ise, barışçıl yolların tükenmesi sonucunda çatışmacı bir strateji izlemektedir.

Çatışmacı güvenlik stratejileri; askeri güç, ekonomik yaptırım ve boykot gibi diplomatik yöntemlerin yetersiz kalması sonucunda başvurulan bir strateji olup, şiddetinin artırıldığı zaman dünya geleceğini dahi tehlikeye sokabilen yapıya sahiptir. Öyle ki 1962 yılında Küba Füze Krizi olarak bilinen bunalım, dünyayı bir nükleer savaş eşiğine getirmiştir. Soğuk Savaş yıllarının sonlarına gelindiğinde analiz biriminin merkezine devleti alan çatışmacı güvenlik anlayışı, bilgi teknoloji alanındaki yenilikler, küreselleşme ve diplomasi kavramının gelişimi gibi etmenler vasıtasıyla gücünü ve etkisini giderek yitirmiş, askeri güce sık başvurulmayan, daha yapısal bir hale bürünmüştür (Şengöz, 2020: 7-8).

1.2. Terörizm/Uluslararası Terör Kavramına Genel Bir Bakış

Bir şiddet türü olarak bilinen terörizm konusu ele alınmadan önce terör ve terörizm arasındaki kavramsal farklılıkları tespit etmek gerekmektedir. Çoğu zaman birbirlerinin yerine sıklıkla kullanılan bu iki kavram arasında teknik olarak önemli farklılıklar bulunmaktadır. Kökünü Latince "terrere" kelimesinden alan terör, korkudan titreme/dehşete düşmek gibi bir anlama karşılık gelmektedir. Terör kavramı, "bireylerde korku, sindirme, ürküntü ve yıldırma yaratmaya yönelik olarak belli bir düşünce ya da davranışları benimsetmek için zor kullanma, tehdit etme ya da şiddet eylemleri bütünü" olarak tanımlanmaktadır (Saral, 2016: 25). Terörün içerisinde mutlaka bir şiddet eylemi barındırdığı doğrudur ancak her şiddet eylemi/durumu terör olarak yorumlanmamaktadır.

Amaç ve kapsam bakımından terör kavramı, terörizmden ayrılmaktadır. Gül (2012: 9)'e göre terörist eylemi terör eylemden ayıran en önemli unsur, içerisinde bir siyasi amaç barındırmasıdır. Nitekim terörizm, *terör yöntemlerinin siyasi veya ideolojik bir amaçla, örgütlü, sistematik ve sürekli bir biçimde kullanılmasını benimseyen bir siyasal şiddet stratejisi* olarak tanımlanmaktadır (Salman 2021: 36). Hoffman (1998: 13)'ın da belirttiği gibi terörizm, şiddet ve korkunun yanında içerisinde siyasi bir içerik ve mesaj barındırarak kendisine anlam kazandırmaktadır. Chomsky (2003: 44)'e göre terörizm, bir hükümetin politikalarını etkileyecek ölçüde kolektif şiddet ve gizem içermektedir. Wilkinson (1979: 51)'a göre ise: *Siyasal istekleri kabul ettirmek üzere kişileri, grupları, toplumu ve hükümeti yıldırmak için sistematik olarak öldürme veya tahrip etme tehdidinin kullanılması* şeklinde tanımlanmaktadır.

Terörizmin tartışmalı bir olgu olduğunu savunan Schmid (2004: 380), terördeki meşruluğun göreceliliğini savunmuştur. Yani siyasi amaç güdülerek içerisinde örgütsel şiddet barındıran bir olay, kimilerine göre terör eylemi, kimilerine göre ise özgürlük mücadelesi olarak nitelendirilmektedir. Bu

görecelilik kimi zaman terör kavramın anlaşılmasına terör eylemlerinin adil bir şekilde tespit edilmesine gölge düşürmektedir. Jongman (2015), terörizmin ortak nitelik ve amaçlarını ortaya çıkarmak için yüzü aşkın farklı terör tanımlarını incelemişlerdir. Bu tanımlamalarda en çok üzerinde durulan unsur ve sıklıkları ortaya koymuşlardır. Tablo 2'de görüleceği üzere en çok tekrarlanan unsur şiddet, güç (zor kullanma) en az kullanılan unsur ise savaş metodu, stratejik ve taktiktir.

Tablo 2: Terörizm Tanımında En Çok Tekrarlanan Unsurlar

Unsur	Sıklık (%)
Şiddet, güç (zor kullanma)	83,75
Politik/siyaset (politik amaçlı hareket etme)	65
Korku, terör (halka korku ve tedirginlik yaratma)	51
Tehdit içerme	47
Psikolojik etkiler ve beklenen tepkiler	41,5
Hedef ile kurban arasında ilişkisiz	37,5
Amaçlı, planlanmış, organize hareket	32
Savaş metodu, stratejik, taktik	30,5

Kaynak: Jongman, 2015; Salman, 2021

İlk terör faaliyetlerinin Roma İmparatorluğu dönemine kadar uzandığı bilinse de modern terör olarak nitelendirilen dönemler, Tablo 3'te de görüleceği üzere dört başlık altında incelenmektedir. Rapoport (2013: 47), *Four Waves of Modern Terorism* adlı çalışmasıyla modern terörizmi dört ana dalgaya bölmüştür. Bunlardan ilki; 1878-1919 yılları arasındaki *Anarşist Dalga*, ikincisi *Sömürgecilik Karşıtı Dalga* (1920-1960), üçüncüsü *Yeni Sol-Marksist Dalga* (1960-1990), dördüncüsü ise *Dini-Köktendinci Dalga* (1979-günümüze) olarak sınıflandırılmaktadır (Kaplan, 2016: 4).

Tablo 3: Modern Terörist Dalgaları

1	Anarşist Dalga (1878-1919)
2	Sömürgecilik Karşıtı Dalga (1920-1960)
3	Yeni Sol-Marksist Dalga (1960-1990)
4	Dini-Köktendinci Dalga (1979-günümüze)

Kaynak: Rapoport, 2013

II. Dünya Savaşı'nın sonundan itibaren terörizm kavramı kendini yenileyerek bir sonraki döneme geçmiştir. Teknolojik gelişmeler ve bilgi devrimi, terörizm meselesinde de varlığını ve etki boyutunu göstermiştir. Tarih boyunca gelişimini sürdüren terörizm, Soğuk Savaş Dönemi'nin sonuna doğru uluslararası bir boyut kazanarak güvenlik teorileri kapsamında dünya siyasetini şekillendirmiştir. Bununla birlikte internetin yaygınlaşmasıyla birlikte dijitalleşen devletlere, kurumlara ve bireylere yönelik saldırı faaliyetleri, terörizm kavramının dönüşümünü özetlemektedir.

1.2.1. Terörizm Kavramının Tarihsel Gelişimi

İdeoloji, örgüt ve şiddet unsurlarını bir bütün olarak içerisinde barındıran terörizm, tarihsel çerçevede incelendiğinde şiddet eyleminin başlangıç olarak kabul edildiği olayların da göz önünde bulundurulması gerekmektedir. İdeolojik ve siyasi amaçlar güdülerek oluşturulan terörist eylemlere verilebilecek örnekler tarihin ilk yıllarına kadar dayanmaktadır.

Tarihte bilinen ve akademik literatüre geçen ilk terörist topluluk, Walter Laqueur tarafından açıklanmaktadır. Lanqueur (2017: 7), Milattan Sonra (MS) 73-66 yılları arasında dini temellerle oluşturulan ve Romalılara yönelik saldırı organizasyonları gerçekleştiren örgüte mensup *Sicariiler'*i ilk terörist grup olarak nitelendirmiştir. Çakmak (2008: 18)'a göre ise ilk terör topluluğu MS 6-135 yılları arasında faaliyet gösteren *Jewish Zelaots*[7] adlı oluşumdur. Sicarii'ler, bu örgüte mensup olup radikal eylemleri sonucunda ayrışan ve Zelaots'tan sonra devamlılığını sürdüren bir alt grup olarak değerlendirilmiştir. Sicarii'lerden sonra ortaya çıkan ikinci terörist topluluk, 1090 yılında Hasan bin Sabbah tarafından oluşturan *Haşşaşin'*lerdir. Bu oluşum, İslam'ın İsmailiye mezhebine bağlı olmakla birlikte mevcut dönemde Selçuklu İmparatorluğu'na karşı mücadele etmiştir. Bu iki örgütten sonra dünyanın çeşitli zamanlarında ve çeşitli yerlerinde terör faaliyetleri kendisini göstermiştir. Terörizmin, literatürde bir milat olarak kabul edilebileceği en belirgin dönem, 16. yüzyıl olarak belirtilmektedir. Bu dönemler, başta Rapoport olmak üzere pek çok tarihçi tarafından modern terörizmin başlangıcı olarak da adlandırılmaktadır. Fransız İhtilali'nden sonraki 1793-1828 yılları arasındaki dönemin *Terör Rejimi* olarak nitelendirilmesi, terörizm kavramının miladı açısından önem arz etmektedir (Yayla, 2015: 340-345).

Anarşi kavramının kendisinden en çok bahsettirdiği 19. yüzyılda terör faaliyetleri dünya üzerinde etkisini giderek artırmıştır. Bu dönemdeki en kapsamlı terör organizasyonu olarak bilinen örgüt, *Narodnaya Volya (Halkın İsteği)'*dır. Bu yıllarda fikirsel motivasyonunu anarşi ve devrimcilik kavramından alan örgütler; ABD ve birçok Avrupa ülkesinde çeşitli intihar saldırılarının yanında siyasi figürlere ve devlet görevlilerine karşı suikastlar da düzenlemiştir. Laqueur (2017: 15-21) tarafından *Anarşist Terör Çağı* olarak da nitelendirilen bu dönem (1878-1919), uluslararası bir hüviyet kazanarak amacına ulaşmış ve modern terörizm çağının ilk halkasını oluşturarak ardından gelen dönemlere de referans olmuştur.

20. yüzyıldan itibaren terörizm, mevcut yerel düzeyini de genişleterek ulus-aşırı bir nitelik kazanma yoluna gitmiştir. 1900'lü yılların ilk çeyreğinde, özellikle I. Dünya Savaşı'nın bitişi itibariyle terörizm dalgalarının ilham kaynağı Marksist-Leninist ideolojiler olmuştur. Anarşist terör

[7] Din adamları tarafından yönetilen bu örgüt, Filistin'de MS.6-135 yılları arasında bölge halkının en yoksul tabakası tarafından oluşturulmuştur. Roma, Yunan ve Yahudi yönetimlerine karşı çeşitli eylemlerde bulunmuştur. Ayrıntı için bkz, (Çakmak, 2008).

dalgasının sömürge toplumları üzerine etkisi yüksek olmuştur. Nitekim anarşist dalganın şiddet vasıtasıyla siyasi bağımsızlığın kazanılabileceğine dair verdiği mesaj, toplum üzerindeki etkisini daha da perçinlenmiştir. I. Dünya Savaşı sonrası Wilson'un işaret ettiği self determinasyon sömürgeciliğe karşı oluşan terör dalgasının daha da somutlaşmasına olanak sağlamıştır. Nitekim bu büyük savaş, otoriter rejimlerinin çoğalmasını ve artırdıkları şiddetin sonucu olarak terörist unsurların hak arayışına girmesini mümkün kılmıştır (Demirel, 2007). II. Dünya Savaşı sonrasında terörist faaliyetleri giderek artarak daha geniş etki boyutuna ulaşmıştır. Nitekim 1950'li yılların başında Ortadoğu, Afrika ve Asya'da sömürge toplumlarında oluşan milliyetçi ayaklanmalar neticesinde birçok toplum kısmen de olsa özgürlüklerini sağlamış ve Avrupa'daki terör faaliyetlerine ilham kaynağı olmuştur (Hoffman, 1998). Özellikle İrlanda Cumhuriyet Ordusu (IRA) ve Bask Yurdu ve Özgürlük (ETA) adlı örgütler bu dalgada adlarından en çok söz ettiren organizasyonların başında gelmiştir. Örgütlerin ulusal özgürlük mücadelesinin birçoğunun başarıya ulaşmasının gerekçesiyle bu dalga 1960'lı yıllardan itibaren siyasi etkisini giderek yitirmiştir (Biçer, 2020: 921-925).

Üçüncü dalga olarak nitelendirilen Yeni Sol-Marksist dalga, fikirsel bütünlüğünü çatışmadan ziyade uzlaşma üzerine oluşturmuştur. Bunun yanında Soğuk Savaş döneminin 1960'lı yılarında SSCB'nin ABD'ye karşı görece daha barışçıl olması, bu dalganın Amerikan karşıtlığı çerçevesinde gelişmesine olanak sağlamıştır. Kendinden evvelki dalgalara nazaran üçüncü dalgada iletişim teknolojileri ve medya, kitleler üzerinde propaganda yapma noktasında önemli bir rol oynadığından ötürü 1960'lı yıllar terörizm tarihi için bir dönüm noktası olarak nitelendirilmektedir. Bu dalgada, verilen zarardan ziyade verilen mesajlar daha çok önemsendiğinden ötürü can kaybının kendinden önceki dalgalara kıyasla daha az olduğu savunulmaktadır. Emperyalizm karşıtlığı, sosyalizm, milliyetçilik ve özgürlük gibi unsurlar bu dalganın anahtar kavramları olmuştur. Bu dönemde topluma ve devletlere verdikleri zayiat bağlamında en bilinen terör örgütleri, Japonya'da Birleşik Kızıl Ordu, İtalya'da Kızıl Tugaylar, Almanya'da Baader Meinhof, İngiltere'de Öfkeli Tugaylar, ABD'de Kara Panterler olarak bilinmektedir (Yayla, 2015: 354-355).

Terör organizasyonlarının uzun bir süre hâkim ideolojisi olan devrimcilik, 1980'li yılların ortalarından itibaren etkisini giderek kaybetmiştir. Bu yıllardan itibaren terör faaliyetleri daha çok bir coğrafyada yoğunlaşmış ve örgütlerin motivasyon kaynağı din temelli olmuştur. Ortadoğu'da yaşanan önemli siyasi gelişmeler, dördüncü dalga olan dini dalganın meydana gelmesine neden olmuştur (Kurt, 2019: 142). İran, Afganistan, İsrail ve Filistin'de gerçekleşen siyasi-askeri olaylar bu terör dalgasının oluşmasına neden olmuştur. 1979 yılındaki İran İslam Devrimi, dördüncü dalganın başlangıcı olarak değerlendirilmektedir. Rus işgaline karşı direnen Taliban, 11 Eylül saldırılarını gerçekleştiren El Kaide ve son yıllarda ortaya çıkan Irak Şam İslam Devleti (DEAŞ), bu dalgada adından en çok söz ettiren ve güncelliğini halihazırda koruyan terör örgütleri olarak nitelendirilmektedir (Biçer, 2020: 928).

1.2.2. 21. Yüzyılda Terör

Teknolojinin ilerleme hızı, iç savaşlar sonucu kitlesel olarak yapılan göçler, 21. yüzyıl itibariyle çok kutuplu sistemde terörizme destek veren ülkelerin artması, uluslararası terörizmi tetikleyen en önemli faktörlerden birisidir (Kartal, 2014: 54). Terörizm de küreselleşmeden nasibini alıp değişim göstererek NATO-AB gibi uluslararası kuruluşların dikkatini çekmiş, uluslararası terörizmi kabul edip bu konuda pek çok kez stratejik eylem planları ortaya koymuşlardır. Bu denklem içerisinde devletlerin de terörist unsurlara örtülü sağladığı destekler, sorunların kolektif biçimde çözümünü de engellemiştir. Çeşitli aktörler tarafından gerçekleştirilen terör eylemlerinin tarihsel dönüşümü sorgulandığında; mevcut dönemin siyasi konjonktürü dahilinde hedefler, amaçlar, stratejiler ve askeri araçlar değişim göstermiştir. 21. yüzyılda terörün geleneksel/konvansiyonel terörden ayrılmasının yeni tip silahlar, mesajın niteliği, hedef gruptaki değişim gibi sebepleri vardır. Ancak bu dönemi diğer dönemlerden keskin olarak ayırt eden unsur, küreselleşme ve sürekli kendisini yenileyen teknoloji gerçeğidir.

21. yüzyıl terör anlayışında milat olarak 11 Eylül 2001 saldırıları kabul edilmektedir. Hala etkilerini sürdürmekte olan dördüncü terörist dalganın yarattığı büyük bir yıkım olarak nitelendirilen bu saldırı, başta ABD olmak üzere pek çok ülkenin iç ve dış politikadaki gidişatlarını doğrudan veya dolaylı bir şekilde etkileyecek ölçüde siyasi tarihte yer alan önemli bir olay olarak değerlendirilmektedir. Öyledir ki iç savaş, ekonomik problemler ve benzeri sorunlar neticesinde Doğu'dan Batı'ya veya Güney'den Kuzey'e yapılan göçmen-mülteci-sığınmacı faaliyetlerinde iltica edilen yerdeki yerli halkın, göçmenler üzerinde önyargılarının artmasına sebebiyet verecek kadar sosyolojik derinlikte bir etkisi de olmuştur. Nitekim çeşitli kimlikler vasıtasıyla saldırıların düzenli bir şekilde sürmesi ve hala devam eden dördüncü terör dalgası, bu tip sosyolojik soruları doğurmanın yanında günümüzde göç alan yerlerde artan aşırı sağcı partilerin ortaya çıkıp ırkçı politikaların oluşturulmasında da ciddi ölçüde sorumluluk sahibidir.

El Kaide tarafından düzenlenen 11 Eylül saldırılarının uluslararası kamuoyunda geniş bir etkiye sahip olması nedeniyle ABD ve Avrupa ülkelerinin başını çektiği uluslararası kuruluşların bu ve benzeri olaylara karşı önlem almaya gayret göstermesi kaçınılmaz olmuştur. Terörist faaliyetlerin ulus-aşırı bir nitelik kazanmasının sonucunda devlet terörizmi ciddi bir sorun olarak kabul edip küresel çapta kapsamlı bir biçimde işbirliğine gitmiştir. NATO, saldırılardan hemen sonra Washington Anlaşması'nın 5. maddesini yürürlüğe koyarak küresel çapta bir işbirliği başlatmıştır (The North Atlantic Treaty, 1949). Aynı zamanda BM de olayın ardından saldırıların barışı ve güvenliği tehdit ettiğini, saldırıya uğrayan ülkelerin bireysel veya kolektif olarak meşru müdafaa hakkının olduğunu bildirmiştir. AB, terör saldırılarının ardından ortak bir bildiri yayımlayarak ABD'ye yönelik saldırılara karşı işbirliği gerektiğini belirtmiştir (Erdoğan, 2011). Bu verilerden de anlaşılacağı üzere Soğuk Savaş döneminin yarattığı dost-düşman kavramı sonraki dönemde ciddi bir değişime uğrayarak, terörizmin herkesin ortak düşmanı olduğu algısı yayılmaya başlamıştır.

Uluslararası sistemde güç boşluğundan faydalanan ABD, bu algıyı yöneterek terörizme karşı küresel çapta işbirliğine soyunmuştur.

Terörizmdeki dört dalgadan sonra beşinci bir dalganın varlığı, literatürde tartışılan bir konu olmaktadır. Beşinci bir dalganın varlığını savunan Jeffrey Simon (2010), bu dalganın diğer dört dalgadan çok daha farklı dinamikler içerdiğini belirtmektedir. İlk dört dalgadaki ideolojilerin (anarşizm, sömürge karşıtlığı, yeni sol/Marksizm ve köktendinci) beşinci dalgaya tamamen hâkim olamayacağını vurgulamıştır. Çünkü Simon (2010: 48)'a göre beşinci dalga, teknolojik bir hüviyet taşımaktadır ve bu dalgada silahlar, teknoloji sayesinde daha önlenemez hale gelmektedir ve hatta bu unsurlar yerine internet terör faaliyetlerinde daha yaygın olarak kullanılmaktadır (Biçer, 2020: 932).

İKİNCİ BÖLÜM

2. ULUSLARARASI GÜVENLİKTE YENİ BİR ALAN: SİBER UZAY

Kavram itibariyle yeni bir dinamik olarak değerlendirilen siber uzay, günümüzde insan hayatının hemen hemen her noktasında bulunarak kendini sürekli yenileyen işlevsel bir alandır. İnternet kullanımının bilgisayarlar ve akıllı telefonların yaygınlaşmasıyla birlikte bu kavrama olan bağlılık giderek artmıştır. İnternet, kimi insanlara göre gündelik ihtiyaçları karşılayıp hayatı kolaylaştıran bir araç iken, kimilerine göre de bizzat insan hayatını şekillendirip kendi içine hapseden tehlikeli bir yapıdan ibarettir. Günümüz dünyasında her iki durumun da gerçekleştiğini söylemek mümkün olacaktır. Şüphesiz siber uzayın varlığı pek çok alanda insan hayatını kolaylaştırırken pek çok alanda da doğası gereği risk ve tehdit barındırmaktadır.

Kavramın evrenselliği gereği felsefe, sosyoloji ve tarih gibi birçok alanda akademik incelemeler yapılmaktadır. Bu incelemeler üzerine yapılan çalışmalar, kavram hakkında yapılan farklı tanımları, yorumları ve değerlendirmeleri mümkün kılmaktadır. Son dönemde pek çok disiplin içerisinde tartışılan bu kavramın, uluslararası ilişkiler disiplini içerisinde de var olması olağan karşılanmalıdır. Devletler ve hükümet-dışı kuruluşlar, siber uzaya yönelik algılarını oluşturup yöntem ve eylem planlarını belirlemeden önce bu kavramın uluslararası ilişkiler disiplini içerisinde incelenmesi fayda olacaktır.

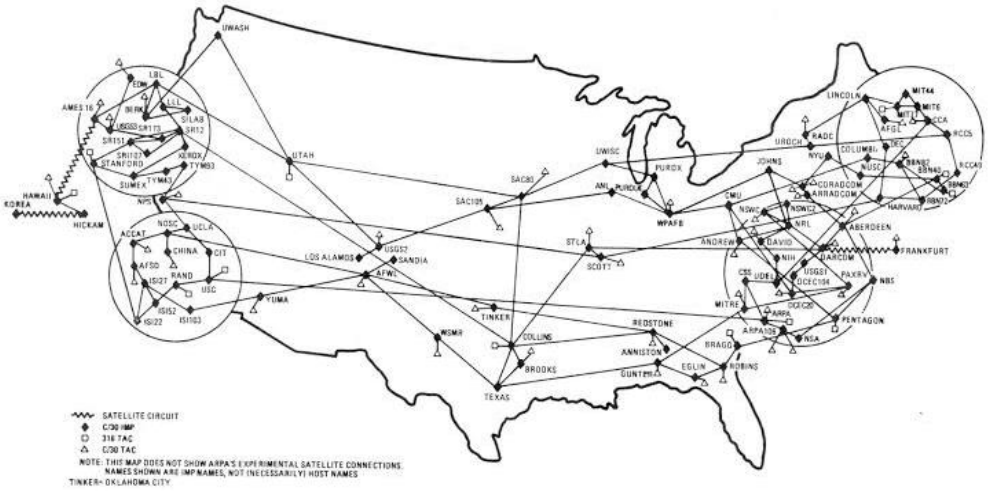
Belirsizlik nedeniyle uluslararası sistem içerisinde yer alan tüm aktörler, siber uzay çerçevesinde güvenlik ihtiyacı hissetmektedir. Güvenliği sağlamak için bu alana ne kadar yatırım yapılırsa, risk ve tehdidi de bir o kadar tetiklemektedir. Bu durum da aktörleri devamlı bir şekilde siber uzaya yatırım yapmaya yönelterek teknolojik rekabetin içine almaktadır. Uluslararası sistemde siber uzayın oluşturduğu güvenlik boşluğu, uluslararası ilişkiler disiplini içerisinde yepyeni bir alan açılmasına olanak sağlamıştır. Siber uzay, literatürü zenginleştirmesinin yanında var oluşu itibariyle realist çizgiden giden disiplinin de çehresini genişletip alternatif paradigmalar ve yaklaşımlar sunan anahtar bir kavram olarak değerlendirilmektedir.

2.1. Siber Uzayın Tanımı ve Literatürdeki Yeri

Siber uzayın isim babası olan William Gibson, 1982 yılındaki *Burning Chrome* adlı romanında "sibernetik" ve "uzay" kelimelerini bir araya getirip "siber uzay" kavramını oluşturmuştur. Gibson (1988)'a göre evren içerisindeki her bilgi sonsuz, karmaşık ve tartışmaya açıktır. Daha sonra bu

kavram Libicki tarafından literatürde kullanılmak üzere "siber ortam" olarak belirlenmiştir. Libicki (2009)'ye göre bu ortam, dünyada somut olarak nitelendirilen her şeyden uzak sanal bir alem içerisindedir ve "fiziksel katman", "söz dizimsel katman" ve "semantik katman" olarak üç ayrı katmanın birleştiği yer olarak değerlendirilmektedir. Siber uzayın boyut kazanarak disiplin içerisinde tartışılan bir konuma gelmesi ve 21. yüzyıla damga vurması, teknik bir boyutun yanında ekonomik, siyasal, sosyal ve kültürel dinamikleri içinde barındırdığından dolayı sistem içerisinde önemli bir unsur olarak değerlendirilmektedir (Akyeşilmen, 2019: 107). Siber uzay, pek çok değişkeni bir arada barındıran ve küreselleşme boyunca yarattığı sınırsız dalgayla bilgiye erişimin ve iletişimin anlık olarak gerçekleştiği yeni bir çağı mümkün kılmıştır. Bilimsel olarak bu kavramın içeriğine, hakkında geliştirilen tanımlamalara ve alana yaptığı katkılara değinmeden evvel internetin tarihsel gelişimini değerlendirmekte fayda vardır.

Şekil 1: ARPANET Haritası



Kaynak: Özgüç, 2020

Kullanımını ilk olarak Soğuk Savaş'ın ortalarında gördüğümüz internet, bilgi transferini sağlamak için kullanılmıştır. Örneğin 1957 yılında SSCB Sputnik adlı ilk yapay uydusunu uzaya gönderirken bilgi transferinden faydalanmıştır. ABD'nin Advanced Research Projects Agency-Gelişmiş Araştırma Projeleri Dairesi Ağı (ARPA)'nı oluşturmasından sonra bilgi transferini geliştirerek SSCB'den gelecek herhangi bir tehdide karşı hazırlıklı olmayı amaçlamıştır (Tarhan, 2018). Askeri ve bilimsel araştırmalara ek olarak teknolojik opsiyonlarının gösterdiği dönüşümler, kullanım alanını daha da genişletmiştir. Licklider (1960: 8)'in, bilgisayarın global şebekesini önerdiği "kısa notlar serisi", Kleinrock (1976: 269)'un, internet bağlantısının temelini geliştirdiği paket anahtar teorisinden ARPA'ya kadar giden süreç, internetin ortaya çıkışının altyapısını oluşturmaktadır. Dünyadaki ilk paket dağıtımı ve evrensel internetin öncülü olarak değerlendirilen ARPANET, ABD'nin Savunma Bakanlığı ağ bünyesine aittir. İlk olarak sadece 15 bilgisayarın

birbirine bağlı olabileceği ve özel kullanıcılara kapalı olan bir ağ modülü iken 1970'li yıllarda bu fikir daha da geliştirilmiştir.

İnternetin 1970'li yıllarda görece biraz daha olgunluğa ulaşmasının arkasında Tomlinson'un katkıları büyüktür. Elektronik posta (e-posta) mekanizmasının oluşturması ve 1972 yılındaki Telnet Protokolüyle uzaktaki bilgisayarlara bağlanmaya çalışarak internet vasıtasıyla ilk dosya transferini gerçekleştirmiştir. Bununla birlikte Tomlinson, kurduğu ekiple birlikte TENEX adında bir işletim sistemini geliştirerek çok sayıda bilgisayar arasında dosya transferi imkanını sağlamıştır. Hatta Bob Thomas'ın TENEX sistemi içerisinde yazdığı deneysel yazılım Creeper, ilk solucan virüs olarak tarihe geçmiştir. Tomlison, "send message"ın sesli harflerini atarak oluşturduğu "SNDMSSG", yerel kullanıcılar arası posta programında iyileştirmeler yapmıştır. Bu yolla bir kullanıcının diğer kullanıcıların posta kutularına mesaj oluşturmasına, adres vermesine ve mesaj göndermesine imkân sağlanmıştır (Patil, 2013: 71).

1980'li yıllardan itibaren e-postayı geliştirme çalışmaları devam etmiştir. Truscott ve Ellis'in başlattığı Usenet çalışması bir önceki versiyonlardan teknik problemleri gidererek e-posta iletişiminin kullanımını artırmıştır. Eric Thomas tarafından yazılan "LISTSERV" adlı yazılım, çok sayıda kişiye e-posta göndermeyi sağlayan mekanizmayı oluşturmuştur. Ayrıca bu, gönderenin bir grup kişiye ulaştıracağı ilk elektronik posta listesi yazılım uygulaması olarak literatüre girmiştir. Uygulamanın 1986'da piyasaya sürülmesinden sonra, 1997'de Lyris "ListManager", 1997'de "Sympa", 1998'de "GNU Mailman" gibi diğer liste yönetim araçları geliştirilmiştir (L-Soft, 2021). Başlangıçta tartışma forumlarında grup sohbeti için tasarlanan Internet Relay Chat (IRC), 1988'de tanıtılmasının ardından sohbet ve veri aktarımlarının yanı sıra özel mesaj yoluyla bire bir iletişimin sağlanmasını mümkün kılmıştır. IRC yazılımı ayrıca, SSCB'de medyada haber yasağının sürdüğü sıralarda 1991'deki darbe girişimini raporlamak için kullanılmıştır. Bu sistem, birkaç ay önce Körfez Savaş'ında da aynı teknikle kullanılmıştır (International Rescue Committee, 2015).

İnternet ve siber uzayın gelişimi ve giderek sosyal hayatın içerisine girmesi ve insan ihtiyaçlarına karşılık vermesi açısından 2000'li yıllar bir kırılma noktası niteliği taşımaktadır. Bu yılların başı itibariyle blog siteleri popüler hale gelerek, çoğunlukla bilimsel-kültürel içerikler ve insan hayatını kolaylaştıran tarzda yazılar yazılmaya başlanmıştır. İnternette Web 1.0, 2.0 ve 3.0 devrimleri, bilgi paylaşımının kapsamı genişletip kategori çeşitliliğini artırarak insan hayatına etki boyutunu daha da kuvvetlendirmiştir (Kutup, 2010: 14). Siber uzayı anlamak açısından 2000'li yılların önemi farklı bir meseleye daha uzanmaktadır. Bu yıllarda, ilk sosyal medya yazılımı yazılmış ve sosyal amaçla kullanılan ilk internet sitesi olarak hayata geçmiştir. Randy Conrads'ın, "classmates" sitesini kurarken amacı, üyelere geçmiş öğrenci hayatları boyunca edindikleri arkadaşlarını bu site vasıtasıyla bulmalarına yönelik olmuştur. Bu uygulama tarzı daha sonra pek çok yazılımcının ilham kaynağı olmuş ve güncele uyarlanarak gündelik hayatı çevreleyen dinamik bir yapı haline gelmiştir (Patil, 2013: 72).

Etki boyutu ve uluslararası sisteme kattığı önem açısından siber uzay, özellikle Soğuk Savaş'ın sonlarından itibaren uluslararası ilişkiler disiplini içerisinde yer edinmeye başlamıştır. Disiplin kurulduğundan beri güvenlik teorilerinde literatüre hâkim olan paradigma realizm olduğundan dolayı siber uzaya yönelik ilgi kısıtlı olmuştur. Çünkü bu paradigmada siber uzay güvenlik minvalinde değerlendirilmemektedir. Siber uzay hakkında yapılan güvenlikçi çalışmaların çeşitliliğinin artması, alana yapılan katkıların devamlılığı açısından oldukça önemlidir.

2.1.1. Alana Yapılan Katkılar ve Önemli Çalışmalar

İsminin ve işlevinin karşılığı olarak daima dijital bir perspektiften değerlendirilen siber uzay, teknik yönü ağır basan bir dinamik olarak kabul edilmektedir. Bilgisayar veya yazılım gibi alanlarda yapılan teknik çalışmaların haricinde faaliyet alanının merkezinde insanı bulundurduğundan dolayı bu kavramı sorgulamak, meydana getirdiği sebep ve sonuçları irdelemek gerekmektedir. Dolayısıyla siber uzayın uluslararası ilişkiler bilim dalı içerisinde değerlendirilmesi, bilindiği üzere alan içerisinde farklı paradigmaların tartışılmalarına da ön ayak olmuştur. Ayrıca siber uzay ve uluslararası ilişkilerin kesiştiği noktaların artması, bu kavramların güvenlik teorileri içerisinde sıklıkla değerlendirilmesini mümkün kılmıştır. Özellikle Soğuk Savaş sonrası dönemde uluslararası sistemde belirsizlikler artmış ve bu da güvenlik alanına sıçramıştır. 21. yüzyıldan itibaren küreselleşme dalgasının daha çok bilişim, iletişim ve teknoloji üzerine olduğundan dolayı güvenlik kaygılarının da dijitale doğru kaydığı, yadsınamaz bir gerçeklik olarak değerlendirilmektedir.

Uluslararası sistemde geleneksel güvenlik anlayışının yerini asimetrik güvenliğe bıraktığı gerçeği, literatürde sıklıkla dile getirilmektedir (Çelik, 2018: 112). Erendor ve Tamer (2017: 114)'e göre, 2000'li yılların başından itibaren hemen hemen her politik veya askeri çatışmaların mutlaka bir siber boyutu olmuştur. Bu durum da güvenlik çerçevesinde uluslararası ilişkiler ve siber uzayın, aralarında her ne kadar spesifik farklar bulunsa da kavramsal olarak bir arada kullanılmasını mümkün kılmıştır.

Eren (2017a: 24-27)'e göre siber güvenlik, doğası gereği askeri, siyasi ve ekonomik yapıyı bir arada barındıran, algı yönetiminin yapıldığı ve çevresel sorunlara yol açan güvenlik sektörü olarak değerlendirilmektedir. Siber uzay içerisinde tehdit algısının aktörden aktöre farklılık göstererek nesnel bir forma büründüğü düşünülmektedir ve geleneksel perspektifin dışında bir inceleme gerekliliği vurgulanmaktadır. Bu bağlamda siber uzay, devlet-dışı aktörlerin de siber güvenlik denklemine katıldığı çok boyutlu bir yapı olduğundan dolayı Kopenhag Ekolünün "güvenlikleştirme" teorisi üzerinden değerlendirilmektedir. Kopenhag Ekolü teorisyenlerinden Hansen ve Nissenbaum (2009: 1123), siber uzayın ayrı bir sektör olarak değerlendirildiğini savunmaktadır (Eren, 2017b: 230).

Choucri (2015), siber uzay ile uluslararası ilişkiler arasındaki temel farklılıkları ortaya koyarak yedi farklı ilkeyle bu düşüncesini güçlendirmiştir. Tanımlanan bu farklılıklar; *geçicilik, fiziksellik, nüfuz etme, akışkanlık, katılım, atfedilebilirlik ve hesap verme zorunluluğu* olarak gösterilmektedir. *Geçicilik* ilkesinde, siber uzayın doğası gereği göreceli, değişken ve sınırsız oluşu, realist bir paradigma içerisinde değerlendirilen uluslararası ilişkiler disiplininin "kesinlik" anlayışıyla pek uyuşmamaktadır. Siber uzay, *fiziksellik* vurgusuyla uluslararası ilişkilerdeki birçok somut şeyden (savaş, antlaşma, coğrafya gibi) daha soyut nitelik taşımaktadır. Aynı zamanda hukuk, uluslararası ilişkilerin en önemli özelliği olarak belirtilirken siber uzayda hukuk, kanun, kural gibi konuların olmaması *nüfuz etme* ilkesi açısından önemli bir farklılıktır. Ulus-devlet sistemi içerisinde dengeli ve sabit gitmeye gayret gösteren uluslararası sistemin durağanlığı, siber uzayın değişkenlik ve adaptasyon seviyesinin yüksek olması hasebiyle *akışkanlık* kazanmaktadır. Keza *katılım* boyutunda da aktör farklılıkları görülmektedir. Nitekim uluslararası ilişkiler içerisinde bir eylemi yapan kişi/kişilerin kim olduğu bilinirken aynı durum siber uzayda tam tersidir. Eylemi gerçekleştiren kişi/kişiler istemediği sürece kendilerinin bilinmemesi, siber saldırının başarısıyla doğru orantılıdır. Bu durum *atfedilebilirliği* de beraberinde getirerek, siber uzayda bir eylemin kim/kimler tarafından yapıldığını bulmanın zorluğunu ortaya koymaktadır. Saldırıyı gerçekleştiren bir aktör ise, *hesap verme zorunluluğu* vardır. Ancak siber uzayda kimlik tespiti yapılamadığı için de hesap verme durumu doğal olarak olmayacaktır. Tüm bu farklılıkların yanında siber uzay ile uluslararası ilişkilerin güvenlik çerçevesinde ortak bir şekilde değerlendirilmesi için; "güvenliğini sağlanması ve saldırılara karşı korunması gereken aktörler kim/kimlerdir, devletler siber uzay içerisinde aktör olarak görülmeli midir, anarşik olup olmadığı tartışılan ve pek çok tanım içeren siber uzayın kapsamı ne kadardır, sınırları veya merkezi var mıdır, yönetişim meselesinin ulusal veya uluslararası güvenliğe etkisi var mıdır, varsa nelerdir?" gibi soruların cevaplanması gerekmektedir (Choucri, 2015).

Ekonomik, siyasal ve sosyokültürel açıdan pek çok değişkeni içerisinde barındıran siber uzay/siber güvenlik hakkında yapılan tanımlara bakıldığında ilk olarak belirtilecek husus şüphesiz bilgi gizliliği ve güvenliğinin sağlanması olmuştur. Singer ve Friedman (2015: 28-31)'a göre bu kavram, dijital verilerin oluşturduğu alan olarak nitelendirilmektedir. Bilgi ağının genişlemesi ve kullanım alanının artması sebebiyle siber uzay; kara, deniz, hava ve uzaydan sonra harbin beşinci boyutu olarak nitelendirilmektedir. Özellikle istihbarat alanında güvenlik tehdit algılamasında önemli bir değişiklik meydana gelmiştir. Bayraktar (2014: 121)'a göre bilgi teknolojilerindeki gelişmelerin bir sonucu olarak aktörler, geleneksel istihbarat yöntemini terk edip özel istihbarat anlayışına geçiş yapmıştır. Buradan verilecek örnekle birlikte 21. yüzyıl itibariyle aktörler, siber güvenlik algısının iyiden iyiye şekillendirmiştir. Siber uzayın kapsayıcı bir bütün olarak evrenselliğine dikkat çeken Uluslararası Telekomünikasyon Birliği (International Telecommunication Union-ITU), siber uzay dahilinde oluşan güvenlik kavramını*: araçlar, politikalar, güvenlik kavramları, kılavuzlar, risk yönetimi yaklaşımı, eğitim ve teknolojiyi içeren önlemler bütünü* olarak belirtmektedir ve bu bağlamda siber güvenliğe önem veren aktörler; bilgiyi

korumak için bilgisayar sistemlerinin güvenlik açıklarını kapatmak, gerçekleşebilecek her saldırıyı bertaraf etmek için güncelliğini korumalıdır (ITU, 2010).

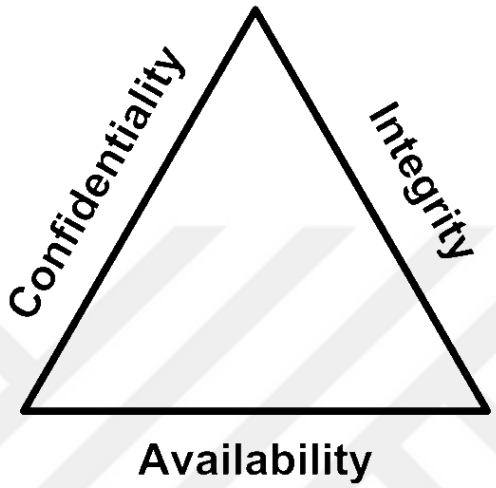
Aktörlerin siber uzay içerisinde güçlü olmak için yaptığı her yatırım bu alanın sınırlarını da bir o kadar katlayarak genişletmiştir. Siber güç, siber güvenlik, siber savaş ve siber terör gibi unsurlar da aktörlerin siber uzaya dahil olarak bu unsurları kullanması itibariyle literatür içerisinde de sıklıkla dile getirilmektedir. Uluslararası sistem dahilinde önde gelen aktörlerin siber uzay tanımlamalarına bakıldığında ABD Savunma Bakanlığı (2013)'nın tanımı şu şekilde olmuştur: *İnternet, telekomünikasyon ağları, bilgisayar sistemleri ve gömülü işlemciler dahil olmak üzere, birbirine bağlı bilgi teknolojisi altyapı ağlarını ve dijital verilerini içeren küresel bir alandır.* ABD aynı zamanda siber uzayda karşılaşacağı tehditleri pasifize etmek için caydırıcılık, esneklik, uluslararası katılım gibi her türlü enstrümanın kullanılması gerektiğini meşru kılmaktadır (CISA, 2009). AB'nin: *Bir telekomünikasyon ağı yoluyla uzaktan da erişilebilen nesneler arasındaki bağlantılar ve ilişkiler kümesi* olarak tanımladığı siber uzay (ENISA, 2015), NATO'ya göre ise: *Bilgisayar ağlarını kullanarak veri depolamak, değiştirmek ve iletmek suretiyle bilgi sistemleri arasında fiziksel ve fiziksel olmayan bileşenlerin oluşturduğu çevre* şeklinde nitelendirilmektedir (Schmitt, 2013a). Türkiye Cumhuriyeti (T.C) Ulaştırma Denizcilik ve Haberleşme Bakanlığı (UAB) tarafından 2019'da hazırlanan *Ulusal Siber Güvenlik Stratejisi* belgesi içerisinde yer alan tanıma göre siber uzay, *tüm dünyaya ve uzaya yayılmış durumda bulunan bilişim sistemlerinden ve bunları birbirine bağlayan ağlardan oluşan veya bağımsız bilgi sistemlerinden oluşan sayısal ortam* olarak açıklanmaktadır (UAB, 2016).

Aktörlerin siber uzay içerisinde oluşu ve devlet nezdinde kabulünün gerekliliği tartışılırken bir diğer tarafta siber uzayın güvenlik boyutunda bir ihtiyaç olduğu gerçeği de dile getirilmektedir. Nitekim uluslararası ilişkiler bağlamında siber güvenlik, özellikle Soğuk Savaş sonu itibariyle "low politics" yani "hayati olmayan ikinci plandaki politikalar" olarak değerlendirilen siber uzay (Clark ve Choucri, 2013: 28), 2007'deki Estonya Saldırıları, 2010'daki Stuxnet saldırılarıyla birlikte Wikileaks, Pizzagate gibi önemli skandallar ve Arap Baharı'nın kitlesel bir eyleme dönüşmesindeki sosyal medya etkileri devletlerin ilgi alanlarını bu yöne çekmiştir. Sosyal medya, diplomatik meselelerin tartışıldığı, anlaşma metinlerinin paylaşıldığı ve hatta liderlerin açıklamalarının yer aldığı geniş yelpazeli etki boyutu oldukça yüksek olan bir mecra haline gelmiştir (Çelik, 2018: 117).

Siber uzay hakkında yapılan tanımlamalara bakıldığında birbirinden farklı görüşlerin siber uzayı algılama biçimi, amaç ve çıkarları doğrultusunda yaptıkları farklı tanımlar gözlemlenmektedir. Tüm bu tanımlar göreceli olduğundan dolayı, literatür içerisinde net bir tanım geliştirmek zordur. Ancak yapılan tüm yorumlar ortak bir çerçeve içerisinde değerlendirildiğinde ana hedef, bilginin gizliliği ve güvenliğinin korunmasıdır. Şüphesiz her aktör, tanımlarının ve amaçlarının merkezine bu unsuru almaktadır. Gorman (2006: 242), siber uzay ekseninde güvenliği kontrol altına almak için

yaptığı tanımı üç sacayağına (CIA üçlüsüne)[8] dayandırmaktadır. Şekil 2'de de görüleceği üzere bunlar; bilginin gizliliği (confidentiality), bütünlüğü (integrity) ve erişilebilirliğidir (availability). Bahsi geçen bu üç unsur, bilgi güvenliğin bileşenleri olarak yorumlanmaktadır (Singer ve Friedman, 2015: 57) ve bu bileşenlere yapılan saldırılar ise siber saldırı olarak değerlendirilmektedir. Bundan dolayı da siber uzayı güvenli kılmak için her bir aktör bu üç unsuru korumalıdır.

Şekil 2: CIA Üçlüsü



Kaynak: Reedphish, 2014

Gizlilik ilkesi, bir aktörün veya kullanıcının verilerini özel veya gizli tutma çabaları olarak tanımlanmakta ve bilgiyi kimin/kimlerin göreceği sorusuna dair cevaplar aramaktadır. Bu ilke, sistem uygulamalarına yetkisiz erişim sağlanarak önemli verileri ve bilgileri ele geçirme amacıyla doğrudan saldırı yoluyla ihlal edilebilmektedir. Elektronik gizli dinleme ve ağ keşfi gibi örnekler bir saldırganın sisteme yaptığı saldırı çeşitlerinin başında gelmektedir (Walkowski, 2019). Dolayısıyla bu tür saldırılardan kaçınmak için kullanıcılar, bilgi veya veri gizliliği çerçevesinde kişisel mahremiyete odaklanarak depolanan ya da saklanan verileri yetkisiz kişilere karşı korumalıdır. Güvenliği tesis etmek için şifreleme, şifreli iletişim bağlantıları en makul önlemlerin başında gelmektedir. Güvenlik duvarının inşa edilmemesi veya ihlal edilmesi, CIA üçlüsünün diğer ilkelerini yüksek olasılıkla etkileyecektir (Reedphish, 2014). Bilginin tam ve eksiksiz olması, bilgi güvenliğinin önemli bileşenlerinden birisi olan bütünlük ilkesinin en önemli özelliğidir. Netice itibariyle bilginin bozulmamış olması önemlidir. Dolayısıyla bilgi ne kadar orijinal ise, o kadar güvenilirdir (Limaye, 2013: 275). Akyeşilmen (2019: 87)'e göre bu ilke, "bilgiyi kim değiştirebilir?" sorusuna odaklanmaktadır. Bilginin güvenliğini ve bütünlüğünü korumak için de en önemli araçlar

[8] Baş harflerini confidentiality, integrity ve availabilityden aldığından dolayı CIA üçlüsü olarak adlandırılan bu üç ilke, herhangi bir aktörün güvenlik altyapısının temelini oluşturmaktadır. Dolayısıyla her siber güvenlik politikası için amaç ve hedef olarak işlev görmektedir. Bilgi güvenliği CIA üçlüsü için oldukça önemlidir çünkü herhangi bir verinin sızdırıldığı, sistemin siber saldırıya uğradığı veya bir hesabın ele geçirildiği an mutlaka bu üç ilkeden birisi ihlal edilmiştir. Ayrıntı için bkz, (Walkowski, 2019).

dijital imza ve sertifika gibi unsurlardır. Gerek görüldüğü zaman kullanıma hazır olması ve olağanüstü durumlarda da işler vaziyette olması şartı koşulan ve istenildiği zaman bilgiye ulaşılabilirliği sorgulayan ilke, erişilebilirliktir. Karar vericiler şüphesiz en savunmasız olduğu anlarda kriz yönetimini işleyebilmek için erişilebilirlik ilkesine önem vermektedir. Erişilebilirlik kalitesini ölçmek için DDoS (Distributed Denial of Service)[9] saldırılarına karşı dayanıklılığına bakmak elzemdir (Akyeşilmen, 2019: 85-90).

Bilgi güvenliğinin siber uzay hakkındaki önemi çeşitli görüşler tarafından dile getirilerek siber güvenlik çalışmalarında farklı tanımların olduğu literatür içerisinde önemli bir ortak argüman olarak değerlendirilmektedir. Ancak tek başına güvenliği bu üç bileşene indirgemenin yeterli olmadığı savunulmaktadır. Firestone'un, 2018'de yayımladığı *An Information Security Overview* adlı raporunda belirlediği 3A formülü, doğru kişinin doğru zamanda doğru kaynaklarla doğru nedenlere erişimini sağlamayı öncelemektedir. Firestone (2018: 47), CIA üçlemesinin ortaya sunduğu argümanları genişleterek farklı perspektifler sunarak alana katkı yapan bir çalışmadır. Bu formülde kimlik doğrulama (authentication), yetkilendirme (authorization) ve inkâr edememe (non-repudatiation) ilkeleri mevcuttur.

Her bir aktörün yaptığı tanımların farklılığına bakıldığında, siber uzay kavramının aktörlerin algılarına göre şekillendiği gözlemlenmekte ve nihayetinde keskin ve net bir tanımının olmadığı için göreceli bir kavram olarak nitelendirildiği vurgusu yapılmaktadır (Çahmutoğlu, 2020a: 1-4). Akyeşilmen ve Kurnaz (2020:7)'a göre siber uzay hakkında gerçekleştirilen tanımların birçok veriyi bir arada içerecek ölçüde kapsamlı olmasına rağmen literatürde yapılan tanımlamalarda hukuk ve insan hakları vurgusunun eksikliği göze çarpmaktadır. Türkiye'nin hazırlamış olduğu Ulusal Siber Güvenlik Stratejisi'nde geliştirdiği tanım, diğer tanımlara oranla daha liberal ve evrensel bir tanım olmasına rağmen insan hakları ve hukuka yapılan vurgu konusunda ise tıpkı diğer örneklerde olduğu gibi eksik değerlendirilmektedir. Son zamanlarda uluslararası çapta yıkıcı saldırıların gerçekleştiği bilinmektedir ve belli başlı ülkelerin siber uzayı önemli gündem maddesi haline getirerek güvenlik kaygılarını bu alana taşıdıkları gözlemlenmektedir.

2.1.2. Güvenlik Kaygılarını Siber Uzaya Taşıyan Başlıca Devletler

Küreselleşme ışığında teknolojik gelişmelerin mevcudiyeti, devletleri ve o devletlerin vatandaşlarını dijital bir hayata doğru sürüklemektedir. Bilgiye kolay erişim, etkili ve hızlı sesli-görüntülü iletişim ve insan hayatını kolaylaştıran birçok farklı unsur değerlendirildiğinde devletlerin de bu teknolojik imkanları kullanarak vatandaşlarının huzuruna sunması Bıçakcı (2014: 102)'ya

[9] Dağıtılmış Servis Engelleme Saldırıları, genellikle Dağıtılmış Hizmet Reddi (DDoS) saldırıları ismiyle adlandırılmaktadır. Online hizmete dayalı tüm işletme, kurum ve kuruluşları hedef alan DDoS saldırıları, hedefteki web kaynağına birden çok istek göndererek web sitesinin çok sayıda isteği işleme kapasitesini aşmayı ve doğru şekilde çalışmasını engellemeyi amaçlamaktadır. Ayrıntı için bkz, (Kapersky, 2021).

göre, dijital bir hayat çerçevesinde siber uzay teknolojisinin sivilleştiğini gösterir. Devlet kontrolünde olan birçok altyapıların internete bağlılığı sonucu bir nevi ihtiyaç olarak değerlendirilen siber uzay, genişlemesini sürdürerek devletleri de içine alan bir yapı haline gelmiştir. Çevre, enerji ve sürdürülebilirlik, ulaşım, iletişim gibi birçok alanda vatandaşlarına hizmet de sunmayı amaçlayan devletler, özellikle 2000'li yılların sonundan itibaren ulusal ve uluslararası alanda kamuoyu oluşturmak için sosyal medyayı da kullanmaya başlamış, siber uzay kapsamında çeşitli devletlerle de mücadele etmek istemiştir (Darıcılı, 2014: 9).

Devletlerin siber uzaya müdahil olması, siber güvenliğin jeopolitik boyutunu da tartışmaya açmıştır. Bilgi çağının yaşandığı 21. yüzyılda verilerin güvenliğini sağlamanın gerekliliği, sınırlarının olmaması ve siyasi, sosyokültürel sonuçlarının olması siber uzayın çok boyutlu ve devamlı değişkenlik gösteren akışkan bir kavram olduğunu açıklamaktadır. Hakkında farklı tanımların yapılması ve ortak bir görüş birliğinin olmamasının yanında devletler son dönemlerde siber uzayı güvenlik kapsamına almıştır. Daha çok internet altyapılarına yönelik yapılan saldırıların şiddetinin ve etki boyutunun artması sonucu devletlerin yayımladığı stratejik belgeler, siber uzayı dikkate aldıkları ve bu alanda güvenlik kaygıları taşıdıklarını göstermektedir (Luiijf vd., 2013: 7).

Bilginin değerli sayıldığı ve güç olarak nitelendirildiği uluslararası sistemde bu unsurun korunması da zorunluluk olarak nitelendirilmektedir. Uluslararası ilişkilerin geleneksel güvenlik çerçevesine bakıldığında korunması gereken yapının, kimden veya kime karşı korunacağı bilinmektedir. Dolayısıyla alınacak önlemler, düşmanın kimliğine göre belirlenmektedir. Geleneksel güvenlikte düşmanı bilmek ve tanımak, güvenliği sağlamanın olmazsa olmaz kuralıdır. Ancak konu siber güvenlik olduğunda, düşmanın kim olduğunu ve nereden geleceğini bilemeyen aktör, savunma mekanizması geliştirme hususunda bir o kadar da zorlanmaktadır. Siber uzay, referans nesnesi devlet olmayan bir güvenlik biçimi oluşturduğu için kimlik tespiti, zarar boyutu tahmini gibi pek çok unsuru belirlemek oldukça zordur (Akyeşilmen ve Kurnaz, 2020: 18-19). Devletlerin bu konuya yaklaşımı özellikle yaşanan önemli olaylardan (Estonya saldırıları, Stuxnet saldırıları, Wikileaks gibi) sonra daha da artmıştır. Zira bir önceki başlıkta da belirtildiği üzere siber uzay, yaşanan önemli gelişmelerden sonra devlet nezdinde alçak politikadan (low politics), yüksek politikaya (high politics) doğru devinim göstermiştir (Choucri ve Clark, 2012: 17-19)

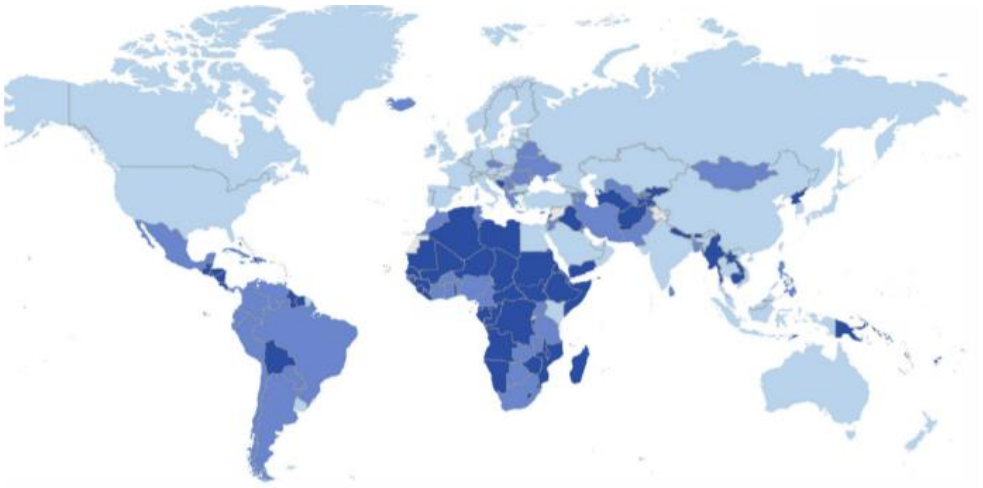
Siber saldırıların yarattığı etki ve tahribat küreselleştikçe, devletlerin ilgi ve odak noktası da o oranda siber uzaya doğru yönelmiştir. Ulusal gücün ölçüt ve belirleyicileri arasında askeri imkanların haricinde siber gücün de son zamanlarda yer aldığı bilinmektedir. Devletler askeri alanda nasıl saldırı ve savunma kapasitelerini geliştiriyorsa siber uzayda da savunma ve saldırı yönlerini artırmak zorundadır. Siber saldırı gücü yüksek olan devletler, caydırıcılık unsuru olarak bunu kullanabilirken, saldırı gücü görece daha zayıf olan devletler siber saldırılara daha fazla maruz kalmaktadır. Ancak unutulmaması gerekir ki ülkenin kritik altyapı sektörleri, kurumları ve kuruluşları siber alana ne kadar bağımlıysa, siber saldırılara karşı o kadar savunmasızdır (Çeliktaş, 2018: 475). Bununla

birlikte Devletlerin risk ve tehdit tespiti noktasında bir aksiyon planı belirlemesi, o planı devamlı yenilemesi ve mevcuttaki plana (CIA üçlüsü veya 3A formülü gibi) sadık kalması elzemdir.

Birçok devlet, siber güvenlik politikası oluşturmak suretiyle siber uzaya, güvenlik kaygıları içerisinde yer vermek istemiştir. İlk olarak ABD, dijital ortamda kendisine yapılan saldırıları korumak için 1998 yılında bir kanun yayımlamıştır (Pernik vd., 2016). Bunun yanında 2003 yılında da kapsamlı olarak ilk strateji belgelerini oluşturmuşlardır. Bu belgeler yıllar geçtikçe devamlı olarak yenilenmiştir. Son imzalanan belge, 2018 yılında *Siber Caydırıcılık İnisiyatifi* olarak kayıtlara geçmiştir (Kızılay, 2020: 38). ABD'den sonra siber uzayda en çok aktif olan ülkeler sırasıyla Çin ve Rusya'dır. Bu üç ülkeden sonra stratejik belgeler yayımlayan ve siber uzaya yatırım yapmaya başlayarak etkin bir güç olmayı amaçlayan ülkeler sırasıyla Fransa, İsrail, İngiltere, Hindistan, Güney Kore, Kuzey Kore, Almanya, Türkiye, Brezilya, Kanada İtalya, Japonya ve İran'dır (Billo ve Chang, 2004: 93). Birçok devlet, siber güvenlik güç ve kabiliyetleri lehine aldıkları hukuki, teknik ve kurumsal tedbirler kapsamında kapasitelerini geliştirmeye ve uluslararası işbirliğine önem vermiştir.

Çeşitli şirketler ve kuruluşlar, ülkelerin siber güvenlik kapasitesini ölçerek analizlerde bulunmaktadır. Bu doğrultuda en kapsamlı çalışmaları ITU gerçekleştirmiştir. Çeşitli endekslerle ülkelerin amaç, kapsam ve yeterliliklerini değerlendirmişlerdir. Bu doğrultuda, *Küresel Siber Güvenlik Endeksi* ve *Ulusal Siber Güvenlik Endeksi* adında çalışmalar yapılmıştır (ITU, 2020). Şekil 3'te görüleceği üzere Küresel Siber Güvenlik Endeksi (2019)'nde devletler, ulusal güvenlik kaygılarını uluslararası boyuta taşıyarak dış politikada da caydırıcı olmayı amaçlamaktadır. ITU, ülkelerin küresel düzeyde siber güvenliğe olan bağlılığını ölçmek amacıyla; ülkelerdeki siber güvenlik bilincinin diğer ülkelerle kıyaslanmayı, küresel ve bölgesel düzeyde ülkelerin siber güvenliğe bağlılığını ve ülkeler arasındaki farkların siber güvenlik inisiyatifine katılım düzeyini tespit edip tartışmayı amaçlamaktadır. Beş adet göstergeye odaklanılan bu endekste; hukuk, teknik kurumların varlığı, organizasyon, kapasite ve işbirliği unsurlarına bakılmıştır. Tüm bu unsurlar değerlendirildiğinde siber güvenlik yönünden en güçlü ülkeler sırasıyla: İngiltere, ABD, Fransa, Litvanya, Estonya, Singapur, İspanya, Malezya, Norveç, Kanada ve Avusturalya'dır.

Şekil 3: Küresel Siber Güvenlik Endeksi (2019)



(Gelişmişlik seviyesi en yüksekten (açık mavi) en düşüğe doğru (koyu mavi) değişim göstermektedir).

Kaynak: ITU, 2020: 13

Zayıftan en zayıf ülkelere doğru ise sırasıyla: Orta Afrika Cumhuriyeti, Ekvator Ginesi, Kiribati, Vatikan, Eritrea, Kuzey Kore, Dominik, Yemen, Komoros, Kongo ve Maldivler'dir (ITU, 2020: 61-64). Bu istatistiğe bakıldığında devletlerin gelişmişlik ve teknolojik imkanlara erişilebilirlik seviyesine göre siber uzaya yakınlık-uzaklık yorumu yapılabilir ve bu alanda yoksunluk yaşayan devletler uluslararası gelişmelerden ve caydırıcı bir dijital güç olmaktan geri kalırken, teknolojik yetersizlikten dolayı siber uzaya yönelik hiçbir güvenlik kaygısı taşımamaktadır. Siber tehditlere yönelik savunma mekanizmasını geliştirerek yönetim kapasitesini artırmayı hedefleyen devletler ise *Ulusal Siber Güvenlik Endeksi* çerçevesinde değerlendirilmektedir. Kaynaklarının değerlendirilmesi ve ülkelerden alınan veriler ışığında kapasitelerinin ve dijitalleşmelerinin ölçüldüğü endekste kapasitesi en yüksek ülkeler sırasıyla: Yunanistan, Çek Cumhuriyeti, Estonya, Litvanya, İspanya, Belçika, Slovakya, Hırvatistan, Fransa ve Finlandiya'dır. Dijitalleşme düzeyine bağlı kapasiteler baz alındığında ise sıralama değişmektedir. Bu endekse göre dijital kapasitesi en yüksek devletler İsviçre, Güney Kore, İzlanda, Birleşik Krallık, Hollanda, Norveç, Danimarka, İsveç, Singapur ve Lüksemburg'dur (NCSI, 2021).

Siber savunma alanına yatırım yapan devletler McAffee (2012)'nin siber savunma raporunda, daha çok siber saldırı alanına yatırım yapan devletler ise Çeliktaş (2018: 477)'ın çalışmasında detaylı olarak anlatılarak puanlanmıştır. Öncelikle siber savunmaya yönelik yatırım yapan devletlere bakıldığında Tablo 4'te görüleceği üzere ilk sırayı 10 puanla İsrail almaktadır. Ardından 9 puanla ABD, Fransa, Almanya, İngiltere gelmektedir. Onun arkasında 8 puanla Kanada ve Japonya, 7 puanla Çin, Rusya, İtalya, Güney Kore bulunmaktadır. 7 puanla Brezilya, Hindistan, Türkiye bu listede yer alırken İran ve Kuzey Kore 6 puanla sonuncu sırada yer almaktadır.

Tablo 4: Ülkelere Göre Siber Savunma Güç Puanlaması

No	Ülke	Puan (1-10)
1	İsrail	**10**
2	ABD, Fransa, Almanya, İngiltere	**9**
3	Kanada, Japonya	**8**
4	Çin, Rusya, İtalya, Güney Kore	**7**
5	Brezilya, Hindistan, Türkiye	**6**
6	İran, Kuzey Kore	**3**

Kaynak: McAfee, 2012

Siber savunmaya yapılan yatırımlara bakıldığında Tablo 5'te yer alan bilgilere göre siber saldırı puanı 5'ten yukarı olan devletler ABD, Çin, Japonya ve Almanya'dır. Saldırı kapasitesi 4 puandan yukarı olanlar Rusya, İngiltere, Kuzey Kore, Fransa ve Kanada'dır. 3 puandan yukarıda olan devletler Hindistan, Brezilya, İtalya'dır. 3 puanın aşağısında sırasıyla İsrail, Türkiye, İran ve Kuzey Kore bulunmaktadır. En yüksek puana sahip ülke 8,95 ile ABD olurken en düşük puana 0,82 ile Kuzey Kore sahip olmuştur. Puanlamalar yapılırken ülkelerin siber savunma ve saldırı alanına ayırdıkları ekonomik bütçeler baz alınmıştır.

Tablo 5: Ülkelere Göre Siber Saldırı Güç Puanlaması

No	Ülke	Puan (≥),(≤)
1	ABD, Çin, Japonya, Almanya	**≥ 5**
2	Rusya, İngiltere, Kuzey Kore, Fransa ve Kanada	**≥ 4**
3	Hindistan, Brezilya, İtalya	**≥ 3**
4	İsrail, Türkiye, İran ve Kuzey Kore	**≤ 3**

Kaynak: Çeliktaş, 2018: 472

Küreselleşme çağında devletlerin siber uzaya yaptıkları yatırım, uluslararası alanda güvenlik sorunlarını ortaya çıkarmaktadır. Etki boyutu yüksek olan saldırılar, devletlerin savunma mekanizması geliştirerek caydırıcı olmayı amaçlamasını ve bununla birlikte siber uzayı yüksek politika olarak görmesi, alana yönelik önemi giderek artırmıştır. Öyle ki günümüzde devletler, güvenliklerini sağlamanın ulusal siber uzay güvenliğini sağlamaktan geçtiğinin bilincinde olduğu için bu alanda etkin bir güç olmayı amaçlayarak siber güvenlik silahlarını artırarak envanterlerini genişletmektedir. Bununla birlikte devletlerin, stratejik belgeler yayımlayarak güvenliklerini sağlamaya çalışması, siber güvenlik kapsamında bir gereklilik olarak değerlendirilmektedir. Aksi taktirde siber uzayın kötüye kullanımı sonucu siber saldırılar, siber terör ile ilişkilendirilmektedir. Devlet kaynaklı veya devlet-dışı örgütlerin-bireylerin organizasyonu vasıtasıyla siber terör, yıkıcı etkileriyle bilinmektedir ve karar vericiler tarafından bu olgunun varlığı suiistimal edilmeden, etki boyutunun da sınırsızlığı göz önünde bulundurularak devletlerin siber terörle mücadelede işbirliği yoluyla çözüm üretmesi gerekmektedir.

2.1.3. Siber Uzayın Terörle İlişkilendirilmesi ve Siber Terör Kavramı

Siber uzayın aktörleri olarak kabul edilen devletler, devlet-dışı aktörler ve teröristler, sınırsız saldırı girişiminde bulunabilir. Nye (2010: 9)'a göre siber uzay kapsamındaki bir aktör herhangi bir ülkeye, örgütlere veya iştirakindeki özel şirketlere siber saldırı gerçekleştirebilir. Saldırı eylemleri nicelik olarak devlet-dışı aktörlerde daha fazla görülmektedir. Bunun sebebi olarak, devlet-dışı aktörlerin geleneksel yaklaşımda varsayılan uluslararası sistem içerisinde karar veren tek yetkili merciinin devlet olduğu tezine karşı mücadele üzerinden okunmalıdır. Devlet otoritesini sarsmak için teknolojik imkanlardan faydalanılarak saldırı imkanının oluş(turul)ması, bireysel ve kolektif suçların terör boyutuna ulaşmasına zemin hazırlamıştır. Bu minvalde siber uzay, terörle ilişkilendirilerek 21. yüzyılda yeni bir terör dalgasının habercisi olmuştur.

Teknolojik ilerleme, küreselleşme ve modern devletlerin dijitale geçmesiyle birlikte ulus-devlet sisteminin güvenlik anlayışında taze ve dinamik bir kavram hüviyetinde olan siber uzay, bu alanda var olmak isteyen aktörlerin güvenlik ihtiyaçlarını şekillendirmiştir. Siber uzayın küresel bir boyut kazanmasından öncesine kadar gelinen süreçte devletler, "kimin güvenliği?", "kime karşı güvenlik?" gibi sorulara cevap arayarak geleneksel çerçevede güvenlik politikası oluşturmuştur. Ancak siber uzayın varlığının kabul edildiği ve ilgi alanının bu yöne doğru evrildiği uluslararası sistemde güvenlik politikası oluşturmak, devletler için oldukça güç olmuştur. Nitekim siber uzay, güvenlik teorilerinde ezber bozan bir yapı olarak değerlendirilmektedir. Şöyle ki; siber uzayda geleneksel anlayışta tespit edilmesi gereken iki unsurdan en az birisi (ikisinin de bir arada bilinmediği durumlar mümkündür) bilinmemektedir. Yani "kime karşı korunacağız?" sorusu cevapsız kalmaktadır. Saldırıyı gerçekleştiren aktörlerin verdiği mesajlara bakılarak kim/kimler olduğunun, ne/ne amaçla yaptığını bulmak ve tahmin yürütmek dışında pek bir alternatifi kalmamaktadır. Üstelik siber uzayda evrensel olarak kabul edilmiş bir hukuksal normun da olmaması (devletlerin iç hukukundaki kanunlar haricinde), kimliğin tespit edilmesine rağmen kanunen bu saldırıları meşru kılmaktadır. Dolayısıyla siber terör, kendisini daha çok uluslararası alanda göstererek etki ve şiddet boyutlarının sınırlarını zorlamaktadır.

Konvansiyonel terör saldırılarında uygulanan yöntemler (bomba, suikast gibi) ışığında uygulanan şiddetin can ve mal kayıpları gibi tahribat derecesi yüksek sonuçlar doğururken siber terör; devletlerin enerji ve iletişim altyapısı başta olmak üzere, bankalar, e-posta zincirleri gibi internet altyapılarını hedef alarak çoğunlukla ekonomik zarar vermeyi veya kamuoyunda yankı uyandıracak skandalları teşhir yoluyla duyurmayı amaçlamaktadır. Bu tip saldırıların yarattığı tahribat konvansiyonel teröre göre daha fazla amaca yönelik veya tahammül edilebilir olarak değerlendirilmesinin yanında internet var olduğu sürece bu saldırıların devamlılığında sınır olmayacağı için önlenemez bir tehlikeye de davet çıkarmaktadır. Suç şebekelerinin internet ortamında sıklıkla kullandığı ağlarda (Silk Road, Dark Web gibi), suç boyutunun insan hayatına etkisi noktasında önlenemez bir halde olduğunu da gözler önüne sermektedir. Özel şifrelemeler ve

yüksek güvenlik duvarı içeren yazılımlarla korunan bu ağlar, siber terörün sadece devlete yönelik yapılmadığını, insanlığın hatta tüm canlıların tehlike altında olduğunu göstermektedir. Dolayısıyla siber terörün, konvansiyonel teröre oranla daha tahammül edilebilir olduğu savı göreceli bir argüman olarak değerlendirilmektedir.

Siber terör kavramı, ilk olarak Soğuk Savaş'ın sonlarına doğru dile getirilmiş olup tıpkı siber uzay gibi farklı yorumlar ve farklı tanımlarla değerlendirilmiştir. Siber terörizm adı altında yapılabilecek en kapsamlı tanım, *teknoloji sistemleri kullanarak uzak sayısal girişimden kaynaklanan fiziksel hasar, kişisel yaralanma veya can kayıpları ile ilgili, politik olarak motive edilmiş bir şiddet eylemi* şeklinde yapılmaktadır (HAVELSAN, 2018). Kavram ilk olarak ABD'de kullanılmıştır. Ülke içinde kişi başına düşen bilgisayarın artması, bağımlılık oranlarını da artırdığından dolayı "elektronik Pearl Harbor" söylemi kullanılarak ülkenin 1941 yılında yaşadığı travmayla ilişkilendirilmiştir. 90'lı yıllarda taze bir travma olarak da ortaya çıkan 11 Eylül saldırılarından sonra teröre karşı duyulan güvenlik kaygısı siber uzaya da sıçramıştır (Alnıak, 2004: 93).

Siber terörle ilgili geliştirilen tanımlar, bilgisayar ağlarının ve kritik altyapıların güvenlik açığının ulusal güvenliği risk altına alma durumu noktasında birleşmektedir. Lewis (2002: 2), siber terörü *kritik ulusal altyapıları kapatmak, bir hükümeti ya da sivil nüfusu zorlamak veya korkutmak için bilgisayar ağı araçlarının kullanılması* olarak tanımlamaktadır. Devletler ve kurumlar nezdinde korku iklimi yaratan siber terör; psikolojik, politik ve ekonomik alanda duyulan güvenlik kaygılarını siber uzayla ilişkilendirmiştir. Modern zamanın en büyük korkularından birisi olarak adlandırılan siber terörün bu denli tehlikeli olmasının sebebi bilinmeyen bir tehdit olmasıdır. Bilinmeyen tehdit, bilinen bir tehdide göre daha korku verici olarak değerlendirilmektedir. Dolayısıyla direkt bir şiddet eylemi olarak gelmese dahi varlığının sürekli korku yaratması, bilgi eksikliği veya daha kötüsü yanlış bilgi, Weimann (2004: 3)'a göre bombaların etkisi kadar güçlü olabilir.

Lewis (2002: 3), ulusların savunmasızlığını dijitale olan ilişkisine bağlamaktadır ve bu bağlılık devam ettiği sürece yeni güvenlik açıkları meydana geldiğini belirterek savunmasızlık durumunu *elektronik bir aşil topuğuna* benzetmektedir. Ona göre siber terörün literatür içerisinde değerlendirilebilmesi ve tartışılması için dört farklı bileşkeden bahsedilmektedir. Saldırıların tarihsel bağlamının tespiti, altyapının hasara yatkınlığı, altyapının dijitale bağlılığı ve teröristlerin siyasi hedef ve motivasyonu olarak dile getirilen bu unsurlar ışığında siber terörün değerlendirilebilmesi mümkündür. Mevcut analizler ışığında devletler ve kurumların siber teröre maruz kalmamak için yöntemler geliştirdiği ve bu yöntemlere stratejik güvenlik belgelerinde yer vermektedir. Bundan hareketle siber terör, ulusal güvenlik sorunu olarak görülmektedir.

Clarke ve Knake (2011: 9), "siber" ve "terör" kavramlarının bir arada kullanılmaması gerektiğini savunmaktadır. Sebep olarak da terörist olarak kabul edilen/tanınan kişi-örgütlerin siber

terör gerçekleştirdiğine dair elde kanıt olmadığını göstermektedir. Modern terör dalgasında bulunan köktendinci terör örgütlerinin internet kullanımı sınırlı olarak nitelendirilmektedir. Teröristler; büyükelçiliklere, demiryollarına ve otellere yönelik saldırıları planlamak veya interneti para toplamak, militan kazanmak gibi iletişim ve propaganda amaçlı kullanmıştır. Dolayısıyla teröristlerin, siber saldırı yaptığına dair bir iddiada bulunmak yanlıştır. Ancak yazarlara göre şu ana kadar yapılmamış olması, şu andan sonra yapılmayacağı anlamına gelmemektedir. Nitekim yıkıcı bir siber saldırı düzenlemek, nükleer bomba yapmak gibi büyük bir endüstriyel çaba gerektirmediğinden iyi finanse edilen bir terörist grup, para karşılığında siber saldırı yapacak yetenekli bir hacker tutabilir. Ancak bu eylemin hayata geçmesinin zor olarak değerlendirilmesinin sebebi hacker ve terör örgütü arasındaki güven eksikliğidir (Clarke ve Knake 2011: 9-15).

Siber terör hakkındaki tartışmalara ve terör örgütlerinin siber uzayı kullandığına dair kanıtlar olduğunu tezini savunan Yonah Alexander, Aralık 2001'de "Irak Ağı" kavramını ortaya atmıştır. Alexander (2000: 41)'a göre, bu ağda Irak hükümetinin desteklediği hackerlar, ABD şirketlerine karşı hizmet reddi saldırıları gerçekleştirmiştir. Ancak bilindiği üzere siber saldırılarda saldırganların kimliği tespit edilemediğinden dolayı mevcut siyasi **ortam** ve söylemlerdeki ipuçlarından yola çıkılarak en olası senaryo kurgulanmıştır. Netice itibariyle saldırıların kesin olarak El Kaide tarafından yapıldığı kanıtlanamadığından, literatürde geçerlilik açısından Clarke ve Knake (2011: 9-15)'in söylemleri daha çok dikkat çekmektedir (Weimann, 2004: 22).

Siber altyapı ve internet teknolojisi, insan hayatında önemli bir yere sahiptir. Bundan dolayı da çoğu ülkenin güvenlik duvarlarında ciddi ölçüde açıkların meydana gelmesi sürpriz değildir. Nesnelerin İnterneti (Internet of Things-IoT)'nde güvenlik açıkları, devletin dijitaldeki bütün altyapılarını kapsamaktadır. Siber terör daha çok toplumun ortak kullanım alanları, kamu kurum/kuruluş altyapıları, üretim, enerji ve ulaşım tesisleri, ekonomik kaynaklar gibi yapıları hedef almaktadır. Tablo 6'da görüldüğü üzere bu saldırılar sekiz başlıkta özetlenmektedir:

Tablo 6: Siber Terör Hedef Alanları

No	Siber Terör Hedef Alanları
1	Gayrimenkul ve Mülkiyetleri Etkileyen Siber Terör Saldırıları
2	Havacılık Alanını Etkileyen Siber Terör Saldırıları
3	Perakende Sektörünü Etkileyen Siber Terör Saldırıları
4	İnşaat Sektörünü Etkileyen Siber Terör Saldırıları
5	Nakliye ve Taşımacılık Altyapılarında Siber Terör Saldırıları
6	Güç ve Enerji Altyapılarında Siber Terör Saldırıları
7	Sağlık Hizmetlerini Etkileyen Siber Terör Saldırıları
8	Telekomünikasyon Altyapısını Etkileyen Siber Terör Saldırıları

Kaynak: HAVELSAN, 2018

Gayrimenkul ve mülkiyetler, bilgi toplamak için oldukça elverişli bir alan olduğundan saldırganların tercih ettiği öncelikli alanlar arasında olmuştur. Siber terör saldırılarında yaygın olarak otomasyon mekanizmaları ve IoT sistemleri hedef alınmaktadır. Havacılık alanı ise yaygın olarak siber terör saldırı unsurlarında kullanılmakta ve sıklıkla havalimanı içerisinde bulunan elektronik sistemlerdeki bilgi akışına (kokpit-uçak iletişimini bozmak, uçak saatlerinin dijital gösterimiyle birlikte check-in sistemini hacklemek gibi) yönelik saldırılar gerçekleşmekte olup çoğunlukla drone ile havadan müdahale yapılmaktadır. Topluma hizmeti amaçlayan ve ticaretin önemli bir dinamiği olarak kabul edilen perakende ve inşaat sektörünün altyapılarına yapılan siber saldırılar, perakende sektöründe ürünlerin tedariki ve stok durumu gibi unsurlara, inşaat sektöründe ise sanayi makinelerine zarar vererek ciddi mali kayıplara yol açmaktadır. Keza ulaşım sektöründeki altyapılara yapılan siber saldırılar, ticaret başta olmak üzere pek çok açıdan devletleri ve şirketleri ekonomik sıkıntılara sürüklemektedir. Ulaşım ağında teknoloji sıklıkla kullanıldığı için özellikle hızlı tren gibi daha dijital sayılabilecek bir ulaşım aracının elektronik sistemine yönelik terör saldırıları, ciddi boyutta can ve mal kayıplarına yol açabilir. Güç ve enerji sistemleri, saldırganların en iştahlı olduğu alan olarak nitelendirilmektedir. Nitekim etki boyutunun ağırlığı ve medyadaki yansımaları bu alana yönelik saldırıları cazip kılmaktadır (HAVELSAN, 2018).

Kapsamı bakımından geniş bir ağa sahip olan ve nükleer santralleri de içine alan enerji bağlantılarına yapılabilecek herhangi bir saldırı, can ve mal kayıplarının yanında hedef haricindeki diğer birimlere de zarar verme potansiyelini taşımaktadır. Devletlerin belki de en kritik altyapılarından birisi olan sağlık hizmetleri, vatandaşa kamusal hizmeti sağlamak açısından hayati bir konumdadır. Teknolojinin ilerlemesi sonucu sağlık sektöründe elektronik cihazların yaygınlaşması, tedavi amacıyla kullanılan pek çok aracın (kalp pili, akıllı saatler gibi) siber terör saldırısı sonucu kontrol altına alınıp kötü amaçla kullanılabileceği anlamına gelmektedir. Tüm bu sektörlerin akabinde son olarak değinilecek alan iletişim-haberleşme sektörüdür. Tarihin her döneminde en etkili araçlardan birisi olan iletişim ağları, elektronik ortamda kullanılmaya başladığından beri tehlikeli hale gelmiştir. Günümüzde telekomünikasyon altyapıları, internetin olduğu her yerde zaman veya yer fark etmeksizin açık hedef halindedir. Üstelik mobil cihaz sayılarının günden güne katlanarak artması, haberleşme altyapılarının genişlemesiyle akıllı ev-akıllı otomobil gibi örneklerin bu altyapıya bağlı olması siber terörün seçeneklerini de genişletmiştir (HAVELSAN, 2018).

Geleneksel güvenlik araçlarının ulaşması zor olan bir eğilim haline gelen siber uzay, terör unsuruyla alan içerisinde varlık gösteren aktörlere yönelik ciddi bir tehdittir. Siber terör ciddiyetini koruyan ve giderek büyüyen bir tehdit olarak görülmektedir. Terör saldırısında bulunanların amaçlarının genellikle ekonomik zarar verme odaklı olduğu da göz önüne alındığında, devletler arasında kritik ekonomik altyapılara yönelik saldırıların olma ihtimalinden de bahsedilebilir. Bunun yanında siber terör, suç örgütleri için de cazip bir alan olarak değerlendirilmektedir. Çünkü küresel

piyasa ekonomisini reddeden örgütler için ölümcül bir araç olmasa da potansiyel olarak yararlı bir araç olarak görülmektedir.

2.2. Siber Uzayda Varlık Gösteren Aktörler, Yöntem ve Amaçları

Modern bir ulus devletin yaşamsal fonksiyonlarını gerçekleştirebilmesi için geleneksel araçların yanında 21. yüzyılın özel bir gerçeği olan teknolojinin de göz önünde bulundurulması elzemdir. Bu doğrultuda siber uzaydaki güvenlik tehditleri, teknolojik gelişmişlik ile doğru orantılıdır. Nitekim potansiyel tehditlere önlem almak için teknolojik altyapıya ciddi oranda yatırımlar yapılması gerekmektedir. Teknolojik altyapı imkanlarının genişlemesi ve kapasitenin ileri düzeyde tutulmasına karşı siber tehditlerin kapsamı ve boyutu da aynı oranda genişlemektedir.

Siber uzayda tehdit yaratan aktörler; devletler, hacktivistler ve terörist organizasyonlar gibi farklı kimliklerdir. Devletlerin karşılaştığı tehditlerde de en çok dikkat edilmesi gereken aktör, devletten devlete değişiklik göstermektedir. Birçok devlet konvansiyonel savaş stratejilerinin yanı sıra siber savaşa karşı çeşitli hazırlıklar ve tatbikatlar gerçekleştirmektedir. Nitekim gelişmiş ülkelerde oluşturulan ulusal savunma sistemleri, ileri düzeydeki bilgi teknolojileri vasıtasıyla korunmaktadır. Ulusal savunma ve bilgi depolama gibi alanlarda teknolojiden en iyi seviyede faydalanmanın getirdiği sonuçlarla birlikte, savunma sistemlerinin güvenliği açısından da önemli hassasiyetler ve prosedürler mevcudiyetini korumaktadır. Gelişmiş teknoloji vasıtasıyla rakip görülen ülkelere üstünlük sağlanmasının bir neticesi olarak, terör grupları tarafından hedef alınıp haberleşme, savunma veya temel altyapı hizmetleri gibi alanlar zarara uğramaktadır.

Siber saldırıların ve tehditlerin teknolojik gelişmeler paralelinde artışı, 21. yüzyıldan itibaren devletleri siber güvenlik alanına yoğunlaşmıştır. Devletlerin ulusal güvenliklerinde siber güvenlik ihtiyacının oluşmasına ön ayak olan gelişmeler hiç şüphesiz ortaya çıktığı andan itibaren internet ve yarattığı engeller olarak karşımıza çıkmaktadır. Bu engeller, kişi ve kurumlarla birlikte devletlerin de güvenliğini sarsacak (kişisel ya da kamusal bilgilerin sızdırılması, ticari bilgilerin çalınması gibi) tahribatlara da yol açabildiği için 2000'li yılların başından itibaren hükümetler, siber güvenliği önceleyerek bu alanda aksiyon almaya ve eylem planları oluşturmaya karar vermiştir (Akyeşilmen, 2019: 129).

2.2.1. Devletler

Ulusal güvenlik bağlamında pek çok ülke ulusal siber güvenlik stratejisi yayımlayıp, teknolojik altyapılara yatırım yaparak güçlenmeyi amaçlamış ve alan içerisinde kendisini göstermeye çalışmıştır. Siber güvenlik stratejisini geliştirmeye çalışan devletler, bu alanı öncelikli güvenlik alanı olarak kabul ederek çağa ayak uydurmaya çalışmıştır. Devletlerin siber güvenlik politikaları oluşturmasında 2007'deki Estonya saldırısı bir dönüm noktası teşkil etmektedir. Nitekim bu olaydan

sonra birçok ülke siber güvenlik stratejisini oluşturma ve eylem planlarını gerçekleştirmeye başlamıştır (Tarhan, 2020: 42). Hatta Avusturalya bu konuda bir ilke imza atarak 2016 yılında siber uzay ile alakalı elçilik açmıştır (Siber Bülten, 2016).

Devletlerin siber güvenlik politikaları oluşturduğu yıllara bakıldığında ABD, 2003 yılında siber güvenlik eylem planı oluşturarak ilk adımı atmıştır. Asya kıtasında ilk olarak 2005 yılında Çin'in Ulusal Enformatizasyon Planı (National Informatization Plan) kabul edilir. Okyanusya ülkesi olan Avusturalya, 2009 yılında siber uzaya resmi olarak giriş yapmıştır. Avrupa'da ise 2010 yılında İngiltere ve Sırbistan ilk ülkeler kabul edilirken, Afrika'da 2011 yılında Güney Afrika, siber güvenlik alanında stratejik belge yayımlayan ilk ülke olmuştur. Bu devletler, Tablo 7'de detaylı olarak görülmektedir.

Tablo 7: Ülkeler ve Siber Güvenlik Eylem Planlarının Oluşturulma Yıllı

<table>
<tr><th>Asya</th><th>Avrupa</th><th>Afrika</th><th>Amerika</th></tr>
<tr><td rowspan="2">Afganistan: 2014
Bangladeş: 2014
İsrail: 2011
Hindistan: 2013
Japonya: 2015
Ürdün: 2012
Pakistan: 2014
Katar: 2013
G. Kore:2009
Rusya: 2011
Çin: 2005
S.Arabistan: 2013
Singapur: 2013
Türkiye: 2013
İran: 2010</td><td rowspan="2">Avusturya: 2012
Belçika: 2014
Çekya: 2015
Hırvatistan: 2014
Kıbrıs: 2012
Estonya: 2014
Litvanya: 2011
Karadağ: 2013
Hollanda: 2012
Norveç: 2012
Polonya: 2013
Sırbistan: 2010
Slovakya: 2008
İspanya: 2013
İsveç:2015
İsviçre: 2012
İngiltere: 2010</td><td rowspan="2">Mısır: 2012
Gana: 2014
Kenya: 2014
Mauritius: 2015
Fas: 2013
Nijerya: 2014
G. Afrika: 2011
Uganda: 2014</td><td>Brezilya: 2012
Kanada: 2013
Kolombiya: 2011
Trinidad-Tobago:2012
ABD: 2003</td></tr>
<tr><td>Okyanusya</td></tr>
<tr><td></td><td></td><td></td><td>Avusturalya: 2009
Yeni Zelanda: 2011</td></tr>
</table>

Kaynak: Azmi vd., 2016: 17

Siber uzayı kimi devletler daha çok politik/ekonomik çıkar için kimileri ise bölgesel hegemonyasını artırarak dış politikada elini güçlendirmek için kullanmaktadır. Devletler, siber uzayı uluslararası rekabetin temel dinamikleri arasında kabul etmektedir. ABD'nin, Gelişmiş Kalıcı Tehditler (Advanced Persistent Threats-APT)[10] olarak adlandırdığı hükümet kurumları veya şirketlerinin çok zamanlı saldırılarının yarattığı zorlukların yanında potansiyel tehdit olarak gördüğü aktörler Çin, İran, Rusya ve Kuzey Kore'dir. ABD, bu ülkelerin düzenlediği siber operasyonları demokrasilerine bir meydan okuma olarak görmektedir (CISA, 2009).

[10] Gelişmiş Kalıcı Tehditler (Advanced Persistent Threats-APT), genellikle yabancı bir devlet olan ve bir kuruluşu hedef alarak karşı taraftaki varlığı başarılı bir şekilde ele geçirmeden durmayan, uzun süreli erişime sahip olarak veri elde etmeye çalışan tehdidi tanımlamak için kullanılır. Ayrıntı için bkz, (Akın ve Sağıroğlu, 2017: 4).

Devletler için siber güvenliği tesis etmek ve kendisini sürekli olarak yenileyerek çağa ve teknolojik gelişmelere ayak uydurabilmenin yanında caydırıcılık ve güç unsuru da bir o kadar önemli bir husustur. Devletlerin birbirine karşı üstünlük kurma çabası, Soğuk Savaş ve önceki dönemlerde açıkça gözlemlenen bir olgudur. Bunun yanında geleneksel güvenlik anlayışının değişmesi, özellikle Soğuk Savaş döneminden sonra siber uzayın uluslararası ilişkiler literatüründe yüksek politika olarak kabul edilmesi sonrası siber güç kavramı ortaya çıkmış ve devletler nezdinde önem kazanmıştır. Siber gücü var olan bilgilerin haricinde yeni bir unsur olarak kabul eden Nye (2010: 5), siber alan içerisinde birbirine bağlı bilgi kaynaklarının kullanılmasını siber güç olarak tasvir etmiştir ve siber uzaydaki aktörleri çeşitlilik, anonimlik ve fiziksel mesafenin yokluğu olarak üç özellik üzerinden açıklamıştır.

Siber güç ve caydırıcılık, bu alanda var olmak isteyen her devlet için olmazsa olmaz bir kavram hüviyetindedir. Devletlerin etkin bir şekilde hakimiyetini sağlaması için pek çok farklı dinamiği içerisinde bulundurması ve mümkün olduğu süre içerisinde belirli aralıklarla kendisini yenilemesi gerekmektedir. Öyle ki Zhang (2012: 803)'a göre siber güce sahip olan bir devletin sahip olması gereken özellikleri belirtirken bahsi geçen dinamiklere dikkat çekmiştir. Bu özellikler: İnternet ve bilgi teknolojisi yetenekleri, bilgi teknolojisi endüstrisi yetenekleri, internet pazarının yetenekleri, internet kültürü, internet diplomasisi/dış politika yetenekleri, siber askeri güç ve bir siber uzay stratejisine katılmaya ulusal ilgi şeklinde verilmiştir.

Siber güvenliğin caydırıcılık boyutuna bakıldığında saldırıyı gerçekleştiren veya gerçekleştirecek aktörün tespit edilmesinin zorluğu, caydırıcılık unsurunun devreye girmesini de güçleştirmektedir. Çünkü caydırıcılık düşmanı ikna etmenin yollarından birisi olarak değerlendirilmekte olup, Wheatley ve Hayes (1996: 4)'e göre, *bir eylemi korku veya şüphe aracılığıyla önleme veya vazgeçirme* olarak açıklanmaktadır. Siber saldırılara karşı kimlik tespitinin yapılamaması, devletler nezdinde caydırıcılık oluşturmanın oldukça zor olarak değerlendirilmesine sebep olmaktadır. Nye (2010: 11), siber caydırıcılık unsurunun oluşturulması için saldıran ve saldırılan aktörün aralarındaki asimetrik bağın önemine vurgu yapmaktadır. Bir devlet gücü gereği belirli ölçülerde kimlik tespiti yapabilecek mekanizmalara sahiptir, aynı zamanda saldıran tarafın başka bir devlet olması durumunda tespitin daha rahat yapılabileceği ve diplomatik araçların kullanılarak yasal açıdan teminatının alınması mümkündür.

Devletler siber caydırıcılık stratejisi oluştururken alabileceği hasar karşısında güçlü önlemler geliştirip savunma örgütlenmelerini güçlendirmeye odaklanmıştır. Bu doğrultuda devletler, siber caydırıcılık faaliyetlerini gerçekleştirebilmek için gerek bireysel gerekse AB-NATO gibi uluslararası örgütler vasıtasıyla çeşitli işbirliklerine gitmiştir. Diplomasi kavramının siber uzaya uygulanması sonucunda devletler teknolojik alanda kurumsallaşmak için farklı adımlar atmaya başlamıştır. Buna ABD Dışişleri Bakanlığı'nın siber diplomasi ofisi kurması örnek olarak verilebilir. Ayrıca bu noktada Çin'in de önemli girişimleri olmuştur. Merkezi İnternet Güvenliği ve Lider Bilgi Grubu

adında diplomasi ajansları kurulmuştur. Aynı zamanda bu iki ülke çeşitli konularda bir araya gelip siber diplomasi kavramını uluslararası ilişkiler disiplininde test etmek suretiyle 2015 yılında Siber Casusluk Anlaşması yapmıştır (Korhan, 2020: 58).

Siber güvenlik içerisinde devletlerin gelişim göstermesi, asimetrik tehlikeyi çağırmaktadır. Nitekim önemli askeri, ekonomik, kamusal veya kişisel bilgilerin bir veri vasıtasıyla internet ortamında saklanması, saldırıya açık ve ulaşılabilmesi mümkün bir durum olarak nitelendirilmektedir. Asimetrik tehdit de bu noktada devreye girerek devletler; devlet-dışı organizasyon, örgüt veya çıkar gruplarının açık hedefi haline gelmektedir. Gizli bilgilere ulaşılabilirliğin mümkün olduğunu Nye (2010: 16-18), "gücün yayılması" (diffusion of power) olarak adlandırmaktadır.

2.2.1.1. Devlet Destekli ve Devlet Dışı Aktörler

Teknolojik unsurların ve seçeneklerin artması hususunda 21. yüzyıldan itibaren insanlığın dijital bir çağa entegre olması ve zaman geçtikçe bu alana bağlılığının artması birtakım risk unsurlarını da içerisinde barındırmaktadır. Saldırıya açık durumda olan kişisel veriler, saldırganların nitelikleri doğrultusunda kolay bir şekilde erişilebilir konumdadır. Halihazırda siber uzayın asimetrik doğası, saldırganlara birçok imkân tanımaktadır. Düşük maliyetle maksimum zarar, yasal açıdan rahatlık, casusluğun gizlilik seviyesi gibi örnekler saldırganlar için siber uzayı daha cazip kılmakla birlikte asimetrik doğasının olduğunu da gözler önüne sererek devlet-dışı aktörlerin sayılarının ve faaliyetlerinin artmasına olanak sağlamaktadır. Bununla birlikte devlet-dışı aktörlerin kimliğinin tespit edilmesinin zorluğu dikkate alındığında hackerların ve hacktivistlerin kendilerini örgütlerinin ismiyle açıklaması sayesinde devlet-dışı aktörlerin kim/kimler olduğu anlaşılmaktadır. Buna verilecek en büyük örnek şüphesiz geniş çapta duyurulan birkaç web tahribatının, bilgi sızıntılarının, hizmet reddi saldırılarının ve bazen ulusal güvenlik veya askeri meselelerle ilgili diğer siber eylemlerin sorumluluğunu üstlenen kolektif bir ekipten oluşan Anonymous'tur.

Siber milis olarak adlandırılan ve Rusya destekli olduğu iddia edilen bir hacker topluluğun Estonya'ya gerçekleştirdiği saldırı, pek çok kaynak tarafından ilk asimetrik örnek olarak karşılansa da miladı 1989 yılındaki Wank Solucanı (The Wank Worm) olarak kabul edilir. Çünkü bu ve beraberindeki saldırı çeşitlerinde (Tablo 8'de ayrıntılı olarak görülmektedir) hükümet destekli veya devletler kontrolünde olduğu iddia edilmeyen biçimler gözlenebilir. Daha açık bir ifadeyle devlet-dışı aktörlerin kendi aralarında gerçekleştirdiği saldırılar olarak literatüre geçmektedir (Sigholm, 2016: 3).

Tablo 8: Devlet Dışı "Hacktivist" Siber Eylemlerinin İlk Örnekleri

1989	**Wank Solucanı** Nükleer silahları protesto etmek için NASA'nın bilgisayar ağına sızma ve Galileo sondasının güçlendirici sistemini beslemek için radyoaktif plütonyum kullanımı.
1995	**Strano Ağı Oturma Eylemi** Nükleer ve sosyal konulardaki politikaları protesto etmek için Fransız hükümetinin bilgisayarlarına yönelik bir "ağ saldırısı".
1998	**"UrBaN Ka0s" Hacklemeleri** Doğu Timor halkının zulmüne odaklanan Endonezya hükümeti web sitelerinin manipüle edilmesi.
1998	**Elektronik Rahatsızlık Tiyatrosunun "Web Sitesi Girişleri"** Zapatistaları desteklemek için Pentagon ve Meksika hükümetinin web sitelerine yönelik hizmet reddi saldırıları.
1999	**"Team Spl0it" Savaş Karşıtı Bilgisayar Korsanlığı** Kosova ihtilafına bir son verilmesi çağrısında bulunan web tahribatı.

Kaynak: Sigholm, 2016: 3

İnternete erişimin ve kullanımının artmaya başladığı 1990'lı yıllarda gerçekleşen siyasi olaylar (bunda SSCB'nin dağılmasının payı büyüktür) neticesinde devlet-dışı aktörlerin siyasi amaçlar güden siber saldırı girişimleri gerçekleşmiştir. Kosova Savaşı sırasında bu tarz saldırıların gerçekleştiği ve dijital ortamda provokatif girişimleri tetiklediği bilinmektedir. Savaş esnasında adını I. Dünya Savaşı öncesi Sırp askeri toplumundan alan ve "Kara El" olarak bilinen Sırp merkezli bir grup hacker, Kosovalı Arnavut bir web sitesine saldırılar gerçekleştirerek NATO ülkelerinin askeri bilgisayarlarını sabote etmekle tehdit etmiştir ve Denning (2001: 17)'e göre bu çatışmalar, "ilk internet savaşı" olarak adlandırılmaktadır. Benzer provokasyon eylemlerinin sıklıkla yapıldığı bu dönemde çok sayıda dijital saldırılar gerçekleşmeye devam etmiştir.

Siber saldırıların ekonomik tahribatının fazla olduğu bilindiğinden dolayı hacktivist olarak tanımlanan örgütlerin yaşattığı krizler uluslararası kamuoyuna yansımıştır. Bilinen örneklere bakıldığında 2009 yılında birçok ülkede hem devlet hem de özel kuruluşlara ait gizli bilgilere erişen "GhostNet" siber casusluk ağının yarattığı tahribatın yüksek olduğu söylenmektedir. Ayrıca Rohozinski (2009: 35)'in çalışmasında belirttiği üzere GhostNet Çin hükümeti tarafından desteklenmektedir. Bu savı desteklemek için saldırıları gerçekleştirilen sunucu sinyallerinin Çin'in Hainan adasından alındığı belirtilmiştir (Chang, 2019). Ancak Çin hükümeti bu iddiaları reddettiğinden ve saldırılara bizzat destek verdiğine dair geçerli bir kanıt bulunmadığından dolayı saldırının tüm yükünü doğrudan Çin'e bağlamak yanlış olacaktır.

GhostNet örneğine dair bir çıkarım yapılması gerekirse siber uzaya yatırım yapan çeşitli hükümetlerin, devlet-dışı aktörlerle gayri resmi yoldan işbirliğine gitmesi olağan karşılanmaktadır. Çünkü bu alanda yetkinlik derecesine sahip olan yazılımcıların, hackerların ve bağlantılı mühendislerin niyetlerinin iyi ya da kötü olduğuna bakılmaksızın tecrübelerinden faydalanılması devletler tarafından elzem karşılanmaktadır. Aynı zamanda devlet-dışı aktörlerin ekonomik açıdan

arzularının ve güvenliğinin devletler tarafından sağlanması ve bunun yanında gerek görülmesi halinde devlet yetkililerini de zor duruma sokacak gizli bilgilere erişilmesi, devlet-dışı aktörler çerçevesinde kazan-kazan niteliğindedir. Siber olaylar anonimlik içerdiğinden saldırgan aktörler minimum risk ile eylemlerini gerçekleştirdiğinden dolayı kendilerini denetleyen veya cezalandırabilecek hiçbir unsur yoktur. Bu durum siber uzayda uluslararası sistem tarafından tanınmayan devletler için muazzam bir asimetrik avantaj sağlamakladır (Sigholm, 2016: 25). Netice itibariyle siber saldırılarda devlet-dışı aktörlerin varlığı, bu tarz devletlerin faydalanabilmesi açısından çok hayati bir seçenek olarak değerlendirilmektedir.

Devlet-dışı aktörlerin çoğalmasında siber uzay, Gady (2011)'e göre onlarca yıl önce başlayan bir süreci hızlandıran ve güçlendiren bir kuvvet çarpanı olarak açıklanmaktadır. Yasal çerçevelerin yoksunluğu bu alanda varlık gösteren örgütleri özgür kıldığından özellikle uluslararası örgütlerin bu alanda gösterdiği çaba her ne kadar etki oranı yüksek olmasa da önemli bir dinamiktir. Bu alanda kapsamlı olarak hazırlanan ve taraf devletlerin tüm devletleri kapsadığı Cenevre ve Lahey Sözleşmeleri gibi genel kabule dayalı uluslararası anlaşmaların tesis edilmesi elzemdir. Nitekim devlet-dışı aktörlere devlet müdahalesinin azaltılması veya yasal düzenlemelerle kontrol altına alınması, siber uzayı şimdiki halinden görece daha güvenli bir ortama kavuşturabilir.

2.2.2. Amaçlar, Araçlar ve Saldırı Yöntemleri

Günümüzde siber uzayda var olan ve bu alan içerisinde etkinliğini artırmak isteyen aktörlerin en çok ilgilendiği husus güvenlik olmuştur. Bu çerçevede aktörler öncelikli olarak kendi güvenliğini korumak istemiş ve tercihlerine bağlı da saldırı unsuru olarak geliştirilen araçlardan faydalanmışlardır. Siber uzaydaki aktörlerin çokluğu da amaçlar, araçlar ve saldırı yöntemleri yelpazesinin çok geniş olmasına sebep olmaktadır. Çünkü herhangi bir aktörün bu alanda var oluş amacı veya saldırı yaparken kullandığı araçlar aktörden aktöre farklılık göstermektedir. Siber saldırıların silah olarak kullanılması noktasında üç farklı ayrım vardır. Bunlardan ilki sentaktik saldırıdır. İkincisi semantik saldırı, üçüncüsü ise karışık saldırılar olarak adlandırılmaktadır (Brenner ve Goodman, 2002: 4). Sentaktik saldırılar, bilgisayar sistemlerini hedef alan saldırı tipi olup zararlı kodlar veya yazılımlar, DDoS saldırıları ve sistemi engellemek suretiyle yapılan saldırı çeşitleridir. Semantik saldırı türünde ise bilgisayar işletim sistemleri veya yazılımları hedef alınmamaktadır. Bu saldırı çeşidinde elde edilen bilgilerin doğruluğu değiştirilmektedir ve genelde devletlerin ve önemli kuruluşların kurumsal internet sitelerine veya kritik altyapı sistemlerine yönelik saldırılar gerçekleşmektedir. Son olarak bu iki saldırıların bir arada yapılmasına karışık saldırılar adı verilmektedir (Polat, 2015: 139).

Siber uzayda kullanılan araçlara bakıldığında literatürde en sık rastlanılan araçlar; çeşitli zararlı yazılımlar, virüs, trojan, bakteri olarak adlandırılan ve etki derecesi birbirine benzer veya farklı

yönleri bulunan saldırı çeşitleridir. Kapsamlı bir şekilde bu saldırı araçlarına bakılması ve tanımlarının yapılması gerektiğinde:

- Bilgisayar Virüsleri: Bir program ürünü olarak kendisini kopyalayarak hedefteki bilgisayara sızmasıyla bilinmektedir. Aktif hale geldiğinde sayısız virüs yükleyerek hedefteki bilgisayarın çökmesine, bilgilerin silinmesine ve yerleştiği bilgisayarın işleyişini olumsuz biçimde değiştirmesine sebep olmaktadır (Güntay, 2014: 83).
- Solucan *(Worm):* Bağımsız bir bilgisayar programı olan solucan, kopyalanarak çoğalmaktadır. Kısa sürede çeşitli varyasyonlarla hızlı bir şekilde yayılmasıyla bilinmektedir. Üstelik bunları yaparken karşı bilgisayar sistemlerinin tanıyamayacağı ölçüde yazılımlara zarar vermeden gizli bir şekilde varlıklarını sürdürmektedir. Çoğunlukla e-postalar vasıtasıyla bulaşmaktadır (Karnouskos, 2011: 4491).
- Truva Atı *(Trojan)*: Eriştiği bilgisayar sisteminde fark edilememesinden dolayı ismine Truva Atı adı verilen bu yazılım, aslında yararlı bir enstrüman olarak görülen ancak eriştiği sisteme ciddi ölçüde zararlar veren hasar derecesi yüksek bir saldırı çeşididir (Güntay, 2014: 83).
- Mantık Bombası *(Logic Bomb):* Genellikle bir program içinde çalışan ve belirli bir olay veya zaman gerçekleşene kadar etkin olmayan kodun bir kısmı olarak tanımlanmaktadır. Mantık bombaları, çok sayıda casus yazılım ve av kaldırma sağlayıcısının bu tür işlevleri finansal kazanç için kötüye kullandığı bilinmektedir (Science Direct, 2016).
- Arka Kapı *(Black Door):* Bir diğer ismiyle tuzak kapı olarak da adlandırılan bu yazılım, yalnızca bunu kullanan aktör tarafından bilinmektedir. Normalde bilinen yollarla erişilmesi gereken kimlik bilgilerine gizli yollarla arkasında iz bırakmadan girildiğinden dolayı buna arka kapı denilmektedir (Güntay, 2014: 84).
- Kaydedici *(Keylogger)*: Adından da anlaşılacağı üzere bilgisayar sistemine eriştiği andan itibaren gerçekleştirilen her eylemi kaydederek servis sağlayıcısına görüntülerini servis etmesiyle bilinmektedir (Yener, 2013).
- *Botnet*: Uzaktan kontrol edilmenin amaçlanarak bilgisayar sistemlerine yerleştirildiği bu yazılım çeşidindeki faaliyetlere bakıldığında dolandırıcılık, özel bilgi, kimlik ve veri hırsızlığı gibi özellikleri içerisinde barındırarak hedeflenen sistemi uzaktan kontrol etmektedir (Yener, 2013).
- Kök Kullanıcı Takımı *(Rootkit)*: İşletim sistemlerinde minör boyutta var oldukları için fark edilmesi oldukça zor olan Kök Kullanıcı Takımları, hedefteki bilgisayarda gizlenmesi ile bilinen zararlı programdır (Güntay, 2014: 84).
- Fidye Yazılımı *(Ransomware):* Kötü amaçlı yazılım programlarından birisi olan bu program, bulaştığı sistemde sistemin bir kısmını veya tamamını şifreleyerek, verilerin kullanıcı tarafından görüntülenmesini engellemektedir ve kullanıcılardan talep edilen paranın ödenmesi beklenmektedir. İnsanlar üzerindeki etkisi itibariyle fidye yazılımları en

tehlikeli siber terör araçlarından birisi olarak değerlendirilmektedir. Wannacry, NotPetya, SimpleLocker, CryptoLocker, TB-Locker, WinLock en çok bilinen fidye yazılımlarıdır (Yener, 2013).

- Script: İnternet sayfalarında işlevini sürdüren kodlar bütünüdür. Scriptler vasıtasıyla hedeflenen yere toplu saldırılar gerçekleştirilmektedir (Güntay, 2014: 84).

Mevcut kötü amaçlı yazılımların kullanılmasıyla pek çok aktör, saldırgan veya saldırılan konuma düşmüştür. Ancak hangi aktörün, hangi saldırıda hangi enstrümanı kullandığının tespit edilmesi oldukça zordur. Kesin olarak belirtilebilecek husus, kurumlar teknolojik enstrümanlara ve araç gereçlere sahip olan hemen hemen her aktör, bu tür saldırılardan etkilenme potansiyeli taşımaktadır. Siber saldırı faaliyetlerinin genişlemesi, saldırı faaliyetlerinin hangi alana yönelik olduğuna dair tartışmalar, uluslararası araştırma kuruluşlarınca her yıl düzenli olarak değerlendirilmektedir. Teknolojik gelişmelerin her geçen yıl üzerine koymasıyla daha kapsamlı bir şekilde genişleyen siber saldırı faaliyetlerinin hangi alanlarda yoğunlaştığının analizi yapılmaktadır. Karafloski (2021)'nin araştırmasına göre siber suç faaliyetleri son 5 yılda %15 artmıştır. 2020 yılında yapılan siber saldırılar en çok hırsızlık, itibar zedelemek ve siyasi rüşvet alanlarında yoğunlaşmıştır. 2020'de yapılan saldırılar bir önceki yıla göre değerlendirildiğinde finans sektöründe %238 artmıştır. Bulut tabanlı saldırılar, özellikle 2020 yılı içerisinde Ocak ve Nisan ayı aralığında %630 seviyelerinde artış göstermiştir. Fidye yazılımı üzerine saldırılar ise %148 oranında artış göstermiştir.

PurpleSec Firması (2021), ortaya çıkan siber tehdit unsurlarını analiz ederek 2021'deki temel siber güvenlik tehditlerini sıralamıştır. Buna göre ilk olarak Koronavirüs (Covid-19) sürecinin yarattığı karantina ve evden çalışma durumunun yaratacağı güvenlik tehditlerinden bahsedilmektedir. Öte yandan fidye yazılım (*ransomware)* olarak adlandırılan saldırıların da yıkım etkisi oldukça büyük olmaktadır. Yıl bazlı yarattığı tahribatlara bakıldığında 2018'de 8 milyon dolar, 2019'da 11,5 milyon dolar, 2020'de ise 20 milyon dolara kadar çıkmıştır. Bununla birlikte fidye yazılımı saldırısı, 2020'de bir Alman vatandaşın ölmesiyle alakalı skandal bir olayla da anılmaktadır (Cimpanu, 2020). 2021 yılında sürekliliğine devam eden temel siber güvenlik tehditlerinin en çok arttığı alanların başında madencilik, ulaştırma, inşaat ve enerji sektörü gelmektedir. Ayrıca tedarik zinciri sektöründe yoğunlaşmasının kaçınılmaz olacağı savunulmaktadır. Bu tip saldırılardan kaçınmak için ise kullanıcıların güvenlik kontrollerini sağlaması gerekmektedir. Bu çerçevede güvenlik merkezlerine yönelimin artması olağan karşılanmaktadır. Çünkü, siber saldırıları meydana geldiklerinde azaltmak veya önlemek için gerçek zamanlı izleme, tespit ve müdahale sağlamaktadır. Bununla birlikte çok faktörlü kimlik doğrulaması gibi güvenlik algoritmalarının daha da kapsamlı geliştirmelerle kullanıcıların en çok tercih edeceği uygulamalar olacaktır (Firch, 2021).

Bu bölüme son bir değerlendirme yapılması gerektiğinde artık silah kavramının değiştiğine yönelik yapılacak olan yorumdur. Uluslararası çatışmaların doğasında iki büyük değişim meydana

gelmiştir. Bunlardan birincisi, teknolojinin gelişim göstermesiyle birlikte silah kavramı da değişmiştir ve siber uzayın imkân ve kabiliyetleri artmıştır. İkincisi ise siber tehdit vurgusunun farklı bir yapıya bürünmesi ve bu yapının uluslararası toplum tarafından bizzat algılanmasıdır. Nitekim siber tehdit uluslararası bir boyut kazanmakla birlikte tüm dünyayı ilgilendiren evrensel bir sorun olma noktasında elde ciddi göstergelerin (fiziksel zarar, can kaybı) olması, kabul edilebilirliğini de mümkün kılmaktadır (Yayla, 2014: 184).

2.3. Siber Terörizm

"Siber uzay" ve "terörizm" kavramlarının birleştirilmesiyle oluşturularak yeni ve tek bir anlam kazanan "siber terörizm", literatüre ilk olarak 1980'de girmiştir ve bu kavramı ilk olarak Barry Collin kullanmıştır. Collin (1997: 16), siber terörizmi tanımlarken devletlerin mevcut dönemdeki bilgisayar teknolojilerine olan ön yargı ve endişesinden yola çıkmıştır. Terzi (2018: 76)'ye göre siber terörizm, teknoloji ve internet unsurlarının artması sonucu ortaya çıkan tehdittir. Siber terörizme kırmızı ringa balığı[11] benzetmesinde bulunan Clarke ve Knake (2011: 4), ise böyle bir olgunun kanıtlanamayacağından dolayı varlığından da söz edilmesini gerekli görmemektedir. Weimann (2004: 3)'a göre siber terörizm, çağımızın "yeni terörü" olarak nitelendirilmektedir ve bu kavram psikolojik, politik ve ekonomik kaygıları bir arada bulunduran bir korku bütünü olup, medyanın da oluşturduğu algı neticesinde kendisine dramatik bir boyut kazandırmaktadır. Sigholm (2016: 13)'e göre siber teröristler, saldırılarını gerçekleştirmek için bilgisayar ve ağ teknolojilerini kullanan ve kamuoyunda korku yaratan kişilerdir ve bu kişiler siber uzayda bu tür saldırıları gerçekleştirmeyi başarırlarsa, sonuçlar önemli olabilir ve bu nedenle hiçbir zaman göz ardı edilmemelidir.

Cuevas ve Rennison (2016: 41)'a göre siber teröristlerin izlediği temel motivasyonların başında politik amaç gelmektedir. Genellikle kimlik vurgusu yapan suç şebekelerinin önemli tarihi olaylara göndermeleri, ya da bir ülkeye spesifik bir konu üzerinden saldırı gerçekleştirmeleri yaptığı bilinmektedir. Bir diğer motivasyon kaynağı para ve eğlencedir. Tabi bunları tetikleyen en önemli unsur kişisel ego ve kendini sahada test etme güdüsüdür. Başka bir bakış açısıyla ise genellikle asosyal olarak değerlendirilen bu kişilerin kendilerini bir gruba ait hissetmek istemeleri, kimi saldırganların saldırıyı gerçekleştirmek için en önemli motivasyonudur (Yalman, 2018: 261).

Siber terörizm, internet kullanımındaki hızlı büyümenin ve ortaya çıkan "bilgi toplumu" tartışmasının yaygınlaşmaya başladığı 1990'lı dönemlerde kendisini çok daha derin hissettirmeye başlamıştır. Özellikle kurumlarını teknolojik imkanlarla donatan devletler, dijitale yüksek oranda bağlı olduğundan dolayı daha da tehlike içerisinde olmaktadır. Nitekim bilindiği üzere 1990'ların

[11] 18. ve 19. yüzyıllarda sıklıkla kullanılan bir İngiliz deyimi olarak kayıtlara geçen kırmızı ringa balığı, dikkat ve ilgi odağını gerçeklerden ayırarak bilinci yanıltmayı amaçlayan bir deyim olarak tanımlanmaktadır. Ayrıntı için bkz, (History Extra, 2021).

başında ABD'nin karşı karşıya geldiği potansiyel tehditler bu minvalde gerçekleşmiştir ve "elektronik Pearl Harbor" terimi ortaya çıkmıştır. Bu noktada George W. Bush'un henüz göreve gelmeden önce siber terörizm hakkındaki tutumu belirleyici olmuştur. Bush, ABD kuvvetlerinin yeni tehdit ve zorluklara karşı yetersiz finanse edilmesinden şikâyet ederek devletin ilgi ve odak noktasını kitle imha silahlarına ve siber terörizme yöneltmiştir. Nitekim Bush'un göreve geldiğinde yaptığı ilk icraatlardan biri Siber Uzay Güvenlik Ofisi'nin kurulması olmuştur (Green, 2001).

2000'li yıllardan itibaren, özellikle 11 Eylül saldırısından sonra terörizme yönelik söylemlerin çehresinin genişlemesiyle siber uzayda da terörizmin kendisini daha derinden hissettirdiği bir döneme doğru girilmiştir. Öyle ki Ulusal Şehirler Birliği tarafından 2003 yılında 725 şehirde yapılan bir ankete göre siber terörizmin, şehir yetkililerinin korku listesinin başında biyolojik ve kimyasal silahlarla birlikte yer aldığı sonucuna ulaşılmıştır (Weimann, 2004). 11 Eylül örneği ile ABD, siber terörizm kavramını uluslararası siyasete yerleştirerek sistem içerisinde meşruluk sağlamayı amaçlamıştır.

Günümüzde kritik altyapılara yapılan saldırılar olarak kendisini gösteren siber terörist aktiviteler korku ve endişe vermenin yanında kendisine karşı geliştirilen koruma amaçlı yazılımlara karşı da direnç göstererek güncel kalabilen bir organizma olarak nitelendirilebilir. Bu doğrultuda terör örgütlerinin ellerinde bulundurduğu konvansiyonel kitlesel imha silahlarından da ayrılmaktadır. Ayrıca, terör eylemini fiilen gerçekleştiren kişi/kişiler terörist olarak adlandırılırken Denning (2001: 2)'e göre siber terör eylemini gerçekleştiren kişiler "hacktivist" olarak nitelendirilmektedir ve bu kavram "hacklemek" den türetilmiştir. "Hacklemek" tanımsal olarak, bilgisayar işletim sistemlerindeki güvenlik açıklarını ortaya çıkarmaya, avlamaya veya başka bir şekilde istismar etmeye çalışmak suretiyle çevrimiçi ve gizli olarak yürütülen siber faaliyetler bütünüdür. Hacktivist kavramı çeşitli yerlerde ve çeşitli durumlarda kullanılıp kullanılmama durumu değişkenlik gösteren bir niteliktir. Örneğin, bir e-posta virüsü, kimi zaman hacktivizm, kimi zaman da siber terörizm olarak nitelendirilmektedir. Ya da bir aktör, hedeflediği şey hakkında bilgi toplamak için kendisi gibi olan diğer kişilerle örgütlenmek ve siber terörizm faaliyetini gerçekleştirmek için interneti kullandığında bu aktör hem bilgisayar korsanı hem siber terörist hem de hacktivist olarak adlandırılabilir (Denning 2001: 4-12).

Hacktivistlerin sıklıkla kullandığı önemli silahlar; e-posta saldırıları, bilgisayar virüsleri ve bilgisayar solucanlardır ve genellikle politik süreçler içerisine dahil olmayı tercih etmektedirler. Weimann (2004: 4)'a göre hacktivizm, politik olarak motive olmasına rağmen, siber terörizm anlamına gelmemektedir. Genel olarak işleyen bir yapıyı bozmak ve protesto etmek isteyen hacktivistler, ahlaki kısıtlamaya sahip olmayarak bilgisayar korsanlarıyla benzer yöntemler kullanarak siber terörizm tehdidini taşımaktadır.

2.3.1. Siber Terör Kapsamında Değerlendirilen Önemli Siber Saldırılar

Siber terör kapsamında değerlendirilen saldırılara değinmeden evvel internetin, sosyal medyanın ve mobil cihazların dünya üzerindeki kullanım yaygınlığına bakılması gerekmektedir. We Are Social (2021)'ın 2021 yılında yayımladığı rapora göre dünya nüfusunun %59'u (4,66 milyar insan) internet kullanmaktadır ve %53 kadarı (4,20 milyar insan) sosyal medya kullanıcısıdır. Dünya nüfusunun %66 kadarı ise (5,22 milyar insan) mobil cihaz kullanıcısıdır. Tüm bu istatistiklere bakılıp 2020 yılına göre bir değerlendirme yapıldığında ciddi oranda bir artış gözlemlenmiştir. Buna göre internet kullanıcı sayısı 2020 yılına göre %7,3 (+317 milyon insan) artmıştır. Sosyal medya kullanıcı sayısı, %13,2 (+490 milyon insan) artmıştır ve son olarak dünya üzerinde mobil cihaz kullanıcısı sayısını 2020 yılına göre karşılaştırıldığında %1,8 (93 milyon insan) artmıştır (Kemp, 2021).

Her geçen gün kullanıcı sayısının arttığı internet ekosisteminde insanların hayatlarının gittikçe dijitale doğru yöneldiğini görmek mümkündür ve internetten talep edilen şeyler de insandan insana farklılık göstermektedir. Yine We Are Social (2021)'ın insanların neden internet kullandığına dair yaptığı araştırma sonucu hazırladığı rapora göre insanların büyük bir bölümü bilgi toplamak için interneti kullanmaktadır. Bu oranı takip eden unsurlar sırasıyla iletişim kurmak, rezervasyon yapmak, araştırma yapmak, dizi-film seyretmek, müzik dinlemek, gezecek turistik yerler aramak, sağlık ile alakalı araştırmalar yapmak, oyun oynamak ve yeni insanlarla tanışmaktır (Bayrak, 2021). İnternet kullanımının ve teknolojik imkanının gittikçe artması, siber terör unsurlarını da tetiklediğinden dolayı bu mecrada güvenlik ihtiyacının doğmasına neden olmuştur. Bu ihtiyacın talep haline dönüşmesi, insanlığın her geçen yıl daha fazla dijitalle bütünleşmesinin sonucunda güvenlik açıklarının doğması ve kişisel bilgilerin de tehlike altına girmesine zemin hazırlamıştır. Steve Morgan (2019: 4)'a göre en çok saldırı yapılan 5 sektör:

- Sağlık sektörü
- İmalat sektörü
- Finansal sektörler
- Devlet ve iştirakleri
- Ulaşım sektörüdür.

Teknolojik gelişme ve dijitale yönelişin, evrensel geçerliliği olan savaş hukukundan çok daha geç ortaya çıkmasından dolayı mevcut savaş kuralları ve düzenlemelerinin siber saldırılar, savaş veya terörle ilişkilendirilmesi oldukça zor olmaktadır. Rid (2013: 4)'e göre siber saldırılara gereğinden fazla önem verilmektedir çünkü gerçekleşen bir siber saldırının suç veya terör faaliyeti olarak değerlendirilmesi için kabul edilmiş herhangi bir savaş ile aynı sonuçları doğurması gerekmektedir ancak bu mümkün görünmemektedir. Yalman (2018: 259)'a göre ise siber suç genel bir suç kavramıdır ancak siber terörizm daha ayrıntılı bir kavram olduğu için daha özel olarak

değerlendirilmektedir. Bu sebepten ötürü de her siber suç faaliyeti, siber terörizm olarak nitelendirilmese de her siber terörizm faaliyeti, bir siber suç olarak nitelendirilmektedir. Dolayısıyla hangi saldırıların savaş veya terör saldırısı olup olmadığına dair ortak bir kanı oluşmamaktadır. Ancak buna rağmen genel olarak siber terör olarak kabul görülmüş ve etki derecesi yüksek önemli saldırılar değerlendirildiğinde çeşitli olaylar tarihleriyle birlikte şu şekilde sıralanabilir:

- 1991 yılındaki I. Körfez savaşı sırasında bir grup Hollandalı hacker, ABD'nin Pentagon merkezli bilgisayar sistemine erişerek ülkenin savaş operasyon bilgilerini kopyalamış ve mevcut yöntemleri de değiştirmiştir (Yalman, 2018: 262).
- 1996 yılında Central Intelligence Agency (CIA) internet sitesine bir saldırı gerçekleşmiş ve sayfadaki bilgiler değiştirilmiştir. Bu olayla hemen hemen aynı tarihlerde gerçekleşen farklı bir olay ise bir hacker grubu, ABD Adalet Bakanlığı sitesini ele geçirerek sayfada Adolf Hitler'in fotoğrafını paylaşmışlardır (Çetinkaya, 2011).
- Yine 1996 yılında "Tubac Amaru" adındaki bir terör örgütünün gerçekleştirdiği Japonya Büyükelçiliği saldırısının planları, saldırıdan hemen sonra örgütün sempatizanları tarafından örgütün internet sitesinde paylaşılmıştır (Terzi, 2018: 81).
- 1999 yılında NATO'nun Sırbistan'a düzenlediği harekât neticesinde NATO üye ülkelerinin askeri haberleşme sistemlerine yönelik bir siber saldırı girişimi gerçekleşmiştir. ABD, kendisinde oluşan sıkıntıları giderebilmek adına virüse bulaşmış sistemlerini temizleyebilmek için bir haftalık süreyle dünyadaki tüm sunucularını kapatmıştır (Bıçakcı, 2012: 210).
- 2001 yılında ABD'nin California eyaletindeki elektrik hizmet sağlayıcısına saldırı düzenlenmiş ve bu saldırının sonucu olarak eyalette bir gün süreyle elektrik kesintisi uygulanmıştır (Yalman, 2018: 262).
- 2007 yılında, "Tallinn'in Bronz Askeri" adlı Kızıl Ordu Anıtı'nın, Estonya hükümeti tarafından yerinin değiştirilmesi sonrası, sistematik bir siber saldırı girişimi gerçekleşmiştir. Saldırılar öncelikli olarak finans merkezleri ve bankaları hedef almıştır. Ardından Estonya parlamentosunu, bakanlıklarını, medya organlarını, güvenlik ve ulaşım alt yapısını da hedef alarak kapsamı ve etkisinin şiddetini artırmıştır. Bu olay öncesi, elektronik ve dijital alandaki yatırımlarıyla oldukça güvenli bir konumda duran Estonya, ciddi ölçüde bir prestij kaybı yaşamıştır. Bu saldırının arkasındaki gücün kim olduğu net bir şekilde kanıtlanmamış olsa da Rusya'daki internet sitelerinde, Estonya'ya yönelik yapılan saldırının yöntemlerinin bulunması, saldırı iddialarını Rusya'ya yıkan en büyük veri olarak karşımıza çıkmaktadır (Bayraktar, 2015: 41)
- 2014 yılında Ukrayna'da internetin kesilmesine sebebiyet veren Rusya'nın Kırım'ı işgal etmesini destekleyen bir DDoS saldırısı meydana gelmiştir. Yine aynı yıl bir grup hacker, Ukrayna Cumhurbaşkanlığı seçiminden 3 gün önce seçim komisyonu sistemini ele

geçirmek suretiyle saldırılar gerçekleştirmiştir. Bu iki saldırının da arkasında Rusya'nın olduğu iddia edilmektedir (Yalman, 2018: 263).

- Yine 2014 yılında 500 milyon Yahoo kullanıcısının bilgileri çalınmıştır. Bu yaşanan olaydan daha önce de buna benzer saldırı faaliyetleri gerçekleşmiştir. Buna göre My Space'in 359 milyon, LinkedIn'in 159 milyon ve Adobe'un 152 milyon kullanıcısının bilgileri çalınmıştır (2018). 2016 yılında UBER firması, 57 milyon üzerinde sürücü bilgisinin saldırganlar tarafından çalındığını açıklamıştır. 2017 yılında ise 412 milyon kullanıcı hesabı Friendfinder sitesinden çalınmıştır (Ulutaş, 2018: 92). Buna benzer son bir olay olarak ise 2021 yılı Kasım ayındaki saldırı verilebilir. Haskoloğlu'nun bu tarihte saldırıyı gerçekleştiren hackerlar ile iletişime girerek yaptığı habere göre bir grup hacker, Yemeksepeti uygulamasındaki 50 milyon Türk vatandaşının bilgilerini çalarak Darkweb'e satmıştır (Webteknohaber, 2021).
- 2015 yılında bir grup hacker, Alman politikacılar tarafından kullanılan bilgisayarları ele geçirerek, gizli bilgileri çalmış ve karşılığında milyonlarca avro istemişlerdir. İddialara göre Almanya'nın Ukrayna'yı desteklemesi üzerine tepki göstermek için bu saldırının da arkasında da bir Ruslar gösterilmiştir (Yalman, 2018: 264).
- 2016 yılında yine Ukrayna'ya yönelik DDoS saldırısı gerçekleşmiş ve bu saldırı sonucunda 225,000 Ukrayna vatandaşının elektrikleri kesilmiş, telefon hatlarını da işlevsiz hale getirmiştir (Yalman, 2018: 264).
- 2017 yılında WannaCry adındaki bir fidye yazılımı vasıtasıyla 99 farklı ülkede eş zamanlı operasyonlar yapılarak 75 bin civarında kullanıcıya yönelik saldırı gerçekleşmiştir. Küresel bir saldırı olması ve eriştiği ülkelerin çok olması, siber terörizm eylemlerinin açıklanabilir en somut örneği niteliğindedir (Birkan Anıl Yılmaz, 2020: 69).
- İnternet üzerinden ATM'leri kontrol etmek için ATM yazılımı geliştirmeleri yapan ve bazı yıllarda ciddi spekülatif haberlerle gündemi meşgul eden Barnaby Jack, literatür içerisinde "Jackpotting" olarak da bilinmektedir. 2010 yılında gerçekleşen önemli bir olay sonrası adından ilk defa söz ettirmiştir. Bu olay, ABD'nin Las Vegas eyaletinde düzenlenen Black Hat Briefings adlı konferansa katılım gösteren saldırgan, bir telefon modemi kullanarak rastgele bir ATM'ye bağlanıp, herhangi bir şifre girişi yapmadan ATM içerisindeki tüm parayı çekmiştir. 2018 yılında ise FBI'ın aldığı "ATM cihazlarına saldırı gerçekleşecek" istihbaratı sonrası yerli halkta aşırı derecede korku ve endişe oluşmuş, ardından buna benzer bir olay yaşanmıştır ancak bunu Barnaby Jack'in düzenlediği kanıtlanmamıştır (Yalman, 2018: 266).

Siber uzayda gerçekleşen bu tarz saldırılar sonrası devletler, terörle mücadele hususunda uluslararası işbirliğini artırmak istemiştir. Siber terörizmle mücadele noktasında yalnızca politik düzlemde kalınmamış, ekonomik gerekçeler de göz önünde bulundurularak pek çok devlet tarafından bu alana ciddi fon ayırılmıştır. Siber uzayda devletler nezdinin aşılarak küresel bir farkındalık

durumuna gelinmesi için düşünce kuruluşları, sivil toplum örgütleri, özel şirketler ve hükümet-dışı örgütler, ayrıntılı bir şekilde konuyla alakalı çalışmalar yapmaya başlayarak alana katkıda bulunmak istemişlerdir.

2.4. Uluslararası ve Bölgesel Örgütlerin Siber Uzaya Yaklaşımı

Uluslararası ve bölgesel örgütlerin siber uzaya yaklaşımı genellikle siber uzayda yer alan tehdit ve tehlikelere karşı önlem almak, farkındalık oluşturmak veya bir eylem planı gerçekleştirmek ekseninde şekillenmiştir. Bu doğrultuda siber terörizm olgusunun önemine vurgu yapılmış, kolektif bilincin oluşturulması için sistematik çalışmaların gerekliliği tartışılmıştır. Bu çerçevede verilecek ilk örnekler NATO, BM, AB gibi geniş çaplı küresel örgütlerden gelmektedir. Aynı zamanda örgütler, güven artıcı önlemler alarak[12] bu önlemleri siber uzay içerisine de uyarlamaya çalışmışlardır. Bu çalışmalar nezdinde BM, Avrupa Güvenlik ve İşbirliği Teşkilatı (AGİT) ve Güneydoğu Asya Ülkeleri Birliği (ASEAN)'nde güven artırıcı önlemler siber uzaya adapte edilerek siber uzayla alakalı kapsamlı çalışmalar yapılmaktadır (Ziolkowski, 2013: 538).

2.4.1. Birleşmiş Milletler (BM)

BM, üye sayısı itibariyle en geniş çaplı uluslararası organizasyon olduğu için siber uzayda alınabilecek kararların bağlayıcılığı ve baskınlığı noktasında kilit bir oluşumdur. BM'nin siber güvenlik noktasında ilk tecrübesi Rusya'nın 1998 yılında BM Genel Kurulu Birinci Komitesi'nde sunmuş olduğu "Uluslararası Güvenlik Bağlamında Bilgi ve Telekomünikasyon Alanındaki Gelişmeler" başlıklı karar taslağı olmuştur (United Nations Digital Library, 1998). Bu tasarı sonrası BM'nin siber uzaya olan ilgisi daha somut bir boyuta erişmiştir. Bu doğrultuda BM nezdinde siber güvenlikle ilgili tartışmalar için çalışma düzeyinde bir platform sağlamak amacıyla ilk adım 2001 yılında atılmıştır. BM Genel Kurulu Birinci Komitesi tarafından uluslararası bilgi güvenliği alanındaki ve potansiyel tehditleri ve bunlara yönelik olası önlemleri içeren bir Hükümet Uzmanları Grubu *(Group of Governmental Experts)* kurulmuştur. 25 devlet uzmanının yer aldığı bu grupta küresel bilgi ve telekomünikasyon sistemlerinin güvenliğini güçlendirmek amaçlanmakta ve aynı zamanda kapasite geliştirerek siber uzayda işbirliği imkanları aranmaktadır (United Nations, 2019).

Areng (2013, 568)'e göre BM, siber güven inşası konusunda temel bir konsensüs geliştirerek kriz yönetimi ve kapasite geliştirme konularında işbirliği yapma ihtiyacına ilişkin didaktik bir dil benimsemiştir. İdealist bir perspektif çizen BM, bu tür bir işbirliğini teşvik etmek için uygun

[12] Devletlerin birbirine savaş ilanı halinde savaşın veya başka herhangi bir silahlı çatışmanın çıkmasını önlemeye çalışmak için uluslararası politika oluşturmanın amaçlanmasıdır. Siber uzay için uyarlanması *Confidence Building Measures for Cyberspace* olup CBM olarak kısaltılmaktadır. CBM'ler Siber uzayla ilişkilendirildiğinde ise internetin kendine has özellikleri nedeniyle, siber uzay için CBM'lerin geliştirilmesinin zor olduğu açıklanmaktadır ancak iyi bir şekilde kurgulandığında bunun mümkün olduğu anlatılmaktadır. Ayrıntılı bilgi için bkz, (Ziolkowski, 2013).

kararların belirlenmesinden uzak bir konumda olsa da üye devletlerin takip etmesini gerektiren bağlayıcılığı yüksek bir organizasyondur. Nitekim yaptığı çalışmaların güvenlik temelli olması da suçun takibi, tespiti ve yorumlanması için oldukça değerlidir. Bu doğrultuda BM, Bölgelerarası Suç ve Adalet Araştırma Enstitüsü *(UN Interregional Crime and Justice Research Institute)* tarafından 2004-2010 yılları arasında siber suçlardan sorumlu olan saldırganların yetenekleri, demografik yapıları ve tehlike seviyelerinin sınıflandırılmasını sağlamak, mücadele etmek ve aynı zamanda gerçekleşmesi muhtemel siber terörist faaliyeti önceden tespit etmek için bir mekanizma gerekliliğine dair araştırma projesi yayımlamıştır. Bu çerçevede ABD Savunma Bakanlığı'nın ortaya koyduğu "Siber Genom Projesi" çerçevesinde siber saldırıların altyapısı analiz edilmeye çalışılmış, potansiyel saldırıyı önlemek adına çeşitli manevralar değerlendirilmiştir (Cho vd., 2015: 1221).

BM'ye ait bir uzmanlık kuruluşu olan ITU, bilgisayar teknolojileri ile alakalı güncel küresel sorunlara odaklanan ve çeşitlilik barındıran BM nezdinde önemli bir yapı olarak değerlendirilmektedir. Klasik uluslararası kuruluşlardan farklı olarak ITU, hükümetlere ek olarak özel sektör ve bilim dünyasından önemli isimlerin de bilgi ve uzmanlık alanına başvurmaktadır. Siber güvenlik konusunda ise gelişmekte olan ülkelerde kritik altyapı koruması ve kapasite geliştirme konusunda en iyi uygulama kılavuzlarının geliştirilmesini amaçlamaktadır (Eldem, 2021). ITU kapsamında değerlendirilecek en önemli organizasyonlardan birisi, devlet ve özel sektörlerin bir arada olduğu bir girişim olan Siber Tehditlere Karşı Uluslararası Çok Taraflı Ortaklık *(The International Multilateral Partnership Against Cyber Threats-IMPACT)*'dır. Bu girişimde bir kriz sırasında yardıma çağrılabilecek bilgisayar teknolojileri uzmanlarının yanı sıra, kaynakları bir havuzda toplamak ve siber uzmanlar arasındaki işbirliği oluşturmak amaçlanmaktadır (Areng, 2013: 565-570).

2.4.2. Kuzey Atlantik Antlaşması Örgütü (NATO)

Çok yönlü ve çok kutuplu bir örgüt niteliğinde olan NATO, siber uzayda işbirliği noktasında ciddi adımlar atmaktadır. NATO, bir savunma paktı niteliği taşıdığından dolayı örgüte üye devletlere yönelik meşru müdafaa hakkını tetikleyen bir siber saldırı meydana gelmesi durumunda aralarındaki iş bölümü konusunda ortaya bir konsensüs koymak, ona riayet ederek daha kurumsal ve planlı adımlar atmak üye devletler için elzemdir. Ancak ortaya konulan her metnin koşulları açısından bağlayıcılık sağlanması için BM'den referans alınması zorunludur. Siber güvenlik konusunda NATO'nun aldığı bir kararın, BM'nin herhangi bir kararıyla çelişkili olması NATO'nun kurumsal yapısına ve devletlerin siber güvenlik politikalarının işleyişine zarar verecektir. Bu noktada siber saldırılara karşı NATO'nun aldığı sorumluluk kanunu şu şekilde ortaya konulmuştur (NATO, 2021):

- NATO'nun kendisi siber saldırı altında kalabilir ve bununla birlikte kendi savunma hakkını talep ederek karşılık verebilir.

- NATO'ya üye devletlerden herhangi birine siber saldırı olması halinde üye devletler meşru müdafaa hakkını kullanabilir.
- Bir veya daha fazla NATO üyesinin saldırı altında olması halinde bunlardan birkaçı toplu olarak savunma hakkını kullanabilir.
- NATO'ya yönelik siber saldırılar gerçekleşmesi ve aktörlerin tespit edilmesi halinde askeri operasyonlar yürütmesi söz konusu olabilir (Klabbers, 2013: 487).

NATO'nun siber güvenliğe daha çok yoğunlaştığı dönemine bakıldığında, Soğuk Savaş sonrası döneme odaklanmak gerekmektedir. Stratejik konseptlerinde değişikliğe gitmeyi hedefleyen NATO, özellikle 1990'lı yılların başından itibaren kapsamlı bir dönüşüm yoluna girmiştir. 1994 yılında Rusya-Çeçenler arasında geçen çatışmalarda Çeçenlerin interneti de bir saldırı unsuru olarak kullanmasından sonra uluslararası sistemde bilgi savaşı tartışmaları başlamıştır (Polat, 2015). Bunun üzerine NATO, teknolojik gelişmeleri takip etmek ve siber güvenlik dinamiğini kavramak adına Siber Savunma Yönetim Kurulu *(Cyber Defence and Management Board /CDMB*)'nu oluşturmuştur. Ardından 1996 yılında daha kapsamlı bir oluşuma imza atarak NATO İstişare, Komuta ve Kontrol Ajansı *(NATO Consultation, Command and Control Agency/NC3A)* oluşturularak kurumsal adımlar atılmaya başlanmıştır (Ada ve Çakır, 2017: 633-638). 1990'ların sonuna doğru toplantı ve istişare odak noktasını siber güvenliğe kaydırma çabasına giren NATO, çeşitli konferanslar ve forumlar düzenleyerek bilgi çağının gereksinimlerine ayak uydurmak istemiştir.

1999 yılında düzenlenen Washington Zirvesi'nde Yeni Stratejik Konsept yayımlanmış ve bu konsept içerisinde hibrit savaş kavramına yer verilmiştir. Gerekçe olarak da teknolojik gelişmeler sonrası bilgiye erişim ve kabiliyetlerini geliştirmek noktasında devlet-dışı aktörlerin de devletten bir farkının olmadığı vurgusu yapılarak tehdit yelpazesinin genişlediği bildirilmiştir (NATO, 1999). 11 Eylül terör saldırılarının akabinde direkt olarak NATO'ya veya NATO üyelerine yapılabilecek dijital saldırının ihtimalleri tartışılmaya başlanmış ve hissedilen bu endişe 2002'deki Prag Zirvesi'nde dile getirilmiştir. *Prag Yetenek Taahhütleri* ek metninde örgüt yapısının siber savaş nezdinde dönüşüme girdiği açık olarak belirtilmiştir (NATO, 2002). Ayrıca zirvede NATO'nun muhabere ve bilgi sistemlerinin korunması hususuna ilk defa değinilmiştir ve siber güvenlik, beş önemli tehditten biri olarak kabul edilmiştir (Polat, 2015: 135-138). 2006 yılında gerçekleşen Riga Zirvesi'nde ise bilişim sektöründeki gelişmeler takip edilerek örgütün kapsamlı bir koruma mekanizmasına ihtiyacının olduğu vurgusu yapılmıştır (NATO, 2006b).

Estonya saldırıları sonrası NATO, örgüt içerisindeki siber güvenlik çalışmalarını hızlandırarak 2008'deki Bükreş Zirvesi'nin gündem maddesi haline getirmiştir. Zirveden sonra NATO Siber Savunma Yönetimi Otoritesi'nin *(Cyber Defense Management Authority)* Brüksel'de kurulmasına karar verilmiş ve siber güvenlik adında örgütsel anlamda en önemli somut adımlardan biri atılarak örgüt bünyesinde ilk Siber Savunma Politikası oluşturulmuştur (Bıçakcı, 2014: 107-110). Üye

devletlerin kapsamlı işbirliğine gitmesinin gerekliliğine vurgu yapılan 2010 Lizbon Zirvesi (NATO, 2010) ve akabinde 2013 yılında siber uzaya hukuksal bir form kazandırmayı amaçlayan "Tallinn El Kitabı'nın"[13] temelleri Bükreş'te atılan adımların bir ürünü olarak değerlendirilmektedir.

Siber savunma kapasitesini geliştirip ortak akılla hareket etme hususunda NATO, transatlantik ilişkilerin de önem kazandığı girişimlere imza atmıştır. Bu doğrultuda önemli bir adım olarak 2016 yılındaki Varşova Zirvesi'nde AB ile siber güvenlik alanında işbirliği zemini aramıştır ve nihayetinde bu iki örgüt arasında "Siber Savunmaya İlişkin Teknik Anlaşma" imzalanmıştır. Bu çerçevede NATO'nun *Computer Incident Response Capability (NCIRC)* ile AB'nin *Computer Emergency Response Team (CERT-EU)* arasında bilgi ve tecrübe paylaşımı noktasında işbirliğine gidilmiştir. Zirvede kara, deniz ve havanın yanında siber uzayın harbin dördüncü boyutu olarak tanınması, önemli bir dönüm noktası olarak değerlendirilmektedir (Seren 2016: 9).

2.4.3. Avrupa Birliği (AB)

AB bünyesinde siber güvenliğin kurumsal bir perspektif kazanması Estonya saldırılarına dayanmaktadır. AB'yi direkt olarak etkileyen bir olay olarak değerlendirilen bu saldırılar, pek çok alanda olduğu gibi bu alanda da bir dönüm noktası niteliği taşımıştır. Estonya saldırıları sonrası AB bünyesinde yer alan ülkelerin bilişim alanında yaşadığı güvenlik sıkıntıları (özellikle Hırvatistan, Macaristan, Portekiz gibi ülkelerin internet kaynaklı çok sayıda güvenlik problemi yaşaması), birliğin odak noktasının siber güvenliğe daha fazla yönelmesine zemin hazırlamıştır (Eurostat, 2016). Bu çerçevede siber uzayda ciddi ve somut adımların atılmasını amaçlayan AB, siber güvenlik politikası ve stratejisi oluşturmak suretiyle kapsamlı çalışmalar ortaya koymuştur.

Eren (2017b: 230)'e göre AB'nin yasal düzenlemelerle siber güvenlikte kurumsallaşması noktasında 4 farklı dönüm noktası mevcuttur. Bunlar:

- Verilerin Korunması Direktifi (1995),
- Elektronik Haberleşme Sektöründe Gizliliğin Korunması Direktifi (2002),
- Bilgi Sistemlerine Saldırılar Hakkında AB Konseyi Çerçeve Kararı (2005),
- Verilerin Saklanması Direktifi (2006) olarak gösterilmektedir.

2004 yılında kurulmuş olan ENISA *(European Union Agency for Network and Information Security)* vasıtasıyla siber uzayda kurumsallaşma adımları atılan birliğin bünyesinde, çeşitli koordinasyonlar sağlanarak gizli bilgilerin ve kritik altyapıların korunması noktasında bir adım

[13] Yirmi ünlü uluslararası hukuk akademisyeni ve uygulayıcısı tarafından üç yıllık bir projenin ürünü olan Tallinn El Kitabı, uluslararası hukuku siber savaşa entegre etmeye çalışmaktadır ve siber çatışmaları yöneten "95 kara harfli kural" dan bahsetmektedir. Ayrıntı için bkz, (Schmitt, 2013b).

atılmıştır (ENISA, 2015). AB'nin siber güvenliğini sağlama noktasında etki alanını genişleten ENISA, zaman geçtikçe daha aktif bir konuma gelerek üye devletlerin bilgilendirilmesi, ortak forumlar düzenlenmesi gibi birçok alanda önemli bir hizmet mekanizması haline gelmiştir. Böylece risk yönetiminin sağlanması için AB standartlarının geliştirilmesini desteklemek ve sınır ötesi siber tehditlerin önlenmesine, tespit edilmesine ve bunlara yanıt verilmesine olanak sağlamayı kendisine misyon edinmiştir. ENISA koordinasyonunda AB ülkelerinin katılım gösterdiği ilk forum olan Siber Avrupa *(Cyber Europe)* 2010 yılında gerçekleşmiştir (ENISA, 2011). Ayrıca 2010 yılında kabul edilen AB İç Güvenlik Stratejisi içerisinde siber güvenlik düzeyinin yükseltilmesi hedeflenmiştir. 2012 yılında tüm AB kurumlarını kapsayacak bir ağ olan *CERT-EU* oluşturulmuştur. Onun hemen akabinde ise Avrupa Siber Suç Merkezi kurulmuştur (Areng, 2013: 565-570).

Belirtilen düzenlemelerin ve gelişen sürecin akabinde AB'nin siber güvenliğini sağlama noktasında bağlayıcı kapsamlı bir metin hazırlanmıştır. Avrupa Komisyonu, 2013 yılında Avrupa Birliği için Siber Güvenlik Stratejisi *(Cybersecurity Strategy for the European Union)*'ni yayımlayarak siber güvenlikte eylem planlarını ve bu süreçteki yasal düzenlemeleri ortaya koymuştur. Eren'e (2017b: 234) göre bu stratejik belge, roller ve sorumluluklar bağlamında Kopenhag Ekolünün analiz çerçevesinde değerlendirilen "güvenlikleştirme" teorisinin önemli bir ürünüdür. AB içerisinde bulunan 12 ülkenin ortak faaliyeti sonucu çeşitli alanlarda çalışma yapılması üzerine bir konsorsiyum COURAGE *(Cybercrime and Cyberterrorism European Research Agenda)* kurulmuştur. 2016 yılımda kurulan bu konsorsiyumda siber suç ve siber terörizm hakkında için ölçülü, kapsamlı ve ilgili bir araştırma gündemi sunulması amaçlanmıştır. COURAGE, üç temel ilkeyi benimsemiştir. Bunlar:

- Gerçek dünyadaki ihtiyaçlara ve deneyimlere dayalı olarak boşlukları, zorlukları ve engelleri belirlemek için kullanıcı merkezli bir metodoloji,
- Bir sınıflandırma sunmak ve konuya ilişkin tüm paydaşlarla ortak bir anlayış oluşturmak için analitik ve semantik bir yaklaşım ve
- Etkili test ve doğrulama çözümleri kullanarak karşı önlemlerin pratik uygulamalarını teşvik etmek için rekabetçi ve pazar odaklı bir yaklaşımdır.

Aynı zamanda AB vatandaşlarının ve ülkelerindeki kritik altyapılarının güvenliğini önemli ölçüde iyileştirmek ve suç araştırmacılarını desteklemek hedeflenmiştir. Buna göre konsorsiyum, araştırma gündemine yansıtılacak ve siber suçlulara ve siber terör faaliyetlerine karşı sürekli odaklanma yoluyla vatandaşların bilgi paylaşımına katılımını artırmayı öncelikli hedefleri arasına koymuştur. Çeşitli alanlarda işbirliğinin de önünün açılmasına ön ayak sağlayan AB, örgütsel formda siber güvenliğin ilerlemesine katkı sağlama hususunda kurum içerisindeki birimlerle etkin ve aktif olarak çalışmalar yürüterek NATO ile de işbirliği yapmaktadır. AB ve NATO, içerisinde ortak üyelerin bulunduğu ve bu üyelerin de ortak çıkarlarının doğrultusunda birbirini tamamlayan iki temel

örgüt konumundadır. Bilindiği üzere Varşova Zirvesi'nde alınan kararlar neticesinde *CERT-EU* üzerindeki işbirlikleri gerçekleştirilerek siber yetenekleri artırma noktasında önemli adımlar atılmaktadır (European Commision, 2016).

2.4.4. Diğer Bölgesel Kuruluşlar

Siyasi-askeri, ekonomik, çevresel ve insani boyutları birleştirerek güvenlikle alakalı diyalog kanallarını artırmaya odaklanarak şeffaf ve güven artırıcı düzenlemelerle dünyanın en büyük bölgesel güvenlik kuruluşu konumunda olan AGİT (OSCE, 1990), siber güvenliğe verdiği önemle de dikkat çeken bir kuruluş olarak nitelendirilmektedir. 2005 yılından itibaren, siber suçlarla mücadele ve siber terörizm konularını tartışmak gibi siber güvenlik konularıyla da ilgilenen AGİT, 2013 yılında *Siber Alandan Kaynaklanan Tehditlere Odaklanan Terörist Saldırılardan Nükleer Olmayan Kritik Enerji Altyapısının Korunması Hakkında İyi Uygulamalar Kılavuzu*'nu yayımlayarak teşkilatın siber güvenlik hakkındaki rolüne ve gelecekle alakalı değerlendirmelerine yer vermiştir (OSCE, 2013).

Başta Çin ve Rusya olmak üzere birçok Asya ülkesini içerisinde barındıran kapsamlı bir bölgesel güvenlik örgütü konumunda olan Şangay İşbirliği Örgütü (ŞİÖ), güvenlik temelinde pek çok alanda olduğu gibi siber uzayda da etkin bir şekilde var olmaktadır. Örgütün siber güvenlik alanında yaptığı en kapsamlı çalışma, 2009 yılındaki *Uluslararası Bilgi Güvenliği Davranış Kuralları'dır.* Çerçeve niteliğinde olan bu çalışmayla birlikte üye devletler, bilgi alanındaki hak ve sorumlulukları belirleyerek ortak tehlike ve zorlukları tespit edip işbirliğini geliştirmeyi amaçlamaktadır (CIS Legislation, 2009). Areng'e (2013, 576-581) göre ŞİÖ, BM'de siber ve bilgi güvenliği arasındaki iki blok arasındaki felsefi ve politik tartışmalardaki iki ağırlık merkezinden biri olarak görülmektedir.

Asya-Pasifik bölgesinde siyasi ve güvenlikle alakalı diyaloğu güçlendirmek amacıyla oluşturulan ASEAN, oluşturduğu Bölgesel Forum *(ASEAN Regional Forum-ARF)* vasıtasıyla bölge dahilinde güvenlik temelli işbirliği ekseni oluşturmaya çalışmaktadır (Austuralian Goverment Department of Foreign Affairs and Trade, 2021). ARF, 2013 yılındaki toplantısında siber güvenlik vurgusunu yapmış ve azgelişmiş ülkelerdeki güvenlik sorunları hakkında işbirliği çağırısında bulunmuştur. Ortak çalışmalar gerçekleştirmek amacıyla örgüt bünyesinde çok sayıda eğitim, seminer, konferans ve forumlar düzenlenmekte, işbirliği yolları aranmaktadır (U.S Mission to ASEAN, 2013). ASEAN, Çin ve Japonya ile işbirliği geliştirmeyi hedefleyerek her iki ülkeyle de siber güvenlik noktasında antlaşmalar yapmıştır. Bu bağlamda 2013 yılında *Japonya- ASEAN Dostluk ve İşbirliği* imzalanarak siber saldırılara ortak ve proaktif yanıt vermek suretiyle bilgi güvenliğini sağlamak amaçlanmıştır (Ministry of Internal Affairs and Communications of Japan, 2013). Yine 2013 yılında Çin ile gerçekleştirilen görüşmede taraflar siber güvenlikte işbirliğinin, en

iyi uygulamaların paylaşımı hakkında mutabakata vararak işbirliğinin sürekliliği vurgulanmıştır (Areng, 2013: 585).

2002 yılında Bağımsız Devletler Topluluğu (BDT) üyesi ülkeler (Rusya, Ermenistan, Belarus, Kırgızisan, Kazakistan ve Tacikistan) tarafından kurulan Kolektif Güvenlik Antlaşması Örgütü (KGAÖ), bölgesel güvenlik ve kriz yönetimini tesis etmek bağlamında Asya'da bulunan önemli bir güvenlik yapılanmasıdır. Chernenko (2013)'ya göre KGAÖ, NATO'ya karşı "karşı blok" olarak tanımlanmaktadır ve NATO'dan farklı olarak küresel kriz yönetimi hırsına sahip değildir ve üye ülkelerinin sınırları dışındaki operasyonlarda yer almaya çalışmamaktadır. Kuruluş ayrıca siber güvenlikte işbirlikçi çözümlere büyük önem vermektedir. Bu doğrultuda çalışmalarını yürüten KGAÖ, organizasyon içerisinde bilgi güvenliğini oluşturmak için ortak eylem programları gerçekleştirmektedir ve "Proksi" adı verilen ortak operasyonla üye devletlerin bilgi güvenliği sağlanmaya çalışmaktadır (Mshvidobadze, 2012).

ÜÇÜNCÜ BÖLÜM

3. DOĞU PERSPEKTİFİNDEN SİBER SAVAŞ VE SİBER UZAY

Doğu perspektifinden siber uzay kavramına bakıldığında bu bölgede artan siber saldırılar, ekonomik ve siyasi açıdan ciddi kriz yaratma potansiyeli taşımaktadır. Öyle ki Asya kıtasındaki bölgesel örgütlerin güvenlik önceliklerinde siber uzaya verilen önem oldukça dikkat çekici olmuştur. Bölgede çok sayıda terör faaliyetinin gerçekleşmesi ulus ötesi sorunların doğmasına sebebiyet vermekle birlikte devletler, siber alandaki güvenliklerine önem vermektedir. Mevcut güvensizlik ortamında bölgede siber ittifakların kurulması, ikili antlaşmaların yapılması ve devletlerin bireysel güç arayışına girmesi, siber uzayın Doğu perspektifinden farklı okunmasına sebebiyet vermektedir.

Siber tehditlerdeki artışlara ek olarak siber saldırı yöntemlerinin yapısında genişleme meydana geldikçe tehditlerin doğasında da değişiklik olmaktadır. Nitekim Thomas'ın (2009: 8-9) da belirttiği üzere dolandırıcılık, kimlik hırsızlığı gibi vakalar artmasında bilgisayar ağlarını kontrol eden çok sayıda kötü amaçlı yazılımın (özellikle truva atı olarak adlandırılan trojanlar) rolü büyüktür. Doğu ülkeleri, siber güvenliğin sağladığı ölçütlerle teknolojik imkanlara sahip olma ve onları kullanma kabiliyeti noktasında geniş siyasi ve sosyal farklılıklara sahiptir. Örnek vermek gerekirse otoriterlik yönü baskın olan devletlerde (İran, Kuzey Kore, Rusya, Çin) yapının işleyişinin bozulmaması için teknolojik imkanların hepsi veya bir kısmı devletin tekeline geçmekte ve vatandaşın erişimi kısıtlanmaktadır. Daha demokratik devletlerde ise (Hindistan, Japonya, Güney Kore) vatandaşın özgürlüğü ön planda olduğu için siber uzayda yetki alanı daha geniş bir çerçeveden değerlendirilmektedir.

Siyasi ve ekonomik konjonktürde çeşitli gereksinimleri (ekonomik, demokratik, hukuksal vb.) karşılayamadıklarından dünyadaki gelişmelerden geri kalmış veya Batı tarafından çeşitli yaptırımlarla izole edilen birçok devlet, sosyoekonomik gerekçeler de hesaba katılırsa bulunduğu konum gereği saldırganların uğrak noktası olmuştur. Yolsuzluk, kara para aklama, şantaj, tehdit gibi birçok siber suç faaliyetinin gerçekleşme sıklığı, devletlerin otoritesini sarsacak boyuta ulaştığından dolayı Asya devletleri siber uzayı tekeline alma girişiminde bulunmaktadır. Bu noktada çalışmada incelenecek olan Asya devletlerinin suç oranlarına 2021 Dünya Barış Endeksi çerçevesinde bakıldığında (Tablo 9'da da görüleceği üzere) suç oranı en yüksek ülkeler sırasıyla Rusya, Kuzey Kore, Hindistan, İran, Çin, Güney Kore ve Japonya olmuştur. Endeksteki verilere bakıldığında ülkelerdeki suç oranlarının otoriter yönetim unsuruyla paralel bir ilişkisi söz konusudur. Aynı paralellik, siber uzayda terör faaliyetlerinde doğrudan veya dolaylı yoldan etki edilme hususunda da

kurulmaktadır. Her ne kadar hangi siber saldırıyı hangi ülkenin yaptığı veya destek verdiğine dair kesin bir kanıt bulunmasa da siber uzayda varlığını sürdürmek isteyen devletlerin bu alanda uzman olan aktörlerden teknik anlamda faydalandığı gerçeğini göz önünde bulundurmak gerekmektedir. Nitekim devletler, siber güvenliğini oluşturmak için saldırı unsurlarını da ellerinde bulundurmak suretiyle kötü amaçlı yazılımları kullanabilmektedir. Özellikle kendi içlerinde oluşturdukları siber ordular ve uzmanlaşmış personeller, devletlerin siber güvenliğini sağlamak ve saldırı faaliyetlerini yürütmek için kilit rol oynayan aktörlerdir (Güntay, 2014: 96-101).

Tablo 9: 2021 Küresel Barış Endeksi[14]

Ülke	Sıralama (1-163)	Puan (1-5)
Çin	85	2,043
İran	129	2,4
Rusya	156	3,033
Kuzey Kore	153	2,93
Güney Kore	51	1,85
Hindistan	144	2,52
Japonya	7	1,389

Kaynak: Vision of Humanity, 2021

Çalışmada incelenecek olan ülkelerde siber uzay, askerî açıdan da önemli bir koz olarak değerlendirilmektedir. Hatta kimi devletler siber uzayı "hard power" kapasitesinde değerlendirerek güvenlikleştirmiştir (Thomas 2009: 11). Bu ülkeler arasında dikkatleri en çok üzerine çeken devlet Çin olmuştur. 2000'li yıllardan itibaren Çin'in kat ettiği teknolojik ilerleme ve ekonomik gelişim, küresel rekabette siber uzayda kendisinden en çok söz ettiren ülke olmakla birlikte, küreselleşen dünyaya ekonomik ve stratejik açıdan da gerçekleştirdiği uzun vadeli planlar ve politikalar nezdinde küresel bir güç olarak adından daha da söz ettireceği tahmin edilmektedir. Çin'in siber politikayı, dış politika aracı olarak kullanması ve bu uğurda ABD'ye de sözünü geçirme durumu da siber uzayı bambaşka bir boyuta taşımaktadır. Saldırı ve savunma prensiplerini "strateji" çerçevesinde uygulayan ve bu uğurda atacağı her adımı kurgulayan Çin, uluslararası sistemde yerini almaktadır.

Yapılan araştırmada bir diğer göze çarpan devlet Kuzey Kore olmuştur. Kuzey Kore, uluslararası sistemdeki yeri itibariyle saldırı kapasitesinin ve verdiği zararların bilançosundaki dengeler baz alındığında siber uzayda dikkatleri üzerine çeken caydırıcılık kapasitesi yüksek bir ülke konumundadır. Oluşturduğu nükleer tesisler ve bu tesislerde gerçekleştirdiği tatbikatlarından dolayı BM tarafından kendisine uygulanan ambargolar, ekseriyette rejim yapısı ve politik tutumlarının bir sonucu olarak değerlendirilmektedir. Ayrıca uygulanan ambargolardan dolayı yaşadığı ekonomik sıkıntılarla baş edebilmeyi başaran bir ülke olan Kuzey Kore, hemen hemen gerçekleştirdiği tüm

[14] Ülkelerin barışçıl seviyesini ölçen, her biri 1-5 arasında değişen 23 nicel ve nitel göstergeden oluşan bu endekste, skor ne kadar düşükse ülke o kadar barışçıldır. Ayrıntı için bkz, (Vision of Humanity, 2021).

siber saldırılar finans kuruluşlarına ve online bankaların işletim sistemlerine yoğunlaşmıştır. Bunun yanında eğitim alanına ciddi yatırımlar yapması, öğrencilerin her birisiyle yetenekleri dahilinde teker teker ilgilenme durumu, siber uzaydaki konumunu güçlendirmek için gerektiği ölçüde hacklenecek ülkelerin kültürlerini de bilmeleri açısından öğrencileri yurt dışına da göndermeleri dikkat çeken önemli bir husus olarak karşımıza çıkmaktadır.

Uluslararası sistemden tecrit edilmişlik ve uygulanan ambargolar bakımından bir diğer göze çarpan ülke ise İran'dır. Yaşadığı ekonomik sıkıntılar İran'ı da siber uzaya yöneltmiş ve saldırı kapasitesini ciddi ölçüde artıran bir ülke konumuna gitmiştir. İran'ın saldırı perspektifi genelde çok kapsamlı olmasa da uğradığı Stuxnet saldırısı sonrası daha keskin bir duruş sergilediği gözlemlenmektedir. Bu ölçüde işbirliği kapasitesini de güçlendirerek Rusya ile müttefiklik ilişkilerini güçlendirmiştir. Rusya'ya bakıldığında ise ülkede dış ve iç politikada etkin bir şekilde siber güvenliği kullanmayı arzulayan bir perspektif çizilmektedir. Bilgi güvenliği kavramına verdiği önem doğrultusunda doğrudan veya dolaylı yoldan oluşturduğu hacker gruplarıyla siber uzayı devlet kontrolünde tutmaktadır. Ayrıca Çin, Kuzey Kore, İran ve Rusya'nın siber uzayda ABD ile mücadele içinde olduğu gözlemlenmiştir. Bu mücadele, çalışma içerisinde ilgili ülkelerin başlıklarında incelenmiştir.

Siber uzayda güçlü konumda olan Asya ülkelerinin en dikkat çeken noktalarından birisi de ülkelerin yönetim şekli, rejim tipi ve demokratiklik durumudur. Bahsedildiği üzere tecrit edilmişlik seviyesi, suç oranlarının yüksekliği, rejim tipi, yönetim biçimi ve demokratiklik durumu ile bir ülkenin siber uzayda saldırganlığı noktasında paralel bir ilişki kurulmaktadır. Buna göre suç oranı yüksek olup, demokrasiden uzak olan otoriter rejimler (Çin, İran, Rusya, Kuzey Kore) siber uzayda daha saldırgan görüntü çizmektedir. Suç oranı düşük olup, tam demokrasi ile yönetilen ülkeler (Güney Kore, Japonya) ise siber uzayda daha az saldırgan bir görüntü çizmektedir. Tablo 10'da görüleceği üzere The Economist Intelligence Unit (2021)'in hazırlamış olduğu demokrasi endeksinde 167 ülkede demokratiklik durumu ölçülmüştür. Değerlendirme kriteri olarak beş farklı ölçüte odaklanılmıştır. Bunlar; seçim süreci ve çoğulculuk, hükümetin işleyişi, siyasi katılım, demokratik siyasi kültür ve sivil özgürlüklerdir.

Tablo 10: Araştırmada Yer Alan Ülkelerin Demokrasi Endeksi Sıralaması, Rejim Tipi ve Yönetim Biçimi

Ülke	Sıralama (1-167)	Rejim Tipi	Yönetim Şekli
Çin	151	Otoriter Rejim	Komünist Devlet
İran	152	Otoriter Rejim	Teokratik Cumhuriyet
Rusya	124	Otoriter Rejim	Federal Cumhuriyet
Kuzey Kore	167	Otoriter Rejim	Diktatörlük

Tablo 10: (Devamı)

Ülke	Sıralama (1-167)	Rejim Tipi	Yönetim Şekli
Güney Kore	23	Tam Demokrasi	Cumhuriyet
Hindistan	53	Kusurlu Demokrasi	Federal Cumhuriyet
Japonya	21	Tam Demokrasi	Parlamenter Monarşi

Kaynak: The Economist, 2021; Nation Master, 2013

Otoriter bir rejim olup komünist tek parti yönetiminde olan Çin, demokrasi endeksinde 151'inci sıradadır. Bir diğer otoriter ülke Kuzey Kore ise demokrasi endeksinde 167'yle son sıradadır ve diktatörlük ile yönetilmektedir. Bir başka otoriter ülke olan İran, dini ideolojilerinin hâkim olduğu yönetim şekli olan teokrasi ile yönetilmektedir ve demokrasi endeksinde 152'nci sırada olup Çin'in hemen arkasından gelmektedir. Çalışma içerisinde son otoriter ülke konumunda olan Rusya, federal cumhuriyet olup yarı başkanlık sistemi ile yönetilmektedir ve demokrasi endeksinde 124'üncü sıradadır.

Siber yetenekleri doğrultusunda Asya'da güçlü denebilecek diğer üç ülkeye bakıldığında demokrasi endeksinde 21'inci olan Japonya ve 23'üncü olan Güney Kore'de tam demokrasi rejimi uygulanmaktadır. Japonya parlamenter monarşi ile yönetilirken Güney Kore cumhuriyet ile yönetilmektedir. Federal cumhuriyet şekliyle yönetilen ve demokrasi endeksinde 53'üncü sırada olan Hindistan'da ise rejim tipi kusurlu demokrasidir. Bu noktada suç oranı yüksek olup, Rusya'yla aynı tip yönetim biçiminde (federal cumhuriyet) olan Hindistan'ı diğer ülkelere nazaran daha az saldırgan yapan unsurlar; demokrasi endeksindeki sıralaması ve kusurlu da olsa demokrasiyi benimsemesiyle birlikte siber uzaydaki gelişmişlik seviyesi çalışmadaki diğer ülkelere oranla daha az olması durumudur.

3.1. Siber Uzayda Asya Perspektifi

Asya, siber güvenlik güç kapasitesinde önemli ülkeleri içine alan, bilişim altyapısı ve teknoloji alanında potansiyeli giderek artan bir kıtadır. Siber uzayda kendilerine gelebilecek saldırılara karşı güvenlik arzlarını ve savunma örgütlenmelerini maksimum seviyede tutmayı hedefleyen devletler Rusya ve Çin olarak görülmektedir. Batı tarafından çeşitli yaptırımlarla izole edilmesine rağmen saldırganlık kapasitesinin sınırlarını zorlayan ve bunun için evrensel normlarla eğitim seferberliği başlatan devletler İran ve Kuzey Kore gibi ülkelerdir. Hindistan, Güney Kore, Japonya gibi devletler ise Batı ile işbirliğine önem vererek bu noktada bahsedilen diğer devletlerden ayrılmaktadır. Dünya siyasetinde yer edinebilmek için imkanlarını hazır hale getirmek isteyen bu devletler siber alanda yoğun bir çaba sarf ederek kapasitelerini geliştirmeyi amaçlamışlardır. Gayri Safi Milli Hasılası yüksek olan G8 ülkeleriyle birlikte siber uzayda adından söz ettiren birçok Asya ülkesi mevcuttur. Listedeki bu ülkeler Tablo 11'de de gösterildiği üzere Çin, Hindistan, Güney Kore, Kuzey Kore, İsrail, İran, Brezilya ve Türkiye'dir.

Tablo 11: Siber Güvenlik Sınıflandırması

Sıra	Ülke
1	ABD, Çin, Rusya
2	Fransa, İngiltere, İsrail
3	Hindistan, Güney Kore, Almanya, Türkiye
4	Brezilya, Kanada, İtalya, Japonya, İran

Kaynak: Çeliktaş, 2018: 474

Asya kıtasında bölge ülkeleri ekonomik kaynaklarını ve bölgesel çıkarlarına uygun bir şekilde kullanabilmek için ekonomik imkanlarını bu yönde seferber etmektedir. Bu çerçevede Asya ülkeleri, kaynaklarını daha verimli kullanmalarını sağlamak için giderek web tabanlı teknolojilere yönelmektedir. Bununla birlikte Güney ve Güneydoğu Asya ülkelerine bakıldığında bu ülkeler arasındaki ekonomik ve teknolojik gelişmişlik, siber uzaya da yansımıştır. Çin, Japonya, Güney Kore, Singapur, Hindistan gibi devletler, Endonezya, Malezya, Filipinler ve Tayland gibi diğer devletlerden daha ileri düzeydedir. Lakin bu ülkelerin de Brunei, Kamboçya, Laos, Myanmar, Vietnam gibi ülkelerden daha ileri düzeyde olduğu bilinmektedir. Ek olarak belirtmek gerekirse iki bölge ülkesi dışındaki diğer tüm Asya ülkelerinin teknolojik altyapısı, Kuzey Amerika'daki ülkelere kıyasla daha geridedir. Doğu Asya bölgesinde siber uzaya duyulan ihtiyaç, güvenlik arzları paralelinde gerçekleşmiştir. Özellikle bölgede siber suçların oranlarının yükselişe geçmesi, siber güvenlik tedbirlerinin alınma şiddetini de aynı ölçüde artırmıştır (Thomas, 2009: 16-21). Devletlerin birbirleriyle olan askeri mücadelesi, teknolojik devinimle birlikte Asya-Pasifik ve Güney Çin Denizi bölgesindeki rekabette kendisini iyiden iyiye hissettirmektedir.

Asya devletlerinde sosyal ve politik sistemlerde büyük farklılıklar bulunmaktadır. Şüphesiz bu farklılıklar devletlerin siber güvenlik sorunlarına yaklaşımlarını şekillendirmektedir. Bu farklardan en belirgini, her bir devletin bir siber tehdit tanımı olduğundan dolayı güvensizliğe verilen tepki, tehdidin tanımını şekillendirmektedir. Devletler tarafından oluşturulan bu tanımda rejim farklılığı büyük bir ölçüt olarak karşımıza çıkmaktadır. Bu bağlamda "rejim ne kadar otoriter olursa, vatandaşların çevrimiçi materyallere erişim hürriyeti de bir o kadar düşüktür" yorumu yapılmaktadır. Kuzey Kore, Çin veya İran gibi otoriter rejimler, vatandaşlarının devletin uygunsuz bulduğu içerik barındıran web sitelerini ziyaret etmelerini düzenli olarak yasaklamaktadır. Öte yandan Çin, uluslararası web sitelerine yurtiçi erişimi engellemek için küresel bilgisayar firmalarıyla *(Yahoo ve Google gibi)* ortaklıklar kurmuştur (Thomas, 2009: 16-21). Tıpkı bunun gibi bir örneği yine otoriter bir ülke konumunda olan Rusya'da da *(Google yerine Yandex, Gmail yerine Mailru, Facebook yerine Vk gibi platformlar)* görmek mümkündür.

Çin, 2019 yılında yayımladığı Beyaz Kitap'ta, Asya-Pasifik bölgesinde "büyük ülke rekabeti" olgusundan bahsetmektedir. Kitapta ABD'nin Asya-Pasifik askeri ittifakları ve konuşlandırmalarıyla birlikte askeri müdahaleyi de güçlendirdiği iddia edilmektedir. ABD'nin kilit ortaklarının Güney

Kore, Japonya ve Avustralya olduğunu belirtmekle beraber Avusturalya ile askeri ittifakını ve Asya-Pasifik'teki askeri katılımını güçlendirerek güvenlik işlerinde daha büyük bir rol aradığı vurgulanmaktadır. Dünyanın ekonomik, teknolojik ve stratejik merkezi Asya-Pasifik'e doğru kaymaya devam etse bile, bölgenin bölgesel güvenliğe belirsizlikler getirerek büyük ülke rekabetinin odağı haline geldiği ifade edilmektedir. Ayrıca kitapta, Asya-Pasifik ülkelerinin giderek daha fazla ortak kaderi olan bir topluluğun üyesi olduklarının farkında oldukları ileri sürülmüştür. Farklılıklar ve anlaşmazlıkları diyalog ve istişare yoluyla ele alarak Asya'nın dengeli, istikrarlı, açık ve kapsayıcı güvenliği için Çin liderliğindeki bir güvenlik örgütlenmesinin hızla ortaya çıkmasının gerekliliği savunulmaktadır (Mallick, 2019). Bu örgütlenmenin sağlanmasında ihtiyaç duyulması halinde her türlü güvenlik aracının kullanılabilecek olması da Çin'in bu kararlılığını gözler önüne sermektedir.

Kaspersky firmasının yaptığı araştırmaya göre 2020 yılının ilk çeyreğindeki APT faaliyetleri Asya'da yoğunlaşmıştır. Saldırılarda en çok hedef alınan devletler arasında Japonya, Güney Kore ve Güneydoğu Asya ülkelerinin olduğu gözlemlenmiştir. Öte yandan Covid-19 salgını da Mart 2020'den itibaren çeşitli APT grupları tarafından kötü amaçlar doğrultusunda kullanılmaktadır. Bu gruplar "siber korona"[15] çatısı altında birçok saldırıya imza atmaktadırlar. Kaspersky bu noktada, *Kimsuky, Hades* ve *DarkHotel* gibi saldırgan grupların finansal kazanç ve jeopolitik amaçlar güderek APT faaliyetlerini gerçekleştirdiğini savunmaktadır (Anadolu Ajansı, 2020).

3.2. Doğu Perspektifinde Asya Devletleri

Asya bölgesi, siber saldırı güçleriyle birlikte siber uzaydaki yeteneklerini de kuvvetlendirmek için bu alana bağımlılığını kanıtlayan bir coğrafyadır. Nitekim siber gelişmişlik hakkında yapılan araştırmalarda gelişmişlik seviyesi yüksek ülkelerin haricinde siber kapasitesini en çok geliştiren ülkeler Asya kıtasında yer almaktadır. Çin, İran, Rusya ve Kuzey Kore gibi ülkeler siber uzaya önemli yatırımlar yapan ülkelerin başında gelmektedirler. Çin, önemli altyapılara sahip bir ülke olarak 2050 yılına kadar elektronik egemenliği hedefleyen ve düşman kuvvetlerinin altyapılarını etkisiz hale getirebilmeyi de içeren bir "siber doktrin" benimseyen nadir ülkelerden biridir. Aynı zamanda hava, deniz, karadaki donanmanın önemi kadar siber uzayın da o derece önemli olduğu, Çin Halk Özgürlük Ordusu (PLA) tarafından belirtilmektedir (Alexander, 2007: 59).

Rusya, en az Çin kadar önemli siber saldırı ekipmanları ve altyapısına sahiptir ve özellikle 2010 sonrası bu alanda ciddi yatırımlar yapmaktadır. İran da aynı şekilde siber savunma konseptini geliştirmekle birlikte saldırı kapasitesini de ciddi oranda artırmaktadır. Bu noktada geliştirdikleri siber polis birimi FATA, dijital suçlarla mücadele noktasında önemli ölçüde işlev görmektedir

[15] Covid-19, bilişim ve teknoloji dünyasında da bir dijital salgına neden olmuştur. Saldırganların Covid-19 teması kullanarak sahte mobil uygulamalar aracılığı ile hedef odaklı ya da gelişi güzel saldırılar düzenlediği gözlemlenmiştir. Ayrıntı için bkz, (CyberMack, 2020).

(Çahmutoğlu, 2021). İran bu noktada Rusya ve Hindistan gibi ülkelerden eğitim desteği almaktadır. Bu noktada ayrı bir parantezi Kuzey Kore'ye açmak gerekmektedir. Nitekim Kuzey Kore'nin teknolojik durumu, bahsi geçen diğer devletlerden geri kalır durumda değildir. Tıpkı Çin gibi Kuzey Kore ordularının bir siber ordu birimi olduğu bilinmektedir ve Kuzey Kore'nin siber uzaydaki saldırı kapasitesi gün geçtikçe genişlemektedir. Bahsedilmesi gereken bir diğer ülke ise Hindistan'dır. Nitekim Hindistan, siber kabiliyetini dış politikasında kırmızı çizgisi olarak kabul ederek kapasitesini genişletmektedir. Hindistan, Keşmir sorunu sırasında maruz kaldığı siber saldırılara karşı savunma konseptini geliştirmek için çeşitli girişimlerde bulunarak 1998 yılında siber savaşı da içine alan güvenlik doktrini ilan etmiştir. Bu doktrin, Hindistan'ın siber uzayda atacağı adımların miladı olarak kabul edilmektedir. Hindistan ayrıca, eş zamanlı bir şekilde üniversite birimleriyle siber savaş üzerine uzman alt birimler kurarak kendilerine yönelecek siber tehditlere karşı hazır hale gelebilmek için çeşitli yatırımlar yapmaktadır (Gürkaynak ve İren, 2011: 269-270). Güney Kore ve Japonya da kendilerine yapılan siber saldırılar noktasında savunma konseptlerini geliştiren ülkeler olarak bilinmektedir. Her iki ülke de işbirliğini ön planda tutup, siber uzayda kapasitelerini geliştirmeyi amaçlamaktadır.

3.2.1. Çin

Soğuk Savaş'ın sonlarına doğru teknolojik gelişmelere önem vermeye başlayan Çin, bu alana yatırım yapan ülkelerin başında geldiği için özellikle siber uzay ve yapay zekâ noktasında yaptığı yenilikler doğrultusunda ABD'yle birlikte dünyanın önde gelen ülkelerin başında gelmektedir. 2021 verilerine göre 1,402 milyar nüfusu ile dünyanın en kalabalık ülkesi konumunda olan Çin'de 989 milyon internet kullanıcısı bulunmaktadır (Vinny Halo, 2021). Çin, siber uzayda önemli bir aktör olmasının yanında internet kullanan geniş nüfusu sayesinde dünyada internet kullanıcılarının dörtte birini kendi bünyesinde barındırmaktadır.

Çin'de ilk internet denemesi ve çağdaş projeler dahilinde teknolojik alandaki yatırımlar, Deng Xiaoping döneminden itibaren başlamıştır. 1986 ve 1987 yıllarında ilk e-postalar gönderilmiştir. 1998 yılından itibaren Çin'de internete girebilen bilgisayar sayısı 747 bine kadar artış göstermiştir. Bu yıllarda ayrıca uluslararası piyasalarda listelenen ağ şirketleri açılarak ülke sınırları dışına çıkılmıştır. Pekcan (2020: 207-208)'a göre Çin'in 1999 yılında yaşadığı iki olay, bilgi teknolojileri konusuna verdiği önemin daha da artmasına sebebiyet vermiştir. Bu olaylardan ilki Falun Gong[16] olayı, bir diğeri ise NATO'nun Sırbistan'a müdahalesi sırasında Belgrad'daki Çin Büyükelçiliği'nin bombalanmasıdır. Falun Gong olayıyla birlikte Çin, internette özgürlük kavramını değerlendirmeye

[16] Bir diğer ismiyle Falun Dafa, birtakım egzersizlerle beden ve zihnin geliştirilmesiyle alakalı bir sağlık uygulamasıdır. Program geliştiricisi Li Hongzhi, Budist ve Taoist öğretilerle oluşturduğu programı önce Çin'e, sonra tüm dünyaya yaymayı başarmıştır. Çin, bu uygulamayı "şeytani din" olarak tanımladıktan sonra uygulama kullanıcıları interneti kitlesel bir eyleme dönüştürmek suretiyle Pekin meydanında uygulamadaki öğretileri uygulayarak protesto eylemi gerçekleştirmiştir. Bunun üzerine kriz derinleşerek can kayıplarının artmasıyla sonuçlanmıştır. Ayrıntı için bkz, (Pekcan, 2020: 209-220).

alarak internetin örgütlenmeye ve toplumsal kaosa sürüklenebileceği öngörüsünde bulunup internet üzerinde sansür, engel gibi hamleler yaparak tekelleştirme girişiminde bulunmuştur. NATO'nun Sırbistan'a müdahale ederken Çin Büyükelçiliği'ni bombalaması sonrası ABD'nin bu eylemi yanlışlıkla gerçekleştirdiğini belirtmesi Çin'i ikna etmek için yeterli olmamıştır. Negro (2017: 44)'ya göre bu olay sonrası Çin, teknolojik savaş yollarına başvurmayı amaçlamış ve bu alana ciddi yatırımlar yapmıştır.

2000'lerden itibaren Çin'de siber uzayda kurumsallaşma adımları atılmıştır. Bu doğrultuda teknik-hukuksal düzenlemeler, eğitimler ve uluslararası toplantılar vasıtasıyla siber yetenekleri geliştirme çabasına gidilmiştir. 2005 yılında ilan edilen Ulusal Enformatizasyon Planı; bilgi toplumunun desteklenmesi, e-devlet uygulaması, internet kültürünün benimsenmesi, ulusal bilgi güvenliği sisteminin kurularak bilgi teknolojilerindeki rekabetin sağlanması, bilgi teknolojisinin yasal bir zemine dayandırılması gibi hedef ve misyonlardan bahsedilen bir plan olarak değerlendirilmektedir. 2000'li yıllardan itibaren siber uzayda gelişim göstererek ilerleyen Çin'in siber savaş stratejileri, Siboni (2012, 51-55)'ye göre dört farklı operasyonun birleştiği bir sacayağına oturmaktadır. Bunlar; bilgisayar ağlarına saldırı, elektronik savaş, bilgisayar ağı koruması ve bilgisayar ağı sömürüsü olarak açıklanmaktadır (Pekcan, 2020: 209-220).

3.2.1.1. Çin'in Kurumsal Mekanizmaları ve Uygulamaları

Çin hükümeti ülkenin ekonomik ve askeri gücünü mümkün olan en yüksek seviyeye ulaştırmayı hedeflediğini, uyguladığı politikalar vasıtasıyla açıkça belirtmektedir. Bunu yapmak için de siber savunmalarının temellerinin güçlü olması gerektiğini savunan Çin hükümeti bu amaçla, yapay zekâ gibi teknolojik unsurlara büyük ölçüde yatırımlar yapmaktadır. Başkan Xi Jinping (2018) 'in *siber güvenlik olmadan ulusal bir güvenlik olamaz* sözü hükümet politikalarını somutlaştıran bir ifade olarak değerlendirilmektedir. Çin ayrıca yüz tanıma, araç ve akıllı telefon izleme ve vatandaş gözetimi gibi kamu güvenliğini gözeten teknolojik hamlelerle büyük adımlar atmayı amaçlamaktadır. Aynı zamanda savunma mekanizmasını geliştirme yolunda olan Çin, devlete ait iki savunma elektroniği şirketi China Electronics Corporation (CEC) ve China Electronics Technology Group (CETC)'un yan kuruluşları olan ChinaSoft ve China Cybersecurity aracılığıyla faaliyetlerini sürdürmektedir. Ayrıca ülke içerisinde hızla artan ürün ve hizmet talebinden dolayı büyüyen yüzlerce özel siber güvenlik şirketi bulunmaktadır. Aynı zamanda yabancı yatırımcılar ve özel şirketler siber uzayda faaliyetlerini artırarak ülkeye maddi gelir sağlama hususunda önemli rollere sahiptir (Austin, 2018). Çin'in siber uzayda uluslararası alandaki gelişiminde kamu ve özel sektörden çeşitli aktörler bulunurken ulusal alanda mücadele boyutunda tek aktörün ordu olduğu gözlemlenmektedir.

Çin'in askeri gücüne değinmeden evvel sivillerden aldığı destekten söz etmek gerekir. Çin'deki güçlü sivil-asker birliği, 1927'deki Çin İç Savaşı'nın ilk günlerine kadar uzanmakta ve Mao Zedong'un "Halk Savaşı" doktrini içerisine tezahür ettirilmektedir. PLA'nın devam eden yapısal

reformları, Halk Kurtuluş Ordusu Stratejik Destek Gücü (People's Liberation Army Strategic Support Force-PLASSF)'nün görevlerini düzenleme ve yürütme şeklini, özellikle zaman içinde geliştikçe daha da değiştirmektedir. Siber ve savaşla ilgili diğer bilgi unsurlarını birleştirirken PLASSF, organizasyonundaki ulusal siber keşif, saldırı ve savunma yeteneklerini birleştirerek sinerjiler üretmektedir. PLA'nın kilit Çin telekomünikasyon şirketleri ile yakın ilişkisinin, Batı hükümetlerini ve ticari endüstrileri destekleyen mikro-elektronik tedarik zincirlerinin devlet destekli yapılanmaları için olanak sağladığı belirtilmektedir (Ng, 2020).

Başkan Xi Jinping tarafından Sivil Askeri Siber Entegrasyon, yeni merkezin ana misyonlarından biri olarak tanımlanarak Entegre Askeri ve Sivil Kalkınma Merkez Komisyonu ile Çin'in ilk siber güvenlik inovasyon merkezi aynı yılda kurulmuştur. Bununla birlikte devlete bağlı siber milisler, sivil toplum geliştirme çabalarının en açık ürünlerinden biri olmuştur ve çok geniş çaplı bir üyelik tabanına sahip olarak Çin'in siber uzayda etki nüfuzunu artırmıştır. Çin hükümeti, milislerin istedikleri gibi faaliyet göstermeleri için görev verdiği takdirde normal PLA siber birimlerin çalışmalarını baltalayabileceği olasılığının bilincinde olduğu için, bu kuruluşları saldırgan siber operasyonların aksine siber gözetim ve casusluk yapmakla görevlendirmiştir. Bu noktada *patriotic hackers (vatansever hackerlar)* denilen grubun, Çin'de en bilindik siber milis grubu olduğu belirtilmektedir. Bu bilgisayar korsanları, genellikle Çin Komünist Partisi'nin benimsediği ve sürdürdüğü popüler milliyetçilik tarafından yönlendirilmektedir. Ayrıca siber korsanların, uluslararası operasyonlarda kimliğinin deşifre edilmesi durumunda Çin hükümeti genelde bu durumu inkâr ederek iddialardan sıyrılma yoluna gitmektedir (Ng, 2020). Devlet, siber uzayda ulusal çıkarlarını ön planda tutmuştur ve yaptığı her girişimi kendi tekeline alarak ulusal menfaatler paralelinde gerçekleştirmiştir.

Çin, Soğuk Savaş'ın sona erdiği tarihten itibaren siber uzaya yönelik ilgisini yıllar boyu üzerine koyarak artırmıştır (Gürkaynak ve İren 2011: 268). Çin yaptığı siber girişimlerde ve yetiştirdiği hacktivistleri sahaya sürme stratejisinde gizliliği esas almaktadır. Çin bu noktada ABD'nin yazılım altyapıları yerine kendi yazılımlarını geliştirmeyi ve kullanmayı tercih ederek ilerlemeye devam etmiştir. Milli savunmasında siber güvenliğin önemini açık bir şekilde belirten Çin hükümetinin geliştirdiği stratejilerde ön plana çıkan husus düşmana karşı bilgi üstünlüğü sağlamak ve istihbarat toplamak suretiyle çeşitli siber araçları kullanmaktır. Siber saldırı yönünde atılan adımlar konusunda Çin'in birtakım gruplarla sıkı bir temas halinde olduğu bilinmektedir ve Çin, her ne kadar gizliliği esas alsa da uluslararası kamuoyu tarafından tepki görmektedir.

Çin hükümetinin 2004 yılında yayımladığı Beyaz Kitap'ta askeri bilişim sistemlerini güçlendirmek için teknolojik kapasitenin artırılması hedeflenmiştir. Nitekim kitabın ikinci bölümünde belirtildiği üzere, bilim ve teknoloji ile güçlü bir ordu kurmayı amaçlamaktadır. Çin Halk Kurtuluş Ordusu (People's Liberation Army) olan PLA, bilimsel ve teknolojik ilerlemelerden yararlanarak savaş yeteneklerini geliştirmeye çalışıp sadece niceliksel bir ölçek yerine nitel

verimlilik oluşturmayı ve orduyu insan gücü yoğun olandan teknoloji yoğun olana dönüştürmeyi hedeflemektedir. *Yetenekli İnsanlar İçin Stratejik Projeyi* uygulayan PLA, yeni tipte yüksek kalibreli askeri personelin eğitilmesine odaklanmaktadır (China's National Defense, 2004).

2006 yılında yayımlanan Beyaz Kitap'ta, kamu hizmetlerinde ve resmî kurumlarda bilişimin geliştirilmesi amaç olarak belirlenmiştir. Çin'in siber güvenliği ordu tarafından gerçekleştirildiği için PLA bu noktada siber güvenliğin yönlendirilmesi ve siber altyapının genel durumu gibi sorumluluklarla önemli roller üstlenmektedir. Çin'in siber güvenlik ağı *Mavi Ordu* adı verilen teknik birim tarafından kontrol edilmektedir. Bu birim, Genelkurmay bünyesinde önemli faaliyetler gerçekleştirmektedir. Bilgisayar ağındaki donanımı geliştirmeyi amaçlayan Genelkurmay 3. Dairesi, sinyal istihbaratı ve siber savunmayla ilgili faaliyetlerin yerine getirildiği birim olarak karşımıza çıkmaktadır. Bu dairede tıpkı ABD'deki Ulusal Güvenlik Ajansı (NSA) gibi, Çin'in de çeşitli yerlerine yerleşmiş bölgesel komutanlıklar ile sinyal aracılığıyla istihbarat toplanmaktadır. Genelkurmay 4. Dairesinin görevi ise hedefe ve potansiyel tehditlere karşı tedbir almak ve geleneksel elektronik taarruz yapmaktır. Bilgi harekâtı ve siber saldırı birimleri bu daireye bağlı çalışmaktadır. Aynı zamanda elektronik istihbarat ve sinyal istihbaratı elde etme zorunluluğu olduğu için Genelkurmay'ın 3. Dairesine de yardımcı olmaktadır (Güntay, 2016: 132).

2019 yılında yayımlanan Beyaz Kitap'ta Çin'in yeni dönemdeki ulusal savunması ele alınmıştır. Bu raporda terörle mücadele ve aşırıcılığa, Çin ve Rusya ile rekabete ve olası çatışmaya odaklanan ABD stratejisindeki büyük değişime açık ve ayrıntılı bir cevap verilmiştir. ABD ve Çin'in şu anda süper güçlerle rekabet ettiğini ve Çin'in büyüyen askeri güçlerinin ABD'ye meydan okuyabilecekleri noktaya kadar geliştikleri işaret edilmektedir. Çin bu kitapta, ABD ile stratejik rekabetinde siber güvenliğin de önemli bir ölçüt olacağını belirtmiştir (Cordesman, 2019). Aynı zamanda PLA'nın mevcut koşullarda yönetilme şekillerini ifade etmek için inovasyon, liderliğin ve komuta sistemlerinin iyileştirilme vurgusu yapılmaktadır. Bununla birlikte halk savaşının genel gücünü belirterek Mao Zedong'un doktrini desteklemeye devam edilmektedir. Raporda ayrıca askeri güçlerin modernizasyonu ve genişlemesi, tamamen savunmacı perspektifte değerlendirilmektedir (Mallick, 2019). Bu doğrultuda PLA, bilgi çağındaki yeniliklerden faydalanmayı ve yeni savaş yollarına hazırlanmayı amaçlamaktadır. Nitekim 2012'den 2021'e kadar Çin'in savunma harcamaları 98 milyar dolardan 210 milyar dolara yükselmiştir ve yıllar geçtikçe bu giderek katlanmaktadır (Euronews, 2021a).

2019'daki Beyaz Kitap'ta, Çin'in silahlı kuvvetleri siber uzay yeteneklerinin geliştirilmesi belirtilmektedir. Bu bağlamda ulusal siber sınır, savunmasını güçlendirip ağ müdahalelerini derhal tespit edip karşı koymak için inşa edilmiştir. Sınır, bilgi ve siber güvenliği koruyup ulusal siber egemenliği, bilgi güvenliğini ve sosyal istikrarı kararlılıkla sürdürmektedir. Çin, tehditleri algılama noktasında stratejik hayati çıkarların merkezine siber güvenliği almaktadır. Bu durum kitapta şöyle belirtilmiştir: *Dışardaki alan, uluslararası stratejik rekabette kritik bir yerdir. PLA siber savaşta,*

düşmanın keşiflerini ve iletişim uydularını yok etmek, zarar vermek ve bunlara müdahale etmeyi amaçlamaktadır. Yapılması istenilen şey ise kitapta tam olarak *"düşmanı kör ve sağır etmek"* olarak belirtilmiştir. Çin, siber uzayın barışçıl kullanıldığına dair ısrar ederken Beyaz Kitap, Çin'in uyduları korumak, alana güvenli bir şekilde girmek, çıkmak ve açık bir şekilde kullanma yeteneğini korumak için ilgili teknolojiler ve yetenekler geliştirdiğini belirtmektedir (Mallick, 2019). Son olarak 2020 yılında yayımlanan Beyaz Kitap'ta yapay zekaya verilen önemden ve yapılması muhtemel projelerden bahsedilmiştir. Bu projeler genel hatları itibariyle yapay zekâ uygulamasının çeşitli sektörlerde (kamu, ulaşım, sağlık, yiyecek-içecek, konaklama, oyun, ticaret gibi) kullanılacak olmasıyla alakalı olmuştur. Bu bağlamda Çin'deki yapay zekâ teknolojisinin son beş yılda neredeyse %50 oranında büyüdüğü bilgisi verilmiştir (China, White Paper 2020).

Çin'in dahil olduğu siber saldırılara bakıldığında arasında düşmanlık ilişkisi olan devletlerle sorun yaşamıştır. Tibet bölgesinde ve Güney Çin Denizi ile alakalı olan çatışmalarda da gerçekleşerek Asya-Pasifik bölgesinin önemli konularından birisi olmaktadır. Araştırmacılar, analistler ve mühendislerden oluşan bir grup olan Cisco Talos, 2019 yılında Merkezi Tibet Yönetimi (CTA) tarafından yürütülen bir posta listesi kullanarak kötü amaçlı bir Microsoft PowerPoint belgesi sağlayan yeni bir siber casusluk faaliyetini ortaya çıkarmıştır. Belge, CTA'nın *tibet.net* web sitesinden indirilebilen "Tibet hiçbir zaman Çin'in bir parçası değildi" başlıklı yasal bir PDF dosyasının kopyasıdır ancak kötü amaçlı yazılım olan trojan içermektedir. E-posta, ExileRAT olarak adlandırılan dosyaları dağıtmak için Tibet yanlısı gruplara ve bireylere yönelik hazırlanmıştır. Saldırı, sistem ve kişisel bilgileri çalabilen, işlemi sonlandıran, gözetim ve veri hırsızlığı yapan bir mekanizma üzerine inşa edilmiştir. CTA ve Tibet'teki sivil toplum kuruluşlarını hedef alan son siber saldırı girişimi, Çin devlet destekli bilgisayar korsanları tarafından yürütülen kapsamlı siber saldırılarından sadece bir tanesidir. Burada amaç öncelikle CTA'nın ağ sistemine girmek ve sonuç olarak faaliyetleri izlemek ve çeşitli sosyal mühendislik tekniklerini kullanarak bilgi elde etmektir. Kötü amaçlı yazılım alıcılarının yalnızca bir kısmının kötü amaçlı bir bağlantıyı (yanlışlıkla olsa bile) tıklamasını veya virüslü bir dosyayı indirmesini umarak aynı adreslerden birçok e-posta adresine ortak e-posta gönderme şeklinde gerçekleştirilmektedir. Bu saldırı türü *mızrak avı* olarak bilinmektedir ve bu saldırılar genellikle aynı anda çok sayıda kurbanı hedef alacak şekilde tasarlanmıştır (Dalha, 2018).

Güney Çin Denizi'ndeki çatışmaların siber boyutuna bakıldığında Filipinler ile Çin arasında yaşanan bir krizden söz edilmektedir. Filipinler cephesinden Çin'e karşı net karşı bir duruş beklenirken Başkan Rodrigo Duterte, savaş veya yatıştırma arasında bir tutum sergilemektedir. Buna karşın Çin'in Güney Çin Denizi'ne yaklaşımı tek boyutlu veya basitleştirilmiş taktiklere dayanmamaktadır. Çin, kaynak açısından denizin tek taraflı kontrolünü sağlamak ve çevresini de güçlendirmek için önemli ölçüde stratejik amaçlar gütmektedir. Bu stratejik amaçlar, siber saldırı olarak açıklanmaktadır. EnSilo (2019) adlı şirketin yayımladığı bir raporda, Çin siber casusluk grubunun Nisan 2019'da Filipinler'deki hükümeti ve özel kuruluşları hedef alan iki kötü amaçlı

yazılımı bölgede kullandığı saptanmıştır. Yine eş zamanlı olarak Filipinler'in çeşitli hükümet web sitelerinin kaynak koduna eklenen Çince komut dosyalarının çeşitli sistemleri ele geçirmeyi ve hedef kullanıcılardan bilgi toplamayı amaçladığı tespit edilmiştir. Ayrıca bunun yanında Çin, Güney Çin Denizi meselesinden bağımsız olarak da Filipinler'e defalarca siber saldırılarda bulunmuştur (Manantan, 2019).

Çin, Hindistan'la yaşadığı sınır sorunları sebebiyle siber uzayda da birçok kez karşı karşıya gelmiştir. Hindistan, Çinli hacker gruplarının kendi bilgi teknolojilerine ve bankacılık sistemlerine yönelik sürekli bir şekilde binlerce saldırı gerçekleştirdiğini iddia etmiştir. Bu şikâyet üzerine Hindistan hükümeti, ülke içerisinde kullanılmakta olan Çin'e ait dijital uygulamaları yasaklayarak önlem almıştır. Çin'in siber saldırılarda ana hedeflerinden birinin de Tayvan olduğu belirtilmektedir. Hatırlanacağı üzere iki ülke arasındaki isim meselesi, II. Dünya Savaşı'nın sonlarına kadar dayanmaktadır. İç savaş sonrası galip gelen komünist parti Çin Halk Cumhuriyeti'ni kurmuş, mağlup olan milliyetçiler ise Tayvan adasına kaçarak bölgeyi Çin Cumhuriyeti olarak ilan etmiştir. İki tarafın da Çin'i temsil ettiği kaos ortamında BM'nin verdiği karar, temsil hakkının Çin Halk Cumhuriyeti'ne verilmesiyle sonuçlanmıştır. Bu karar sonrası Çin, Tayvan'ı "tek ülke iki sistem" şeklinde yönetmek istemiştir ancak Tayvan bunu kabul etmemiştir ve bu sorun günümüze kadar süregelmiştir (Pekcan, 2020: 218-222). Siber uzay noktasına odaklandığında ise Çin ile Tayvan arasındaki ilk siber savaş, 1999 yılında gerçekleşmiştir. İki ülke arasında yaşanan "devletlerarası ilişki" meselesi sonrası Çin, Tayvan'ın kamusal sitelerine saldırılar gerçekleştirerek işlevsizleştirmiştir. Yine buna benzer bir saldırı ise 2003 yılında gerçekleşmiştir (Spade, 2017: 72-76).

Çin, siber uzayda gerçekleştirdiği dijital reformlar, geleceğe yönelik yatırımlar ve projelerle birlikte uluslararası alana açılan bir ülke olarak değerlendirilmektedir. Bu noktada Çin'in küresel sistemde zıt kutbu olarak görülen bir diğer güçlü aktör ABD ile rekabet içine girmesi kaçınılmaz olmaktadır. ABD siyasal, ekonomik ve teknolojik olarak Çin'i önemli bir tehdit olarak algılamaktadır. ABD, Çin'in teknolojik altyapılarını hangi amaçlarla kullandığı noktasında kaygılarını sıklıkla belirttiği bilinmektedir (Spade, 2017: 74). Bununla birlikte Rusya, İran ve Kuzey Kore'de potansiyel ve kapasitelerine göre değişim gösteren diğer tehditler olarak görülmektedir.

ABD menşeli siber güvenlik şirketi olan Mandiant'ın 2013 yılında yayımladığı APT raporunda Çin kontrolünde bir siber saldırı birliği olduğundan söz edilmektedir. Raporda birliğin konumu ve kurumsal yapısı gibi spesifik bilgiler yer almaktadır. PLA merkezine ciddi ölçüde yakın bir bölgede olan bu konum, Şangay ilinin Pudong bölgesinde bulunmaktadır. 12 katlı bu binada personel sayısı hakkında net bir sayı verilmemiştir ancak tahmini olarak bini aşkın personel belirtilmiştir (Mandiant, 2013). Nitekim Çin'in bu hacker birliğine, devlet elinden destek verildiği raporda belirtilmiştir. Ancak Çin bu iddiayı yalanlamıştır ve bu rapordan yaklaşık iki ay sonra yeni bir Beyaz Kitap yayımlamıştır. Bu kitapta silahlı kuvvetlerin kara, hava, deniz birliğinin tüm asker ve personel sayıları verilmiştir. Çin, Mandiant Raporu'nu reddetmiş, sonrasında derhal Beyaz Kitap'ta bu

bilgileri vererek, şeffaf ve savunmasız bir ordusunun olduğunu göstermek istemiştir (Kara, 2013: 66-67). ABD, Çin'i kendisine potansiyel tehdit olarak görmesine karşın ülke ile yakın temas kurarak ortak çalışmalar yürütmek istemiştir. Bu hususta da Çin'in ABD'ye karşı tutumu, kendi dış politika gerçeklerinden ödün vermemesine bağlı olarak gelişmiştir. Bu noktada dikkat çekilmesi gereken mesele ABD'nin Çin'e karşı verdiği tavizlerdir. Çin ve potansiyel tehdit olarak görülen ülkelerin ne kadar caydırıcı bir güç olduğu bu örnekten hareketle net bir biçimde anlaşılmaktadır (Cilluffo, 2013: 4-8).

ABD ve Çin arasında ekonomik casusluk konusunda 2015 yılında yapılan anlaşmada siber uzay faaliyetleri ve yönetimine yönelik farklı yaklaşımlar yer almaktadır. Bu anlaşma bir noktaya kadar ABD ve Çin'in yaklaşımlarını da ortaya koymaktadır. Örneğin ABD, siber uzayda bir ülkenin kendi kaderini kendisinin belirlemesine önem vermektedir. Uluslararası etkileşimlerde bu özgürlükleri artırmayı hedeflemekte ve internet üzerinden serbest bilgi akışının stratejik ve diplomatik başarının anahtarı olduğuna inanmaktadır. Bu noktada Çin ise, ekonomik rekabeti ABD ile ilişki kurmanın bir yolu olarak görmekte ve siber uzayı ABD ile rekabet etmek için başarıyla kullanabileceği asimetrik bir araç olarak görmektedir. Çin fikirlerin hem içerden hem dışarıdan gelmesine karşı sürekli olarak duyarlı olmaya gayret göstermektedir. Anlaşmada her iki tarafın da uluslararası toplum içinde siber uzayda uygun devlet davranışı normlarını belirleme, geliştirme ve teşvik etme noktasında siber suçlarla ilgili sorunlarla mücadelede üst düzey bir ortak diyalog bağlantısı kurmaya karar vermişlerdir. Ancak ABD'de Çin'in anlaşmaya uyup uymayacağı konusunda şüpheler bulunmaktadır. Nitekim Jinping'in Çin hükümetinin özel şirketlere rekabet avantajı sağlamak amacıyla siber özellikli fikri mülkiyet hırsızlığına girmemesini veya bilerek desteklememesini sağlama anlaşması, bu anlaşmanın üzerine duyulan şüpheleri haklı çıkarmıştır (Brown ve Yung, 2017).

Siber uzayda ABD'den farklı bir yol izleyen Çin'de gizlilik ve iletişim hakları, siber politikalarının geliştirilmesinde önemli bir rol oynamıştır. Çin siber egemenliğin önemini vurgulamaktadır. Cumhurbaşkanı Xi Jinping, Aralık 2015 Dünya İnternet Konferansı'nda devletlerin kendi ülkelerinde siber uzay için kendi kurallarını belirlemelerine izin verilmesini istemiştir. Böylece Çin bilgi akışını kontrol etmek için yasal sistemleri de geliştirme arayışına girmiştir. Jinping hükümeti bu bağlamda 2017 yılında yürürlüğe girecek yeni bir siber güvenlik yasasını kabul etmiştir. Bu yasayla birlikte Çin, internet güvenliğini sağlamanın yanında bilgi, iletişim ve bilgisayar güvenliğini artırıcı önlemler almıştır (Zhao ve Xia, 2018). Çin ve hükümet gözetimini artırmak isteyen birkaç Asya ülkesi, bilgi güvenliği için bir uluslararası davranış kuralını savunmaktadır. Davranış kuralları lehine devletler, bu görüşe göre siber uzayda davranışı yönlendiren uluslararası normlar ve kurallar belirlemeye çalışmaktadır. Bu noktada Brown ve Yung (2017)'a göre siber uzayın ulus-ötesi ve özerk doğası, sosyal ve ekonomik kalkınmanın yanı sıra uluslararası güvenliğe de meydan okumaktadır.

Covid-19, siber saldırıda yeni hedefleri ortaya çıkartan bir salgın olarak karşımıza çıkmaktadır. Örneğin Güney Koreli bilgisayar korsanları Dünya Sağlık Örgütü'nü, Kuzey Kore ise Japonya ve ABD'deki yetkilileri hedef almıştır. Son zamanlarda ABD, kendi bünyelerine yapılan siber saldırılarda sorumluları FBI ve İç Güvenlik Bakanlığı'nca ilan etmektedir. Mayıs 2020'de Çin'in en yetenekli bilgisayar korsanlarının ve casuslarının, Covid-19 için aşı ve tedavi geliştirmeye çalışan Amerikan araştırmacılarının araştırma verilerini çalmaya çalıştıklarına dair bir uyarı bildirisi ortaya koyulmuştur. Bahsi geçen kamuoyu uyarısı taslağında, Çin'in aşılar, tedaviler ve testlerle ilgili yasadışı yollarla değerli fikri mülkiyet ve halk sağlığı verilerini ele geçirmeye çalıştığı savunulmaktadır. Hatta Covid-19'dan önce bile ABD, Çin'in biyolojik araştırmalarla ilgili fikri mülkiyeti çalma çabalarından şüphelenilen davaları takip etmiştir. Bu noktada ABD'nin Siber Güvenlik Direktörü Christopher Krebs, ABD'nin kendi çıkarlarını agresif bir şekilde koruyacağını belirterek mevcut ve olası tehditlere karşı ülkenin farkındalık durumunu ortaya koymuştur (Sanger ve Perlroth, 2020).

ABD'deki siber güvenlik uzmanları, FireEye (2020)'in hazırladığı bir raporda şüpheli Çinli grupların siber saldırılarında ciddi bir artış olduğunu tespit etmiştir. APT41 adını verdiği ve birçok müşterinin hedef alındığı bilgisayar korsan grupları, medya şirketleri ve kâr amacı gütmeyen kuruluşlara saldırılar gerçekleştirmişti. Raporda, *son yıllarda gözlemlenen Çinli siber casuslar tarafından yapılan en geniş çaplı saldırı* ibaresi, saldırıların şiddetini deklare etmek açısından önemli olmuştur. Raporda ayrıca APT41'in ABD, Kanada, İngiltere ve Meksika'daki şirket ağlarına girmeye çalıştığını ve bu ülkelerdeki yazılım kusurlarını kötüye kullandığı belirtilmiştir. Çin tarafında da bu tarz şikayetler meydana gelmektedir. Mart 2020 yılında Çinli güvenlik şirketi Qihoo 360, CIA hack grubunun (APT-C-39), 11 yıl boyunca Çin'e yönelik havacılık, petrol, gaz ve teknoloji gibi sektörler üzerinden saldırılar gerçekleştirdiğini iddia etmiştir. Raporda: CIA tarafından sivil havacılığın saldırıya uğrayan bilgi teknolojisi sektörlerinin yalnızca Çin'de değil, aynı zamanda diğer ulus devletlerdeki yüzlerce ticari havayolunu da kapsadığı vurgusu yapılmıştır. ABD'nin iddiaları reddetme ihtimaline karşı raporda, hackerların CIA ile bağlantılı olduklarına dair sayısız kanıt bulunduğuna dair ibareler de yer almaktadır (Doffman, 2020).

3.2.2. İran

1993 yılından itibaren internete erişimi sağlayan ve bu konuda Ortadoğu'da ilk örnek niteliğinde olan İran, siber uzaya yönelik görüşlerini her zaman kendine has bir çerçeveden oluşturarak alan içerisindeki özgünlüğünü koruyan devletlerden biridir. Siber uzayı tehdit unsuru görmenin yanında bir fırsat alanı olarak da değerlendiren İran, ilk uluslararası bağlantıyı Trans-Avrupa Eğitim ve Araştırma Ağları Birliği (Trans-European Research and Educational Networking Association-TERENA) aracılığıyla oluşturmuş ve daha sonra ticari İnternet Servis Sağlayıcısı (Internet Service Provider-ISP) hizmeti vermeye başlamıştır (Çahmutoğlu, 2021: 7-8).

Kurumsallaşma alanında attığı adımlar, stratejik anlamda siber uzayı ideolojik kimliğinin de belirleyici bir unsur olduğu algılama biçimi sonrası oluşturduğu politikalar ve gerçekleştirdiği saldırıların hepsi İran'a özgü olmuştur. Bu doğrultuda İran'ın siber politikasını önemli iki olay şekillendirmiştir. Bunlar Yeşil Hareket Gösterileri ve Stuxnet saldırılarıdır. İran, Stuxnet saldırısından oldukça etkilenmiştir. Nitekim saldırı neticesinde İran'ın nükleer faaliyetlerine darbe vurulmuştur ve bu olay sonrası İran, siber kapasitesini geliştirme yoluna gitmiştir. Yeşil Hareket Gösterileri de İran'ın siber uzaya müdahale etme ve kapasite geliştirme adımlarını hızlandırma noktasında etki derecesi yüksek bir olaydır. 2009 yılında seçimlere şaibe karıştığı iddiaları sonrası sosyal medyadan örgütlenme gerçekleşmiş ve akabinde İran hükümeti internet erişimini engellemiştir. Ülke içindeki muhaliflerin yurtdışına sürgün edilmesi sonrası uluslararası çapta da ses getiren bir olay niteliğinde olmuştur. Protestoların bastırılması hususunda İran'ın siber gücü önemli bir rol oynamıştır (Theohary, 2020). Bu bağlamda attığı en önemli adımlardan birisi olan "Ulusal Bilgi Ağı" projesi, bu olay sonrası oluşturulmuştur.

İran'ın ulusal siber altyapısının gelişimi Soğuk Savaş ve sonraki dönemler için özel şirketlerle kurduğu temaslar vasıtasıyla gerçekleşmiştir. Özellikle Almanya ve Fransa'daki şirketlerin İran'a yaptığı yatırımlar sonucu teknolojik anlamda bilgi sahibi olmaya başlayan İran, Batı ile Doğu arasında bir köprü konumunda olmayı amaçladığı için ticari anlamda da merkezi bir konumda olmayı amaçlamıştır. Bu doğrultuda hem karadan hem havadan hem de denizden ulaşım ağlarını aktif tutarak internet altyapısını da bu oranda geliştirmiştir (Ministry of Information and Communications Technology, 2011).

İran'ı siber güvenlik perspektifinde özgün kılan en önemli etmen, gerçekleştirilen saldırılarda temel felsefenin düşmana olabildiğince fazla hasar verilmesidir. Bu çerçevede bilgisayar ve ağ güvenliği şirketi olan MalCrawler (2016), yaptığı bir araştırmada devletlerin siber uzaydaki amaçlarını ölçmüştür. Rusya, Çin ve İran'daki hackerları inceleyen şirket, sunduğu raporda devletlerin siber saldırı yaparken neyi amaçladığını ve ne gibi önceliklerinin olduğunu açıklamıştır. Bu bağlamda Çinli hackerlar, saldırıyı gerçekleştirirken yeni teknik bilgiler ve buna benzeyen tüm verileri çalmayı hedeflerken Rus hackerlar ise genelde eriştiği sistemi daha sonra da kullanabilmek için kopyalama işlemine gitmeyi hedeflemektedir. Araştırmada İranlı hackerların ise saldırılan kişi/kurumlara mümkün olduğunca fazla hasar vermeyi amaçladığı gözlemlenmiştir (Jones, 2016).

3.2.2.1. İran'ın Kurumsal Mekanizmaları ve Uygulamaları

İran'da siber savunma mekanizmasını ordu ve askeri birimler kontrol etmektedir. İran'ın yurtiçi ve yurtdışı siber politikaların planlaması bu birimler tarafından yapılmaktadır. İran'ın saldırı biçimleri genellikle "bir makro düzey etkiye birçok mikro düzey tepki" şeklinde gerçekleşmektedir. Nitekim bu durum diğer alanlarda olduğu gibi siber alanda da bu şekildedir (Kara, 2013).

İran'ın siber güvenlik kurumlarına bakıldığında dokuz farklı oluşumun varlığından söz etmek mümkündür. Bunları kısaca açıklamak gerekirse:

- Ulusal Pasif Savunma Örgütü: 2010'da kurulan bu örgüt İran'a saldırı gerçekleşmesi halinde ülkenin internet altyapısının görebileceği zararları minimize etmeyi amaçlamaktadır. Bu bağlamda örgüt, Stuxnet saldırısından alınan dersin bir sonucu olarak değerlendirilmektedir (Peskin, 2020).

FATA: 2011 yılında kurulan İran Siber Polis Birimi, dolandırıcılık ve veri hırsızlığı gibi suçlara yönelik incelemelerde bulunmaktadır (Siboni ve Kronenfeld, 2012).

- Siber Güvenlik Yüksek Konseyi: Ayetullah Ali Hamaney'in öncülüğünde 2012 yılında kurulan bu konseyde, siber güvenlik ve internet politikalarının devlet tekelinde bulundurulması amaçlanmaktadır. Bu konseyde ayrıca İran'ın siber güvenlik bütçesi belirlenmektedir (Radio Farda, 2020).
- Besic Siber Konseyi: İran ordusu tarafından 2014 yılında kurulan bu konsey, profesyonel olmayan gönüllü hackerlardan oluşmakta ve paramiliter bir güç olarak kabul edilmektedir (Theohary, 2020).
- Mabna Enstitüsü: Ordu ve hükümetin ortak bir şekilde kontrol ettiği telekomünikasyon sahtekarlığı ve veri hırsızlığı yapan bir kurumdur (Theohary, 2020).
- Maher: Siber Savunma Müdahale Timi olarak da adlandırılan bu örgüt, İran'da İletişim ve Bilgi Teknolojileri Bakanlığı'na bağlı olarak oluşturulmuştur. Maher, İran'ın siber savunmasında önemli bir role sahiptir ve saldırı anında acil komutun çalışması sonucu devreye girerek bilgisayar güvenliğini sağlamaktadır. Hükümet sitelerinin yanı sıra devletin izin verdiği özel şirketlerinin de sitelerini korumakla görevlendirilmektedir (Siboni ve Kronenfeld, 2012).
- Devrim Muhafızları Ordusu: Ülkedeki siber saldırı politikalarının belirlendiği en önemli kurumlardan biridir ve siber yeteneklerini geliştirme noktasında uluslararası çapta ses getiren bir oluşumdur (Adem Yılmaz, 2020: 367).
- Ashiyane Dijital Güvenlik Ekibi: İran'da en çok bilinen hacker gruplardan birisi olan Ashiyane, ismini dünya çapında duyuran profesyonel bir ekipten oluşmaktadır (Adem Yılmaz, 2020: 367).
- Pardis Teknoloji Parkı: İran'ın Silikon Vadisi olarak tanımlanmaktadır ve içerisinde teknoloji sektöründen yüzlerce şirketi barındıran Pardis Teknoloji Parkı, 2001 yılında Cumhurbaşkanlığı Ofisi ve Teknolojisi İşbirliği Bürosu tarafından kurulmuştur (Adem Yılmaz, 2020: 368).

İran'ın siber uzayda strateji oluşturma noktasında savunma ve saldırı unsurlarına verdiği dikkat ve gösterdiği önem doğrultusunda iki temel stratejiden bahsedilmektedir. Bunlardan ilki gelebilecek tehdide karşı savunma kapasitesinin en iyi seviyeye çıkarılmasıdır. Diğeri ise bölgesel ve küresel güçlerle siber uzayda mücadele edebilmek adına karşı tarafa verilebilecek en büyük hasar verilmelidir (Adem Yılmaz, 2020: 368). Savunma mekanizmasında en önemli çalışma İran Dijital Kale *(Dejfa)* adındaki ulusal siber güvenlik duvarıdır. Devletin internet altyapılarına yönelik gerçekleşme ihtimali bulunan saldırıların tespit edilip aksiyon alındığı birim olarak değerlendirilmektedir (Çahmutoğlu, 2020b). Saldırı noktasında ise İran, siber uzaydaki ofansif yeteneklerini sergilemek için kendisine önemli hedef noktaları oluşturmuştur. Bu noktalar ortaya konulurken ölçüt olarak ideolojik, siyasal ve ekonomik gerekçeler alınmıştır ve bahsi geçen ölçütlerdeki çıkarlarına ters düşen ülkeleri hedef olarak belirlemiştir. Bu bağlamda İran, çoğunlukla ABD, Suudi Arabistan ve Körfez ülkelerine olmak üzere, İsrail, Güney Kore ve Türkiye'ye siber saldırı operasyonları gerçekleştirmiştir. İran ayrıca sosyal medya unsuruna da önem vermiş ve bu alanda operasyonlar gerçekleştirerek özellikle 2011 yılında ülke adına propaganda faaliyetlerinde bulunmuştur (Romm vd., 2018). İran'ın APT33 isimli hacker grubu, Güney Kore ve Suudi Arabistan'a yönelik başta havacılık ve enerji olmak üzere pek çok sektörde siber saldırılar gerçekleştirmiştir. FireEye şirketinin yaptığı araştırmalar sonucu APT33'ün İran'a ait olduğu tespit edilmiştir (O'leary vd., 2017).

İran'ın Suudi Arabistan'a ve Körfez ülkelerine yönelik gerçekleştirdiği siber saldırılara bakıldığında genel olarak ideolojik etkilerin ön planda olduğunu söylemek gerekmektedir. İran'ın siber uzayda bu bölgelere saldırı kapasitesini genişletmesi, Ortadoğu'da süregelen vekalet savaşlarının bir tezahürü olarak değerlendirilmektedir. Aynı zamanda Suudi Arabistan ve Körfez ülkelerinin siber savunma kapasitelerinin düşük olması nedeniyle İran, saldırgan tutumunu daha rahat bir şekilde artırmaktadır. Suudi Arabistan ve Körfez ülkelerine yönelik yapılan saldırılar genelde devlet kurumları ve özel şirketlere yönelik yapılmıştır. Ortadoğu'daki güvenlik şirketleri, gazetecileri ve insan hakları savunucularını hedef alan *Thamar Reservoir* saldırıları, Suudi Arabistan'ın resmi kurumlarına yönelik yapılan *Shamoon-2* ve Körfez ülkelerindeki özel şirketlere yapılan *Leafminer* saldırıları bunlara örnek olarak verilebilir. Ayrıca İran, siber saldırı gerçekleştirdiği sıralarda zaman zaman Hizbullah ve Hamas gibi oluşumları aracı olarak kullanmaktadır. Bu bağlamda Hizbullah ve Hamas araç olarak kullanılmak suretiyle ABD ve İsrail'e yönelik saldırılar gerçekleşmiştir. İran'ın araç olarak kullandığı unsurlardan bir diğeri de Kuzey Amerika'da olmuştur. İran, Meksika'da ABD karşıtı hackerlarla temas kurarak ABD'ye yönelik operasyonlar geliştirmektedir (Adem Yılmaz, 2020: 367).

İran'ın siber saldırı ve savunma yaparken izlediği birtakım perspektif ve prensipler mevcuttur. Düşman olarak görülen ülkelere yönelik devlet nezdinde söylemler de gerçekleştirilmektedir. Bu doğrultuda İran Savunma Bakanı, ABD'nin siber terörün başında bulunduğunu ve diğer ülkelere çeşitli suçlamalarla siber terörün arttırılması için ortam sağladığını iddia etmektedir. Bakan ayrıca

İran'ın siber alanda alt edilemeyeceğini belirterek diplomatik söylemlerle güç gösterisinde bulunmuştur (Kara, 2013: 67). İran, düşman gördüğü ülkelere karşı siber uzay içerisinde korku ve caydırıcılık yaratmak amacıyla mikro düzeyde pek çok saldırı faaliyetleri gerçekleştirmektedir. İran'ın bu yaklaşımına karşılık ABD'de daha çok savunma odaklı strateji gerçekleştirildiği için istihbarat birimlerinin güçlü olduğu bilinmektedir. Siber espiyonaj (spyware) ve gözetim (surveillance) amaçlı ürünler geliştiren ABD, bu noktada küresel şirketlerden de faydalanmaktadır. Bu şekilde istihbarat ve siber savunma anlamında kapasitesini geliştirmektedir. Fakat ABD, siber saldırılara karşı koymak için ise sadece resmî kurumları aracılığıyla bir çalışma gerçekleştirmektedir (Çahmutoğlu, 2020b).

Siber uzay içerisinde ABD-İran rekabetinin miladı, İran'ın İsfahan kenti yakınlarındaki Natanz nükleer santrallerini kontrol eden bilgisayar sistemlerine sızarak fiziksel hasara yol açan Stuxnet isimli virüsün yarattığı yıkıma kadar dayanmaktadır. ABD ve İsrail'in ortak bir çalışması olduğu öne sürülen bu virüs, İran'a ciddi ölçüde hasar vermiştir (Baram ve Lim, 2020). Bu doğrultuda ABD'ye yönelik saldırı perspektifini geliştiren İran, siber yeteneklerinin kapsamını ve niteliğini artırarak tehdit olarak kabul ettiği ülkelere yönelik planlamalar yoluyla siber saldırılar düzenlemek suretiyle agresif bir siber saldırı stratejisi geliştirmiş ve saldırgan bir ülke konumuna gelmiştir (Darıcılı 2019: 411-415).

Siber uzayda ABD-İran rekabeti gün geçtikçe katlanarak arttığı savunulmaktadır. ABD, İran'ı askeri, ekonomik ve diplomatik alanlarda olduğu gibi siber alanda da potansiyel bir tehdit olarak görmektedir. İran'ın ABD'ye yönelik yaptığı saldırılar, özellikle İran'a yapılan Natanz'daki Stuxnet saldırılarına karşılık gelmese de önemli kurumların ve bakanlıkların internet sitelerinin ele geçirilmesi şeklinde gerçekleşmiştir. Kudüs Gücü komutanı Kasım Süleymani'nin Amerika'nın hava saldırısıyla öldürülmesi üzerine gerçekleştirilen siber saldırı, İran'ın bu tarzda gerçekleştirdiği operasyonlara örnek olarak verilebilir (Milliyet, 2020). Bu saldırı biçimi her ne kadar nükleer tesislere yapılan operasyon ile denk olmasa dahi, ülkenin güç ve kapasitesini kanıtlar niteliktedir.

İran'ın ABD'ye yönelik gerçekleştirdiği önemli saldırılara göz atıldığında bunlar: Yazılım geliştiricisi şirket olan Cylance'ın (2014: 3) önemli altyapılara yaptığı saldırılardan sonra İran'ı "Yeni Çin" olarak adlandırdığı *Cleaver Operasyonu,* ABD'nin J.P. Morgan, Bank of America Merrill Lynch gibi önemli finans kuruluşlarına ve banka sitelerine yönelik yapılan *Ababil Operasyonu,* ABD'nin Bowman'daki altyapı tesislerine yönelik gerçekleştirilen *Bowman Avenue Barajı Saldırısı*, İran'ın kurmuş olduğu Mabna Enstitüsü'nün gerçekleştirdiği veri hırsızlığı operasyonları, ABD savunma sanayisini hedef alan ve Higgins (2014) tarafından siber casusluk operasyonu olarak nitelendirilen *Safran Gülü Operasyonu*, Las Vegas'ın en büyük kumarhane işletmelerinden birisi olan Sands'a yönelik gerçekleştirilen *Las Vegas Sands Şirketi Saldırısı* ve son olarak ABD'deki yapım şirketi HBO'yu hedef alarak uluslararası çapta bilinirliği olan dizilerin

(Game of Thrones gibi) yayımlanmamış bölümlerinin çalındığı *HBO'ya Karşı Veri Hırsızlığı ve Gasp Saldırısı* olarak belirtilmektedir (Adem Yılmaz, 2020: 369).

İran, ABD'nin APT olarak nitelendirdiği kategorinin içerisinde yer alan bir ülkedir ve bu konuda İran kaynaklı birçok APT grubu bulunmaktadır. En önemlileri APT33, APT34, APT39, Charming Kitten ve MuddyWater adlı aktörlerdir. Bu APT'ler teknik olarak sırasıyla incelendiğinde İran'ın genel olarak hedef aldığı birimler; petrokimya tesisleri, havacılık, enerji ve savunma/uzay endüstrisinin altyapılarıdır. Aynı zamanda yüksek profilli kişiler hedef alınmaktadır. Bununla birlikte devlet destekli ağlar ve APT'lerle ulusal kritik altyapıları ve güvenlik kurumları hedef alınmaktadır. Aynı zamanda istihbarat ve casusluk için de çalışan birimleri vardır. Özellikle Charming Kitten ve MuddyWater grupları bunlara örnek olarak karşı devletin askeri, diplomatik ve güvenlik faaliyetlerini tehdit etmektedir. Bu gruplar, tıpkı bir Stuxnet solucanı gibi tespit edilemeden gizlice çalışabilmektedirler. Çeşitli saldırgan APT grupları ve istihbarat gruplarının faaliyetleri göz önüne alındığında Çahmutoğlu (2020b)'na göre İran'ın siber alanda henüz nasıl bir strateji ve politika izlediğine dair net bir görüş mevcut değildir. İran'ın savunma odaklı olduğu gibi saldırı odaklı da çalıştığı savunulmaktadır. Buna göre İran'ın siber komutanlığında siber savunma ve saldırı kapasitesine sahip özel birimlerin bulunduğu bilinmektedir. Devlet destekli olan faaliyetler ise daha çok siber korsan grubu olarak anılan organize oluşumlarla ve İran istihbarat servisine bağlı hacker gruplarıyla yapılmaktadır. ABD tarafından da bu grupların her biri siber tehdit olarak adlandırılmaktadır.

Çin'in, ABD'den taviz alarak elde ettiği jeopolitik kazanımlara benzer bir kazanç elde etme gibi bir imkânı olmadığı için İran'ın ABD ile işbirliği daha sınırlı bir düzeyde gerçekleşmiştir. Aynı şekilde Rusya da İran'la aynı kategoriye girmektedir. Rusya ve İran, Çin ve ABD'ye nazaran siber alandaki ilişkilerini geliştirmek için farklı bir metot gerçekleştirmiştir. Kamuoyuna daha açık biçimde gerçekleştirilen bu işbirliği çalışmalarında en çok dikkat çeken husus, Rusya'nın diğer ülkelere yaptığı siber saldırı operasyonlarını İran bilgisayar korsanlarının kullandığı altyapıdan faydalanarak gerçekleştiriyor olmasıdır. Özellikle ABD'nin İran'ın misilleme ve siber caydırıcılıklarına yönelik kötü niyetli aktör algısıyla birlikte İran'a karşı misilleme olarak elindeki yegâne koz olan finansal kuruluşlarla yapılan caydırıcılık hamlesi, İran'ın saldırganlık iştahını artırmıştır (Cilluffo, 2013). Bu hususta İran'ın sanayi sektöründeki fiziksel altyapılara yönelmesi dikkat edilmesi gereken bir diğer önemli meseledir.

ABD, İran sanal aktörlerinin ne gibi faaliyetlerde bulunduğuna ilişkin tam bir açıklama yapmakta tereddüt etmektedir. Buna rağmen sanayi sektörünün kontrol sistemlerini ya da fiziksel altyapıyı hedef almak için siber becerilerini kullanma konusunda İran'ın yanına Rusya, Çin ve Kuzey Kore'yi de dahil etmesi dikkat edilmesi gereken önemli bir mesele olarak karşımıza çıkmaktadır. Amerikan istihbarat yetkilileri, İran'ın sanal faaliyetlerinin İran Devrim Muhafızları Ordusu olan Pasdaran tarafından yürütüldüğünü iddia etmektedir. Yetkililere göre Pasdaran, siber saldırılar için

bazen paravan şirketler kullanmakta, bazen de bizzat kendi birliklerince düzenlemektedir. İran'ın geçmişteki siber saldırıları, DDoS, internet sitelerini bozmaya ya da kişisel veri hırsızlığına kadar farklı özellikler göstermektedir. ABD'deki Siber Güvenlik ve Altyapı Güvenliği Dairesi'nin Ocak 2020'de yayımladığı uyarı, İran'ın faaliyetlerinin sınırlarını genişletebileceği, bulaştığı sistemlerde her türlü verileri silen zararlı yazılımları ya da siber kinetik saldırıları kullanabileceğine dikkat çekmektedir (CISA, 2020b).

3.2.3. Rusya

2000 yılından itibaren devlet nezdinde siber güvenlik politikalarını oluşturmaya başlayan Rusya'nın teknoloji ve internet kavramlarına SSCB döneminden miras kalan aşinalığı sayesinde günümüzde siber uzayda en etkili devletlerden birisi olarak bilinmesine olanak sağlamıştır. Rusya'nın günümüzdeki siber güvenlik stratejisinin temeli olarak değerlendirilen uygulama da 1980'li yıllarda SSCB ordusundan Mareşal Nikolai Ogarkov'un hazırladığı *Revoluation in Military Affairs* programıdır (Darıcılı ve Özdal, 2017: 121).

Rusya ve siber uzay denildiğinde akla gelen ilk bilgi güvenliği kavramı olmaktadır. 1994'ten itibaren Rus-Çeçen savaşında Çeçenlerin bilgi teknolojilerini kullanma ve uluslararası kamuoyuna duyurabilme kabiliyetinden alınan ders çerçevesinde üzerine yoğunlaşılan bir kavram olan bilgi güvenliği, Rusya'nın siber güvenliği algılama biçimini şekillendirmektedir. Çeçen savaşının yarattığı olumsuz etkilere karşı askeri ağ teknolojileri ve enformasyon savaşı alanına yönelik düzenlemeler oluşturulmuştur (Darıcılı ve Özdal, 2017: 123). Siber uzayda etkisini artırmak için işbirliği ve anlaşmalardan kaçınmayan Rusya, Iasiello (2020)'ya göre Batı'nın elindeki gelişmiş bilgi teknolojilerinin kendi aleyhine kullanılmasından çekinmektedir. Bu bağlamda Moskova hükümeti, siber güvenlik politikalarını oluştururken katı bir pencereden bakmakta ve otoriter kimliğe bürünmektedir. Tıpkı Çin ve İran gibi Rusya da kontrolünde tuttuğu siber ordular vasıtasıyla hem sınır içinde ulusal güvenliği sağlamak için etkinliğini artırıyor hem de çok sayıda sınır dışı operasyonlar yaparak siber uzayı dış politika unsuru olarak kullanmaktadır (Acar, 2020a: 91-99). Nitekim Darıcılı (2014: 6)'ya göre Estonya, Gürcistan, Kırgızistan ve Ukrayna'ya karşı gerçekleştirdiği siber operasyonların altında dış politik çıkarlar vardır ve sorunların çözülmesi kapsamında saldırılar gerçekleşmektedir.

Siber faaliyetler açısından yapılan istatistiklerde dünyada ilk beş ülkeden biri olan ve dünyanın en gelişmiş hackerlarını ülkesinde bulunduran Rusya, potansiyel tehdit algısının yoğun olduğu bir coğrafyada bulunduğundan dolayı siber uzayda hem korumacı hem saldırgan politikalar benimsemektedir. Rusya, olası bir siber saldırı veya savaş durumunda karşı tarafın bilgi teknolojilerine dayanan altyapısını ortadan kaldırabilmenin yanında finansal ve askeri sektörler ile sivil iletişim sistemlerini çalışamaz duruma sokabilecek önemli teknolojik altyapı ve donanımlara sahip bir ülkedir. Ayrıca Rusya'nın doğrudan veya dolaylı yollardan hackerlara verdiği destek

yadsınamaz bir gerçek olarak değerlendirilmektedir. Bu noktada ABD'den daha fazla hacktivist gruplarının bulunduğu söylenmektedir (Gürkaynak ve İren, 2011: 267). Dolayısıyla direkt devlet vasıtasıyla gerçekleştirilen ve hedef ülkenin ekonomik kaynakların bloke etmek amaçlarını taşıyan siber saldırılarla kendi gücünü dünyaya göstererek siber motivasyonunu arttırmaktadır.

3.2.3.1. Rusya'nın Kurumsal Mekanizmaları ve Uygulamaları

Bilgi güvenliği kavramını siber güvenliğinin merkezine yerleştiren Rusya'nın özellikle 2000 yılından itibaren yayımladığı stratejik belgeler, siber güvenlik politikasını belirleme noktasında önemli kaynaklar olarak değerlendirilmektedir. Bu bağlamda 2000 yılında açıklanan *Rusya Federasyonu Ulusal Güvenlik Konsepti* belgesinde Rusya'nın siber gücünü oluşturma hususlarından bahsedilmiş, tüm kurumların ve birimlerin bu hedef doğrultusunda çalışmasının gerekliliği vurgulanmıştır (Acar ve Pekcandanoğlu, 2020: 171-174).

Rusya'nın siber güç olma noktasında oluşturduğu en kapsamlı belge, *Rusya Enformasyon Güvenliği Doktrini*'dir. Rusya'nın siber güvenliğini oluşturma hususunda yol haritasını ve atacağı adımların belirlediği bu belgede ülke çıkarının gerektirdiği ölçüde yapılacak faaliyetler, resmi ağızdan kapsamlı olarak açıklanmıştır. Rusya, ilerleyen yıllarda hazırladığı belgelerde geleceğe yönelik planlardan da söz etmiştir. Bu bağlamda 2009 yılında oluşturulan *2020'ye Doğru Rus Ulusal Güvenlik Stratejisi*, siber uzayda 10 yıllık bir faaliyet planın oluşturulduğu ve içeriği itibariyle tamamen enformasyon güvenliği politikalarının içinde bulundurulduğu belgedir. Bundan iki yıl sonra 2011 yılında siber savaş alanında ilk doktrin olan *Bilgi Çağında Rus Silahlı Kuvvetleri'nin Faaliyetlerine İlişkin Kavramsal Görüşler* adlı belge oluşturulmuştur. Bu doktrinde ilk kez siber savaş vurgusu yapılarak siber uzayda Rus askeri varlığının kabul edildiği kayıtlara geçmiştir. 2013 yılında Rusya Genelkurmay Başkanlığından Gerasimov'un, *Military Industrial Kurier Dergisi*'nde yayımlanan *The Value of Science in Prediction* adlı makalesi, literatür içerisinde oldukça ses getirmiş ve nihayetinde bu makale, *Gerasimov Doktrini* olarak tanımlanmıştır (Gerasimov, 2013). Makalede, askeri olmayan yöntemlerin genel savaş prensiplerine dahil edilerek daha az konvansiyonel güçle daha fazla etki yaratmak üzerine incelemeler mevcuttur. 2013 yılında *Rusya Federasyonu Devlet Politikasının Uluslararası Enformasyon Güvenliği Alanındaki Temel Prensipleri* adıyla yayımlanan belgede, Rusya'nın enformasyon ve bilgi güvenliği noktasında belirleyici noktalardan bahsedilmiştir ve sınır dışındaki güçlerle rekabet edilebilirliğin tartışıldığı bir belgedir (Darıcılı ve Özdal, 2017: 123-127).

2016 yılında hazırlanan *Rusya Federasyonu Enformasyon Güvenliği Doktrini*, bilgi güvenliği noktasında halihazırda en kapsamlı belge olarak değerlendirilmektedir (The Ministry of Foreign Affairs of the Russian Federation, 2016). Belgede bilgi güvenliğinin önemi vurgulanmış ve beş kısma bölünerek incelenmiştir. Siber uzayda etkinlik ve bilgi güvenliği hususu, bu belgede fazlasıyla üzerinde durulan konular olmuştur. Belge ayrıca, milli güvenliğin ulusal çıkarlar çerçevesinde

vurgulandığı ve dış politika çıkarlarının da içeriğe dahil edildiği geniş kapsamlı bir doktrin hüviyetindedir (Acar, 2020b: 92). Göçoğlu ve Aydın (2019: 246)'a göre Rusya'nın siber güvenlik politikalarını belirlemek için oluşturduğu stratejik belgeler, ülkenin siber güvenlik politikası oluştururken savunmacı bir anlayış benimsemektedir ve savunma üzerine oluşturulacak politikalarda müttefiklik ilişkilerini geliştirmek Rusya adına oldukça önemlidir. Bu bağlamda Batı karşıtı ülkelerle işbirliği sağlama amacında olan Rusya; Çin ve İran ile işbirliği veya çeşitli operasyonlar gerçekleştirmek amacıyla bir araya gelmektedir. Örnek olarak bilgi güvenliği noktasında bir araya gelen Çin ve Rusya, 2016 yılında siber forum oluşturmuştur ve bu forumda iki ülke arasında işbirliği gerçekleşmektedir (Wei, 2016).

Odak noktasına siber güvenliği alan Rusya, internetin korunması adına 2019 yılından itibaren internet hukuku hususunda yasal düzenlemeler de gerçekleştirmektedir. Bu doğrultuda belirlediği hedefler; sınır içerisinde internet güvenliğini sağlamak için niteliği yüksek ekipler ve sağlam altyapılar oluşturmak, internet üzerinden sınırların tercihe bağlı açılıp kapatılabileceği bir merkezi kontrol mekanizması oluşturmak ve uluslararası bir internet modeli oluşturarak hem kendisine denk hem de kendisinden daha az siber kabiliyeti olan ülkelere örnek ülke konumunda olarak alan içerisindeki devletlerle işbirliği oluşturmaktır (Epifanova, 2020). Rusya'nın, bilgi teknoloji dahilinde siber uzayda işbirliği geliştirme noktasında ikili veya çok taraflı müzakerelerde dikkat ettiği unsurlar ve anlaşmalarda belirlediği şartlar şöyle sıralanmaktadır:

- Bilgi teknolojileri hükümetler arasındaki anlaşmazlıkları çözmeye zorlamak için bir araç olarak kullanılmalıdır ve bu soruna ilişkin anlaşmalar, uluslararası barış ve güvenliği güçlendirme görevinde önemli bir faktör haline gelme potansiyeli taşımaktadır.
- Ulusal kalkınma için küresel bilgi ve iletişim ağlarının istikrarlı işleyişinin ve güvenli kullanımının yönetiminin sağlanması gerekmektedir. Rus hükümetine göre bu faaliyet, ulusal toplumların ekonomik, sosyal, politik ve kültürel gelişiminde ve kültürel kimliklerini ve manevi birliklerini korumada bir faktör olarak küresel ağlara olan güveni artıracaktır.
- Ülke içerisinde aktif bir şekilde internet kullanan vatandaşları, bilgi teknolojilerinin güvenli kullanımını sağlayacak ölçüde eğitildiği zaman ülkenin siber güvenlik standartları yükselecektir. Aynı zamanda bilgi teknolojileri kötü amaçla kullanan vatandaşlara yönelik hukuksal düzenlemelerin oluşturularak caydırıcılık unsuru sağlanmalıdır.
- Terör eylemlerinde bilgi teknolojisi unsurunun kullanımına karşı önlemler geliştirmek gerekmektedir.
- Devletlerin egemen eşitliği ilkelerine uyarak ve diğer devletlerin içişlerine karışmama ilkesi benimsenmelidir. Siber uzaydaki faaliyetlerin yalnızca uluslararası işbirliği ilkeleri temelinde yürütülmesinin yanında temel insan hak ve özgürlükleri başta olmak üzere

devletlerin siber uzayda yürüttüğü faaliyetlere saygı gösterilmesi gerekmektedir (Grigoriev, 2010: 5-8).

Rusya, ülke içerisinde ve dışarısında teknik açıdan siber güvenlik mekanizmalarını belirlemek için attığı kurumsal adımlarında çeşitli birimler oluşturmuştur. Bu birimler hem resmi olarak devlet kurumu hem de Rusya'nın siber politikalarının belirlendiği devlete bağlı kuruluşlar olarak karşımıza çıkmaktadır. Bunlar:

- Rusya Federal Güvenlik Servisi (FSB): Rusya'nın siber güvenlik politikalarını belirleme hususunda önemli bir işleve sahiptir ve iç istihbarattan sorumlu kurum olarak ortaya çıkmıştır.
- Federal Koruma Servisi (FSO): Bilgi Güvenliği konusunda söz sahibi olan FSO, bilgi ve enformasyon güvenliğini sağlamak suretiyle bilgi güvenliği politikalarının oluşturulmasında önemli yetkilere sahiptir.
- Teknik ve İhracat Kontrollü Federal Servisi (FSTEC): Siber güvenlik politikaları oluşturma hususunda önemli yetkileri bulunan FSTEC, Rusya Savunma Bakanlığı'na bağlıdır. Ana görevi hassas teknoloji ihracatının kontrol edilmesi ve lisanslanması üzerinedir.
- Dış İstihbarat Servisi (SVR): Rusya'nın dış istihbarat sorumluluğunu yürütmekle görevlendirilmiştir. Bununla birlikte stratejik sinyal istihbaratı, telsiz haberleşmesi, askeri ve ticari uydu sistemlerinden istihbarat toplamak gibi görevleri vardır.
- Ana İstihbarat Direktörlüğü (GRU): 1996 yılına kadar FSO'nun yürüttüğü işi yapmıştır. Rusya Savunma Bakanlığı'na bağlı olarak faaliyetine devam eden GRU, en büyük istihbarat servisi olarak açıklanmaktadır. Hatta Rusya'nın gerçekleştirdiği siber saldırılarda en büyük pay GRU'ya aittir. Rusya'nın yürütmekte olduğu bilgi savaşları kapsamında Estonya, Gürcistan, Ukrayna, Türkiye ve ABD'ye yönelik yapılan saldırıları GRU organize etmiştir (Acar, 2020b: 97).

Rusya'nın siber saldırılar düzenlemesi, dış politik çıkarlarına verdiği önem dahilinde adım atılabilecek her alanda var olmasına bağlanmaktadır. Örneğin Rusya'nın enerji alanında yaşadığı bir sorun, siyasi ve ekonomik çıkarlarıyla bağlantılı olup ulusal çerçevede değerlendirildiğinden ülkede algılanan her tehdit güvenlik sorunu olarak görülmektedir. Bu bağlamda tüm enstrümanları kullanan Rusya, yaşadığı uluslararası krizleri çözmek adına siber operasyonlara da başvurmaktadır. 2007 yılında teknolojik açıdan yüksek bir gelişim mesafesi kat eden Estonya'ya yönelik yapılan siber saldırılar, Rusya'nın bir nevi güç gösterisi olarak yorumlanmaktadır. Saldırı sonrası Estonya'nın imajı zedelenmiştir (Connell ve Vogler, 2017). Rusya'nın gerçekleştirdiği bu tarz operasyonlara 2008 Gürcistan, 2009 Kırgızistan ve 2014 Ukrayna saldırıları örnek olarak gösterilebilir. Gürcistan'a gerçekleştirilen saldırı, hibrit savaş örneği taşımaktadır. Rusya, Gürcistan'a hem siber saldırı

faaliyetlerinde bulunmuş hem de ülkeyi işgal etmiştir (Acar, 2020a: 62). 2009 yılında Kırgızistan'da Manas Askeri Üssü'ne yönelik DDoS saldırıları gerçekleştirmiştir. 2014 yılında Ukrayna'ya karşı gerçekleştirilen siber saldırı, Ukrayna'nın AB ve NATO ile yakınlaşma iddialarının artması sonrası gerçekleşmiştir. Hibrit savaş stratejisine benzer bir stratejinin uygulandığı bu saldırılarda, Rusların yoğun olarak yaşadığı Donbass (Donetsk ve Lugansk) bölgesindeki yerlileri kışkırtma çabasına girmenin yanında ülkenin önemli teknik birimlerine siber saldırılar gerçekleştirmektedir. 2021 yılı sonu itibariyle Rusya bölgeye askeri ekibini göndermiş ve bunun üzerine Ukrayna'nın talebi doğrultusunda NATO ülkeleri havadan ve karadan bölgede kendisini göstermeye başlamıştır (Euronews, 2021b). Rusya'nın Ukrayna'ya yönelik yürüttüğü siber operasyonlarda Kırım meselesine karşı da bir hamle gerçekleştirmiş ve Ukrayna'nın resmi mobil telefon şirketinin altyapısını çökertmiştir (Darıcılı, 2014: 11-18).

İran ve Çin'de olduğu gibi Rusya da ABD'nin APT kategorisinde yer almaktadır. Bu doğrultuda ABD Siber Güvenlik ve Altyapı Güvenlik Ajansı (CISA), Rusya'dan gelen siber saldırıları ve tehlikeleri ayrıntılı bir şekilde analiz etmektedir. İç Güvenlik Bakanlığı (DHS) ve Federal Soruşturma Bürosu (FBI) ile gerçekleştirilen ortak bir analitik çalışmada, CISA'nın Rusya hakkında tek bir başlık altında sunduğu madde madde raporların yanında, güncel olarak gelen siber saldırıların da bilgilendirilmesi yapılmaktadır. Bu çerçevede CISA'nın hazırladığı raporlar, "teknik uyarı", "analiz raporu" şeklinde, DHS ve FBI ile ortak hazırlanan raporlar ise "ortak analiz raporu" adlı başlıkta sunulmaktadır. 2016 yılındaki Ortak Analiz Raporu (NCCIC ve FBI, 2016) ve 2017 yılındaki Analiz Raporlarında (NCCIC, 2017), Rusya'nın gerçekleştirdiği siber aktiviteler ışığında *Grizzly Steppe* adını verdiği oluşumun, devlet kurumlarına, siyasi partilere ve üniversitelere yönelik gerçekleştirilen siber saldırılara vurgu yapılmıştır.

APT28 ve APT29'un gerçekleştirdiği saldırılar, saldırı biçimleriyle birlikte ayrıntılı bir şekilde gösterilmiş, ne gibi önlemlerin alınması ve uygulanması gerektiği de beraberinde raporun sonuna doğru önerilmeye çalışılmıştır. 2018'de hazırlanan ve *Enerji ve Diğer Kritik Altyapı Sektörlerini Hedefleyen Rusya Hükümeti Siber Etkinliği* başlığıyla sunulan teknik uyarı raporunda Rusya, dosya sunucularına, e-posta sunucularına ve etki alanı denetleyici sistemlerine yönelik saldırı gerçekleştirmiştir (CISA, 2018a). Son olarak 2018'de hazırlanan ve *Ağ Altyapısı Cihazlarını Hedef Alan Rusya Devletinin Desteklediği Siber Aktörler* başlığıyla sunulan teknik uyarı raporunda ise Rus siber aktörlerinin, ağ yönetimi faaliyetleriyle ilişkili bir dizi eski veya zayıf protokol ve hizmet portundan yararlandığı bildirilmiştir. Rus siber aktörler bu cihazlardan yararlanmak için güvenlik açıklarından veya kötü amaçlı yazılım yüklemesi yerine, çeşitli güvenlik açıklarından faydalanmıştır. Bunlar: *Eski şifrelenmemiş protokollere veya kimliği doğrulanmamış hizmetlere sahip cihazlar, kurulumdan önce güvenliği yeterince tanımlanmamış cihazlar ve kullanımı ölmüş cihazlar* olarak tanımlanmaktadır. Bu unsurlar hem fikri mülkiyete hem de ABD nüfusunun sağlık ve güvenliğini destekleyen ABD kritik altyapısına kesintili ve sürekli bir şekilde erişim sağlamaktadır (CISA, 2018b).

ABD'nin *Grizzly Steppe* adı verdiği kod ile Rusya'nın ABD resmî kurumlarına yaptığı siber saldırılar, 2015 yılından itibaren ABD demokrasisine yönelik gerçekleştirilen bir operasyon olarak adlandırılmıştır. Amerikan hükümeti ve politik gruplar için çalışan 1.000'den fazla kişiye e-posta ile ulaşılmıştır. Bu bilgiler ışığında 2016 yılında görevinin başına gelen 46. ABD Başkanı Donald Trump'ın seçim kampanyalarına ve başkanlık yarışına hile karıştığı yönünde tartışmalar olmuştur. 2017 yılındaki Ortak Analiz Raporu'nu, BGA Security ayrıntılı bir şekilde ele almıştır. Bu raporda adı geçen *Grizy Steppe*, Rus Sivil ve Askeri İstihbarat Hizmetleri (RSAIH) tarafından oluşturulmuştur. RSAIH tarafından gerçekleştirilen bu saldırılar, ABD hükümeti ve vatandaşlarına yönelik devam eden siber operasyonların bir parçasıdır (NCCIC ve FBI, 2016).

Ortak Analiz Raporu (2017)'nda Ruslar tarafından gerçekleştirilen saldırıda, iki grubun farklı şekillerde ortak olarak saldırdığı belirtilmiştir. Gelişmiş Kalıcı Tehdit kategorisinde olup APT29 olarak bilinen aktör grubu, ABD parti sistemlerine 2015 yılında girerken APT28 olarak bilinen ikinci grup ise aynı sisteme 2016 yılının bahar aylarında girmiştir. APT28, siyasi partilere *spear phishing* metoduyla saldırmıştır ve çok sayıda üst düzey parti üyesinin bilgi sızdırmasına yol açan içeriğe erişerek, bilgilerini ele geçirmiştir. Her iki grup da hükümet kuruluşları, düşünce kuruluşları, üniversiteler ve şirketleri hedef alarak bilgisayarlara erişim sağlayarak istihbarat elde etmek amacıyla bilgilere sızdığı ve bunları analiz ettiği söylenmektedir. Bu gruplar, eline geçirdiği bilgileri daha büyük saldırılara referans olarak kullanmaktadır (Uçar, 2017).

3.2.4. Kuzey Kore

Siber yeteneklerini siber saldırılar için seferber eden bir ülke olarak değerlendirilen Kuzey Kore, özellikle ABD ve Güney Kore ile olan ekonomik rekabetlerinde geride kalma durumunu minimuma indirebilmek için tüm kabiliyetini asimetrik askeri alternatifler arasında sıklıkla kullanmaktadır. Bu çerçevede de ABD'nin APT olarak nitelendirdiği ülkeler arasında olan Kuzey Kore'nin Rusya ve Çin'den ayrıldığı nokta saldırganlık seviyesi olarak değerlendirilmektedir. Kuzey Kore uluslararası sistemdeki konumu ve kendisine yapılan yaptırımlar sonucu Rusya ve Çin gibi rasyonel bir çizgide ilerlemek yerine daha saldırgan bir tutum sergilemektedir. Daha çok İran'la aynı özelliklerde olmasına (tecrit edilmişlik ve uluslararası yaptırımlar) rağmen düşmanca tavırlarının şiddeti, Kuzey Kore'yi tüm bu ülkelerden daha ayrı bir kategoride incelenmesini gerekli kılmaktadır.

Kuzey Kore; belirlediği hedeflere kimyasal, nükleer ve balistik füzelerin kullanılması haricinde yıkıcı siber saldırı operasyonları da düzenleyerek uluslararası sistemde adını duyurmaktadır. Kuzey Kore'nin saldırı şiddetinin fazla olmasının altında yatan en büyük etken hiç şüphesiz askeri ve ekonomik açıdan yaşadığı zorluklar olarak değerlendirilmektedir (Siers, 2014: 5-7). Ekonomik koşullar haricinde Kuzey Kore'nin savaşçı tutumunun altında yatan bir diğer sebep ise dünyayı bir zayıflık içerisinde görmesiyle alakalıdır ve ulusal stratejisini daha sert bir perspektiften belirlemiştir. Bunun yanında sistem tarafından birçok konuda tanınmadığı için önünde yasal bir engel

bulunmamaktadır. Bu durum da Kuzey Kore'yi saldırgan tutumları yansıtma noktasında daha özgür kılmaktadır. Güntay (2020a: 262-263)'a göre Kuzey Kore için siber uzay, ülkedeki rejimin özellikleriyle yakından ilişkilidir. Bu bağlamda Kuzey Kore'nin gerçekleştirdiği siber saldırılar göz önüne alındığında dikkat çeken üç farklı özellik ön plana çıkmaktadır. Bunlardan ilki, Kuzey Kore'de geleneksel güvenlik tehditleri geleneksel olmayan tehditlerle birleştirilerek yeni bir saldırı çeşidinin ortaya konulmasıdır. İkincisi, Kuzey Kore'nin kontrolündeki siber korsanlar, birçok politikacının ve üst düzey askeri personelin akıllı telefon sistemlerini ele geçirerek mobil alanlarını da genişletmektedir. Sonuncu unsur ise, ulaşım sistemlerine yönelik gerçekleştirilen ve büyük çaplı felaketle sonuçlanan faaliyetlerin organizasyonu gerçekleştirilmektedir. Bu bağlamda Kuzey Kore kontrolündeki siber korsanlar, tıpkı bir asker gibi yetiştirildikleri için askeri yeteneklerle karşılık vermektedir.

3.2.4.1. Kuzey Kore'nin Kurumsal Mekanizmaları ve Uygulamaları

Kuzey Kore'nin siber uzayda yayımladığı herhangi bir stratejik belge veya doktrin bulunmadığından dolayı ülkenin siber güvenlik stratejisini akademik literatürde tartışmak veya geniş kapsamlı açıklamak oldukça zordur. Hal böyle olduğu için literatür içerisinde yapılan çalışmalar genellikle saldırı, siber bağımlılık ve savunma unsuru üzerine yapılmıştır. Güntay (2020a: 250), Kuzey Kore'nin siber uzaydaki hedeflerini üç farklı temele oturtmuştur. Bunlar:

- Rejimin hayatta kalmasını sağlamak,
- Gücünü sergilemek ve rejimin itibarını uluslararası düzeyde savunmak,
- İç kontrolün ve devlet içi otoritenin sürdürülmesidir.

Cillufo (2017: 4), Kuzey Kore'nin siber uzaydaki hamlelerini üç farklı stratejiye indirgemiştir. Bunlar; bilgisayar ağ saldırısı, bilgisayar ağ sömürüsü ve siber suçlardır. Ağ saldırısı ve ağ sömürüsü tanımlanırken askeri operasyonların varlığına ve espiyonaj unsuruna dikkat çekilmiştir. Hedefte her ne olursa olsun kritik altyapıları siber saldırı yoluyla ele geçirmeye çalışmaktadır ve her saldırı sonrası saldırı konseptini genişletmektedir. Siber suçlar noktasında ise Kuzey Kore kapitalist ülkelerdeki önemli şirketlerin, kişi ve kurumların mal varlıklarına veya çeşitli finansal kuruluşlara yönelik kapsamlı saldırılar gerçekleştirilmektedir. Ayrıca Clarke ve Knake (2010)'nin ortaya koyduğu araştırmada siber savunma, siber bağımlılık ve siber saldırı unsurlarının ölçüt olarak değerlendirildiği ve beş farklı ülkenin (ABD, Rusya, Çin, İran, Kuzey Kore) siber savaş yetenekleri incelenmiştir. Çalışmanın sonucunda Kuzey Kore'nin yetenekleri diğer ülkelere oranla daha yüksek olmuştur. Tablo 12'de de görüleceği üzere araştırmanın bu şekilde sonuçlanmasındaki temel gösterge olarak Kuzey Kore'nin siber bağımlılık ve savunma derecesinin yüksek olması olarak belirtilmektedir. Özellikle siber uzaya olan bağımlılık, yeteneklerin gözlemlenmesi adına belirleyici olmuştur (Güntay, 2020a: 258).

Tablo 12: Devletler Arasında Siber Savaş Yeteneklerinin Karşılaştırılması

Devletler	Siber Saldırı	Siber Bağımlılık	Siber Savunma	Toplam Puan
ABD	8	2	1	11
Çin	5	4	6	15
İran	4	5	3	12
Rusya	7	5	4	16
K. Kore	2	9	7	18

Kaynak: Güntay, 2020a: 258

Tarihsel olarak Kuzey Kore'nin siber uzayda attığı adımlara bakıldığında ülkedeki rejimle paralel ilerlediği savunulmaktadır ve bu doğrultuda siber uzaydaki tüm faaliyetler askeri çerçevede gerçekleştirilmiştir. Kuzey Kore ordusu, 1970'lerden itibaren eğitimin parçası olarak elektronik savaş yeteneğini geliştirmektedir. 1990'larda ABD'nin Çöl Fırtınası Operasyonu sonrası savaş kapasitesinde devrim niteliğindeki gelişimleri ve akıllı silahların çeşitliliğine olanak sağlaması sonucunda "bilgi savaşı" kavramının "elektronik istihbarat savaşı" kavramına evriminin patlak verdiği bu ortamda Kuzey Kore, kapsamlı bir kapasite artırma girişiminde bulunmuştur. Elektronik istihbarat savaşı kavramı, daha modern elektronik istihbarat toplama ekipmanları, bozucular ve radarların tanıtımını içermektedir (Feakin, 2013: 71).

1998 yılında yalnızca siber savaşa odaklanan ve kuruluşundan bu yana boyut ve yetenek bakımından sürekli büyümekte olan Kuzey Kore, Birim 121'i kurmuştur. Genel Keşif Bürosu (RGB) içerisinde yer alan ve Siber Savaş Rehberlik Birimi olan Birim 121'deki hackerların birçoğu, Mirim Üniversitesi tarafından seçilmektedir. Binlerce adayın başvurduğu bu programa yalnızca en başarılı yüz kişi alınmaktadır. Kuzey Kore'nin buradaki temel prensibi, yazılan programlarının daha önce ülke dışında geliştirilmiş bir programdan bağımsız oluşturulması üzerinedir. Bu çerçevede Kuzey Kore'deki hackerların Google ya da CIA'de çalışan bilgisayar programcıları kadar ve hatta onlardan bile iyi olduğu savunulmaktadır (Sözcü, 2014). Nitekim Kuzey Koreli hackerlar 2007'de ilk mantık bombasını test etmiştir. Bu test, BM Güvenlik Konseyi kararının anabilgisayar ve dizüstü bilgisayar satışlarının ülkeye satışını yasaklamasına yol açmıştır. BM'nin bu yasağı, Kuzey Kore ordusunu siber silah geliştirme programlarına devam etmekten caydırmamıştır (Schaap, 2009: 133). Hackerlar, Birim 121'de işe başladıklarında en az dokuz senelik yoğun bir eğitimden geçmiş ve konularında uzmanlaşmış olmaktadırlar. Ülkelere ayrılan hacker grupları, o ülkelere seyahat ederek, belli bir süre orada yaşayıp o ülkenin kültürünü öğrenmektedir (Sözcü, 2014).

Kuzey Kore'nin siber yeteneklerini geliştirmeye odaklanmasının büyük bir bölümü, vatandaşlarını genç yaşlardan itibaren eğitim sürecine yoğunlaştırmakla geçmiştir. Soğuk Savaş döneminin bitişinden itibaren ülke genelindeki en yetenekli öğrencileri bulmak ve ilerde bünyesine kazandırmak için ülke çapında birçok orta okul kurulmuştur. Fen ve matematik alanlarında daha yüksek beceri sergileyen yetenekli öğrenciler seçilerek her biriyle özel olarak ilgilenilmektedir. Bu

yaştan sonra verilen eğitimlerin içeriği olarak programlama, komut otomasyonu, bilgisayarlı hesaplama, teknik keşif ve siber savaş derslerini içermektedir ve bu eğitim beş yıla kadar sürmektedir. Üst düzey mezunlar, RGB veya Kore Halk Ordusu (KPA) Genelkurmayındaki askeri birimlere katılmak üzere gönderilmektedir. Bunun haricinde kimi öğrenciler daha fazla pratik deneyim kazanmak adına fazla eğitim almaları için yurtdışına gönderilmektedir (Feakin, 2013: 72).

Kurumsallaşma şekline ve birimlerin görevlerine bakıldığında Kuzey Kore'nin siber saldırı operasyonlarını RGB kontrol etmektedir. Bu bağlamda RGB'ye bağlı olarak Kuzey Kore'nin gerçekleştireceği operasyonların merkezden yönetilmesi için Office 91 kurulmuştur. Dört alt kuruluşu olan (Birim 110, Birim 35, Birim 121 ve Birim 204) bu departmanda yüzlerce hacker bulunmaktadır ve her alt kuruluşun kendine özgü görevleri vardır. Askeri disiplinin erken yaşlardan itibaren verildiği bilgisayar teknolojisi hususunda uzmanlaşmış personeller, KPA'nın verdiği emirler ve denetimleri çerçevesinde faaliyetlerini sürdürmektedir (Hackett, 2018).

Devletlerarası rekabette ekonominin en önemli araç olduğunun farkında olan Kuzey Kore, finans sektörlerini ve bankaları sıklıkla hedef alarak milyarlarca dolar zarara neden olmaktadır. Bu çerçevede saldırıların çoğu baş düşmanı olarak gördüğü Güney Kore ve ABD'ye yönelik gerçekleşmektedir. Güney Kore'nin 2015 yılındaki uyarısına göz atıldığında Savunma Bakanlığı'nın raporunda, Kuzey Kore'nin yaklaşık altı bin siber savaşçısının, "Güney Kore'yi psikolojik ve maddi açıdan felç etmeyi" hedeflediğini ve Güney Kore'nin askeri operasyonlarını ve hükümet sistemlerini çökertmek için siber saldırılar düzenlediği savunulmuştur (Anadolu Ajansı, 2015). 2017 yılında Kuzey Kore tarafından ortaya atılan iddiaya göre Kuzey Koreli hackerlar, Güney Kore'ye siber saldırı yaparak ele geçirdiği askeri belgelerde, Güney Kore-ABD işbirliğini kanıtlar nitelikte verilerle birlikte Kim Jong-un'a yönelik suikast planı olduğunu tespit etmiştir (Sputniknews, 2017).

Kuzey Kore'nin ABD ile rekabetine bakıldığında tıpkı Güney Kore'ye yapıldığı gibi ekonomik açıdan zarar verilmesi amaçlanmıştır. ABD'nin güvenlik birimlerince hazırlanan raporlara göz atıldığında Kuzey Kore, finans sektörünü hedef alan siber faaliyetlerini gerçekleştirmek için dünya çapında çok çeşitli kötü amaçlı yazılım araçları geliştirmektedirler. Finansal hırsızlığın yanında kara para aklama işlemlerinin de yoğun bir şekilde yapıldığı gözlemlenmektedir. 2019'un sonundan itibaren Kuzey Kore'nin bu yasadışı siber faaliyetlerle yaklaşık iki milyar dolar çaldığı belirtilmektedir. Burada en çok adı geçen örgüt *Lazarus Group* adlı hacker topluluğu olmuştur. ABD'nin raporuna göre bu topluluk, *Hidden Cobra* ile aynı grupta olup bu iki adın yanı sıra, *Guardians of Peace* adıyla da bilinmektedir (Habertürk, 2017).

Kuzey Kore'nin gerçekleştirdiği siber saldırılara bakıldığında ilk olarak Sony'ye yönelik saldırıları akıllara gelmektedir. Kuzey Kore'nin siber aktörleri, 2014 yılında Sony ağlarına girerek *The Interview* adındaki filmi vizyon tarihinden önce internete sızdırmıştır. Aynı zamanda Sony çalışanlarını tehdit edip binlerce bilgisayara zarar vermiştir. Bunun üzerine ABD tarafından

soruşturma açılmıştır ve BM tarafından çeşitli yaptırımlarla karşı karşıya kalınması adına diplomatik baskılar kurulmuştur (CISA, 2020a).

Kuzey Kore 2016'da yeni bir saldırıya daha imza atarak devlet destekli uluslararası bankaların hesaplarını hackleyerek bir milyar dolar çalma girişimleri olmuştur ve Bankalar Arası Finansal Telekomünikasyon Derneği (SWIFT) ağındaki Bangladeş Bankası'ndan 81 milyon dolar çaldığı iddia edilmektedir. Kuzey Kore'nin siber aktörleri, 2017'de Bitcoin dijital para biriminde fidye ödemeleri talep etmesini sağlamak için *WannaCry* olarak bilinen fidye yazılımını geliştirmiştir. Yazılım, 150'den fazla ülkede hastanelerde, okullarda, işyerlerinde ve evlerde yüz binlerce bilgisayara bulaşmıştır. Bunun yanında *FASTCash* olarak bilinen hileli ATM nakit çekme yazılımını, Asya ve Afrika'daki ATM'lerden on milyonlarca dolar para çalmak için geliştirmişlerdir. 2017'deki bir olayda siber aktörler, 30'dan fazla ülkede bulunan ATM'lerden aynı anda nakit çekilmesini sağlamıştır. 2018'deki bir başka olayda ise, siber aktörler aynı anda 23 farklı ülkedeki ATM'lerden nakit çekilmesini sağlamıştır (CISA, 2020a).

3.2.5. Hindistan

Hindistan'ın iki önemli sorundan kaynaklı yaşadığı siber saldırı, ülkeyi siber uzaya dahil etme noktasında önemli bir etkiye sahiptir. Bu bağlamda Keşmir sorunu ve nükleer silah denemeleri, siber uzayda karşılaştığı sorunlara ışık utan önemli olaylar olarak değerlendirilmektedir. Ayrıca 2007 yılından itibaren dijital teknoloji unsurları Hindistan'da siyasi propaganda yapmak için yoğun olarak kullanılmaktadır. Devlet tarafından oluşturulan ve birçoğu orduya bağlı olan siber birlikler, ulusal çapta dezenformasyon operasyonu gerçekleştirmenin yanında uluslararası krizlerde de etkin bir şekilde görev almaktadır.

3.2.5.1. Hindistan'ın Kurumsal Mekanizmaları ve Uygulamaları

Hindistan'ı siber uzaya yönlendiren olaylara göz atıldığında ilk olarak değinilecek olay nükleer saldırılardır. 1998 yılında, nükleer karşıtı bir grup olan *Milw0rm*, Hindistan'ın nükleer testlerini protesto etmek için *Bhaba Atom Araştırma Merkezi (BARC)* ağına saldırı gerçekleştirmiştir. Bir diğer olay ise Pakistan ile yaşanan Keşmir sorunudur. Sorun, 1947 yılından beri süregelen bir kriz olarak literatürde yer almaktadır. Özellikle Pakistanlı hack gruplarının Hindistan web sitelerine saldırısı (Hindistan Parlamentosu, TV ağı Zee, Asian Age gazetesi, Hindistan Bilim Enstitüsü ve Bhabha Atom Araştırma Merkezinin web siteleri) sorunu 1999-2000'li yılların başındaki süreçten itibaren yeniden alevlendirmiştir (Billo ve Chang, 2004: 39).

2000'li yılların başı itibariyle Hindistan, siber alanda kurumsallaşmaya doğru birtakım adımlar atmıştır. Bu çerçevede Hindistan, *Ulusal Savunma Üniversitesi (National Defense University)* ve *Savunma İstihbarat Birimi'nde (Defense Intelligence Agency)* siber savaş, psikolojik operasyon,

elektro-manyetik ve dalga teknolojilerinde uzman alt birimleri olmak üzere çeşitli alanlar oluşturmuştur. Ardından stratejilerin hassas teknolojili silahlara, savaş alanında farkındalığa ve anlık iletişimlere dijital teknolojilerin uygulanmasıyla birlikte *Askeri İşlerde Devrim (RMA)* adlı savunma doktrinine imza atılmıştır. Bu doktrinde, ulusal güvenlik yönetimine yönelik zorluklarla birlikte nükleer tesisleşmesindeki tehditler ele alınmıştır. Hindistan ordusu, kapasitelerini artırmak için doktrinde bir değişikliğe giderek donanım, yazılım ve insan kaynaklarını geliştirme gibi girişimlere yer vermiştir. Bu girişimin ardındaki varsayımlar şunlardır:

- İlgili enstitülere değer katmak için yazılım, donanımdan giderek daha kritik hale getirilecektir.
- Endüstri standartları dünya çapında daha açık ve tekdüze hale gelecek, daha kolay pazara giriş ve yenilik sağlayacaktır.
- Küresel rekabetçilik ve uluslararası iletişim kolaylığı, daha hızlı gelişmelere dönüşecektir (Billo ve Chang, 2004: 39-51).

Hindistan, siber savunma konsepti ve teknolojik altyapılarını geliştirmesi hususunda 2000'li yıllarda büyük oranda ilerleme kat etmiştir. Nitekim bu genişleme 2010'lu yıllardan itibaren kendisini diğer devletlerle işbirliğine dahi götürmüştür. Buna örnek olarak 2014 yılında New York'taki BM zirvesinde İsrail, Hindistan'a siber alanda işbirliği teklifinde bulunmuştur (Siber Bülten, 2014). Bir diğer örnek ise 2017 yılında Rusya ile yapılan bakanlıklar nezdindeki görüşmede siber işbirliği gündeme gelmiştir (T24, 2017). Siber saldırıya uğrama noktasında da saldırgan bir devlet olarak bilinen Kuzey Kore tarafından Hindistan'a önemli saldırılar gerçekleşmiştir. *Lazarus* adlı grup, 2019 yılında Hindistan nükleer santrallerinin yürütüldüğü bilgisayarlar sistemlerine ve yazılımlarına *malware* saldırısında bulunmuştur (Demir, 2019).

Hindistan'da orduya bağlı siber birlikler, dezenformasyonu yaymak ve çevrimiçi siyasetle ilgili kamuoyu tartışmalarını manipüle etmek için çeşitli stratejiler, araçlar ve taktikler kullanmaktadır. Hindistan'da dezenformasyonun kullanımı da kendine özgü olarak gerçekleşmektedir. Normalde dezenformasyon faaliyeti, güvenli olmayan haber kanallarından veya sosyal medya üzerinden yapılmaktadır. Hindistan'da ise bu faaliyet, ana akım medyadan, politikacılardan ve resmi seçim stratejilerinin bir parçası olarak da kaynaklanmaktadır. Hindistan'da siyasi partilerin dijital teknolojiyi etkin bir şekilde kullanıldığı bilinmektedir. Hatta bazı noktalarda özel sektörlerden de çeşitli yardımlar alınmaktadır. Wylie (2018)'ye göre *Cambridge Analytica* adlı şirket 2014 yılından beri başbakanlık yapan Modi hükümeti tarafından yoğun bir şekilde kullanılmıştır. Aynı zamanda *Silver Touch* firması, Modi'nin seçim kampanyalarını yürütmek için *NaMo* uygulamasını oluşturmuştur (Campbell-Smith ve Bradshaw, 2019).

Siber uzayda savunma vurgusuna da önem veren Hindistan, bu konuda yasal düzenlemeler yaparak kurumsallaşma adımları atmıştır. 2019 yılında *Hint Veri Koruma Yasası* adında bir siber güvenlik yasası çıkarmıştır. Bahsi geçen bu yasada birçok yenilik, kapsamlı vizyon ve savunma kapasitesinde denetimi yüksek seviyelere kadar çıkaran önemli hususlar mevcuttur. Aynı zamanda kullanıcı verilerinin kullanıcının direkt rızası *(consent)* olmadan yeniden tanımlanması *(re-identification)* bu yasa içerisinde önemli bir maddedir. Bu durum, kişisel ayrıntıların güvenliğinin sağlanamaması hususunda pek çok araştırmacı tarafından kuşkuyla karşılanmaktadır (Gelecek Burada, 2020).

3.2.6. Güney Kore

II. Dünya Savaşı'ndan sonra büyük bir ekonomik dönüşüm yoluna giren Güney Kore, 1960'lı yıllarda bilgisayar teknolojisiyle tanışmıştır. Ekonomik gelişmişliğin yanında bilgi devriminin gerektirdiği ölçüde dijital teknolojiye de önem veren Güney Kore, Soğuk Savaş'ın sonlarına doğru teknoloji sektörüne yatırımlar yapmaya başlamıştır. Asya'nın yüzü Batıya dönük ülkesi konumunda olan Güney Kore'de 1980'den itibaren ulusal bilgi ve iletişim ağı kurulmaya başlanmıştır. 1990'lardan itibaren dijital teknolojik imkanlarını daha ileri bir boyuta taşıyarak altyapı yatırımlarını zenginleştirmekle birlikte bilgi teknolojisine yönelen Güney Kore, 2000'li yılların başında e-devlet teknolojisine geçmiştir. Bu bağlamda özellikle 90'lı yıllardan itibaren ülke, *Dijital Kore*/*Devlet* gibi sıfatlarla anılmaya başlanmıştır. Güney Kore resmî belgelerine bakıldığında günümüzde kendisini *intelligent digital government* yani *akıllı dijital devlet* olarak tanımlamaktadır. Ülke, 2025 yılında ise temel kamu hizmetleri için %80 dijital dönüşüm oranını, idari ve kamu kurumları için ise %100 bulut dönüşüm oranına ulaşacağını belirtmiştir (Digital Goverment, 2021).

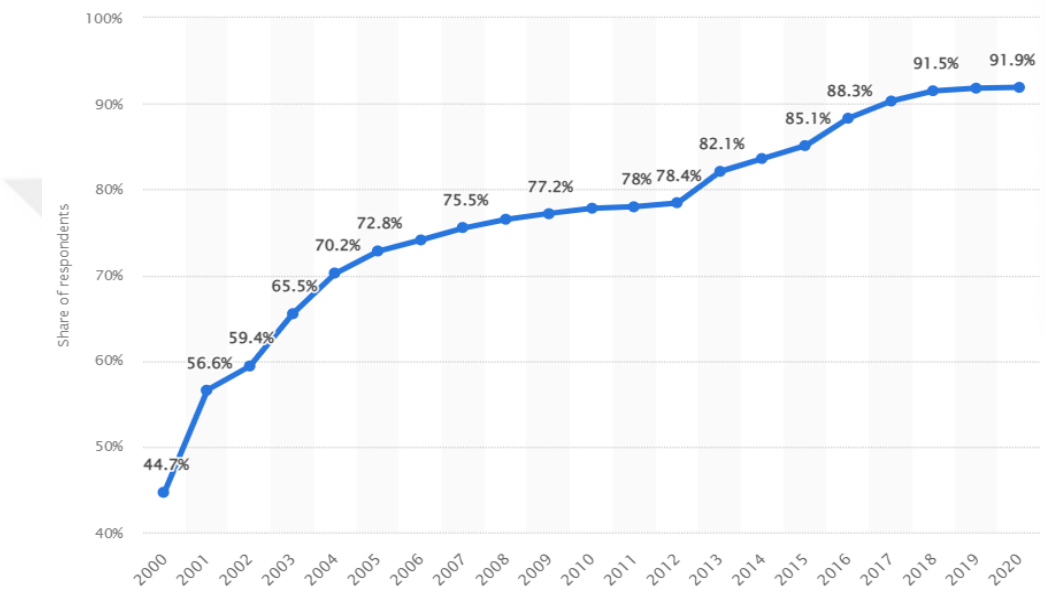
Gösterdiği dijital dönüşümde uluslararası alanda etki göstermeye başlayan Güney Kore, Kuzey Kore ile yaşadığı ideolojik çatışmanın da bir tezahürü olarak uluslararası sistemde daha ılımlı bir perspektif çizerek barışçıl bir kimlikle kendisini dünyaya tanıtmayı hedeflemiştir. Batılı ülkelerle işbirliği imkanını geliştirme çabasına da giren Güney Kore, ABD ile arasında sıkı bir bağ kurarak siber uzay noktasında bölgede aktifliğini sürdürmektedir. Çatışmadan uzak, savunmacı ve ılımlı bir anlayışla ülke, siber uzayda yumuşak güç stratejisini uygulamaktadır. Güntay (2020b: 280)'a göre Güney Kore'nin son yıllarda yaşadığı dijital dönüşüm, bir anda gerçekleşen bir olay olarak değerlendirilmemiştir. Dönüşümün içerisinde sosyokültürel etkiyi de karakterize eden Güney Kore, bu çizgisini gelecek vizyonu haline getirmiştir.

3.2.6.1. Güney Kore'nin Kurumsal Mekanizmaları ve Uygulamaları

Ülkede internetin kullanılması, TCP/IP *(Transmission Control Protocol/Internet Protocol)* adlı araştırma grubunun çalışmalarıyla başlamıştır ve bu grubun geliştirdiği sistem sayesinde ülke 1982'de internet ile tanışmıştır. 1990'larla birlikte Güney Kore'nin yaşadığı ekonomik kriz sonrası

ülke krizi fırsata çevirmek adına dijital alana yatırımlar yapmaya başlamıştır. Nitekim bu yıllarda iletişim teknolojisi alanında yapılan devlet kontrolündeki ilerleme, ekonomik büyümenin de yolunu açmıştır. 1995 yılında ülkeyi bilgiye dayalı bir ekonomiye ulaştırmak amacıyla Kore hükümet tarihinin en büyük projesi olarak adlandırılan *Kore Bilgi Altyapısı (Korea Information Infrastructure-KII)* kurulmuştur. Bu proje sonrasında Kore vatandaşlarının internete erişimi hususunda devlet nezdinde önemli adımlar atılmıştır (Güntay, 2020b: 271).

Şekil 4: 2000'den 2020'ye Kadar Güney Kore'de İnternet Kullanım Oranı



Kaynak: Statista, 2021

Güney Kore, 2000'li yıllardan itibaren e-devlet sistemine geçilerek küresel sistemde adını duyurmuştur. Özellikle oyun sektöründeki yenilikler sonrası Şekil 4'te görüleceği üzere 2000 sonrası ülke içerisinde internet kullanıcısı sayısında ciddi bir artış gözlemlenmiştir. Bunun yanında ülke içerisinde kamu ve özel sektörler dahilinde geliştirilen programlar, oyunlar, ticari siteler, dizi-film gibi dijital içerikler sayesinde yurt dışında da önemli bir pazar alanı oluşturulmasına olanak sağlamıştır.

Güney Kore'nin siber uzayda ortaya koyduğu stratejilere bakıldığında çeşitli konferans ve toplantılarla uluslararası arenada varlığını sürdürmeyi amaçlamaktadır. Ayrıca ulusal ve uluslararası politika oluşturma noktasında ABD ile olan yakınlığını da kullanarak teknolojik imkanlar dahilinde uluslararası piyasalardaki rolünü Batı'ya yönelik oluşturmaktadır. Bu bağlamda Easley (2017: 9)'e göre Güney Kore, özellikle Kuzey Kore meselesinden dolayı ABD'ye bağımlı bir konumdadır Ülkenin ortaya koyduğu stratejik unsurlar değerlendirildiğinde 2011 yılında yayımlanan *Ulusal Siber Güvenlik Hedefler*i adlı belgede beş adet eylem planı bulunmaktadır. Bunlar:

- Özel, kamu ve askeri sektörlerin ortak müdahale sisteminin oluşturulması,
- Kritik altyapının güvenliğinin güçlendirilmesi ve güvenliğin arttırılması,
- Ulusal düzeyde siber saldırıları tespit etmek ve engellemek,
- Uluslararası işbirliği yoluyla caydırıcılık oluşturmak,
- Siber güvenlik altyapısını oluşturmak (Cyberpolicy Portal, 2020).

2013 yılında gerçekleştirilen Seul Siber Uzay Konferansı'nı organize etmesi ve 2014 yılındaki Uluslararası Telekomünikasyon Birliği'nin temsilciliğini yapmasıyla uluslararası alanda önemli adımlar atmıştır. İşbirliği hususunda ABD'nin yanında Meksika, Endonezya, Türkiye gibi ülkelerle teknoloji alanında bir aya gelirken, bölgesel işbirliği noktasında ASEAN vasıtasıyla BM nezdinde önemli bir rol üstlenmiştir (Güntay, 2020b: 274).

Siber güvenliğin bir ulusal güvenlik meselesi olduğunu kabul eden Güney Kore, dünyanın en hızlı mobil bilgi teknoloji altyapılarından birine sahip olmasının yanında siber saldırılara karşı savunma perspektifinde güvenli olmayan bir altyapıya sahiptir. Siber saldırıların sıklığı, Güney Kore hükümetinin siber güvenlik stratejisini yeniden değerlenmesine sebebiyet vermiştir. Bu aşamada kurumsallaşma yolunu tercih eden Güney Kore'de siber güvenlik konularını ele alacak üç kurum oluşturmuştur. Bu kurumlar, ajanslar siber saldırıları ve güvenlik tehditlerini tanımlamak, önlemek ve bunlara yanıt vermekten sorumludur. Bahsi geçen ajanslar ise *Ulusal Siber Güvenlik Merkezi, Kore İnternet ve Güvenlik Ajansı* ve Ulusal Polis Ajansı'nın *Siber Terör Müdahale Merkezi'dir* (Privacy Shield, 2020a). Bu ajanslar Kuzey Kore'den gelebilecek olası siber saldırılara karşı hazırlıklı konuma gelmek ve olası herhangi bir saldırıdan minimum hasarla çıkmak için teknik altyapılarını düzenlemekle görevlidir.

Güney Kore'nin 2009 yılında yaşadığı DDoS saldırısı, strateji geliştirme hususunda önemli bir yere sahiptir. Bu doğrultuda Güney Kore'nin stratejisi, Kuzey Kore gibi bir ülke ile sınırdaş olmanın gerektirdiği ölçüde savunma merkezli bir konseptte oluşturulmak istenmiştir. Nitekim politika yapımında ya da ülke içinde herhangi bir söylemde Kuzey Kore tehlikesine dair vurgular mutlaka yapılmaktadır. Özellikle 2011 yılında yapılan saldırılardan sonra ülkenin savunma mekanizmasında iyileştirilmeye gidilme yönünde daha ciddi adımlar atılmıştır. Bu bağlamda iki yılda bir yayımladıkları *Defence White Paper*, savunma alanına yapılan yatırım ve işbirliği ilişkilerini anlamak açısından önemlidir. 2019 yılında yayımlanan *South Korea Blue House* çerçevesinde savunma noktasında caydırıcılık unsurundan bahsedilmiştir (Platte, 2020: 83-85). Bu kapsamda alınması gereken önlemler olarak belirtilen hususlar:

- Ulusal güvenliği ve çıkarları tehdit eden tüm siber saldırılara mümkün olan en uygun şekilde yanıt vermek.

- Güvenlik açıklarını tespit eden kapsamlı bir sistem gelişimi ortaya koymak suretiyle önleyici kapasiteyi güçlendirmek.
- Siber saldırılarda analiz kabiliyetini geliştirmek adına neden-sonuç ilişkisi oluşturarak suçlu-suçsuz ayrımına gitmektir (Güntay, 2020b: 280).

2016 yılında yayımlanan *Beyaz Kitap*, Güney Kore'nin tehdit çemberindeki ülkeleri ve işbirliği kurabileceği ülkeleri içermektedir. Özellikle finans sektörüne yapılan saldırılar sonrası Kuzey Kore'yi en önemli tehdit olarak belirtilmektedir. Kuzey Kore ile birlikte ABD, Japonya, Çin ve Rusya gibi devletler, Güney Kore'nin siber alanda kendisine denk veya rakip olarak gördüğü devletlerdir. Bu çerçevede kitapta, Japonya ve ABD ile yapılacak işbirliğinin önemli bir ihtiyaç olduğu nitelenmiştir. Güney Kore, 2019 yılında yayımladığı *Ulusal Siber Güvenlik Stratejileri* belgesinde resmi vizyon olarak ulusal güvenliği desteklemek, ekonomik refahı desteklemek ve uluslararası barışa katkıda bulunmak için özgür ve güvenli bir siber alan yaratmayı hedefleyen bir ilkeyi benimsemiştir (Cyber Policy Portal, 2020).

Güney Kore'nin kripto para alanına yatırım yapması, siber alanda kendisine rakip olarak gördüğü ülkeler ve Asya bölgesindeki ülkeler arasında ön plana çıkabilmek adına önemli bir girişim olarak karşılanmaktadır. 2018 yılında Güney Kore yatırım şirketi, Avrupa'nın en büyük kripto para borsası olan *Bitstamp*'ı satın almıştır. Bu durum şüphesiz Güney Kore'nin kripto para biriminin ve onun altında yatan blok zinciri teknolojisinin önemli bir oyuncusu haline geldiğine dair bir işaret olarak görülmektedir. Nitekim Güney Koreli kripto para borsalarının yurtdışındaki genişlemesi, ülke içindeki genişlemesini de güçlendirdiği anlamına gelmektedir (Stangarone, 2018). Öte yandan Güney Kore, 2019 yılında ifade özgürlüğünü daha da zayıflatacak ve ülkedeki çevrimiçi kullanıcıların gizliliğini ihlal edebilme tartışmalarını yaratan yeni bir plan hazırlamıştır. Devlet kontrolünde olan *Kore İletişim Komisyonu*, vatandaşların *Google* ve *Facebook* gibi uygulamalardaki kişisel bilgilerini tutan yabancı internetle ilgili şirketlerin yurt içi faaliyetlerini kapatma yetkisi veren ve çevrimiçi kullanıcıların aktivitelerin denetlenmesini öngören bir yasa oluşturulmuştur (Kang, 2019).

Güney Kore'nin 2021-2025 arası belirlediği ve *e-Goverment Master Plan (e-Devlet Ana Planı)* olarak adlandırdığı eylem planı incelendiğinde dijital devlet inovasyonunda, Covid-19 sırasında gerçekleştirdiği en iyi dijital yönetim uygulamalarından (çevrimiçi okul, aşı kartının dijitale aktarılması, yakınındaki kişinin maskesinin ne kadar kullanıldığını tespit eden uygulamalar gibi) ve 2025 planından (kamu hizmetleri için dijitalleşme hedefleri) bahsedilmektedir. Bu doğrultuda açıklanan strateji: Kamu hizmetlerini dijital olarak tasarlamak, vatandaşların tercih ettiği kanallar aracılığıyla kamu hizmetleri sağlamak, vatandaşların bilgilerinin bir kereliğine mahsus hükümetle paylaşılmasını sağlamak, açık veri ve hizmetleri özel sektöre genişletmektir (Digital Goverment, 2021).

3.2.7. Japonya

Altyapı imkanları doğrultusunda bilgi ve teknolojiye bağlı olan ekonomisini geliştirmek amacıyla dijital alanda var olan Japonya, öncelikli olarak bilgi ve altyapı unsurunu güvence altına almayı amaçlamıştır. Bunun yanında uğradığı önemli siber saldırılar sonucunda siber savunma kapasitesini artırmaya yönelik girişimlerde bulunmuştur. Japonya, bilgi teknolojisi alanında imkanlarını genişlettikten sonra kritik devlet ve askeri kurumlar başta olmak üzere bireyler ve özel şirketlerin teknolojiye olan bağımlılıklarında ciddi bir artış olmuştur. Bu bağımlılığın sonucu olarak özellikle 2000'li yıllardan sonra sıklıkla siber saldırıya maruz kalan ülke altyapısını güçlendirmek için kurumsal adımlar atmıştır. 1990'lardan itibaren siber uzayda potansiyel tehditlere karşı önlemler almaya başlayan Japonya, ilerleyen yıllarda sıklıkla yaşadığı siber saldırılardan sorumlu olarak Çin ve Kuzey Kore'yi göstermiştir. Bu doğrultuda devlet nezdinde önemli birimler oluşturmuştur. Aynı zamanda ülke nezdinde ABD başta olmak üzere pek çok devletle kapasite ve yetenek geliştirme amacıyla işbirliği yoluna gidilmiş ve siber savunmayı merkeze almak suretiyle çok sayıda siber tatbikat düzenlenmeye başlanmıştır. Nitekim 2000'lerden bu yana Asya'da gerçekleştirilen siber savunma tatbikatlarının büyük bir bölümü Japonya tarafından gerçekleştirilmiştir (Demir, 2020: 229).

Japonya, 2010'lardan itibaren siber güvenliğe yasal düzenlemeler getirmiştir ve oluşturduğu birimleri bu düzenlemelere uyulması ve kontrol sağlanması hususunda görevlendirmiştir. Bunun yanında siber diplomasi kavramına da önem veren Japonya, uluslararası güvenliğini tıpkı ulusal güvenlikte olduğu gibi önceleyen politikalar oluşturmuştur. Sınır dışında çeşitli konferanslar ve eğitimlere katılarak işbirliklerini ve ikili diyalogları artırmayı hedeflemiştir. Aynı zamanda bölgesel örgütlerle olan ilişkisini de ileri bir boyuta taşımıştır.

Japonya'nın siber uzaya ve siber güvenlik tehdidine verdiği önem, bağımsız uluslararası kuruluşlarca yapılan anketler neticesinde de görülmektedir. Pew Araştırma Merkezi (2019) tarafından yapılan ve 26 devletin incelendiği ankette siber güvenlik tehdidinin büyüklüğüne dair istatistikte Japonya %81 oranla ilk sırada yer almıştır. Ayrıca dünyadaki endüstriyel üretim robotlarının dördüncü büyük kullanıcısı olan Japonya'da, her 10 kişiden dokuzu 50 yıl içinde robotların ve bilgisayarların şu anda insanlar tarafından yapılan işlerin çoğunu yapacağına dair görüşler vardır (Devlin, 2019).

Siber uzaydaki varlığını daha da ileri bir seviyeye taşımayı amaçlayan Japonya'nın ortaya koyduğu stratejik belgelerden yola çıkılarak siber perspektifinin üç ana prensipten oluştuğu görüşüne varılmıştır. Bunlar; siber uzayda hukukun üstünlüğünü teşvik etmek, güven artırıcı önlemler geliştirmek ve kapasiteyle artırımına giderek işbirliğini inşa etmektir. Bunun yanında yıllık olarak yayımladıkları faaliyet raporlarında, genel olarak askeri güçlerin bilgi ve iletişim ağlarına artan bağımlılığı, saldırgan ve savunmacı siber yeteneklerin geliştirilmesi, hükümet kuruluşlarının ve

çeşitli devletlerin askeri güçlerinin bilgi ve iletişim ağlarına karşı artan siber saldırıların önüne geçilmesi için her türlü tedbirlerin alınması zorunlu koşulmuştur (Cyberpolicy Portal, 2020).

3.2.7.1. Japonya'nın Kurumsal Mekanizmaları ve Uygulamaları

Bilgi ve iletişim teknolojilerinin ilerlemesi sonucu devlet kurumlarının, askeri birimlerin, özel şirketlerin ve bireylerin teknolojiye bağımlılığı söz konusudur. Bu noktada tarih boyunca teknolojiye ve teknolojik yatırıma önem veren Japonya, iç ve dış ticaretinin önemli bir kısmını bilişim teknolojisi aracılığıyla gerçekleştirmektedir. Kritik altyapılarının ve kamusal birimlerin siber tehditlere ve muhtemel saldırılara yönelik korunması hususunda önemli adımlar atan ülke, yaşadığı saldırılar sonrası savunma kapasitesini artırma yoluna gitmiştir (Phys, 2011).

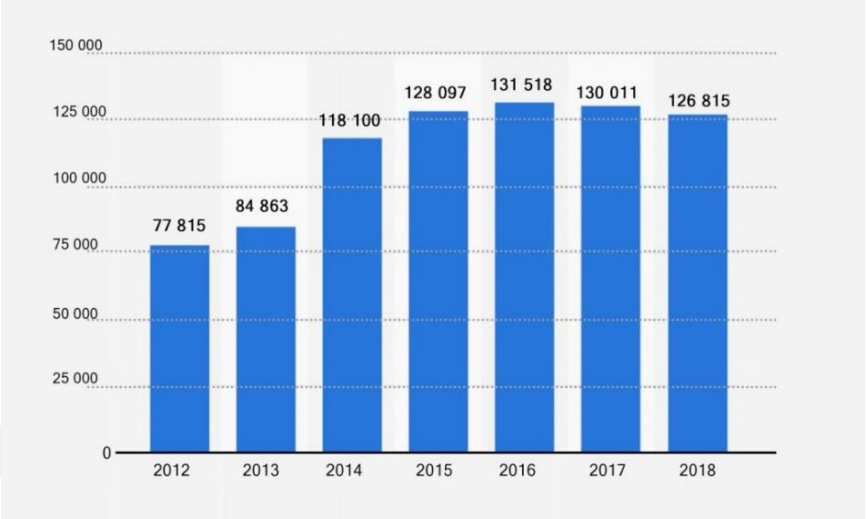
Siber uzayda kurumsallaşmak isteyen Japonya, 2000 yılında bilgi ve telekomünikasyon ağ bağlantılarının oluşturulması adına *Bilgi Teknolojileri Temel Kanunu*'nu çıkarmıştır. Bu kanunla ülke çapında bilgisayar teknolojisi kullanımının yaygınlaştırılması teşvik edilmiştir (Japanese Law Translation, 2000). Siber uzayda kurumsal iletişim ve etkileşimin sağlanması adına 2006 yılında *Ulusal Bilgi Güvenliği Strateji Belgesi* yayımlanmıştır ve dört farklı kurumun ülkedeki teknolojik gelişmeleri kontrol etmek ve siber güvenliği inşa etmek noktasında faaliyetlerde bulunması kararlaştırılmıştır. Bu kurumlar: Ulusal Polis Ajansı, İçişleri ve İletişim Bakanlığı, Ekonomi, Ticaret ve Sanayi Bakanlığı ve Savunma Bakanlığı'dır (Gady, 2017: 17-21).

2009 yılında yayımlanan *Bilgi Güvenliği Strateji Belgesi*'nde dijital ekonomiye değinilmekle birlikte siber tehditlerin bertaraf edilmesi noktasında uluslararası işbirliğinin önemine vurgu yapılmıştır. Belgede ayrıca siber saldırılarda ilk defa devlet ve devlet-dışı aktörler konusu gündeme gelmiştir (Demir, 2020: 231-232). 2010'larla birlikte ülkenin önemli altyapılarına siber saldırı operasyonları gerçekleşmesi üzerine ise savunma altyapısını iyileştirmek amacıyla ülke çapında teknik ve yasal anlamda önleyici hamleler ortaya konulmuştur.

Japonya hükümeti nükleer enerji, savunma sanayi ve üretim tesislerine yönelik yapılan siber saldırıların artması sonucu tehditleri bertaraf etmek amacıyla 2011 yılında *Siber Suç Yasası*'nı çıkarmıştır. Karşı karşıya kaldığı birçok siber saldırıların arkasında Çin'in olduğunu iddia eden Japonya, 2012 yılında acil durumlarda birimler arası iletişimi sağlamak amacıyla *Siber Olaylar Mobil Yardım* adında bir ekip oluşturmuştur (Kallender ve Hughes, 2016). 2013'te Güney Kore'nin yaşadığı banka sektörüne yönelik operasyonlardan sonra Japonya, "bilgi güvenliği" kavramı yerine "siber güvenlik" kavramını kullanmaya başlamıştır ve aynı yıl, *Siber Savunma Birimi*'ni kurmuştur. Yine aynı yıl yayımladığı *Siber Güvenlik Stratejik Belgesi*'nde ise siber uzayın savaş alanı haline geldiğine dair açıklamalar yapmıştır (Demir, 2020: 229-232). 2016 yılında 130 milyar siber saldırıya maruz kaldığını açıklayan Japonya'da siber suç oranında ciddi oranda bir yükseliş söz konusu olmuştur (Varlık, 2019).

Statista'nın 2012-2018 yıllarını baz alarak sunduğu verilere göre Japonya'daki siber suç sayısı Şekil 5'te de görüleceği üzere özellikle 2013 yılından sonra ciddi bir artış göstermiştir.

Şekil 5: Japonya'daki Siber Suç Sayısı (2012-2018)



Kaynak: Statista, 2020

Ülke içindeki suç oranını minimize etmek ve savunma kapasitesini geliştirmek için uluslararası işbirliği yoluna giden Japonya hükümeti, 2012 yılında *Fujitsu* adındaki şirketle ortaklık kurarak *milli güvenlik virüsü* adlı sistemi geliştirmiştir (Eyidilli, 2012). Japonya ayrıca bilgi iletişim araçlarını gözlemlemek ve şartlar doğrultusunda gelebilecek saldırılara yanıt vermek için 2014 yılında *Siber Savunma Grubu*'nu oluşturmuştur (Demir 2020: 235). Siber uzayda hukuksal zemini oturtmak adına kurumsal işleyişini kuvvetlendirmek isteyen Japonya, 2014 yılında hükümete bağlı tüm kurumları harekete geçirmek ve siber güvenlik politikalarını oluşturma noktasında yasal bir çerçeve niteliğindeki *Siber Güvenlik Temel Yasası*'nı çıkarmıştır (The Government of Japan, 2015). 2018 yılında yasada değişikliğe gidilerek siber güvenlik önlemleri doğrultusunda bir Konsey kurulmuştur ve hükümetin görevlerinin bir kısmı Konseye devredilmiştir (Library of Congress, 2018).

Japonya İçişleri ve İletişim Bakanlığı, 2017 yılında yaptığı duyuruda ülkenin kritik altyapılarına yapılan siber saldırıların bir önceki yıllara göre ciddi artış gösterdiğini açıklamıştır. Bakanlık, yaptığı açıklamada, saldırıların yarısının Çin'den başlatıldığını duyurmuştur (Goud, 2017). Siber saldırıları önlemek adına 2018 yılında ortaya koyduğu 10 yıllık savunma planında, Çin ve Kuzey Kore'nin yarattığı tehditlere dikkat çekilmiştir (Tatsumi, 2018). Siber diplomasi kavramıyla birlikte işbirliğini artırma yoluna giden Japonya, 2011'de Londra'da 2012'de Budapeşte'de siber güvenlik konferansları düzenlemiştir. ASEAN ve NATO gibi bölgesel örgütlerle de diyaloğunu artırmıştır. İsrail, İngiltere, Avusturalya ve Estonya gibi ülkelerle işbirliği geliştirmiştir. Ayrıca NATO'nun 2019 yılında gerçekleştirdiği siber savunma tatbikatında gözlemci olarak yer almıştır (Demir, 2020: 240).

Japonya'nın, işbirliği noktasında en çok ABD ile bir araya geldiği gözlenmiştir. Bu bağlamda Japonya hükümeti, karşılaştığı potansiyel tehditler kapsamında ABD ve bu alandaki diğer ülkelerin yetenekleri karşısında geride kaldığını düşünmektedir. Bu bağlamda ABD, Japonya'da şirketleşme faaliyetlerini giderek artırmaktadır. Nitekim son yıllarda ülkedeki Amerikan siber güvenlik şirketlerinin sayısı gitgide artmıştır (Privacy Shield, 2020b). Bunun yanında artan siber saldırılara karşı ortak bir politika geliştirmek adına iki ülke arasında *Siber Savunma Politikası Çalışma Grubu* kurulmuştur (The Japantimes, 2015). Aynı zamanda 2019 yılında bir güvenlik anlaşması imzalanmıştır. Anlaşmanın 5. maddesinde *belirli şartlar altında gerçekleşen bir siber saldırının silahlı bir saldırı olarak kabul edileceği* vurgusu yapılmıştır (Demir, 2020: 241). Bu çerçevede siber tehditlerin en az konvansiyonel tehditler kadar önemli olduğu yorumu yapılmaktadır. Yayla (2013: 203)'ya göre siber saldırıların silahlı saldırı olarak kabul edilmesi, BM Anlaşması'nın 51. maddesinin uygulama alanını genişlettiğinden dolayı uluslararası ortamı yeni karışıklıklara sürükleme potansiyeli taşımaktadır.

SONUÇ

Modern anlamda ilk olarak 1648'deki Westfalya Anlaşması sonrası dile getirilen güvenlik olgusu, 1990'lı yıllardan itibaren post-modern güvenlik olarak incelense de fikirsel temelleri 1648 yılından öncesini de kapsamaktadır. Pre-teolojik ve proto-teolojik olarak iki farklı dönemde incelenen Primitif Güvenlik Dönemi, insanların toplu halde yaşamasından düzenli hayata geçişine ve yerleşik hayattaki toplulukların etnik, kimlik ve sosyoekonomik sınıf farklılıkları, zamanla birbirlerini tehdit olarak görmeye itmiştir. Toplumlar arasındaki anlaşmazlıklar insanları çatışmaya sevk etmiştir. Bu çatışma durumu, günümüz güvenlik algısının şekillenmesine katkıda bulunan savaş kavramının ortaya çıkmasına sebep olmuştur. Savaş kavramı yüzyıllar boyunca belirli aşamalardan geçerek günümüzdeki dünya siyasetinin temellerini oluşturmuştur.

II. Dünya Savaşı'ndan sonra dünya siyasetinde modern güvenlik algısının şekillenmesi pek çok alanda kendisini göstermiştir. 20. yüzyılın ortalarından itibaren meydana gelen teknolojik gelişmeler, dünya üzerinde mevcudiyetini sürdüren her alanda olduğu gibi terörizm meselesinde de etkisini göstermiştir. Bu doğrultuda dördüncü terör dalgasıyla birlikte uluslararası terörizm kavramı, güvenlik yelpazesinin genişleyerek yeniden yorumlanmasına imkân sağlamıştır. Bu kavram 21. yüzyılın başından itibaren siber terör tartışmalarını beraberinde getirmiştir. Günümüzde terör faaliyetleri yaygın olarak internet ortamında gerçekleştiği için kimi yazarlar siber terörü beşinci terör dalgası, siber uzayı da savaş alanı olarak nitelendirse de bu kavramlar hakkında literatürde net bir görüş birliği bulunmamaktadır.

Siber uzayın savaş alanı olduğu göreceli bir kavramdır. Nitekim kimi aktörler siber uzayı daha çok saldırı ve savunma ikilemi dahilinde görür, kimi aktörler de siber uzayı insan hayatını kolaylaştıracak alanlar yarattığını düşünür. Ancak siber uzayda her aktörün güvenlik tehdidi altında olduğunu vurgulamak gerekir. Çünkü siber uzayın savaş olgusu diğer savaş unsurlarından oldukça farklı olarak yorumlanmaktadır. Örneğin konvansiyonel bir savaşın son bulması için dünya üzerindeki tüm silahları yok etmek zor da olsa mümkündür. Ancak 21. yüzyılda hayati normların (sağlık, ulaşım, iletişim gibi) dijitale bağlı olduğu ortamda, siber savaşın son bulması için bütün dijital faaliyetlerin son bulması gerekir. Bu da pek mümkün görülmemektedir. Öte yandan konvansiyonel bir savaşta taraflar, savaşı sonlandırmak için uzlaşma yapmaktadır. Ancak siber savaşta sadece bir taraf bellidir. Zira saldıran tarafın kimliğini siber ortamda tespit etmek oldukça zordur. Bu ve bunun gibi sebeplerden dolayı da siber savaş, aktörlerin iştahını artırmaktadır. Siber uzay ve konvansiyonel savaş karşılaştırıldığında siber savaşın daha tercih edilebilir bir ortam olduğu savunulmaktadır. Zira ölüm oranlarına bakıldığında siber savaşların lehine ciddi bir fark

gözlenmektedir. Aynı zamanda siber tehdit, nükleer tehditten daha güvenli bir alan olarak değerlendirilmektedir.

21. yüzyıl itibariyle küreselleşmenin teknolojik alanda kendisini hissettirmesi sonucu internet kullanımı dünya üzerinde ciddi oranda artmıştır. Bu noktada internet; başta devletler olmak üzere pek çok aktörün ilgi alanı içerisine girmiştir. Kavramın güvenlik yaklaşımları içerisinde ele alınması, alandaki güvenlik çalışmalarının yeni bir boyut kazanarak zenginleşmesine katkı sağlamıştır. Siber uzayın merkeziyetsiz doğası ve fiziki alandan bağımsız olup fiziki alanı etkileyen ve ciddi sonuçlar doğuran beşerî bir formda olması, devlet güvenliğini de önemli ölçüde etkilemektedir.

Devletlerin kritik altyapılarında teknolojinin var olması, savunma kapasitesi geliştirme hususunda zorunluluk olarak değerlendirilmekle birlikte bir aktör siber uzaya ne kadar bağlıysa o kadar fazla güvenliğe ihtiyaç duymaktadır yorumu yapılmaktadır. Bu doğrultuda devletler; bilgileri erişebilir kılmak, kamusal hayatı ve önemli altyapıları modernize ederek çevre, enerji, sürdürebilirlik, ulaşım ve iletişim gibi birçok unsurun daha uygun maliyetlerle alternatiflerinin yaratılması için siber uzaya ihtiyaç duymaktadır.

Devletlerin siber uzaya müdahil olması, siber güvenliğin jeopolitik boyutunu da tartışmaya açmıştır. Bilgi çağının gerekliliklerinin karşılanması için gizlilik ilkesinin daha sağlam temellerle inşa edilmek istenmesi, devletleri bu alanda siber politikaların belirlenmesi için birimler kurmaya ve stratejik belgeler yayımlamaya itmiştir. Bu doğrultuda birçok devlet, siber güvenlik politikası oluşturmak maksadıyla siber uzaya, güvenlik kaygıları içerisinde yer vermiş ve siber uzay dahilinde güç mücadelesi, alana erken yatırımlar yapan devletlerin lehine olmuştur. Soğuk Savaş dönemi ve sonrası dahil, II. Dünya savaşını kazanan tarafın, kaybeden tarafa oranla daha fazla güçlenerek uluslararası sisteme entegre olduğu düşünülmektedir. Teknolojik imkanlara daha erken erişen ve siber uzaya hakimiyeti de aynı paralelde ilerleyen devletler, 2000'li yıllardan itibaren tıpkı II. Dünya Savaşı sonrası uluslararası sistemde olduğu gibi Soğuk Savaş sonrası da siber uzayda hakimiyetini göstermişlerdir.

Siber uzayda varlık gösteren her devlet, kendi siber güvenliğini oluşturmak için saldırı unsurlarını da elinde bulundurmak suretiyle kötü amaçlı yazılımları kullanabilmektedir. Direkt devlet eliyle veya devlet-dışı aktörler kanadıyla gerçekleştirilen siber saldırılar, niceliksel anlamda siber suç oranların artmasına sebep olmuştur. Nitekim gerçekleşen siber saldırıların bir aktöre bağlanmasının zorluğundan dolayı net bir kimlik tespitin yapılamayışı ve kapsayıcı bir yasal düzenlemenin yokluğu, devletler ve diğer aktörleri siber uzayda özgür kılmaktadır.

Siber uzayın devletlerin mutlak otoritesini sarsabilecek potansiyel bir risk unsuru olduğu için devletler bu alana özel bir ilgi duymakta, yetki, yetenek ve hareket kapasitesini artırma arayışına girmektedir. Siber uzayda hareket alanı geniş olan devletlerin saldırı faaliyetlerindeki ve

organizasyonlarındaki sınırsızlıklarının doğurduğu tekelleşme, sadece hedefteki devletler için değil, dünya için de tehlike arz etmektedir.

Devletler, siber tehlikeden kendilerini koruyabilmek için kendi siber güvenlik alanlarını oluşturmaktadır. Ancak bireylerin siber tehlikenin ne kadar farkına vardığı ve siber güvenlik alanı oluşturup oluşturmadığı soru işaretidir. Zira dünyada her geçen gün milyonlarca insanın önemli bilgileri ele geçirilmektedir. Yasal bir zemin oluşturulana kadar insanların da tıpkı devletler gibi kendi siber güvenlik alanını oluşturması gerekli görülmektedir. Bu noktada insanları bilgilendirme ve farkındalık oluşturma noktasında devletler, örgütler ve sivil toplum kuruluşları gibi aktörlere ihtiyaç duyulmaktadır.

Siber uzayda en büyük çatışma alanlarından biri olarak görülen Doğu-Batı mücadelesi, Soğuk Savaş'ın sona ermesinden sonra çok kutuplu sistem içerisinde daha çekişmeli hale gelmiştir. Çok kutuplu düzen dahilinde Doğu devletleri, Batı hegemonyasına karşı 21. yüzyılın dijital anlamda küreselleşmenin gerekliliklerini de yerine getirerek siber uzayda güçlerini gösterme arayışına gitmiştir. Bu bağlamda özellikle Batı tarafından kabiliyetleri kabul edilmeyen, ekonomik yaptırımlara uğrayan, ideolojik ve/veya kültürel anlamda dışlanan Doğulu devletler, siber uzayda kapasite geliştirerek üstünlük kurma çabası içinde olmuştur. Siber uzayı güvenlikleştiren bu devletler, hem kendi coğrafyasında anlaşmazlık yaşadığı devletlere hem de Batı'ya karşı ciddi tehdit oluşturmaktadır.

Rusya ve Çin, savunma ve saldırı mekanizmasını ileri seviyede tutmayı hedeflemektedir Asya'da siber kapasitesi yüksek gücü olan devletlerin başında gelmektedir. Batı tarafından çeşitli yaptırımlarla izole edilmesine rağmen saldırganlık kapasitesinin sınırlarını zorlayarak Batı'ya meydan okuyan devletler olan İran ve Kuzey Kore, kendi coğrafyasında da saldırı faaliyetleri gerçekleştirmektedir ve siber uzaydaki her aktör için asimetrik bir tehdit oluşturmaktadır. 21. yüzyılın getirdiği küreselleşmenin bilişim boyutundan geri kalmamak ve dünya siyasetinde yer edinebilmek için imkanlarını hazır hale getirmek isteyen devletler olan Hindistan, Güney Kore ve Japonya, bu uğurda yoğun bir çaba sarf ederek kapasitelerini ve Batı ile ilişkilerini geliştirmeyi amaçlamaktadır.

Siber güvenlik kapasitesini artırma yoluna giderek siber güç inisiyatifini elinde tutan devletlere bakıldığında Çin, İran, Rusya ve Kuzey Kore çalışma içerisinde en çok dikkat çeken ülkeler olmuştur. Bu devletlerin Batı karşıtı olmalarının haricinde birden çok ortak özelliği vardır. Ülke içi siber suç oranları yüksek olan bu devletlerin, siber güvenliği tekeline almak istediği ve vatandaşlarının erişimini kısıtlama veya engelleme yetkisine sahip olduğunu belirtmek gerekir. Gelebilecek dış tehditlere karşı da misliyle karşılık verecek teknik ekipmanları elinde bulunan bu devletler, oluşturdukları siber ordular vasıtasıyla siber operasyonları yönetmektedir ve ABD ile mücadele hususunda çatışmacı bir profil çizmektedir. Devletlerin, en çok dikkat çeken noktalarından

birisi de ülkelerin yönetim şekli, rejim tipi ve demokratiklik durumudur. Zira siber uzayda kapsamlı bir uluslararası norm oluşmadığından ötürü herhangi bir yaptırım mekanizması da yoktur **ve bu durum** devletlerin otoriter rejimlere sahip olmaları hareket alanlarını daha da genişlemektedir.

Suç oranı yüksek olup, demokrasiden uzak olan otoriter rejimler (Çin, İran, Rusya, Kuzey Kore) siber uzayda daha saldırgan görüntü çizmektedir. Suç oranı düşük olup, tam demokrasi ile yönetilen ülkeler (Güney Kore, Japonya) ise siber uzayda daha az saldırgan bir görüntü çizmektedir. Nitekim çalışma içerisinde gösterilen ve 167 ülkenin incelendiği demokrasi endeksi sıralamasında Çin 151, İran 152, Rusya 124 ve Kuzey Kore 167'nci sırada olmuştur. Dört devletin de rejim tipinin otoriter olmasının yanında Çin komünizm, İran teokrasi, Rusya federal cumhuriyet, Kuzey Kore ise diktatörlük biçiminde yönetilmektedir. Bu bağlamda yapılan çalışmada; siber suç oranı yüksek olup, demokrasi endeksinde son sıralarda olan ve otoriter yönetilen Batı karşıtı Asya devletlerinin siber uzayda daha saldırgan olduğu sonucuna varılmıştır.

Bölgedeki otoriter devletlerin saldırgan olması sebebiyle kendi coğrafyasındaki devletlere ve Batı'ya karşı gösterdikleri sert tutumlar, siber güçler paralelinde ciddi oranda artmıştır. Aynı zamanda bu devletlerin siber güvenliği militarize ettiği gözlemlenmiştir. Özellikle saldırgan devletlerin bunun şiddetini artırarak siber savaşı tıpkı konvansiyonel savaş gibi görmesi, bu devletleri daha da saldırgan kılmaktadır. Bu bağlamda devletler ve devlet dışı aktörlerin saldırgan davranışları, siber uzay dahilinde uluslararası sistemde bilgi güvenliğinin sağlanması ve sürdürülebilirliği açısından endişeyle karşılanmaktadır.

KAYNAKÇA

Acar, Hasan (2020), "Küresel Terörün Uluslararası Politikadaki Yeni Aktörü: Hibrit Savaş Modeli", **Küresel Terör ve Güvenlik Politikaları**, 1.Baskı *içinde* (57-71), Nobel Yayıncılık, Ankara.

_____ (2020), "Rusya'nın Siber Güvenlik Politikası", Fulya Köksoy (Ed.), **Yeni Küresel Tehdit: Siber Saldırılar Siber Güvenlik ve Politika Uygulamaları,** 1.Baskı *içinde* (87-107), Nobel Yayıncılık, Ankara.

Acar, Hasan ve Pekcandanoğlu, Mustafa (2020), "Analysis of Russia's Cyber Security and Cyber Espionage Policies", **Türkiye Rusya Araştırmaları Dergisi**, 3(1), 167-189.

Ada, Mehmet ve Çakır, Hüseyin (2017), "Kuzey Atlantik Antlaşma Örgütü'nün (NATO) Siber Güvenlik Stratejisinin İncelenmesi", **Düzce Üniversitesi Bilim ve Teknoloji Dergisi**, 5(2), 632-656.

Akın, Murat ve Sağıroğlu, Şeref (2017), "Advanced Persistent Threats", **Türkiye Bilişim Vakfı Bilgisayar Bilimleri Ve Mühendisliği Dergisi**, 1(10), 1-10.

Akyeşilmen, Nezir (2019), **Disiplinlerarası Bir Yaklaşımla Siber Politika ve Güvenlik,** 1.Baskı, Orion Kitabevi, Ankara.

Akyeşilmen, Nezir ve Kurnaz, İbrahim (2020), "Küresel Siber Güvenlik: Kavramsal ve Kuramsal Bir Analiz", Fulya Köksoy (Ed.), **Yeni Küresel Tehdit: Siber Saldırılar Siber Güvenlik ve Politika Uygulamaları,** 1.Baskı *içinde* (3-32), Nobel Yayıncılık, Ankara.

Alexander, Keith Brian (2007). "Warfighting in Cyberspace", **National Defense University**, 46(3), 58-61.

Alexander, Yonah (Ed.) (2000), **Cyber Terrorism and Information Warfare: Threats and Responses,** Transnational, Miami.

Alnıak, Okan (2004), "Siber Terörizm Raporu", **Türkiye Asya Stratejik Araştırmalar Merkezi**, https://tasam.org/Files/Icerik/File/siber_terorizm_raporu_84be5753-d219-418f-9a68-e6c719b645b1.pdf (26.01.2021).

Anadolu Ajansı (2015), "Kuzey Kore'nin Ordusu Hakkında Korkutucu İddia", gazetevatan.com: http://www.gazetevatan.com/kuzey-kore-nin-ordusu-hakkinda-korkutucu-iddia-714511-dunya/ (11.03.2021).

_____ (2020), "Siber Saldırganlar Mobil Platformlar Üzerinden Asya'daki Faaliyetlerini Artırdı", https://www.aa.com.tr/tr/sirkethaberleri/bilisim/siber-saldirganlar-mobil-platformlar-uzerinden-asyadaki-faaliyetlerini-artirdi/657065 (25.05.2021).

Areng, Liina (2013), "International Cyber Crisis Management and Conflict Resolution Mechanisms", Katharina Ziolkowski (Ed.), **Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy,** 1st Edition *içinde* (565-588), NATO CCD COE Publication, Tallinn.

Arıboğan, Deniz Ülkü (2017), **Duvar,** 2.Baskı, İnkılap Kitabevi, İstanbul.

Austin, Greg (2018), "How Good Are China's Cyber Defenses?", **The Diplomat,** https://thediplomat.com/2018/07/how-good-are-chinas-cyber-defenses/ (07.08.2021).

Austuralian Goverment Department of Foreign Affairs and Trade (2021), "ASEAN Regional Forum (ARF)", https://www.dfat.gov.au/international-relations/regional-architecture/asean-regional-forum-arf (24.04.2021).

Azmi, Riza vd. (2016), "Motives behind Cyber Security Strategy Development: A Literature Review of National Cyber Security Strategy", https://www.researchgate.net/publication/308470260 (24.09.2021).

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

Baram, Gil ve Lim, Kevjn (2020), "Israel and Iran Just Showed Us the Future of Cyberwar With Their Unusual Attacks", **Foreign Policy**, https://foreignpolicy.com/2020/06/05/israel-and-iran-just-showed-us-the-future-of-cyberwar-with-their-unusual-attacks/ (07.07.2021).

Baylis, John (2008), "Uluslararası İlişkilerde Güvenlik Kavramı", **Uluslararası İlişkiler Dergisi**, 5(18), 69-85.

Bayrak, Halil (2021), "2021 Dünya İnternet, Sosyal Medya ve Mobil Kullanım İstatistikleri", https://dijilopedi.com/2021-dunya-internet-sosyal-medya-ve-mobil-kullanim-istatistikleri/ (09.11.2021).

Bayraktar, Gökhan (2014), "Harbin Beşinci Boyutunun Yeni Gereksinimi: Siber İstihbarat", **Güvenlik Stratejileri Dergisi**, 10(20), 119-147.

_____ (2015), **Siber Savaş ve Ulusal Güvenlik Stratejisi,** 1.Baskı, Yeni Yüzyıl Yayınları, İstanbul.

Bıçakcı, Salih (2012), "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", **Uluslararası İlişkiler Dergisi**, 9(34), 205-226.

_____ (2014), "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", **Uluslararası İlişkiler Dergisi,** 10(40), 101-130.

Biçer, Rüştü S. Salim (2020), "Modern Terörizmin Beşinci Dalgası: Devletlerin Uluslararası Terörist Örgütlerle İş Birliğinin Sebepleri ve Sonuçları", **Güvenlik Stratejileri Dergisi,** 16(36), 915-945.

Billo, Charles ve Chang, Welton (2004), **Cyber Warfare an Analysis of the Means and Motivations of Selected Nation States,** Dartmouth College, Hannover.

Birdişli, Fikret (2010), "Eleştirel Güvenlik Çalışmaları Kapsamında Frankfurt Okulu ve Soğuk Savaş Sonrası Güvenlik Sorunlarına Eleştirel Bir Yaklaşım: Galler Ekolü", **Güvenlik Stratejileri Dergisi**, 10(20), 229-256.

_____ (2020), "Uluslararası Güvenliğin Tarihsel Gelişimi ve Post-Modern Güvenlik Dönemi", **Güvenlik Bilimleri Dergisi**, 18(2), 235-260.

Brauch, Hans Günter (2008), "Güvenliğin Yeniden Kavramsallaştırılması: Barış, Güvenlik, Kalkınma ve Çevre Kavramsal Dörtlüsü", **Uluslararası İlişkiler Dergisi**, 5(18), 1-47.

Brenner, Susan W. ve Goodman, Marc (2002), "In Defense of Cyberterrorism: An Argument for Anticipating Cyber Attacks", **University Of Illionis Journal of Law Technology and Policy,** 1(1), 1-57.

Brown, Gary Yung, Christopher (2017), "Evaluating the US-China Cybersecurity Agreement, Part 1: The US Approach to Cyberspace", **The Diplomat,** https://thediplomat.com/2017/01/evaluating-the-us-china-cybersecurity-agreement-part-1-the-us-approach-to-cyberspace/ (09.04.2020).

Brown, Irene (1966), "Studies on Non-alignment", **The Journal of Modern African Studies**, 2(2), 517-527.

Buzan, Barry ve Hansen, Lene (2009), **The Evolution of International Security Studies,** Cambridge University Press, Camridge.

Campbell-Smith, Ualan ve Bradshaw, Samantha (2019), "Global Cyber Troops Country Profile: India", **Oxford Internet Institute**, https://demtech.oii.ox.ac.uk/wp-content/uploads/sites/93/2019/05/India-Profile.pdf (09.10.2021).

Chang, Gordon (2019), "Busting The Ghost Hackers", **Forbes**, https://www.forbes.com/2009/03/30/ghostnet-spyware-hackers-opinions-columnists-china-obama.html?sh=414d3567e242 (24.02.2021).

Chernenko, Yelena (2013), "NATO and CSTO Approach Security Differently", **Russia Beyond**, https://www.rbth.com/politics/2013/04/04/nato_and_csto_approach_security_differently_24633.html (07.07.2021).

China White Paper (2020), **The AI in China 2020 White Paper**, Daxue Consulting, Beijing.

China's National Defense (2004), "PRC: 2004 White Paper on National Defense Published", https://fas.org/nuke/guide/china/doctrine/natdef2004.html (06.09.2021).

Cho, Hyeisun vd. (2015), "The Study of Prediction of Same Attack Group by Comparing Similarity of Domain", **International Conference on Information and Communication Technology Convergence (ICTC),** 1(1), 1220-1222.

Chomsky, Noam (2003), **Pirates and Emperors, Old and New: International Terrorism in the Real World,** 2th Ed., South End Press, Boston.

Choucri, Nazli (2015), "Explorations in Cyber International Relations", http://ecir.mit.edu/sites/default/files/documents/ECIR%20Final%20Report.pdf (17.12.2020).

Choucri, Nazli ve Clark, Daniel (2012), "Integrating Cyberspace and International Relations: The Co-Evolution Dilemma", **MIT Working Paper**, https://papers.ssrn.com/sol3/papers.cfm?abstract_id=2178586 (06.09.2021).

_____ (2013), "Who Controls the Cyberspace?" **Bulltein of the Atomic Scientists**, 69(5), 21-31.

Cilluffo, Frank (2013), "Cyber Threats from China, Russia and Iran: Protecting American Critical Infrastructure", https://www.govinfo.gov/content/pkg/CHRG-113hhrg82583/html/CHRG-113hhrg82583.htm (26.10.2021).

_____ (2017), "Empty Threat or Serious Danger: Assessing North Korea's Risk to the Homeland" **Commıttee On Homeland Securıty House Of Representatıves One Hundred Fıfteenth Congress**, https://www.congress.gov/115/chrg/CHRG-115hhrg28820/CHRG-115hhrg28820.pdf (17.04.2020).

Cimpanu, Catalin (2020), "First Death Reported Following a Ransomware Attack on a German Hospital", https://www.zdnet.com/article/first-death-reported-following-a-ransomware-attack-on-a-german-hospital/ (11.10.2020).

CISA (2009), "Cyberspace Policy Review", https://www.cisa.gov/publication/2009-cyberspace-policy-review (04.05.2020).

____ (2018), "Russian Government Cyber Activity Targeting Energy and Other Critical Infrastructure Sectors", https://www.us-cert.gov/ncas/alerts/TA18-074A (06.09.2020).

____. (2018), "Russian State-Sponsored Cyber Actors Targeting Network Infrastructure Devices", https://www.us-cert.gov/ncas/alerts/TA18-106A (06.09.2020).

____ (2020), "Guidance on the North Korean Cyber Threat", https://www.us-cert.gov/ncas/alerts/aa20-106a (09.09.2020).

____ (2020), "Potential for Iranian Cyber Response to U.S. Military Strike in Baghdad", https://www.us-cert.gov/ncas/alerts/aa20-006a (17.09.2020).

CIS Legislation (2009), "The agreement between the governments of state members of the Shanghai Cooperation Organization on cooperation in the field of ensuring the international information security", cis-legislation.com: https://cis-legislation.com/document.fwx?rgn=28340 (10.08. 2021).

Clarke , Richard ve Knake, Robert (2011), **Cyber War: The Next Threat to National Security and What to Do About It,** 1th Ed., New York Times Bestseller, New York.

Collin, Barry (1997), "The Future of CyberTerrorism" **Crime and Justice International**, 13(2), 15-18.

Connell, Michael ve Vogler, Sarah (2017), "Russia's Approach to Cyber Warfare", https://www.cna.org/cna_files/pdf/DOP-2016-U-014231-1Rev.pdf (07.06.2021).

Cordesman, Anthony (2019), "China's New 2019 Defense White Paper", https://www.csis.org/analysis/chinas-new-2019-defense-white-paper (05.09.2021).

Copeland, Dale (1996), "Neorealism And The Myth of Bipolar Stability: Toward a New Dynamic Realist Theory of Major War", **Security Studies,** 5(3), 29-89

Cuevas, Carlos ve Rennison, Callie Marie (2016), **The Wiley Handbook on the Psychology of Violence,** Wiley-Blackwell, New Jersey.

CyberMack (2020), "Corona/Covid-19 Mobil Tehdit Raporu", https://www.cybermagonline.com/corona-covid-19-mobil-tehdit-raporu (07.09.2021).

Cyber Policy Portal (2020), "Cybersecurity Policy", **UNIDIR,** https://unidir.org/cpp/en/ (06.05.2021).

Cyberpolicy Portal (2020), "Cybersecurity Policy Strategy Documents", **UNIDIR**, https://cyberpolicyportal.org/en/states/japan (16.10.2021).

Cylance Inc, (2014), "Operation Cleaver", https://scadahacker.com/library/Documents/Cyber_Events/Cylance%20-%20Operation%20Cleaver%20Report.pdf (12.07.2021).

Çahmutoğlu, Ersin (2020), "ABD-İran Krizinin Siber Boyutu: Savaş Zaten Başlamıştı", https://medium.com/@ersincmt/abd-i%CC%87ran-krizinin-siber-boyutu-sava%C5%9F-zaten-ba%C5%9Flam%C4%B1%C5%9Ft%C4%B1-b2fe55d365b (10.11.2020).

_____ (2020), "Siber Uzayda Güç ve Siber Silah Teknolojilerinin Küresel Etkisi", **Analytical Politics**, 1(1), 1-16.

Çahmutoğlu, Ersin (2020), "Gelişen Bir Siber Aktör Olarak İran'ın Stratejik Operasyonları", **Anadolu Ajansı,** https://www.aa.com.tr/tr/analiz/gorus-gelisen-bir-siber-aktor-olarak-iran-in-stratejik-operasyonlari/1850330 (24.01.2021).

_____ (2021), "İran'ın Siber Gücü", **İRAM** https://iramcenter.org//d_hbanaliz/iranin-siber-gucu_1.pdf (05.05.2021).

Çakmak, Haydar (2008), **Teörizm,** Platin Yayınları, Ankara.

Çelik, Soner (2018), "Siber Uzay ve Siber Güvenliğe Multidisipliner Bir Yaklaşım", **Academic Review of Humanities and Social Sciences,** 1(2), 110-119.

Çeliktaş, Barış (2018), "Cyber Security Power Ranking By Country And Its Importance On World Politics", **The Journal of Academic Social Science Studies,** Nr.67, 469-488.

Çetinkaya, Şeref (2011), "Siber Terör ve Siber İstihbarat", **21. Yüzyıl Türkiye Enstitüsü,** https://21yyte.org/tr/merkezler/islevsel-arastirma-merkezleri/terorizm-ve-terorizmle-mucadele/siber-teror-ve-siber-istihbarat (19.08.2021).

Dalha, Tenzin (2018), "The Cyber War Against Tibet", **The Diplomat** https://thediplomat.com/2019/02/the-cyber-war-against-tibet/ (11.09.2020).

Darıcılı, Ali Burak (2014), "Rusya Federasyonu Kaynaklı Olduğu İddia Edilen Siber Saldırılar", **Uludağ Üniversitesi Sosyal Bilimler Dergisi,** 7(2), 1-19.

Darıcılı, Ali Burak (2019), "Analysıs Of Iran's Cyber Securıty Strategy With Regard To The Attack And The Defense Capacıty", ***Turkish Studies Social Sciences,*** 14(3), 409-425.

Darıcılı, Ali Burak & Özdal, Barış (2017), "Rusya Federasyonunun Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi", **Bilig,** Nr.83, 121-146.

Dedeoğlu, Beril (2003), **Uluslararası Güvenlik ve Strateji,** Derin Yayınları, İstanbul.

Değdaş, Ulaş Can (2018), "Uluslararası Hukukta Önleyici Meşru Müdafaa Hakkı", **Hukuk Fakültesi Dergisi,** 4(6), 21-40

Demir, Yeşim (2020), "Japonya'nın Siber Güvenlik Politikası", Fulya Köksoy (Ed.), **Yeni Küresel Tehdit: Siber Saldırılar Siber Güvenlik ve Politika Uygulamaları,** 1.Baskı *içinde* (227-244), Nobel Yayıncılık, Ankara.

Demir, Yiğit Ali (2019), "Kuzey Kore Hindistan'a Siber Saldırı Düzenledi", https://shiftdelete.net/kuzey-kore-hindistan-nukleer-santraline-siber-saldiri-duzenledi (04.11.2021).

Demirel, Emin (2007), **Terör,** Kültür Sanat Yayıncılık, İstanbul.

Denning, Dorolthy Elizabeth (2001), "Activism, Hacktivism, and Cyberterrorism: The Internet As a Tool For Influencing Foreign Policy", **Networks and Netwars: The Future of Terror, Crime, and Militancy,** 2nd Edition *içinde (*239-288), RAND, Kalifornia.

Devlin, Kat (2019), "Cybersecurity Threat Looms Large In Japan", https://www.japantimes.co.jp/opinion/2019/07/01/commentary/japan-commentary/cybersecurity-threat-looms-large-japan/#.XtfHZzozZPY (24.01.2021).

Digital Goverment (2021), "Digital Government Achievements and Mid- and Long-term Plans in South Korea", https://www.dgovkorea.go.kr/event/event3 (07.09.2021).

Doffman, Zak (2020), "CIA Hackers Accused Of 11-Year Attack In New Chinese Cyber Report: This Is What's Behind It", **Forbes,** https://www.forbes.com/sites/zakdoffman/2020/03/03/new-chinese-cyber-report-just-accused-cia-of-11-year-attack-this-is-whats-behind-the-report/#5aa5289a57e6 (09.10.2021).

Easley, Lelif-Eric (2017), "From Strategıc Patıence To Strategıc Uncertainty", **World Affairs,** 180(2), 7-31.

Eldem, Tuba (2021), "Birleşmiş Milletler Sistemi ve Küresel Siberalan Güvenliği Regülasyonu", **Marmara Üniversitesi Siyasal Bilimler Dergisi,** 9(1), 17-45.

ENISA (2011), "Cyber Europe 2010 Report", https://www.enisa.europa.eu/publications/ce2010 report (06.08.2021).

_____ (2015), "Definition of Cybersecurity", **European Union Agency for Network:** enisa.europa.eu/publications/definition-ofcybersecurity (09.12.2020).

Epifanova, Alena (2020), "Deciphering Russia's Sovereign Internet Law", **Dgap Analysis**, https://dgap.org/en/research/publications/deciphering-russias-sovereign-internet-law adresinden (13.10.2021).

Erdoğan, Mustafa (2011), **11 Eylül Dönemi Sonrası ABD ve AB'nin Terör Konusundaki Kurumsal Bakış Açıları**, Yayınlanmamış Yüksek Lisans Tezi, Sakarya Üniversitesi - Sosyal Bilimler Enstitüsü.

Eren, Mehmet (2017), **Avrupa Birliği'nin Siber Güvenlik Politikası,** 1.Baskı, Beta Yayınları, İstanbul.

_____ (2017), "Avrupa Birliği'nin Siber Güvenlik Stratejisi İçin Kuramsal Çerçeve Ve Strateji Belgesi Öncesi AB'nin Eylemleri", **CyberPolitik Journal**, 2(3), 212-245.

Erendor, Mehmet Emin ve Tamer, Gürkan (2017), "The New Face of the War: Cyber Warfare", **Cyberpolitik Journal**, 2(3), 4-57.

Euronews (2021), "Çin, Yüksek Kamu Borcu ve Pandemiye Rağmen 2021'de Savunmaya 210 Milyar Dolar Ayıracak", **Euronews Türkiye,** https://tr.euronews.com/2021/03/05/cin-yuksek-kamu-borcu-ve-pandemiye-ragmen-2021-de-savunmaya-210-milyar-dolar-ay-racak (05.08.2021).

_____ (2021), "NATO Uyardı: Rusya, Ukrayna Sınırına Askeri Yığınak Yapıyor", **Euronews Türkiye,** https://tr.euronews.com/2021/11/15/nato-uyard-rusya-ukrayna-s-n-r-na-askeri-y-g-nak-yap-yor (06.09.2021).

European Commision (2016), "*Cybercrime and cyberterrOrism (E)Uropean Research AGEnda"*, **Cordis,** https://cordis.europa.eu/project/id/607949 (04.10.2020).

Eurostat (2016), "1 Out of 4 Internet Users in The EU Experienced Security Related Problems in 2015", https://ec.europa.eu/eurostat/documents/2995521/7151118/4-08022016-AP-EN.pdf/902a4c42-eec6-48ca-97c3-c32d8a6131ef (06.09.2020).

Eyidilli, Sami (2012), "Japonya'dan "Milli Güvenlik Virüsü", https://webrazzi.com/2012/01/06/japonyadan-milli-guvenlik-virusu/ (11.11.2020).

Feakin, Tobias (2013), "Playing Blind-Man's Buff: Estimating North Korea's Cyber Capabilities", **International Journal of Korean Unification Studies,** 22(2), 63-90.

Firch, Jason (2021), "10 Cyber Security Trends You Can't Ignore In 2021", https://purplesec.us/cyber-security-trends-2021/#Lockdowns (17.10.2021).

Firestone, Adam (2018), "An Information Security Overview", **Security Industry Association,** https://www.securityindustry.org/wp-content/uploads/2018/07/Firestone-Data-Security-071118.pdf adresinden (07.09.2021).

Gady, Franz-Stefan (2011), "From the Middle Ages to the Cyber Age: Non-State Actors", **HuffPost,** http://www.huffingtonpost.com/franzstefan-gady/from-the-middle-ages-tot_b_818650.html (04.09.2020).

Gady, Franz-Stefan (2017), "Japan: The Reluctant Cyberpower", **Asie Visions,** Nr. 91, 5-28.

Gelecek Burada (2020), "Hindistan'ın Yeni Siber Güvenlik Yasası Küresel Tehdit Oluşturabilir", gelecekburada.net: https://www.gelecekburada.net/hindistanin-yeni-siber-guvenlik-yasasi-kuresel-tehdit-olusturabilir/ (14.06.2021).

Gerasimov, Valery (2013), "The Value of Science in Prediction", **Militay Review,** https://www.armyupress.army.mil/portals/7/military-review/archives/english/militaryreview_20160228_art008.pdf (12.08.2021).

Gorman, Sean P. (2006), "A Cyber Threat to National Security?", Philip Auerswald (Ed.), **Seeds of Disaster, Roots of Response: How Private Action Can Reduce Public Vulnerability,** 2nd Edition *içinde* (239-257), Cambridge University Press, Cambridge.

Goud, Naveen (2017), "Cyber Attacks On Japan's Critical Infrastructure Touches 128 Billion Mark", https://www.cybersecurity-insiders.com/cyber-attacks-on-japans-critical-infrastructure-touches-128-billion-mark/ (16.09.2021).

Göçoğlu, Volkan ve Aydın, Mehmet Devrim (2019), "Siber Güvenlik Politikası: ABD, Rusya ve Çin Üzerine Karşılaştırmalı Bir Analiz", **Güvenlik Bilimleri Dergisi,** 8(2), 229-252.

Green, Joshua (2001), "The Myth of Cyberterrorism", **Washington Monthly,** https://washingtonmonthly.com/2001/11/01/the-myth-of-cyberterrorism/ (12.09.2020)

Grigoriev, Dmitry (2010), https://www.files.ethz.ch/isn/115239/2010-04_GlobalCyberDeterrence.pdf (09.10.2021).

Gül, Talip (2012), **Terör ve Terörizm,** 1.Baskı, Step Matbaacılık, İstanbul.

Güntay, Vahit (2014), "Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler", **Güvenlik Stratejileri Dergisi**, 14(27), 79-111.

Güntay Vahit (2016), **Uluslararası İlişkiler Temelinde Siber Güvenlik: Mikro Siber İttifak Teorisi (Micro-CAT),** Yayınlanmamış Doktora Tezi, Karadeniz Teknik Üniversitesi - Sosyal Bilimler Enstitüsü.

_____ (2020), "Güney Kore'nin Siber Güvenlik Politikası", Fulya Köksoy (Ed.), **Yeni Küresel Tehdit: Siber Saldırılar Siber Güvenlik ve Politika Uygulamaları,** 1.Baskı *içinde* (267-282), Nobel Yayıncılık, Ankara.

_____ (2020), "Kuzey Kore'nin Siber Güvenlik Politikası", Fulya Köksoy (Ed.), **Yeni Küresel Tehdit: Siber Saldırılar Siber Güvenlik ve Politika Uygulamaları,** 1.Baskı *içinde* (245-265), Nobel Yayıncılık, Ankara.

Gürkaynak, Muharrem ve İren, Adem Ali (2011), "Reel Dünyada Sanal Açmaz: Siber Alanda Uluslararası İlişkiler", **Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,** 16(2), 263-279.

Habertürk (2017), "ABD: Kuzey Kore, Herkesi 8 Yıldır Hackliyor", https://www.haberturk.com/ekonomi/teknoloji/haber/1530600-abd-kuzey-kore-herkesi-8-yildir-hack-liyor (07.05.2020).

Hackett, James (2018), "The Conventional Military Balance On The Korean Peninsula", https://www.iiss.org/blogs/research-paper/2018/06/military-balance-korean-peninsula (09.05.2020).

Hansen, Lene ve Nissenbaum, Helen (2009), "Digital Disaster, Cyber Security, and the Copenhagen School", **International Studies Quarterly**, 53(4), 1115-1175.

Haser, Demet (2018), **Uluslararası İlişkilerde Güvenlik Kavramı: Soğuk Savaş Sonrası Dönem Güvenlik,** Yayınlanmamış Yüksek Lisans Tezi, İstanbul Ticaret Üniversitesi - Sosyal Bilimler Enstitüsü.

HAVELSAN (2018), "Siber Terör", **Siber Savunma Teknolojileri**, http://sisatem.com.tr/kategori/haberler/68574/siber-teror.html (21.06.2020).

Heywood, Andrew (1997), **Politics,** Red Globe Press, New York.

_____ (2018), **Siyaset,** (Çev. Fahri Bakırcı), BB101 Yayınları, Ankara.

Higgins, Kelly Jackson (2014), "Anatomy Of The New Iranian APT", **Dark Reading,** https://www.darkreading.com/vulnerabilities-threats/anatomy-of-the-new-iranian-apt (16.10.2020).

History Extra (2021), "Why Do We Say Red Herring?", https://www.historyextra.com/period/georgian/why-we-say-phrase-red-herring-hunting-origins/ (11.09.2021).

Hoffman, Banesh (1998), **Inside Terrorism,** 3rd Ed., Carolina UniversityPress, London

Iasiello, Emilio (2020), "Russia and China Are Making their Information Security Case", https://www.cyberdb.co/russia-and-china-are-making-their-information-security-case/ (04.09.2020).

International Rescue Committee (2015), "History of the International Rescue Committee", https://www.rescue.org/page/history-international-rescue-committee (19.09.2020).

İslam Ansiklopedisi (1991), "Asabiyet", https://islamansiklopedisi.org.tr/asabiyet (06.10.2021).

ITU (2010), "Cybersecurity", **Landmark decisions from Guadalajara**, https://www.itu.int/net/itunews/issues/2010/09/pdf/201009_20.pdf (16.08.2021).

____ (2020), "Global Cybersecurity Index 2019", https://www.itu.int/dms_pub/itu-d/opb/str/D-STR-GCI.01-2018-PDF-E.pdf (22.06.2020).

Japanese Law Translation (2000), "Basic Act on the Formation of an Advanced Information and Telecommunications Network Society", http://www.japaneselawtranslation.go.jp/law/detail/?id=3339&vm=02&re= (16.09.2021).

Jervis, Robert (1978), "Cooperation Under the Security Dilemma", **World Politics**, 30(2), 167-214.

Jones, Sam (2016), "Cyber Warfare: Iran Opens a New Front", **Financial Times**, https://www.ft.com/content/15e1acf0-0a47-11e6-b0f1-61f222853ff3 (07.05.2020).

Jongman, Albert (2015), **Political Terrorism: A New Guide to Actors, Authors, Concepts, Data Bases, Theories, and Literature,** Routlage, Philadelphia.

Jopling, Lord (2007), "The Protection Of Critical Infrastructures", https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/270/270907/270907jopling_en.pdf (11.07.2020).

Kallender, Paul ve Hughes, Christopher (2016), "Japan's Emerging Trajectory as a Cyber Power: From Securitization to Militarization of Cyberspace", **Journal of Strategic Studies,** 40(1-2), 118-145.

Kang, Tae-Jun (2019), "South Korea's New Internet Controls Spark Controversy", The Diplomat, https://thediplomat.com/2019/03/south-koreas-new-internet-controls-spark-controversy/ (11.10.2020).

Kant, Immanuel (2020), **Ebedi Barış Üzerine Felsefi Bir Tasarı,** (Çev. Ömer Can Azman), Gece Kitaplığı, İstanbul

Kapersky (2021), "DDoS Saldırısı Nedir?", https://www.kaspersky.com.tr/resource-center/threats/ddos-attacks (09.09.2021).

Kaplan, Jeffrey (2016), "Waves of Political Terrorism", **Oxford Research Encyclopedia of Politics,** https://doi.org/10.1093/acrefore/9780190228637.013.24 (06.12.2020).

Kara, Mahruze (2013), "Siber Saldırılar-Siber Savaşlar ve Etkileri", https://openaccess.bilgi.edu.tr/bitstream/handle/11411/346/Siber%20Sald%C4%B1r%C4%B1lar%20Siber%20Sava%C5%9Flar%20ve%20Etkileri.pdf?sequence=2&isAllowed=y (11.09.2020).

Karnouskos, Stamatis (2011), "Stuxnet Worm Impact on Industrial Cyber-Physical System Security", IECON (Ed.), **37th Annual Conference of the IEEE Industrial Electronics Society**, IEEE, Melbourne, 4490-4494.

Kartal, Atahan Birol (2014), "Uluslararası Terörizmin Değişen Yapısı ve Terör Örgütlerinin Sosyal Medyayı Kullanması: Suriye'de DAEŞ ve YPG Örneği", **Güvenlik Stratejileri Dergisi,** 14(27), 40-77.

Kemp, Simon (2021), "Digital 2021: Global Overview Report", https://datareportal.com/reports/digital-2021-global-overview-report (06.09.2021).

Kızılay, Şeyma (2020), "Soğuk Savaş Sonrası ABD'nin Siber Güvenlik Politikası", **International Journal of Economics Administrative and Social Sciences,** 3(1), 33-44.

Kim, Tongfi (2011), "Why Alliances Entangle But Seldom Entrap States", **Security Studies,** 20(3), 350-377.

Klabbers, Jan (2013), "Responsibility of States and International Organisations in the Context of Cyber Activities with Special Reference to NATO", Katharina Ziolkowski (Ed.), **Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy,** 1st Edition *içinde* (485-504), NATO CCD COE Publication, Tallinn.

Kleinrock, Leonard ve Kermani, Parviz (1976), "Virtual Cut-Through: A New Computer Communication Switching Technique", **Computer Networks**, 3(4), 267-286.

Korhan, Sevda (2020), "Uluslararası İlişkilerde Siber Güvenlik: Caydırıcılık, Güç ve Diplomasi", Fulya Köksoy (Ed.), **Yeni Küresel Tehdit: Siber Saldırılar Siber Güvenlik ve Politika Uygulamaları,** 1.Baskı *içinde* (51-67), Nobel Yayıncılık, Ankara.

Kurt, Selim (2019), "Yeni Terörizm'in Geleceğin Güvenlik Ortamına Etkileri: DAEŞ Örneği", **Akademik Bakış Dergisi,** 13(25), 133-161.

Kutup, Nejat (2010), "İnternet ve Sanat, Yeni Medya ve net.art", **Akademik Bilişim Dergisi**, 10(9), 9-20.

Laqueur, Walter (2017), **A History of Terrorism,** Routledge, New York.

Lewis, James (2002), **Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats,** 1st Ed., Center for Strategic & International Studies, Washington.

Libicki, Martin (2009), **CyberDetterence and CyberWar,** 2nd Ed., RAND Corporation Press, Pittsburgh.

Library of Congress (2018), "Japan: Basic Act on Cybersecurity Amended", https://www.loc.gov/item/global-legal-monitor/2018-12-26/japan-basic-act-on-cybersecurity-amended/ (07.09.2021).

Licklider, Joseph (1960), "Man-Computer Symbiosis", **IRE Transactions on Human Factors in Electronics**, 1, 4-11.

L-Soft (2021), "History of LISTSERV", http://www.lsoft.com/corporate/history-listserv.asp (09.05.2021).

Ludwig, Jessica ve Walker, Christopher (2017), "The Meaning of Sharp Power", **Foreign Affairs,** https://www.foreignaffairs.com/articles/china/2017-11-16/meaning-sharp-power (09.06.2020).

Mallick, Maj Gen (2019), "Vivekananda International Foundation", https://www.vifindia.org/sites/default/files/china-s-defence-white-paper-an-analysis.pdf (06.09.2020).

Manantan, Mark (2019), "The Cyber Dimension of the South China Sea Clashes", **The Diplomat,** https://thediplomat.com/2019/08/the-cyber-dimension-of-the-south-china-sea-clashes/ (17.09.2020).

Mandiant (2013), "Mandiant Exposes APT1: One of China's Cyber Espionage Units & Releases 3,000 Indicators", https://www.fireeye.com/blog/threat-research/2013/02/mandiant-exposes-apt1-chinas-cyber-espionage-units.html (10.02.2021).

McAfee (2012), "57% Believe a Cyber Arms Race is Currently Taking Place, Reveals", https://www.businesswire.com/news/home/20120130005063/en/57-Believe-a-Cyber-Arms-Race-is-Currently-Taking-Place-Reveals-McAfee-Sponsored-Cyber-Defense-Report, (11.10.2020).

McCaffery, Larry (1988), "An Interview with William Gibson", https://www.jstor.org/stable/20134176 (06.10.2020).

Mearsheimer, John (1994), "The False Promise of International Institutions", **International Security,** 19(3), 1-49.

Mearsheimer, John (1995), "A Realist Reply", **International Security,** 20(1), 82-93.

Milliyet (2020), "İranlı Hackerlardan ABD'ye Siber Saldırı, https://www.milliyet.com.tr/galeri/iranli-hackerlardan-abdye-siber-saldiri-6115797/3 (05.09.2020).

Ministry of Information and Communications Technology, (2011), "Head of Iran IT Organization: 40 Articles Related to ICT Development in The Fifth Development Plan", https://www.ict.gov.ir/en/news/5853/Head-of-Iran-IT-Organization-40-articles-related-to-ICT-development-in-the-fifth-development-plan (05.09.2020).

Ministry of Internal Affairs and Communications of Japan (2013), "Joınt Mınısterıal Statement ff The Asean-Japan Ministerial Policy Meeting On Cybersecurity Cooperation", https://www.soumu.go.jp/main_content/000249127.pdf (16.03.2021).

Morgan, Steve (2019), "2019 Official Annual Cybercrime Report", https://cybernetsecurity.com/industry-papers/CV-HG-2019-Official-Annual-Cybercrime-Report.pdf (07.05.2020).

Morgenthau, Hans (1970), **Uluslararası Politika, Güc ve Barış Mücadelesi,** (Çev. Baskın Oran ve Ünsal Oskay), Siyasi Bilimler Türk Derneği Yayınları, Ankara.

Mshvidobadze, Khatuna (2012), "Russia's Military Alliance Tackles Cyber Crime", **The Potomac Institute Cyber Center,** https://pipscyberissues.wordpress.com/2012/11/26/russias-military-alliance-tackles-cyber-crime/ (14.11.2020).

Nation Master (2013), "Government type: Countries Compared", https://www.nationmaster.com/country-info/stats/Government/Government-type (09.08.2021).

NATO (1949), "The North Atlantic Treaty", https://www.nato.int/cps/en/natolive/official_texts_17120.htm (04.06.2020).

_____ (1999), "The Alliance's Strategic Concept", https://www.nato.int/cps/en/natolive/official_texts_27433.htm (09.06.2020).

_____ (2002), "The Prague Summit And Nato's Transformatıon", https://www.nato.int/docu/rdr-gde-prg/rdr-gde-prg-eng.pdf (14.05.2020).

_____ (2006), **Handbook,** Public Diplomacy Division, Brussels.

_____ (2006), "Riga Summit Declaration", https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en (09.05.2020).

_____ (2008), "Bucharest Summit Declaration", https://www.nato.int/cps/en/natolive/official_texts_8443.htm (12.04.2021).

_____ (2010), "Lisbon Summit Declaration", https://www.nato.int/cps/en/natolive/official_texts_68828.htm (07.09.2020).

_____ (2021), "Cyber Defence", https://www.nato.int/cps/en/natohq/topics_78170.htm (12.06.2021).

NCCIC (2017), "Enhanced Analysis of GRIZZLY STEPPE Activity", https://www.us-cert.gov/sites/default/files/publications/AR-17-20045_Enhanced_Analysis_of_GRIZZLY_STEPPE_Activity.pdf (21.03.2020).

NCCIC ve FBI (2016), "Grizzly Steppe: Russian Malicious Cyber Activity", https://www.us-cert.gov/sites/default/files/publications/JAR_16-20296A_GRIZZLY%20STEPPE-2016-1229.pdf (21.03.2020).

NCSI (2021), "National Cybersecurity Index", https://ncsi.ega.ee/ (19.09.2020).

Negro, Gianluigi (2017), **The Internet in China** Palgrave Macmillan, London.

Ng, Jr (2020) "China Broadens Cyber Options", **Asian Military View,** https://asianmilitaryreview.com/2020/01/china-broadens-cyber-options/ (14.12.2020).

Nye, Joseph (2010), "Cyber Power", **Harvard Kennedy School Belfer Center for Science and International Affairs,** https://apps.dtic.mil/sti/pdfs/ADA522626.pdf (16.05.2021).

Nye, Joseph (2009), "Smart Power", **New Perspectives Quarterly,** 26(2), 7-9.

O'leary, Jacqueline vd. (2017), "Insights into Iranian Cyber Espionage: APT33 Targets Aerospace and Energy Sectors and has Ties to Destructive Malware", **Mandiant**, https://www.mandiant.com/resources/apt33-insights-into-iranian-cyber-espionage (14.09.2020).

Organski, Abramo (1958), **World Politics,** Alfred A. Knopf, New York.

OSCE (1990), "Treaty on Conventional Armed Forces in Europe", https://www.osce.org/library/14087 (08.11.2020).

_____ (2013), "Good Practices Guide on Non-Nuclear Critical Energy Infrastructure Protection (NNCEIP) from Terrorist Attacks Focusing on Threats Emanating from Cyberspace", https://www.osce.org/files/f/documents/4/b/103500.pdf (07.09.2020).

Özdemir, Çağatay (2018), **Amerikan Grand Stratejisi,** Seta Yayınları, İstanbul.

Özgüç, Büşra (2020), "ARPANET Nedir?", **Mediaclick Blog,** https://www.mediaclick.com.tr/tr/blog/arpanet-nedir (17.02.2020).

Patil, Rajindra (2013), "Social Media - History and Components", **IOSR Journal of Business and Management,** 7(1), 69-74.

Pekcan, Ceren (2020), "Çin Halk Cumhuriyeti'nin Siber Güvenlik Politikası", Fulya Köksoy (Ed.), **Yeni Küresel Tehdit: Siber Saldırılar Siber Güvenlik ve Politika Uygulamaları,** 1.Baskı *içinde* (205-225), Nobel Yayıncılık, Ankara.

Pernik, Piret ve Wojtkowiak, Jesse (2016), "National Cyber Security Organisation: United States", **NATO Cooperative Cyber Defence Centre of Excellence** https://afyonluoglu.org/PublicWebFiles/NATO/USA-National%20CyberSecurity%20Organization-2015%20Dec.pdf (24.01.2021).

Peskin, Doron (2020), "The Iranian Cyber Threat can no Longer be Underestimated", **Calcalist** https://www.calcalistech.com/ctech/articles/0,7340,L-3827871,00.html (09.06.2021).

Phys (2011), "New Cyber Attack on Japan Parliament", https://phys.org/news/2011-11-cyber-japan-parliament.html (18.10.2020).

Platte, James (2020), "Defending Forward on the Korean Peninsula", **The Cyber Defense Review,** 5(1), 75-92.

Polat, Doğan Şafak (2015), "Nato'nun Yeni Operasyon Alanı: Siber Uzay", **Güvenlik Bilimleri Dergisi**, 1, 135-158.

Privacy Shield (2020), "Japan Country Commercial Guide: Japan Cyber Security", privacyshield. gov: https://www.privacyshield.gov/article?id=Japan-Cyber-Security (14.09. 2021).

_____ (2020), "Korea - Cyber Security" https://www.privacyshield.gov/article?id=Korea-Cyber-Security (17.09.2021).

Radio Farda (2020), "Iran Cyberspace Supreme Council Among 20 Worst Digital Predators in 2020", https://en.radiofarda.com/a/iran-cyberspace-supreme-council-among-20-worst-digital-predators-of-2020/30483664.html (24.06.2021).

Rapoport, David (2013), "The Four Waves of Modern Terrorism", (Steven Chermak vd. Ed.), **Transnational Terrorism,** 2nd Edition *içinde* (46-73), Ashgate Publishing, New York.

Reedphish, (2014), "The CIA Triad", https://reedphish.wordpress.com/2014/05/23/the-cia-triad/ (07.09.2021).

Rid, Thomas (2013), **Cyber War Will Not Take Place,** Oxford University Press, Oxford.

Rohozinski, Rafal vd. (2009), "Tracking GhostNet: Investigating a Cyber Espionage", **Information Warfare Monitor**, https://ora.ox.ac.uk/objects/uuid:6d1260fd-b8ee-4a11-8a5fe7708d54365 1 (09.11.2020).

Romm, Tony vd. (2018), "Sprawling Iranian Influence Operation Globalizes Tech's War on Disinformation", **Washington Post,** https://www.thedickinsonpress.com/news/world/4488804-sprawling-iranian-influence-operation-globalizes-techs-war-disinformation (11.06.2021).

Limaye, Rajashri (2013), "The importance of Information Integrity, Security, Networking and Data Protection", **International Journal of Innovations in Engineering and Technology,** 2(3), 274-281.

Salman, Sarkan (2021), "Terörizm: Kavramsal Bir Çerçeve", **International Humanities and Social Science Review,** 5(1), 35-58.

Sanger, David ve Perlroth, Nicole (2020), "U.S. to Accuse China of Trying to Hack Vaccine Data, as Virus Redirects Cyberattacks", **New York Times,** https://www.nytimes.com/2020/05/10/us/politics/coronavirus-china-cyber-hacking.html?auth=link-dismiss-google1tap (19.06.2021).

Saral, Cevdet (2016), **Terörün Gizli Efendileri,** 2.Baskı, Kripto Basın Yayın, İstanbul.

Schaap, Major Arie (2009), "Cyber Warfare Operations: Development and Use Under International Law", **The Air Force Law Review,** 64, 121-175.

Schmid, Alex (2004), "Terrorism-The Definitional Problem", **Case Western Reserve Journal of International Law,** 36, 375-419.

Schmitt, Michael (2013), "Tallinn Manual on The International Law Applicable to Cyber", https://www.cambridge.org/core/books/tallinn-manual-on-the-international-law-applicable-to-cyber-warfare/50C5BFF166A7FED75B4EA643AC677DAE (16.07.2021).

Science Direct (2016), "Logic Bombs", https://www.sciencedirect.com/topics/computer-science/logic-bomb (14.09.2021).

Seren, Merve (2016), "Siber Tehditlerle Mücadelede Farkındalık ve Hazırlık", **SETA,** 183, 7-25.

Siber Bülten (2014), "İsrail'den Hindistan'a Siber İşbirliği Teklifi", https://siberbulten.com/uluslararasi-iliskiler/israilden-hindistana-siber-isbirligi-teklifi/ (17.11.2021).

Siber Bülten (2016), "Siber Diplomaside Yeni Dönem: Avustralya Siber İşler Elçisi Atadı", https://siberbulten.com/uluslararasi-iliskiler/siber-diplomaside-yeni-donem-avustralya-siber-isler-elcisi-atadi/ (09.01.2021).

Siboni, Gabi (2012), "What Lies behind Chinese Cyber Warfare", **Military and Strategic Affairs,** 4(2), 49-64.

Siboni, Gabi ve Kronenfeld, Sami (2012), "Iran and Cyberspace Warfare", **Military and Strategic Affairs**, 4(3), 86-91

Siers, Rhea (2014), "North Korea The Cyber Wild Card", **Journal of Law & Cyber Warfare**, 4(1), 1-12.

Sigholm, Johan (2016), "Non-State Actors in Cyberspace Operations", **Swedish National Defence College Journal of Military Studies**, 4(1), 1-38.

Simon, Jeffrey (2010), "Technological and Lone Operator Terrorism: Prospects for a Fifth Wave of Global Terrorism", Jean Rosenfeld (Ed.), **Terrorism, Identity and Legitimacy,** 1st Edition *içinde* (272-280), Routledge, London.

Singer, Peter ve Friedman, Allan (2015), **Siber Güvenlik ve Siber Savaş,** Buzdağı Yayınevi, Ankara.

Sözcü (2014),"Kuzey Kore'nin 1800 Kişilik Hacker Ordusu", https://www.sozcu.com.tr/2014/dunya/kuzey-korenin-1800-kisilik-hacker-ordusu-691567/ (21.06.2020).

Spade, Jayson (2017), "Information as Power: China's Cyber Power and America's National Security", **CreateSpace Independent Publishing Platform,** https://www.hsdl.org/?view&did=719179 (16.01.2021).

Sputniknews (2017), "Kuzey Koreli Hackerlar Güney'in Savaş Planlarını Çaldı", https://tr.sputniknews.com/asya/20171010130522517-kuzey-kore-guney-hacker-savas-plani/ (11.09.2021).

Stangarone, Troy (2018), "South Korea's Emergence as an Important Player in Cryptocurrency" **The Diplomat,** https://thediplomat.com/2018/11/south-koreas-emergence-as-an-important-player-in-cryptocurrency/ (17.10.2021).

Statista (2020), "Number of Cyber Crime Related Consultations in Japan from 2012 to 2018", https://www.statista.com/statistics/746985/japan-number-of-reported-cyber-crimes/ (11.05.2021).

_____ (2021), "Internet Usage Rate in South Korea from 2000 to 2020", https://www.statista.com/statistics/226712/internet-penetration-in-south-korea-since-2000/ (16.05.2021).

Şenel, Alaeddin (2017), **İlkel Toplumdan Uygar Topluma,** 1.Baskı, Bilim ve Sanat Yayıncılık, İstanbul.

Şengöz, Murat (2020), "Türkiye Cumhuriyeti'nin Ulusal Güvenlik Paradigması Üzerine Bir Değerlendirme", **Takvim-i Vekayi**, 8(1), 1-71.

T24 (2017), "Rusya ve Hindistan'dan Siber Güvenlik İşbirliği", https://t24.com.tr/haber/rusya-ve-hindistandan-siber-guvenlik-isbirligi,500146 (09.07.2021).

Tarhan, Kamil (2018), **Uluslararası Güvenliğin Bir Bileşeni Olarak Siber Güvenlik**, Yayınlanmamış Yüksek Lisans Tezi, Selçuk Üniversitesi - Sosyal Bilimler Enstitüsü.

_____ (2020), "Ulusal ve Uluslararası Güvenliğin Bir Bileşeni Olarak Siber Güvenlik", Fulya Köksoy (Ed.), **Yeni Küresel Tehdit: Siber Saldırılar Siber Güvenlik ve Politika Uygulamaları**, 1.Baskı *içinde* (33-47), Nobel Yayıncılık, Ankara.

Tatsumi, Yuki (2018), "Japan's Defense Policy Decisions in 2018", **The Diplomat,** https://thediplomat.com/2018/01/japans-defense-policy-decisions-in-2018/ (11.10.2021).

Terzi, Mahir (2018), "Bilgi İletişim Teknolojilerine Dayalı Oluşumlar ile Bu Oluşumların Uluslararası İlişkilere Güvenlik Bağlamındaki Etkisi: Siber Terörizm", **Kara Harp Okulu Bilim Dergisi**, 28(1), 73-108.

The Economist (2021), "Global Democracy Has a Very Bad Year", https://www.economist.com/graphic-detail/2021/02/02/global-democracy-has-a-very-bad-year (16.01.2021).

The Government of Japan (2015), "Cybersecurity Strategy" **National Information Security Policy Council**, https://www.nisc.go.jp/eng/index.html (14.10.2021).

The Japantimes (2015), "U.S. to Take Japan Under Cyberdefense Umbrella as Hacker Threats Grow", https://www.japantimes.co.jp/news/2015/05/31/national/politics-diplomacy/u-s-to-bring-japan-under-cyberdefense-umbrella/ (09.07.2020).

The Ministry of Foreign Affairs of the Russian Federation (2016), "Doctrine of Information Security of the Russian Federation", https://afyonluoglu.org/PublicWebFiles/strategies/Asia/Russia%202016%20Information%20Security%20Doctrine.pdf (21.01.2021).

Theohary, Catherine (2020), "Iranian Offensive Cyber Attack Capabilities", **Congressional Research Service,** https://sgp.fas.org/crs/mideast/IF11406.pdf (16.03.2021).

Thomas, Nicholas (2009), "Cyber Security in East Asia: Governing Anarchy", **Asian Security,** 5(21), 3-23.

U.S Mission to ASEAN (2013), "Statement by the Chairman of the 20th ASEAN Regional Forum", https://asean.usmission.gov/statement-by-the-chairman-of-the-20th-asean-regional-forum/ (18.03.2021).

U.S. Deparment of Defense (2013), "Cyberspace Operations", https://irp.fas.org/doddir/dod/jp3_12r.pdf (14.09.2021).

UAB (2016), "2016-2019 Ulusal Siber Güvenlik Stratejisi", hgm.uab.gov.tr/uploads/pages/siberguvenlik/2016-2019guvenlik.pdf (07.06.2021).

Uçar, Ozan (2017), "Yeni Nesil Küresel Savaş: Siber Saldırılar", **BGA Security**, https://www.slideshare.net/bgasecurity/kresel-siber-sava (17.09.2020).

Ulutaş, Güzin (2018), "Siber Güvenlik", Sağıroğlu ve Alkan (Ed.), **Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık,** 1.Baskı *içinde* (87-101), Grafiker Yayınları, Ankara.

United Nations, (2019), "Group of Governmental Experts", https://www.un.org/disarmament/group-of-governmental-experts/ (17.09.2021).

United Nations Digital Library (1998), "UN. General Assembly (53rd session)", https://digitallibrary.un.org/record/265311#record-files-collapse-header (19.07.2021).

Üçarol, Rifat (2015), **Siyasi Tarih,** 1.Cilt, Der Yayınları, İstanbul.

Varlık, Ergün (2019), "Japonya'ya Yönelik Bir Siber Saldırı ABD'yi Savaşa Sokabilir", **Siber Bülten,** https://siberbulten.com/uluslararasi-iliskiler/abd/japonyaya-yonelik-bir-siber-saldiri-abdyi-savasa-sokabilir/ (07.06.2021).

Vinny Halo (2021), "What Tech Firms Need To Know About China's New Phase of Development", **China Internet Report Retail in Asia**, https://retailinasia.com/uncategorized/china-internet-report-2021-what-tech-firms-need-to-know-about-chinas-new-phase-of-development/ (21.06.2021).

Vision of Humanity (2021), "2021 Global Peace Index", https://www.visionofhumanity.org/maps/ (17.09.2021).

Walkowski, Debbie (2019), "What Is the CIA Triad?", **F5 Labs** https://www.f5.com/labs/articles/education/what-is-the-cia-triad (24.08.2021).

Walt, Stephen (1991), "The Renaissance of Security Studies", **International Studies,** 35(2), 211-239.

Waltz, Kenneth (1988). "The Origins of War in Neorealist Theory", **The Journal of Interdisciplinary History,** 14(8), 615-628.

Webteknohaber (2021), "Milyonlarca Yemeksepeti Kullanıcısının Verilerini Çaldığını İddia Eden Hackerlardan Tehdit Niteliğinde Açıklama", https://www.webtekno.com/yemeksepeti-hackerlardan-aciklama-h117344.html (24.09.2021).

Wei, Yuxi (2016), "China-Russia Cybersecurity Cooperation: Working Towards Cyber-Sovereignty", https://jsis.washington.edu/news/china-russia-cybersecurity-cooperation-working-towards-cyber-sovereignty/ (19.09.2021).

Weimann, Gabriel (2004), **Cyberterrorism: How Real Is the Threat?,** United States Institute of Peace, Washington.

Wheatley, Gary ve Hayes, Richard (1996), **Information Warfare and Deterrence,** NDU Press Book, Washington.

Wilkinson, Paul (1979), **Terrorism and The Liberal State,** New York University Press, New York.

Wolfers, Arnold (1952), "National Security as an Ambiguous Symbol", **Political Science Quarterly,** 67(4), 481-502.

Wohlforth, William (1999), "The stability of a Unipolar World", **International Security**, 24(1), 5-41.

Wylie, Christopher (2018), "Cambridge Analytica Must Answer to India or "Face The Consequences", https://www.cnbc.com/2018/07/11/cambridge-analytica-must-answer-india-says-minister-prasad.html (14.08.2021).

Yalçın, Hasan Basri (2015), "Uluslararası Sistem ve İstikrar: Kavramsal Bir Değerlendirme", **Akademik İncelemeler Dergisi**, 10(1), 209-229.

Yalman, Yıldıray (2018), "Siber Terör, Terörizm ve Mücadele", Sağıroğlu ve Alkan (Ed.), **Siber Güvenlik ve Savunma: Farkındalık ve Caydırıcılık,** 1.Baskı *içinde* (259-280), Grafiker Yayınları, Ankara.

Yayla, Atilla (2015), "Terör ve Terörizm Kavramlarına Genel Bakış", **Ankara Üniversitesi SBF Dergisi,** 45(1), 335-385.

Yayla, Mehmet (2013), "Uluslararası Hukukta Siber Saldırılara Karşı Kuvvet Kullanma", **Türkiye Barolar Birliği Dergisi,** 107, 200-220.

_____ (2014), "Siber Savaş ve Siber Ortamdaki Kötü Niyetli Hareketlerden Farkı", **Hacettepe Hukuk Fakültesi Dergisi,** 4(2), 181-200.

Yener, Yavuz (2015), "8. Yılında Estonya Saldırılarına Çok Boyutlu Bir Bakış", **Siber Bülten,** https://siberbulten.com/siber-saldirilar-2/8-yilinda-estonya-saldirilarina-cok-boyutlu-bir-bakis/ (19.10.2020).

Yener, Zafer (2013), **Siber Uzay Güvenliği: Ulusal Güvenlik Ve Uluslararası Güvenliğe Etkileri,** Yayınlanmamış Yüksek Lisans Tezi, Uludağ Üniversitesi - Sosyal Bilimler Enstitüsü

Yılmaz, Adem (2020), "İran'ın Siber Güvenlik Politikası", Fulya Köksoy (Ed.), **Yeni Küresel Tehdit: Siber Saldırılar Siber Güvenlik ve Politika Uygulamaları,** 1.Baskı *içinde* (365-378), Nobel Yayıncılık, Ankara.

Yılmaz, Birkan Anıl (2020), "Siber Terörizm ve Değişen İstihbarat Anlayışı", **Anadolu Strateji Dergisi,** 2(1), 65-81.

Zhang, Li (2012), "A Chinese Perspective On Cyber War", **International Review of The Red Cross,** 94(886), 801-807.

Zhao, Leo ve Xia, Lulu (2018), "China's Cybersecurity Law: An Introduction for Foreign Businesspeople", **China Briefing**, https://www.china-briefing.com/news/chinas-cybersecurity-law-an-introduction-for-foreign-businesspeople/ (19.08.2021).

Ziolkowski, Katharina (Ed.) (2013), **Peacetime Regime for State Activities in Cyberspace: International Law, International Relations and Diplomacy**, 1st Edition, NATO CCD COE Publication, Tallinn.

ÖZGEÇMİŞ

Muhammed Resul EROĞLU, 2008 yılında Mustafa Necati İlkokulu'nu; 2011 yılında Gazi Ortaokulu'nu; 2015 yılında Konak Anadolu Lisesi'ni; 2019 yılında da Karadeniz Teknik Üniversitesi Üniversitesi – İktisadi ve İdari Bilimler Fakültesi, Uluslararası İlişkiler Bölümü'nü "onur öğrencisi" unvanıyla bitirdi. 2019 yılında Karadeniz Teknik Üniversitesi – Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Anabilim Dalında yüksek lisans programına başladı.

EROĞLU, bekar olup, İngilizce bilmektedir.