

KARADENİZ TEKNİK ÜNİVERSİTESİ * SOSYAL BİLİMLER ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER ANABİLİM DALI

TEZLİ YÜKSEK LİSANS PROGRAMI

SİBER ALANIN GÜVENLİKLEŞTİRİLMESİ:
NATO ÖRNEĞİ

YÜKSEK LİSANS TEZİ

Ferhat KAYA

KASIM-2024

TRABZON

KARADENİZ TEKNİK ÜNİVERSİTESİ * SOSYAL BİLİMLER ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER ANABİLİM DALI

TEZLİ YÜKSEK LİSANS PROGRAMI

**SİBER ALANIN GÜVENLİKLEŞTİRİLMESİ:
NATO ÖRNEĞİ**

YÜKSEK LİSANS TEZİ

Ferhat KAYA

Tez Danışmanı: Doç. Dr. Erol KALKAN

KASIM-2024

TRABZON

ONAY

Ferhat KAYA tarafından hazırlanan “Siber Alanın Güvenikleřtirilmesi: NATO Örneęi” bu Çalışma 25.11.2024 tarihinde yapılan savunma sınavı sonucunda oybirlięi / oyçokluęu ile başarılı bulunarakjürimiz tarafından Uluslararası İliřkiler Ana Bilim Dalı Tezli Yüksek Lisans Programı’nda **yüksek lisans tezi** olarak kabul edilmiřtir.

Jüri Üyesi		Karar		İmza
Unvanı - Adı ve Soyadı	Görevi	Kabul	Ret	
Doç. Dr. Erol KALKAN	Başkan	☐	☐	
Doç. Dr. Vahit GÜNTAY	Üye	☐	☐	
Doç. Dr. Burak HERGÜNER	Üye	☐	☐	

Yukarıdaki imzaların, adı geçen öğretim üyelerine ait olduklarını onaylarım.

Prof. Dr. Haydar AKYAZI

Enstitü Müdürü

BİLDİRİM

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

25.11.2024

Ferhat KAYA

ÖNSÖZ

Yüksek lisansımın ikinci yılında aldığım Siber Politikalar dersi sayesinde ilgimi çeken bu konu dünyaya olan bakış açımı değiştirmiş ve siber alan üzerine çalışmalar yapmama sebep olmuştur. Normal dünyadan daha büyük bir yapıda olan siber alanla ilgili hazırladığım bu çalışmada ilk teşekkürü danışmanım ayrıca hocam Doç. Dr. Erol Kalkan'a borç bilirim. Sonrasında Siber Alan dersi hocam Doç. Dr. Vahit Güntay hocama, eğitim hayatım boyunca bana olan inancını ve desteğini hiçbir zaman esirgemeyen annem Serpil Kaya, babam Refik Kaya ve kardeşim Abdulsamet Kaya'ya, tez döneminde desteğini hiçbir zaman benden esirgemeyen nişanlım Elif Elçi ve sevgili ailesine, içerik bakımından zenginleşmesinde bana kaynak sağlayan arkadaşım Hamza Birlik'e, destekleri ile yanımda olan sevgili iş arkadaşlarıma ve İstanbul İhracatçılar Birliği Genel Sekreterliğine teşekkür ederim.

Kasım, 2024

Ferhat KAYA

İÇİNDEKİLER

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

BİRİNCİ BÖLÜM

1.Kopenhag Okulu ve Güvenlikleştirme	6
1.1.Güvenlik Kavramı.....	6
1.2.Güvenlik ve Devlet	7
1.3.Güvenliğin Kapsamının Genişlemesi.....	8
1.4.Kopenhag Okulu	9
1.5.Güvenlikleştirme Teorisi.....	11
1.5.1.Güvenlikleştirmenin Unsurları	11
1.5.2.Söz-Edim	13
1.5.3.Güvenlikleştirmenin Temel Değerleri ve Süreci	14

İKİNCİ BÖLÜM

2.Siber Alan ve Siber Güvenlik.....	18
2.1.Siber Alan	18
2.2.Siber Alanın Ortaya Çıkışı ve Gelişimi	19
2.3.Siber Alanın Yapısı.....	21
2.4.Siber Güvenlik	23
2.4.1.Siber Alana Yönelik Tehditler.....	23
2.5.Siber Güvenliği Zorlukları.....	24
2.6.Siber Saldırıların Güvenlikleştirmeye Uygunluğu.....	27
2.6.1.Askerî Alanda Siber Güvenlik	28

2.6.2.Ekonomik Alanda Siber Güvenlik.....	28
2.6.3.Siyasi Alanda Siber Güvenlik	29
2.6.4.Toplumsal Alanda Siber Güvenlik	30
2.6.5.Çevresel Alanda Siber Güvenlik	32
2.6.6.Siber Alanın Güvenlikleştirmeye Uygunluk Derecesi	33

ÜÇÜNCÜ BÖLÜM

3.Kuzey Atlantik Anlaşması Örgütü ve Siber Alan.....	35
3.1.NATO’nun Kuruluşu	35
3.2.NATO’nun Soğuk Savaş Dönemindeki Stratejisi.....	40
3.3.Soğuk Savaş Sonrası NATO	44
3.4.NATO’nun 5. Maddesi ve ABD ve Büyük Britanya’nın Siber Politikaları.....	47
3.4.1.NATO’nun 5. Maddesi.....	48
3.4.2.ABD’nin Siber Alan Politikası.....	49
3.4.3.Birleşik Krallık’ın (BK) Siber Politikası.....	55
3.5.Siber Alanın NATO Radarına Girme Süreci	57
3.6.Hibrit Savaşlar Sonrası NATO’nun Savunma Mekanizması.....	58
3.7.NATO’nun Siber Savunma Stratejileri.....	59
3.8.NATO’da Siber Alanın Güvenlikleştirilmesi	60
SONUÇ ve ÖNERİLER	64
KAYNAKÇA.....	67
ÖZGEÇMİŞ.....	75

ÖZET

21. yüzyılda uluslararası arenada bulunan aktörler için güvenlik son derece önemli bir konumdadır. Aktörler için güvenlik kadar önemli bir şey varsa o da zaman ve bilgidir. Bilginin güvenliği ve zaman anlamında sürekli erişilebilir olması ise günümüzde en kritik unsurlar olarak kabul edilir. Bilgi güvenliği, geleneksel güvenlik anlayışlarının yanında günümüzde genişleyen güvenlik yaklaşımları için de son derece elzemdir. Bu yüzden bilgi güvenliği aktörlerin oldukça önem verdiği bir konu olmuştur. Bilgiyi güvenli tutarken ulaşılabilir kılmak da gereklidir. Bu bilginin güvenliği zorlaştırmaktadır. Teknolojik gelişmeler gün geçtikçe hızlanmakta ve normal hayat akışındaki yaptığımız tüm işler artık teknoloji sayesinde somut varlıklar vasıtasıyla yapılabilmektedir. Somut vardıkların ağ sistemleri ile oluşturduğu bu yapı siber alan oluşturmuştur. Bu yapı bilginin depolanması ve sürekli erişilebilir olması açısından ve zaman tasarrufu bakımından oldukça kolaylık sağlamıştır. Ancak güvenli şekilde saklanması ve erişilebilirliğinin sürekli olması açısından güvenlik sorunlarını da beraberinde getirmiştir. Teorik altyapısında Kopenhag Okulu olan bu çalışmada, teknolojinin gelişmesi ile her geçen gün artan bu siber güvenlik sorununa odaklanılmıştır. Siber alanın güvenlileştirme teorisi ile ilişkisinin hangi seviyede olduğu ve güvenlileştirmeye uygun olup olmadığına odaklanılmıştır. Bu incelemeye örnek olarak ise Soğuk Savaş sonrası yeni güvenlik konseptleri geliştirerek kendini güncelleyen NATO'nun siber alana bakışı incelenmiştir. Dünyadaki en büyük güvenlik örgütü olan ve üyelerinin çoğu büyük devletler olan bu örgütün siber alana yaklaşımı genel dünyanın yaklaşımını bizlere sunacaktır.

Anahtar Kelimeler: Kopenhag Okulu, Güvenlileştirme, Siber Alan, Siber Güvenlik ve NATO

ABSTRACT

In the 21st century, security is extremely important for actors in the international arena. If there is anything as crucial as security for actors, it is time and information. The security of information and its constant accessibility are considered the most critical elements today. Information security is essential not only for traditional security paradigms but also for expanding security approaches today. Therefore, information security has become an issue that actors attach great importance to. While keeping information secure, it is also necessary to make it accessible, which makes the security of information difficult. Technological developments are accelerating rapidly, and much of what we do in our daily lives can now be accomplished through tangible assets thanks to technology. This structure, formed by tangible assets connected through network systems, has created cyberspace. It has greatly facilitated information storage, constant accessibility, and time savings. However, it has also introduced challenges related to secure storage and continuous accessibility. This study, grounded in the Copenhagen School theoretical framework, explores the escalating cybersecurity issues driven by technological development. It focuses on the level of the relationship between cyberspace and securitization theory, and whether it is suitable for securitization. As an example of this examination, NATO's view of cyberspace, which updates itself by developing new security concepts after the Cold War, is examined. The approach of this organization, which is the largest security organization in the world and whose members are mostly major states, will provide us with insight into the global perspective.

Keywords: Aberystwyth School, Securitization, Cyberspace, Cyber Security and NATO

TABLÖLAR LİSTESİ

Tablo Nr.	Tablo Adı	Sayfa Nr.
1	Kopenhag Okulunda Yer Alan Süreçler	16
2	Kopenhag Okulunun Geleneksel Yaklaşımdan Ayrılan Yönleri	16
3	Siber Alandaki Kritik Çevresel Sektörler ve Faaliyet Alanları	32



KISALTMALAR LİSTESİ

AB	: Avrupa Birlięi
ABD	: Amerikan Birleşik Devletleri
AGİT	: Avrupa Güvenlik ve İş Birlięi Teşkilatı
ARPA	: İleri Araştırma Projeleri Ajansı
ARPANET	: İleri Araştırma Projeleri Ajansı Aęı
BDT	: Baęımsız Devletler Topluluęu
BK	: Birleşik Krallık
BM	: Birleşmiş Milletler
BMGK	: Birleşmiş Milletler Güvenlik Konseyi
CCDCOE	: NATO Siber Savunma Mükemmeliyet Merkezi
CDMB	: Siber Savunma ve Yönetim Kurulu
CDMA	: Siber Savunma Yönetim Başkanlıęı
CyOC	: Siber Operasyonlar Merkezi
DDoS	: Hizmet Dışı Bırakma
FTP	: Dosya Aktarım Protokolü
ICBM	: Kıtalararası Uzun Menzilli GÜdümlü Füze
IRBM	: Orta Menzilli GÜdümlü Füzeler
MACIA	: Askeri Otoriteler ve Muhabere ve Bilgi Sistemleri Ajansı
MAD	: Karşılıklı Kesin İmha
MC	: Milletler Cemiyeti
MITS	: Mikro Enstrümantasyon ve Telemetry Sistemleri
NATO	: Kuzey Atlantik Anlaşması Örgütü
NCW	: Aę Merkezli Savaş
NCIRC	: NATO Bilgisayar Olaylarına Müdahale Birimi
NC3A	: NATO İstişare, Komuta ve Kontrol Ajansı
NNEC	: NATO Aę ile Etkinleştirilmiş Güç Programı
OPEC	: Petrol İhraç Eden Ülkeler Örgütü
PCCIP	: Kritik Altyapıların Korunması için Başkanlık Komisyonu

PSP : Paket Deęiřim Protokolü
SACT : Transformasyon Yüksek Müttefik Komutanlığı
SSCB : Sosyalist Sovyet Cumhuriyetler Birlięi
STRATCOM : Amerika Birleşik Devletleri Stratejik Komutanlığı'na
TCP : Gönderim Kontrol Protokolü
WHCC : Beyaz Saray Siber Güvenlik Koordinatörü
UNIRAS : Birleşik Olay Müdahale ve Uyarı Hizmeti



GİRİŞ

Teknolojik gelişmelerle birlikte dünya ile bağlantılı bir sanal dünya oluşmuştur. İnsanların gerçek hayatta faaliyette bulunduğu ekonomiden sağlık sistemlerine kadar birçok kritik alan bu oluşan siber dünyaya entegre edilmiş veya edilmeye devam etmektedir. İnsanlar açısından bu siber alan, birçok kolaylık sağlamış ve dünyada en kıymetli şeyler olan zaman ve bilgi için çok önemli bir alan olmuştur. Zaman bakımından baktığımızda işlemlerin sanal ağlar üzerinden yapılabilir hale gelmesi insanlar, kurumlar ve devletler için oldukça zamandan tasarruf edebilme imkânı sağlamaktadır. Bilgi açısından ise bilgiye ulaşmak ve bilgiyi depolamak çok kolay olmuştur. 21. yüzyılda bu iki olgu en kıymetli şeyler olarak karşımıza çıkmaktadır. Siber alanın bu kıymetli değerlere yönelik avantajlar sağlaması alanın değerini artırmış ve her alanda entegrasyon süreçlerini teşvik etmiştir.

Getirdiği büyük yenilikler ve katkılara rağmen siber alan güvenlik problemlerini de beraberinde getirmiştir. Gün geçtikçe alana olan entegrasyonun artması ve teknolojinin gelişmesiyle birlikte bu güvenlik sorunu daha büyük problemler yaratmaktadır. Uluslararası arenada bulunan bütün aktörler bu sorunlardan etkilenmektedir. Bu yüzden devletler ve uluslararası örgütler dâhil uluslararası aktörler, 20. yüzyılın sonlarından başlayarak bu güvenlik zafiyetleri ile ilgilenmeye başlamışlardır.

Çalışma bu aktörlerden biri olan Kuzey Atlantik Anlaşması Örgütü'nün (NATO) incelenmektedir. NATO, Soğuk Savaş sonrası varlığı tartışılan ancak kendini birçok alanda güncelleyen bir örgüt olmuştur. Kendisine yeniden stratejik konseptler oluşturan NATO için, siber alan yarattığı güvenlik sorunları yüzünden iyi bir kaynak olmuştur. NATO, güvenliğin artık bilgi ve zaman merkezli bir yapıda olduğunun farkında olarak siber alanda yaratılacak avantajlar ve dezavantajlara göre siber alanda güç kazanma isteğinde olmuştur. Özellikle üye ülkelerinin de bu farkındalığa sahip olması bu yaklaşımın benimsenmesinde önemli bir unsurdur.

Siber alan, içinde barındırdığı ve gelecekte barındıracağı düşünülen unsurlarla birlikte güvenlik anlamında neredeyse tüm alanları içine dâhil edebilme potansiyeline sahiptir. Ancak devletler için önemli olan; kritik öneme sahip ve varoluşsal tehdit yaratacak sorunlardır. Bu görüş aynı zamanda Kopenhag Okulu akademisyenleri tarafından savunulan güvenlik anlayışı ile örtüşmektedir. NATO'nun güvenlik örgütü olması ve uluslararası arenada büyük devletler olarak

adlandırılan devletleri bünyesinde barındırması, siber alanın güvenlikleştirilme genelleme açısından önemli bir ışık olacağı düşünülmüştür. Ayrıca yapısından dolayı devletlerin görüşlerin yansıtmaktadır. Yani NATO'nun politikaları üye devletlerin politikaları ile uyumaktadır. NATO'nun siber alana bakışı bizlere üye ülkelerin de bakışını nispeten de olsa sunacaktır.

Geleneksel teorilere yapılan eleştirilerle 20. yüzyılın sonlarından itibaren yeni teoriler literatürde konuşulmaya başlanmıştır. Bu yeni teorilere Eleştirel Teoriler denilmiştir. Eleştirel teoriler ve geleneksel teorilerin ortasında yer alan ve üçüncü bir yol olarak kendisini tabir eden Kopenhag Okulu'nun güvenlikleştirme teorisi savunduğu fikirlere baktığımızda siber güvenlik açısından oldukça ilişkili olduğu anlaşılmaktadır. Çalışmada aktarılacak istenen bir diğer unsur da bu yakınlık olacaktır. Kısaca değinmek gerekirse çalışma siber alanın gelişimi, siber alan ile güvenlikleştirme arasındaki uyumun ortaya çıkarılması, NATO'nun Soğuk Savaş sonrası kendini güncellemesi ve siber alanı nasıl güvenlikleştirdiği olguları üzerinde bir araştırmadır.

Araştırmanın Problemi

Araştırma; son dönemlerde popüler konular olan siber güvenlik ve güvenlikleştirme teorisini incelemekte, siber alanın güvenlikleştirmede tehdit objesi olmaya oldukça uygun olduğunu göstermeye çalışmaktadır. Siber alan neden güvenlikleştiriliyor ve hangi unsurlara dayandırılıyor sorunsalı ele alınacaktır. Bu sorunsal uluslararası güvenlik örgütü olan NATO üzerinden bakılacaktır. NATO siber alanı güvenlikleştirme örneği olmasının sebebi, Soğuk Savaş sonrası güvenlik temelli kurulmuş örgütlerin güvenlikleştirme teorisinde olduğu gibi askeri alan dışında farklı alanlarda güvenlik yaklaşımları sergileme çabasının açık örneği olmasıdır. Ayrıca araştırma uluslararası güvenlik örgütlerinin Soğuk Savaş sonrası tartışılan varlıklarına yönelik probleme odaklanacaktır.

Araştırmanın Amacı ve Kapsamı

Araştırma, üç amaca yöneliktir. Birinci amacı, NATO örneği üzerinden siber alanın güvenlikleştirildiğini, bu güvenlikleştirme sırasında kullanılan unsurların nelere dayandırıldığını ortaya koymaya çalışmaktadır. İkinci amacı siber alanın güvenlikleştirilme için oldukça uygun bir yapıya sahip olduğunu kanıtlamak istemektir. Son amacı ise uluslararası örgütlerin özellikle savunma örgütlerinin Soğuk Savaş sonrası kendilerini revize ederek nasıl hayatta kalmaya çalıştıklarını göstermektir. NATO, hem güvenlikleştirme bazlı hem de örgütsel bazlı örneklem olup genelleme için iki odağın da ortak kümesinde yer almaktadır.

Araştırma Soruları

Araştırmanın ana sorusu "Siber alan neden ve nasıl güvenlikleştiriliyor mu?" sorusuna NATO örneği üzerinden genelleme yaparak cevap vermektir. Bu soruya yanıt aranırken araştırmanın

bölümlerinde bazı alt sorular sorularak ana sorunun cevabı bulunmaya çalışılmıştır. İlk bölüm teori olduğu için sadece “Güvenlikleştirme teorisi nedir ve askeri alan dışında hangi alanlar güvenlik konusu yapılabilir?” sorusunu barındırmaktadır. İkinci bölümde “Siber alan ve siber güvenlik nedir?”, “Siber alan güvenlikleştirilme için uygun mudur?” ve “Siber alan neden güvenlikleştirilmeli?” sorularına yanıt aranmıştır. Üçüncü bölümde ise “NATO, Soğuk Savaş sonrası güvenlik alanında hangi konularda kendisini revize etmiştir?”, “NATO, Soğuk Savaş sonrası hangi alanlarda güvenlik çalışmaları yürütmektedir?”, “NATO üyesi devletlerin siber alana bakış açıları nasıldır?” ve “NATO’ üyesi hangi devletler siber alanı güvenlikleştirme politikası uygulamaktadır?” sorularına cevap aranmıştır.

Teorik Çerçeve ve Savlar

Kopenhag Okulunun Güvenlikleştirme teorisi çalışmanın teorik alt yapısıdır. Teorinin hangi dönemde kimler tarafından geliştirildiği ve geleneksel teorilerden farkları ortaya konarak günümüzdeki güvenlik yaklaşımlarına ne gibi katkıları olduğuna değinilmiştir. Böylece çalışmanın ana merkezinde yer alan siber alanın güvenliğe konu olmasının sebepleri ve uluslararası örgütlerin güvenlik konusunda ne gibi değişimler sergilediği daha net şekilde ortaya konmaya çalışılmıştır. Bu teorik alt yapının yanında ortaya konan savlarla araştırma sorusunun cevabına ulaşmak hedeflenmiştir. Araştırmanın savları şunlardır:

- Siber alan, güvenlikleştirme teorisinde yer alan ana güvenlik başlıklarının hepsi için ayrı ayrı tehditler barındırmaktadır.
- Siber alan saldırı yapan için oldukça kolay ve düşük maliyetli fırsatlar sunarken, savunan tarafından oldukça zor ve maliyetli bir alandır. Bu yüzden siber saldırılar yeni bir saldırı silahı olarak karşımıza çıkmaktadır.
- Siber alan diğer iki savlardan ötürü güvenlikleştirilme açısından oldukça uygun yapıya sahiptir.
- Devletlerarası uluslararası örgütlerin politikaları daha çok örgüte üye büyük devletlerin (ekonomik, siyasi ve askeri anlamda güçlü) politikaları ile benzerdir.

Araştırmanın Metodolojisi

Araştırma, bir örnek üzerinden inceleme yaparak, bir merkezden birçok veri elde etmeye çalışılacaktır. Seçilen örnek hem uluslararası örgüt hem de siber alan için ortak kümede yer alan bir örnektir. Örnek olay ayrıntılı şekilde incelenerek siber alanın güvenlikleştirilmesi ve uluslararası örgütlerin değişen güvenlik yaklaşımları açıklanacaktır. Ayrıca nitel araştırma yönteminden faydalanmıştır. Veriler doküman taranması ve araştırma örneği olan NATO ve üye ülkelerinin siyasi elitlerinin söylemleri ile güvenlikleştirici aktörlerin konuşmalarının incelenmesi sonucu elde edilecektir. Elde edilen veriler arasındaki bağ değerlendirilecek ve böylelikle araştırma sorusuna

cevap aranacaktır. Söylem üzerine kurulu bir teorik alt yapı tercih edileceği için siyasi elitlerin söylemleri ayrıntılı şekilde incelenecek ve yorumlanacaktır. Bu yüzden toplantılarda yapılmış konuşmalar, verilmiş röportajlar, ikili ve çoklu görüşmeler sonrası yapılmış bildirimler veri olarak kullanılacaktır. Bu verilerin kimler tarafından söyleme aktarıldığı ve hangi amaçların hedeflendiği soruları, verilerin belirlenmesinde ana hedef sorular olacaktır. Yani teorik alt yapı bu noktada ön plana çıkacaktır.

Bu kapsamda kullanılacak olan kaynaklar; metinler (Kitaplar, bilimsel dergiler, raporlar, yayınlanan bildiriler, süreli yayınlar, gazete vb.), söylemler (Röportajlar, televizyon ile radyo programları vb.), istatistik veriler ve araştırmanın ileriki safhalarında ihtiyaç duyulacak diğer kaynaklardır. Verilerden elde edilecek birincil ve ikincil kaynaklar ile söylemsel analizler birleştirilerek kuramsal çerçevede yorumlanacak ve araştırma sorusuna cevap aranacaktır.

Araştırmanın Değişkenleri

Araştırmada bağımsız değişken; siber alanın güvenlikleştirilmeye uygun yapısı iken bağımlı değişken ise; siber alanın güvenlikleştirilmesidir. Siber alanın yapısı incelenerek siber alanın güvenlikleştirilmeye uygunluğu analiz edilecektir. Kuzey Atlantik Anlaşması Örgütü ise bu araştırmanın örnekleimidir.

Araştırmanın Önemi

Soğuk Savaş ile birlikte artan güvenlik çalışmaları, Soğuk Savaşın bitmesi ile daha farklı yaklaşımları içine alarak uluslararası ilişkiler disiplininin alt başlıkları altında yerini almıştır. İki kutuplu dünya yapısının sona ermesi ile güvenlik çalışmalarının ilgi odağı değişmiş ve çok yapıli sistemde güvenlik yeniden konumlandırılmaya çalışılmıştır. Araştırma, bu yeni konumlandırma çabalarına bir katkı sunma hedefindedir. Son dönemlerde oldukça tartışılan siber alanın bir güvenlik konusu olduğunu, güvenliğin yeni bir boyut kazandığını savunan Kopenhag Okulu'nun güvenlikleştirme teorisi ile ispat etmek amaçlanmaktadır. Böylece hem siber alanın güvenlik çalışmalarına hem de Kopenhag Okulu güvenlik çalışmalarına katkı sunmak hedeflenmektedir. Bu iki önemli konu, iki kutuplu yapının yıkılmasından sonra varlığı eleştiri konusu olan ve yapılarını güncellemeye çalışan uluslararası örgütlerden olan NATO ile sentezlenerek anlatılmaya çalışılacaktır. Böylelikle bu iki önemli konuya hedeflenen katkının haricinde uluslararası örgüt çalışmalarının güvenlik alanına da katkı sunmak amaçlanmaktadır.

Araştırmanın Bölüm Yapısı

Araştırma bölümlere ayrılmasının yanında bölümsel bazda kısımlara da ayrılacaktır. Bunun temel amacı, konunun daha anlaşılabilir yapıda sunulması isteğidir. Araştırmanın ilk bölümü teorik

çerçeveyi ortaya koyma amacındadır bu yüzden ilk bölümün ilk kısmında güvenlik kelimesi analiz edilecek ve yapısı incelenecektir. Güvenliğin dönemsel olarak hangi anlamlarda kullanıldığı ve kapsamı ele alınacaktır. İkinci kısmında, Kopenhag Okulu'nun ortaya çıkışı, gelişimi, okulun akademisyenlerinin görüşleri incelenecek ve kuramsal çerçeve oluşturulacaktır. Son kısmında ise araştırmanın teorik yapısını oluşturan güvenlikleştirme teorisi incelenecektir. Yine bu kısımda birinci ve ikinci kısımlarda elde edilecek bulgular ile güvenlikleştirme teorisinin temel öğelerinden ve sürecinden bahsedilecektir. Güvenlikleştirmenin yapısından dolayı söylemsel analizden bahsedilerek teorisinin söylemsel yanına değinilecek, güvenlikleştirme aşamasının hangi unsurlarla nasıl yapılacağı ortaya konulacaktır.

İkinci bölümde ise siber alan ele alınacaktır. Bu bölümün ilk kısmında siber alanın kelime anlamı, ortaya çıkışı ve gelişiminden söz edilecek, ikinci kısımda siber güvenlik kelimesinin anlamı ile güvenlik anlamında zorluklarına değinilecektir. Bu bölümün son kısmında ise siber güvenlik ile güvenlikleştirme arasındaki bağdan söz edilecektir. Araştırmanın üçüncü ve son bölümünün ilk kısmında örneklem olarak seçilen NATO'nun kuruluş ve tarihinden söz edilecek, bölümün ikinci kısmında NATO'nun Soğuk Savaş sonrası sorgulanması ve güvenlik anlamında yeni bir temele oturtulma çabaları güvenlikleştirme teorisi üzerinden anlatılacak ve son kısmında ise NATO'nun siber alanı güvenlikleştirme eylemi analiz edilecektir.

BİRİNCİ BÖLÜM

1. KOPENHAG OKULU VE GÜVENLİKLEŞTİRME

1.1. Güvenlik Kavramı

Kopenhag Okulunun güvenliğe yaklaşımına değinmeden önce güvenlik kavramının nasıl algılandığına, ne anlama geldiğine ve zaman içerisinde kapsamının nasıl genişlediğine değinilmelidir. Güvenlik kavramının kökeni Latince securitas kelimesidir. Latince se (olmaksızın) ve cura (endişe) kelimelerden türetilen securitas kelimesi tercüme edildiğinde “endişeden uzak olma ve sükûnet” anlamına gelmektedir (Arends, 2009: 5). Yunan tarihinde ise asphaleia kelimesi “yenilgi karşı güvenlik” anlamında güvenlik kelimesine yakın bir anlamda kullanılmıştır (Thucydides, 2000: 42). Bu iki medeniyette bu kavram bir nevi savaştan uzak olma anlamında kullanılmıştır. Bunun başlıca nedeni o dönemlerde sürekli savaşların olmasıdır.

Günümüz uluslararası ilişkiler literatüründe ise güvenliğin tanımı hakkında bir fikir birliğinden söz edilemez. Bu konuda çeşitli görüşler vardır. Buzan’a göre güvenlik “sevgi, güç, özgürlük gibi anlamı farklılaşabilecek” kavramlardan biridir (Buzan, 2015: 7). McSweeney ise güvenliğin tanımlanmasının zor olduğunu dile getirerek “Tıpkı adalet, barış, onur gibi bir kavram olduğunu ve tanımlanmaya direnen bir yapıya sahip olduğunu” ifade etmiştir (McSweeney, 1999: 14). Anlam olarak farklılaşmasının en büyük nedenlerinden biri başına veya sonuna aldığı kavramlar ile yeni anlamlar ortaya çıkartabilme özelliğidir. Ayrıca aynı güvenlik tamlaması kişiden kişiye farklı algılanabilir. Mesela; ekonomik güvenlik kavramı bazı kişiler için geçim sağlayacak bir paranın varlığını ifade ederken bazı kişiler için çeşitli ekonomik saldırıları veya ekonomik stabiliteyi ifade etmektedir.

Güvenlik, ayrıca gündelik hayatta birçok konuda karşımıza çıkabilir. Ancak her alanda farklı bir boyutta karşımıza çıkar. Örneğin; ulusal güvenlik anlayışı bir toplumu kapsarken, bireysel güvenlik ise toplumdaki her bir bireyi ayrı ayrı ele alır. Kısacası güvenlik bazı alanlarda aynı anlamı ifade edebilirken kapsam olarak farklı olabilir (Küçükşahin, 2006: 27). Bu güvenliğin neleri kapsadığının belirlenmesini zorlaştırır çünkü kapsamı her çalışma için farklı olabilir. Güvenlik kavramını tamamlayan kavram tehdit kavramıdır. Tehdidin olmadığı bir düzende güvenlik kavramının gelişimden söz edilemez. Tehditlerin varlığı güvenliğin de varlığını ortaya çıkarmaktadır (Sancak, 2013: 124). Tehdit de değişkenlik gösteren bir kavramdır. Olay, zaman ve

kişiler bakımından farklılık gösterir ancak ortak noktası tehditlerin her zaman yöneldiği bir nesne vardır. Bu nesneye güvenlik çalışmalarında referans nesne adı verilir. Referans nesneler güvenliğin korumayı amaçladığı en önemli varlıktır. Bu nesneler her tehdit için farklılık gösterebilir. Bazen ulusal güvenlik için referans nesne toplumsal sağlıktır bazen ise çevresel sağlıktır. Yani güvenlik, nesnel bir kavram olmaktan ziyade öznel bir anlam taşımaktadır. Ancak genel anlamda “temel değerlere karşı tehdidin yokluğu olarak” tanımlanabilir (Baysal ve Lüleci, 2015: 65). Temel değerler Soğuk Savaş’ın sonuna kadar devletin varlığı olarak düşünülmüş ve güvenlik, askeri tehditlerin yokluğu olarak algılanmıştır. Soğuk Savaş sonrası ise birçok temel değer var olduğu ve bu değerlerin değişkenlik gösterebileceği eleştirel teoriler tarafında ileri sürülmüştür. Bu açıdan günümüzde hala anlamı tartışılmaktadır ancak genel itibari ile birey, kurum ve devletlerin çekindikleri bir durumdan uzak olmasını ifade etmektedir.

1.2. Güvenlik ve Devlet

Güvenlik insan tarihi boyunca var olmuş bir kavramdır. Devlet ise insanların bir araya gelip oluşturdukları bir yapıdır. İnsanlar doğanın düzensiz yapısından dolayı güvenliklerini sağlamak için bazı özgürlüklerinden vazgeçerek devletler kurmuşlardır (Cohen, 1996: 275). Devlet güvenlik için kurulmuş bir yapıdır. Devlet ile güvenlik arasında ilk andan beri bir bağ vardır. Günümüzde tartışılan iki devlet anlayışı vardır. İlki minimal devlet anlayışı iken diğeri maksimal devlet anlayışıdır. Minimal devlet anlayışı devletlerin asli görevlerini insanların güvenliklerini sağlamak olarak görmektedir. Bu anlayışın tam tersine maksimal devlet anlayışı ise devletlerin kendi çıkarlarının var olduğunu ve uluslararası sistemde devletlerin ayrıca kendi güvenliklerini sağlaması gerektiğini savunmaktadır (Buzan, 2015: 55-59). Westfalia ile oluşan uluslararası sistem ve her geçen gün artan küreselleşme ile birlikte maksimal devlet anlayışı daha ön plana çıkmıştır (Baylis, 2008: 71-73). Ancak iki anlayış da güvenlik ile devlet arasında bir bağ olduğunu kabul etmektedir.

Uluslararası ilişkiler literatüründe yer alan teorilerde güvenlik ile devlet arasındaki bağa değinilmiştir. Hobbes, devletin kuruluş amacını, bireylerin güvenliğini sağlamak ve barış içinde mutlu bir şekilde yaşamalarına katkı sunmak olarak görmüştür. Doğal yaşamın özünde savaş vardır ve savaş sürekli varsayımından yola çıkmış ve devletin kurulum amacını güvenlik sağlamak olarak görmüştür (Arslanel ve Eryücel, 2011: 8). Bu fikirlerden yola çıkarak realistler geleneksel güvenlik anlayışını ortaya çıkarmıştır.

Geleneksel güvenlik Westfalia sonrası devletlerin uluslararası sistemdeki en önemli aktörler olduğunu dile getirmiş, güvenliğin devlet merkezli bir yapıya büründüğünü savunmuşlardır (Baylis, 2008: 71-73). Dünyanın anarşik yapısından dolayı devlet merkezli bir yapının olması gerektiğini ve askeri temelli bir güvenlik anlayışının benimsenmesi gerektiğini savunmuşlardır (Wohlforth, 2009: 11-12). Devlet, güvenliğin merkezinde yer alır ve tehditlerden korunması gereken obje olarak

görülür. Devletin varlığını devam ettirmesi ve tehditlerden uzak olması güvenliğin göstergesi olmuştur. Devlet güvenli ve tehlikelerden uzaksa insanların da güvende ve tehlikeden uzak olduđu görüşü hakimdir (Wohlforth, 2009: 11-12). Devlet kendini güvende hissetmelidir ve gelecek tehditlere karşı koyacak askeri güce sahip olmalıdır. Yani devlet, egemenliğı elinde tutan, tehlikelerin hedefi olan ve tehlikelere karşı önlemler alandır. Bu yüzden gelenekselciler askeri ve siyasi olayları yani güvenliğı “Yüksek Politika” olarak görmüş, ekonomi, sağık ve çevre gibi konuları “Alçak Politika” kapsamında saymışlardır (Wohlforth, 2009: 11-12).

Soğuk Savaş’ın son yıllarında geleneksel güvenlik yaklaşımına karşı bazı eleştiriler ortaya çıkmasına rağmen Soğuk Savaş’ın sonlarına kadar bu anlayış genel kabul görmüştür. Soğuk Savaş sonrası güvenliğin sadece devlet merkezli bir yapıda olmadığı ve birçok alanın da artık güvenlik meselesi olabileceğı tartışılmaya başlanmıştır.

1.3. Güvenliğin Kapsamının Genişlemesi

Özellikle 1970’lerden sonra Eleştirel Güvenlik Yaklaşımlarının ortaya çıkması ile birlikte güvenliğin tanımı değişmiş ve kapsamı genişlemiştir. Güvenlik devletin varlığına yönelik tehditlerin yokluğu yerine birçok konuda tehditlerin yokluğu olarak tanımlanmıştır. Böylece askeri meselelerin yanında cinsiyet, siyasi, ekonomik, çevre gibi günlük hayattaki birçok konu güvenliğin konusu olmuştur. Geleneksel yaklaşımın aksine güvenliğin nesnel bir kavram olmadığı görüşü ön plana çıkmıştır (Ergüven, 2016). Ayrıca küreselleşmenin her geçen gün artması nedeniyle ulusal güvenlik yaklaşımları yerini uluslararası güvenlik yaklaşımlarına bırakmıştır. Terörizm, uyuşturucu madde ticareti, salgın hastalıklar, göç ve benzeri konular uluslararası güvenliğı tehdit eden konular haline gelmiştir.

Bu yeni alanların güvenlik meselesi olması ile birlikte güvenlik kendi içinde dört başlıkta genişletilmiştir. Bunlardan ilki, güvenlik ulusal olmaktan çıkarılıp grup ve birey güvenliğine kadar indirgenmesidir. Yani devletin bir bütün olarak güvenliğından bireylerin güvenliğine geçilmiştir. İkinci genişleme, ulusal güvenlikden ulusüstü güvenliğe geçilmesidir. Açlık, küresel ısınma ve salgın hastalıklar gibi konular ulusüstü bir güvenlik sorunu yarattığı için güvenlik, devletlerin sınır güvenliğından stratosferin güvenliğine kadar genişlemiştir. Üçüncü genişleme, devletler güvenliğı sağlamanın yolunu güçlü askeri kapasiteye sahip olma olarak görmektelerdi, bunun nedeni devletlerin tehdit olarak diğerk devletleri görmesi ve güvenliklerine karşı tehditlerin diğerk devletlerden kaynaklanacağını düşüncesi idi. Yani güvenlik askeri alana sıkışmış bir yapıdaydı. Ancak küreselleşmenin getirdiğı çevresel, ekonomik ve siyasi tehditler için güçlü bir askeri kapasite sahip olmak güvenlik için yeterli olmamıştır ve böylece güvenlik askeri bir konu olmaktan çıkmış, çok boyutlu bir yapı haline gelmiştir. Sonuncu genişleme ise ulus-devlet güvenliğı yerine yerel, bölgesel ve uluslararası güvenlik anlayışının benimsenmesidir. Coğrafi olarak güvenlik daha karmaşık bir yapı haline gelmiştir.

Bu genişleme süreci sonrası nesnel bir alan olmaktan çıkan güvenlik kavramı için yeni sorular akla gelmiştir. “Kime göre, neye göre güvenlik?” sorusu ve güvenliğin kimler tarafından sağlanacağı temel tartışılan noktalar olmuştur. Bu sorulara teorik olarak farklı yaklaşımlar olmuş, bu teorilerden biri de Kopenhag Okulu’dur.

1.4. Kopenhag Okulu

Soğuk Savaş’ın iki kutuplu yapısından dolayı o dönemde güvenlik çalışmaları genel anlamda askeri bir merkeze sıkıştırılmıştır. Devletler öncelikli olarak varlıklarına yönelik tehdit olacak konuları güvenlik konusu olarak görmüşlerdir (Sheehan, 2005). Bu bakış açısının asıl nedenlerinden biri dönemin yapısının bunu gerektirmesidir. Dünya ikiye ayrılmış ve iki tarafta diğer tarafın kendisini yok etme amacıyla olduğunu ileri sürmüştür. Bu sebeplerden dolayı dönemin güvenlik çalışmaları daha çok geleneksel güvenlik yaklaşımına yönelik çalışmalar olan askeri güvenlik çalışmalarıdır (Ji, Zhang, ve Zhang, 2019: 99-107). Bu yönde çalışmaların ön planda olmasının bir diğer sebebi ise nükleer silah stoklarının hızlı bir şekilde artması ve nükleer silahların birden çok devletin eline geçmesidir. Silah stokları bu dönemde en yüksek seviyeye ve dünyayı birden çok kez yok edebilecek sayıya ulaşmıştır (Euronews, 2022). Bu sebeplerden dolayı devletler karşı taraftan gelecek askeri tehditlere odaklanmış ve diğer konuları güvenlik konusu olarak görmemiştir.

Ancak 1973 Petrol İhraç Eden Ülkeler Örgütü (OPEC) ambargosu gelecek adına bir fragman olmuştur. Ambargo sonrası sadece askeri konuların güvenlik meselesi olacağı anlayışı sarsılmıştır. Petrol krizi sonrası ekonomik konuların da güvenlik konuları olarak ele alınması gerektiği savunulmuştur. (Ji, Zhang, ve Zhang, 2019: 99-107). Ancak ekonomik sorunların da devletler için hayati öneme sahip olduğu ortaya çıkmış olmasına rağmen o dönemde yükselen nükleer silahlanma yarışından dolayı bu konuya yönelik çalışmalar sınırlı kalmıştır.

Soğuk Savaş’ın son yıllarında nükleer silahlanma yarışının durulması ve barışa yönelik adımların atılmasıyla diğer konuların da güvenlik meselesi olabileceği tartışmaları tekrardan başlamıştır. İki kutuplu yapının çözülmesi, güvenlik kavramının sınır-ötesi bir hale gelmesi ve küreselleşme sürecinin hız kazanması ile birlikte yeni araştırmalar literatürde boy göstermeye başlamıştır. Bu yönde yapılan araştırmalara “Eleştirel Yaklaşımlar” adı verilmiştir.

Eleştirel yaklaşımlar geleneksel yaklaşımların ileri sürdükleri fikirleri eleştirerek ortaya çıkmıştır. Geleneksel kuramda güvenlik daha çok barış ve savaş ile ilişkilidir (Atmaca vd., 2018: 20). Yani güvenlik daha çok kuvvet kullanımı ile ilişkilendirilmiştir. Kuvveti kullanma yetkisi ise devletlere ait olarak görülmüştür. Bu açıdan bakıldığında geleneksel kuram üçlü bir yapıdan oluşmaktadır. Aktör-Tehdit-Politika üçlüsünde aktörler devletlerdir. Tehditler; karşı devletlerden gelen, varoluşu tehdit edecek saldırılardır. Politikalar ise gelecek tehditlere karşı alınan askeri önlemlerdir. Eleştirel yaklaşımlar bu üçlü yapıyı eleştirmişlerdir. Aktör olarak sadece devletlerin

olmayacağını uluslararası örgütler, sivil toplum örgütleri gibi yapıların da aktör olabileceğini, tehdit olarak sadece askeri konuların değil ekonomik, siyasi, cinsiyet gibi gündelik hayatta var olan birçok konunun da güvenlik alanına dâhil olabileceğini savunmuşlardır. Politikalarda ise kuvvet kullanımı dışında normal siyasi süreçlerin var olabileceğini ortaya koymaya çalışmışlardır.

Soğuk Savaş sonrası bu eleştiriler yaklaşımlarla birlikte birçok yeni sayılabilecek teori, güvenlik alanında çalışmalar yapmıştır. Feminizm, İngiliz Okulu ve Paris Okulu bunların en bilindik örnekleri olmuştur. Bu teorilerle birlikte devlet merkezli bir yapıdan uzaklaşmış, devlet dışı aktörlerin de aktör olabileceği dile getirilmiş ve güvenlik sadece askeri konu olmanın ötesine geçmiştir (Akgül-Açıkçeşme, 2011: 46-47). Kopenhag Okulu ise daha çok bu iki kesimin ortasında yer almış ve üçüncü bir yol olarak ortaya çıkmıştır (Huysmans, 1998: 482). Okul, güvenlik alanına yönelik yaklaşımları farklı bir açıdan açıklamaya çalışmıştır. Geleneksel yaklaşımın aksine güvenliğin devlet merkezli ve askeri konulara indirgenmesine yönelik eleştiriler getirirken, aynı zamanda eleştirel yaklaşımın savunduğu tüm konuların güvenliğin alanına girebileceği görüşüne karşı çıkmıştır (Akgül-Açıkçeşme, 2011: 48).

Kopenhag Okulu, Ole Waever'ın 1995 yılında yazdığı “Güvenikleştirme ve Güvenlikdışılaştırma” makalesi ve Barry Buzan, Ole Waever ve Jaap de Wilde'in yazdıkları “Security: A New Framework for Analysis” kitabı ile literatürde yerini almıştır. Bu çalışmalarda güvenliğin boyutları tartışılmış ve devletlerin güvenlik alanında yaklaşımları ele alınmıştır. Sadece devletlerin güvenlik sorunları ile karşılaşabileceği fikrine karşı toplumların da güvenlik sorunları ile karşılaşabileceğini savunmuşlardır. (Baysal ve Lüleci, 2015: 78) Ayrıca Jaap de Wilde, Morten Kelstrup, Pierre Lemaitre ve Elizabeth Tromer gibi akademisyenler de önemli katkılar sunmuştur.

Kopenhag Okulu, güvenliği “tehditlerin sosyal inşası” olarak görmektedir (Buzan, vd., 1997: 34). Waever'a göre güvenlik, bir tehdidin varlığını ve ona karşı alınan önlemleri ifade etmektedir (Waever, 1995: 56). Bu görüş, okulun da güvenliğe bakış açısını göstermektedir. Kopenhag Okulu, güvenliğin devlet temelli askeri konular ile sınırlandırılmayacağını ancak her konunun da güvenlik meselesi olamayacağını savunmaktadır (Akgül Açıkçeşme, 2011: 66). Bu yüzden Kopenhag Okulu geleneksel güvenlik anlayışı ile post-modern güvenlik yaklaşımının arasında bir konumda yer almaktadır (Baysal ve Lüleci, 2015: 65). Güvenliğe bakış açısında üçüncü bir yol olarak görülmektedir. Güvenliği eskiye göre genişletmiş ancak yeni eleştirel yaklaşımlara göre daraltmıştır. Kopenhag Okulu güvenlik için beş başlık belirlemiştir. Bunlar; askeri, siyasi, ekonomik, çevresel ve sosyal konulardır. Her bir konu kendi içinde farklı özelliklere sahip tehditleri barındırmaktadır. Böylece güvenlik, askeri odak noktasi olmaktan çıkmış ve birçok konuda odaklanılması gereken bir olgu haline gelmiştir.

Böylece güvenliği devlet üzerinden yorumlamak yerine konu ve bağlam bakımından yorumlama yolunu seçmişlerdir. Ayrıca güvenlik konularının kimler tarafından dile getirileceği

üzerine bazı fikirler sunmuşlardır. Güvenlik kavramının genişleyen yapısı ve nesnel olmaktan çıkması sonrası bir meselenin güvenlik konusu olup olmadığına kimin karar vereceği sorusunu akıllara getirmiştir. Waever “Bir şeyi güvenlik problemi yapan nedir?” sorusunu sormuş ve bir konunun güvenlik meselesi olarak siyasi güç sahibi kişi veya yapılar tarafından belirlendiği cevabını vermiştir (Waever, 1995: 55). Yani hangi konuların güvenlik meselesi olacağını siyasi aktörler belirlemektedir. Geleneksel görüşte devlet, temel süje olarak yer alırmakta ve güvenlik konusu devlete yönelik tehditleri içermekteydi. Güvenliğin coğrafi açıdan genişlemesi ve süje olarak bireylere kadar indirgenmesi sonrası nelerin tehdit sayılacağı ve güvenlik konusu ile ilişkilendireceği soruları doğmuştur.

Belirlenen beş alan üzerinde güvenliğin kimler ve hangi unsurlar ile güvenlik sorunu yapıldığını açıklamak isteyen okulun akademisyenleri bir teori ortaya çıkarmışlardır. Güvenlikleştirme, okulun düşünürleri tarafından bir konunun güvenlik sorunu nasıl yapıldığını okulun ana temel düşünceleri çerçevesinde ortaya çıkardıkları teoridir.

1.5. Güvenlikleştirme Teorisi

Kopenhag Okulu akademisyenleri bir konuyu güvenlik boyutuna taşıyan şey nedir ve buna karar veren yetki kimdedir sorusuna cevap olarak güvenlikleştirme teorisini ortaya çıkarmışlardır. Güvenlikleştirme 1995 yılında Waever’ın çalışmaları sonucu uluslararası ilişkilerin teorik yapısına girmiştir. Waever’a göre güvenlikleştirme kavramı “Bir konuyu tehdit kategorisine sokan bir söz edim”dir (McDonald, 2008: 566). Bu düşünce, John L. Austin’in söz edimleri kuramından esinlenmiştir. Söz edimden önce güvenlikleştirmenin unsurlarını açıklamak söz edimin güvenlikleştirme sürecinde nasıl işlediğini daha net gösterecektir. Unsurlardan sonra, Austin’in bu söz edimlerine kısaca değinmek teorinin daha net anlaşılmasına olanak sağlayacaktır.

1.5.1. Güvenlikleştirmenin Unsurları

Güvenlikleştirme sürecinin ana unsuru söz-edimdir. Kopenhag Okulu, güvenliği bir söz edim süreci olarak tanımlar, sordukları “Kim ve ne için güvenlik” sorularının cevabının bu süreçten sonra ortaya çıktığını düşünmektedirler. Söz-edimin ne olduğunu açıklamadan önce güvenlikleştirmenin içinde yer alan unsurları kısaca açıklamak gerekir.

(a) Güvenlikleştirici Aktör

Aktör, güvenlikleştirme sürecini başlatan ve sürdüren kişilerdir. Yani bir sorunu güvenlik sorunu yapmaya çalışan kişidir. Söz-edim sürecini yürütür ve bir tehdidin var olduğuna inandırmaya çalışır. Bir tehdidin varlığını dramatize ederek sunar ve olağanüstü yetkiler elde etmeye çalışır. Aktör konu bazında farklılık gösterebilir; hükümet, siyasi partiler, uluslararası örgütler hatta halk aktör

olabilir. Ancak buradan bir kişinin aktör olduğunu çıkarmamak gerekir. Toplumun yapısından dolayı o kişi bir grubun sözcüsüdür. Örnek vermek gerekirse; ekonomik alanda faaliyet gösteren birimlere yönelik bir siber saldırıda bu konuyu gündeme getirecek kişi ekonomik alanda çalışmalar yürüten devlet yetkilisi yani muhtemeldir ki bir bakan olacaktır ancak bu tek başına yapılmış bir hareket olarak düşünülemez bir topluluk yani hükümet kararı olarak görülür.

İşlevsel aktör olarak söz edilen unsur ise güvenlikleştirici aktör veya ikna edilecek kitle değildir. Güvenlikleştirmeye konu olan alanlarda söz sahibi olan ve geniş etki alanına sahip aktörlerdir. Bu alanda en bilindik örnek ise medyadır. Belli bir kesimi etkisi altına alma gücü olduğundan dolayı hem aktörleri hem de kitleleri etkileme potansiyeline sahiptir.

(b) Referans Nesne

Aktör tarafından tehdidin yöneldiği ve kritik öneme sahip olduğu iddia edilen nesnedir. Güvenliğin alanı genişlediği için neredeyse her şey referans nesne olarak aktör tarafından öne sürülebilir ancak güvenlikleştirme konusunda başarılı olma olasılığı referans nesnenin türüne göre farklılık gösterir. Bu yüzden Kopenhag Okulu akademisyenleri referans nesneleri 3 ayrı kategoriye ayırmıştır. Bunlar mikro düzey, orta düzey ve makro düzeydir (Buzan, vd., 1997: 36). Mikro düzey, küçük gruplar ve bireylerden oluşur. Kesim olarak küçük olduğu için bu nesneler üzerinde güvenlik önlemleri almak oldukça zordur. Makro düzey, insanoğlunun genelini ilgilendiren olay örgülerinden oluşur. Geniş bir yelpazeye hitap ettiği için mikro gibi makro düzeyde güvenlik önlemleri almak oldukça zordur. Ancak Soğuk Savaş döneminde bu düzeyde başarılı güvenlikleştirme örnekleri görülmüştür. Özellikle nükleer silahların yayılmasında ve dünya barışının korunması dünya genelinde kabul görmüş güvenlik sorunları olmuştur. Orta düzey ise, belirli bir sınırı olan ve genelde bir topluluğun söz konusu olduğu alanlardır. Bu açıdan güvenlikleştirmeye en uygun referans nesne düzeyi olarak görülmektedir. Çünkü biz duygusunu ön plana çıkarır ve topluluk halinde hareket etmeye oldukça elverişlidir.

(c) Alımlayıcı Kitle

Güvenlikleştirici aktörün, referans nesneye yönelik bir varoluşsal tehdidin var olduğunu inandırmaya çalıştığı kitledir (Buzan, vd., 1997: 37). Bunu yapmasının asıl nedeni güvenlikleştirmenin başarılı olmasında bu kitlenin onayının gerekmesidir. Kitlenin onayı olmadan güvenlikleştirici aktör, olağanüstü önlem alma yetkisine kavuşamamaktadır. Kitle referans nesne ile ilişkili olan kesimler olarak kabul edilir. Güvenlikleştirme için hedef kitle olarak kabul edilen kesim aktör ile referans nesne arasında bir konumdadır (Schneider ve Ingram, 1993: 335). Aktörler, kitlenin duygu, düşünceleri, inanç ve çıkarları gibi bazı özelliklerine bakarak söz-edimde kullanacakları ifadeleri oluşturur (Balzacq, 2005: 184).

Wæver’a göre “Güvenlik, seçkinler tarafından kurumsal bir sesle dile getirilmektedir” (Waever, 1995: 57). Dile getirilen kesim ise bu nesne ile nedensel bir bağa sahip olan kesimdir. Bu kitle her zaman büyük bir kesimi ifade etmez, bazen sadece küçük bir grubun iknası söz konusu olabilir. Ayrıca kitlenin hepsinin ikna edilmesi gerekmez belli bir kesimin ikna edilmesi güvenlikleştirme için yeterli olacaktır (Baysal ve Lüleci, 2015: 6). Bu kesim olayın türüne, kitledeki bireylerin sayısına ve yapısına göre değişkenlik göstermektedir.

Balzacq’a göre iki türlü destek vardır, ahlaki ve resmi destektir. Bu iki destek ne kadar uyumlu olursa o kadar başarılı bir güvenlikleştirme olacaktır (Kurt, 2020: 7-8). Ahlaki destek tek başına olağanüstü önlemleri almaya yetmez ancak başarılı bir güvenlikleştirme için gerekli bir unsurdur. Resmi destek ise tek başına yeterli bir destektir. Bu yüzden resmi desteği verecek otoriteye sahip olan kesim kritik kitle olarak kabul edilir (Miş, 2014).

1.5.2. Söz-Edim

Kopenhag Okulu güvenliği söz-edim süreci olarak görmektedir. Güvenlik unsurlarının bir araya geldiği aşamadır, bir konunun güvenlik sorunu olduğunun siyasi elitler tarafından sunulduğu aşamadır. Waever bu edimi şu şekilde açıklamıştır;

Güvenlik kendinden daha gerçek olan bir şeye ait bir gösterge (sign) değildir; Telaffuz etmek eylemin kendisidir. Eylem, söylemek yolu ile gerçekleşir (bahse girmek, söz vermek ya da bir gemiye isim vermek gibi). Devlet yetkilisi güvenlik kelimesini telaffuz ettiği anda belirli bir gelişmeyi özel bir alana kaydırır ve bu gelişmeyi engellemek için her yöntemi kullanma hakkını talep eder (Waever, 1995: 57).

Söz-edim bir gerçeklik yaratma sürecidir ve Austin bu süreci 3’e ayırmıştır.

Düz söz edimi; kesin anlamlara sahip olan cümlelerdir. Austin bu süreçte sırasıyla şunların gerçekleştiğini söyler; seslendirme edimi, dillendirme edimi ve anlamlandırma edimidir (Çelebi, 2014: 85).

Edim söz edimi; konuşanın dinleyene söylediklerini aktarma edimidir. Bildirme, söz verme, emir verme, bilgi verme gibi edimlerdir. Söylem dinleyiciye aktarılmış olur.

Etki söz edimi; cümleler ile dinleyicinin duygu ve düşüncelerinde istemli veya istemsiz olarak yaratılan değişim edimidir. Söz edimin sonucu olarak kabul edilir (Levinson, 1983: 292).

Austin'e göre bu edimler sonucu yeni bir gerçeklik oluşturulur. Edimler sonucu bir etki ortaya çıkar. Aktör bu edimleri kullanarak gerçeklik oluşturmaya çalışır ve hedef kitle üzerinde bir etki bırakmayı hedefler. Aktörün ilk başta kullandığı düz edimdir. Ayrıca düz edim sırasında edim söz edimi kullanılır. Aktör bir harekette bulunur ve sözcüklerle karşısındaki kesime kendi gerçekliğini geçirmeye çalışır. Karşıdaki kesimin bu edim sonucu etkilenmesi ile etki söz edimi oluşmuş olur (Austin, 1955: 122). Etkinin doğruluğu veya yanlışlığı bu noktada önemli değildir, edimin yapılma amacı sonucu ortaya çıkan yeni gerçeklik önemlidir.

1.5.3. Güvenlikleştirmenin Temel Değerleri ve Süreci

Kopenhag Okulu temsilcilerinden Barry Buzan, Ole Waever ve Jaap de Wilde'in çalışmaları sonucunda Güvenlikleştirme kavramı literatüre kazandırılmıştır. Soğuk Savaş sonrası gelişen güvenliğe farklı bakış açılarından biri olmuştur. Teoride güvenlik, objektif bir tehdit olarak değil, bir süreç olarak ele alınmıştır (Doğan, 2019: 173). Kopenhag Okulu yazarları tarafından Soğuk Savaş sonrasında güvenliğin genişleyen yapısından dolayı her konunun güvenlik sorunu olabileceği fikri yerine belli sınırlamaların getirilmesi gerektiği ifade edilmiştir. Bu yüzden güvenliği bir süreç olarak görmüşler ve güvenlikleştirme teorisini geliştirmişlerdir. Okulun savunucularına göre güvenlikleştirme eyleminin üç temel taşı bulunmaktadır. Bunlardan ilki, tehdidin yöneldiği bir referans nesnenin varlığı, ikincisi bu tehdidi söyleme taşıyan güvenlikleştirici aktör ve sonuncusu ise süreçte var olan ve güvenlikleştirmenin başarısını etkileyen işlevsel aktörlerdir. (Buzan, 2015: 32)

Waever'a göre güvenliğin kapsamının genişlemesi sonrası karşılaşılan en önemli sorunlardan biri "arzu edilen her şeyin güvenlik meselesi yapılabileceği" olanağıdır (Wæver, 1995). Bu sorun güvenliğin sınırının belirlenmesinde güçlük yaratmaktadır. Güvenlikleştirme teorisi, bu sorunun çözümü için "Ne için güvenlik ve kime göre güvenlik?" sorularına yanıt aramış ve beş ana alan üzerinden güvenliğin kapsamını belirleyerek teoriyi oluşturmuştur. Teoride, devletler açısından siyasi konular ve güvenlik konuları adı altında iki konu vardır. Siyasi konular günlük işlemlerdir ve siyasi olarak belli prosedürü izleyerek karar alınan konulardır. Güvenlik konuları ise bir tehdidin varlığı ile ortaya çıkan ve olağanüstü önlemler alınmasına yol açabilecek konulardır. Sadece askeri konuların değil belirlenen beş ana başlığın altındaki tüm meselelerin bu politika seviyesinde yer alabileceğini savunmuşlardır. Yani teori güvenlik alanına dâhil olan konuları ayrı şekilde ele almış ve normal siyasi konulardan ayırmıştır.

Bu fikrin oluşmasının başlıca sebeplerinden biri; geleneksel güvenlik yaklaşımları Amerikan merkezli bir bakış açısına sahipken, Kopenhag Okulu'nun, Avrupa merkezli bir bakış açısına sahip olmasıdır. Soğuk savaş sonrası en büyük etki Avrupa kıtasında ortaya çıkmıştır. SSCB'nin dağılması ile birlikte Orta ve Doğu Avrupa'da siyasi, ekonomik ve toplumsal anlamda bir boşluk oluşmuştur. Bu boşluk Avrupa'daki diğer devletlerin güvenliklerini birçok alanda tehdit etmiştir. Örneğin; sınırların belirsizliğinden dolayı daha yeni bağımsız olan devletlerin kendi aralarında çatışma riski,

ekonomik sorunlardan dolayı bu bölgelerden diğer ülkelere yapılacak göçün yaratacağı toplumsal sorunlar gibi askeri olmayan birçok konu Soğuk Savaş sonrasında Avrupa kıtasının ortasında büyük bir güvenlik zafiyeti doğurmuştur.

Her konuyu güvenlik meselesi yapmak güvenliğin anlamını açıklamayı ve sınırlarının belirlenmesini oldukça güç kılar. Bu yüzden Kopenhag Okulu savunucuları her konunun güvenlik boyutuna taşınamayacağını ve bunun bir sınırı olması gerektiğini savunmuşlardır. Güvenlik kelimesi genel anlamda devletlerin bir konuya aciliyet atfetmesi anlamına gelmektedir ve olağanüstü süreci ifade eder (Baysal ve Lüleci, 2015). Devletin normal akışının dışında gelişen durumlardır ve Waever'e göre, "devletin siyasi düzenini alt-üst eder (Waever, 1995).

Buzan'a göre her konu devletin ilgi alanına girmez, bu tür konular politize edilmemiştir. Bu konular özel ilgi veya görüş gerektirmeyen konulardır. Politize edilmiş konular ise devletin zaman ve kaynak ayırdığı konulardır. Bu tür konular normal siyasi süreç içerisinde incelenir ve üzerinde tartışılan konulardır. Güvenlikleştirilmiş konular ise olağanüstü önlemler alınması gereken aciliyeti olan konulardır. Yani Buzan'a göre 3 tür konu vardır, bunlar siyasi olmayan, siyasi olan ve güvenlikleştirilmiş konulardır (Buzan, vd., 1997: 23-24).

Güvenlikleştirme bir söz-edim süreci olarak ortaya çıkar. Waever'a göre güvenlikleştirme, "bir konuyu tehdit konumuna sokma söylemi" olarak tanımlanmıştır (Waever, 1995: 57). Güvenlikleştirici aktör referans nesneye yönelik bir tehdidin varlığından söz eder. Bu noktada önemli olan aktörün söz-edimde kullandığı referans nesne üzerine yetkin bir kişi veya grup olmasıdır. Genelde bu aktörler, siyasi liderler, hükümetler, bürokratlar, lobi ve baskı gruplarıdır. Aktör referans nesnenin varlığına yönelik bir tehdidin var olduğundan bahseder ve bunu ilgili kitleye kabul ettirmeye çalışır. Bu kitleler konu ve platforma göre değişiklik gösterebilir. Kitleler konuya göre devlet, halk, siyasi veya sosyal gruplar olabilir. Aktör referans nesneye yönelik tehdidin varlığını bu kitleye kabul ettirebilirse bu güvenlikleştirme başarılı olmuş olur. Ancak kitle bunu kabul etmezse güvenlikleştirme başarısız olur.

Güvenlikleştirme sürecini özetlemek gerekirse güvenlikleştirmenin üç ögesi vardır. Birincisi tehdidin yöneldiği referans nesne, ikincisi bu tehdidi söz edim olarak sunan güvenlikleştirici aktör ve sonuncusu ise kabul eden kitlelerdir (Buzan, vd., 1997: 40). Bir sorun tehdit olarak gündeme getirilmelidir ve teoride elit olarak adlandırılan kişiler tarafından sunulması gerekir. Sorun acil önlemler alması gereken bir konu olarak sunulur ve olağan siyasi süreçlerin dışında ele alınmak istenir. Bu istem olağandışı önlemlerin alınması içindir. Ancak bu isteğe sahip olmak için sürecin son adımının yani kitlenin söylemi kabul etmesi gerekir. Başarılı bir güvenlikleştirme sonrası aktör olağanüstü önlemler alma yetkisini elde eder. Normal siyasi süreçte alınamayacak ve tepki çekebilecek müdahaleler, güvenlikleştirme sonrası sıradan olur ve tepki çekmez.

Siyasi elitler güvenlikleştirilmiş konuyu siyasi sürecin dışında tutup artık olağanüstü önlemler alınabilecek seviyeye çıkarır. Kopenhag Okulu savunucuları aslında güvenlikleştirilmeyi savunmazlar, onlara göre konular normal siyasi süreçler içerisinde kalmalı ve gerekli önlemler o süreçler sonrası çıkacak kararlar ile alınmalıdır (Emmers, 2017). Güvenlik için acil süreçlerde güvenlikleştirilme yapılmalıdır. Güvenlikleştirilmenin temel dayanağı da tam olarak tehdide karşı acil önlemlerin alınması gerektiğidir. Konunun derhal gündeme alınması ve kararların hemen devreye sokulması gerekir. Normal siyasi süreçlerde bu oldukça ağır ilerlediği için güvenlik zafiyetleri ortaya çıkabilir.

Tablo 1: Kopenhag Okulunda Yer Alan Süreçler

Siyasi Olmayan	Siyasi Süreç	Güvenlikleştirme
Devlet konuyu ele almaz. Olağanüstü önlemler gerektirmez.	Sorun devletin normal siyasi sürecinde ele alınır. Olağanüstü önlemlere gerek yoktur.	Güvenlikleştiren elit kesim tarafından sorun ele alınır ve olağanüstü önlemler alınabilir.
Konuya aciliyet atfedilmez.	Aciliyet gerekmedikçe atfedilmez.	Aciliyet gerektiren bir konu olarak kitlelere sunulur.

Tablo 1’ de gösterildiği gibi üç adet süreç mevcuttur. Kopenhag Okulu akademisyenleri güvenlikleştirmeyi acil durumlardaki tehditlere yönelik gerekli hamlelerin yapılma süreci olarak tanımlamakla birlikte akademisyenler bu sürecin son araç olması gerektiğini ayrıca belirtmektedirler. Bu yönleri ile geleneksel yaklaşımdan oldukça farklıdırlar. Siyasi süreçlerin daha fazla olması tezini savunan bu düşünürler daha fazla politik sürecin daha faydalı sonuçlar doğuracağına güvenlikleştirmenin sadece son bir araç olarak uygulanması gerektiğini düşünmektedirler. Yani politik süreçlerden sonra çözüm bulunamadığı veya politik süreçler için zamanın kalmadığı durumlarda bir tehdit güvenlikleştirilmeli ve olağanüstü önlem yetkisi verilmelidir. Bu yönünü de göz önüne alarak geleneksel yaklaşımla olan farklılıklarına Tablo 2’de değinmek gerekirse;

Tablo 2: Kopenhag Okulunun Geleneksel Yaklaşımdan Ayrılan Yönleri

Geleneksel Yaklaşım	Kopenhag Okulu
Devlet Güvenliği	Toplum, Birey, İnsan Güvenliği
Askeri ve Siyasi Konular	Toplumsal Konular
Sabit Yöntem	Değişken Yöntem
Güvenlik İçin Politik Süreç Daha Az Olmalı	Güvenlik İçin Politik Süreç Daha Çok Olmalı

Söz-edim olarak özetlemek gerekirse, güvenlikleştirme sürecinde aktör düz söz edim ile birlikte dinleyici üzerinde bir etki söz edimi yaratmaya çalışır ve bunu yaparken uzlaşımsal güçten yani edim söz ediminden yararlanır. Böylelikle kendi yarattığı gerçekliği ortaya çıkarır ve referans nesne ile arasındaki bağ olan dinleyici kitleyi ikna etmeye çalışır.



İKİNCİ BÖLÜM

2. SİBER ALAN VE SİBER GÜVENLİK

2.1. Siber Alan

Siber alan özellikle II. Dünya Savaşı sırasında ve sonrasında dünyada gelişen teknoloji ile birlikte dikkat çekmeye başlamıştır. Siber alan, teknoloji ve ağ sistemlerinin gelişmesi, özellikle de internetin yaygınlaşması ve hayatın olağan akışında bulunan neredeyse tüm alanların ağ sistemine entegre edilmeye başlanması sonucu soyut ve somut varlıkların birleşiminden oluşmuştur (Bıçakçı, 2014: 101-130). Özellikle bilgisayar ve akıllı cihazların her geçen gün gelişmesi siber yapının faaliyet alanını genişletmiştir. Ancak, birçok kolaylığı kendisi ile birlikte getirmesine rağmen bazı problemlerin de kaynağı olmuştur. Bu problemler dolandırıcılıktan terörizme kadar birçok konuyu içinde barındırmaktadır.

Kelime anlamına baktığımızda, sanal bir ortam anlamına gelmesine rağmen siber alanın tanımı üzerinde tam bir uzlaşıdan söz edilemez. Ayrıca birçok yerde siber alan kelimesi yerine siber uzay kelimesi aynı anlamda kullanılır. Oxford English Dictionary siber alanı fiziksel dünyadan ayrılan sanal gerçeklik alanı olarak tanımlar. J. P. Barlow siber uzayı yeni bir sosyal alan olarak tanımlar ve J. P. Barlow'a göre siber uzay, otoriter güç korkusunun olmadığı insanların eylemler sergilediği özgür bir alandır (Elmer, 1996). B. D. Loader'a göre ise sınırların ve fiziksel davranışların olmadığı bilgisayar ortamıdır ve elektronik telekomünikasyon ile bilgisayar ağları genel anlamda internet olarak anılan ortamdır. Ayrıca Loader da yine aynı şekilde bu ortamın tek bir hâkimi olmadığını yani bir otorite tarafından yönetilemediğini düşünmektedir (Loader, 1997).

Genel anlamda baktığımızda soyut olarak kabul edilen siber alanda bir işlem görebilmek için somut varlıklar gerekmektedir. Bilgisayar ve telefon bu alana ulaşım araçlarının en bilindik örnekleri olsa da günümüzde birçok teknolojik alet ile siber alana ulaşılabilir. Kısacası tam bir tanımı olmamakla birlikte siber alan soyut ve somut varlıkların bir araya gelerek oluşturduğu bir alandır. İnsanlar somut varlıkları kullanarak soyut bir ortama erişim sağlar ve yapmak istedikleri birçok işlemi oradan yapar.

Bu oluşan yeni alan, hızlı bir gelişim kaydederek insanlar adına birçok kolaylık sağlamıştır. Ancak bu hızlı gelişimin yanında birçok sorunu da kendisi ile birlikte getirmiştir. Bunun en önemli

nedenlerinden biri insanların normal hayatlarında bulunan olguların bu sanal âlemde olmamasıdır. Yani insanlar belli bir kural ve kaidelere uygun yaşar, sorunları belli karar alma mekanizmalarından geçirerek çözer ancak siber alanda herhangi bir kural veya kaide yoktur (USA Department of State, 2005). Bunun en büyük sebebi ise siber alanın bir otorite gücü tarafından yönetilememesidir. Geleneksel anlamda uluslararası ilişkilerde devletler, uluslararası örgütler, sivil toplumlar gibi birçok aktör bulunmaktadır. Bu aktörler faaliyette bulundukları konularda otorite sahibi olmaya çalışabilir ve başarılı da olabilirler. Günümüzde güvenlik denildiğinde akla ilk devletler veya güvenliğe yönelik kuruluşlar gelir. Ancak siber alanda birçok aktör faaliyette bulunmasına rağmen herhangi bir aktörün tek başına bu alanın otoritesine sahip olduğu söylenemez. Otoritenin olmadığı yerde kural ve kaidede olmaz; olsa bile zorlayıcı unsur olmadığı için havada kalmış olur.

Siber alanın getirdiği tehlikelere siber alanda oluşan otorite boşluğu eklenince bir güvenlik sorunu ortaya çıkmıştır. Bu güvenlik sorununu tanımlamak için literatürde siber güvenlik kavramı kullanılmıştır. Siber güvenlik kavramına tam anlamı ile girmeden önce siber alanın gelişim sürecine, yapısına ve hangi alanlara sirayet ettiğine değinmekte fayda vardır. Çünkü siber alanın gelişimini ve hangi alanları kapsadığını bilmek güvenlik açısından yaratabileceği sorunların neler olduğunu ortaya çıkaracaktır.

2.2. Siber Alanın Ortaya Çıkışı ve Gelişimi

Dünyadaki teknolojinin bütünlüğünü ifade eden (Güntay, 2019: 87) siber alan, fiziksel dünyanın yanında sanal bir dünya ortamını bireylere sunmaktadır. Beyaz Saray tarafından yayınlanan Ulusal Güvenlik Başkanlık Direktifi 54 belgesinde siber alan; “İnternet, telekomünikasyon ağları, bilgisayar sistemleri ve kritik öneme sahip tümleşik işlemciler ve denetleyiciler de dâhil olmak üzere birbirine bağımlı bilgi teknolojisi altyapıları ağı.” olarak tanımlanmıştır (The White House, 2008). Yani siber alan belli cihazlar ile ağ ortamına erişebilme sonucu ortaya çıkmıştır. Bu ağ sistemlerinin en bilineni internettir, erişim sağlayan cihazların ise en bilindik örnekleri telefon ve bilgisayarlardır. Bu yüzden siber uzay gelişimi özellikle internetin gelişimi ve internete erişim sağlayan cihazların yaygınlaşması ile ilişkilendirilmektedir.

İnternetin temelleri Soğuk Savaş yıllarında atılmıştır. Soğuk Savaş’ın iki kutuplu yapısından dolayı devletler her alanda çekişme içerisine girmişlerdir. Özellikle silahlanmanın hızlanması ve istihbarat çalışmaları bu rekabetin ana odak noktaları olmuştur. Bu rekabet dünyayı aşarak uzaya taşınmış ve bu kapsamda Sosyalist Sovyet Cumhuriyetler Birliği (SSCB) 4 Ekim 1957 tarihinde yörüngeye ilk yapay uydu Sputnik I¹ yerleştirmiştir. Yine aynı yılın 3 Kasım’ında ise uzaya canlı bir

¹ SSCB 4 Ekim 1957 tarihinde Sputnik I isimli yapay uyduyu iyonosfer boyunca radyo dalgalarının dağılım özelliklerini incelemek için yörüngeye fırlatmıştır. Bu gelişme sonrası Soğuk Savaş’ta uzayda rekabet alanı olmuştur.

köpeğin içinde bulunduğu Sputnik II göndermiştir. Bu gelişmeler SSCB'nin füze gücünün Amerikan Birleşik Devletleri'ni (ABD) vurma gücüne sahip olduğunun ve uzay alanında rekabetin başladığının göstergesi olmuştur (Çokbıdık, 2018).

Bu gelişmelerin ardından ABD yönetimi, araştırmalarını hızlandırmak ve aradaki farkı kapatmak için İleri Araştırma Projeleri Ajansı'nı (ARPA) kurmuştur. ARPA sadece uzay anlamında çalışma yapan bir kurum değildir. Birçok dalda faaliyet gösteren bilim insanını bir araya getiren bir projedir. Balistik füze savunmasından nükleer testlerin yapıldığı yerin tespitine kadar birçok şey amaçlanmıştır. Amaçlanan şeylere ulaşmak için ise beraber çalışmak gerekmiş ancak bilgisayarların o dönemde sınırlı sayıda ve potansiyellerinin güçsüz olması nedeniyle ortak bir ağ üzerinden iletişim sağlanamamış dolayısıyla oldukça kısıtlı ilerleme sergilenmiştir (Bıçakçı, 2014: 104-107). Zaman içerisinde bilgisayarların gelişim göstermesi, 1958 yılında Ulusal Havacılık ve Uzay Dairesi'nin kurulması ve bu kurumda çalışan bilim insanlarının ihtiyaçları ortak bir ağın kurulması için ön ayak olmuştur. Bu ihtiyaç sonrası 1962 yılında ABD'de İleri Araştırma Projeleri Ajansı Ağı (Advanced Research Projects Agency Network – ARPANET) kurulmuştur. Bu ağ ortak bir ağ oluşumu için temel olmuştur. Daha sonra ARPANET, Soğuk Savaş'ın Batı Bloğu'nda yer alan ülkelerin de kurulmuş ağ sistemleriyle (İngiltere'deki Ulusal Fizik Laboratuvarındaki (National Physical Laboratory) ticari ağı ve Fransa'daki araştırma ağı olan Cyclades) ortak bir yapıda birleştirilmiştir. Böylece birleştirilen ağlarla birlikte internetin (International Network of Computer Networks-Bilgisayar Ağlarının Uluslararası ağı) çekirdeği ortaya çıkmıştır (Brendon, 2010).

Ağ sistemi hızlı bir gelişim sürecine girmiştir. Bu gelişimin en önemli sebebi Soğuk Savaş'ın getirdiği askeri rekabettir. 1962 yılında yaşanan Küba füze krizi, ağ sistemine verilen önemin artmasına sebep olan askeri nedenlerin en iyi örneğidir. Kriz sırasında SSCB'nin denizaltılarına nükleer füze yerleştirme teknolojisine erişilmesi sonrası ABD savunma politikalarında “Karşılıklı Kesin İmha” kavramı (Mutually Assured Destruction-MAD) yerini almıştır. Bu kavram ile bir savaş halinde kazanan tarafın olmayacağı, iki tarafın da birbirini yok edecek güce sahip olduğu anlaşılmıştır. Bu kavramın yanında oluşabilecek çatışmalarda iletişim ağlarının zarar görme riski tartışılmış ve iletişimin devamlılığının sağlanması için çözüm aranmıştır. 14 Mayıs 1948 yılında kurulan ve ABD hükümetine, Milli güvenlik konularında stratejiler sunan Rand Corporation kuruluşunda çalışan Paul Baran “fiziksel saldırı sonrasında kalan en büyük grupla elektrik bağlantısı sağlayarak” iletişimi sürdürebilecek bir ağ yapısını tartışmaya açmıştır (Baran, 1962). Dağınık bir ağ sistemi üzerinden iletişimin kesilmemesi düşünülmüş ve ağ sisteminin alt yapısı buna göre düzenlenmiştir. Sonrasında diğer ağlarla birleşmesi ile birlikte gelişimi için uygun ortam sağlanmıştır.

Bu ağ sisteminin gelişimini etkileyen diğer önemli etkenlerden biri ise Dosya Aktarım Protokolünün (File Transfer Protocol-FTP) geliştirilmesi olmuştur. Birleşme ile birlikte dağınık yapıda birçok sunucunun birbirlerine bağlandığı ve kullanıcı sayısının her geçen gün arttığı ağ

sisteminde FTP sonrası ortak çalışabilme imkânı sağlanmıştır. Ayrıca Paket Değişim Protokolü (Packet Switching Protocol-PSP) ile iletişim olanağı sağlanmış ancak kullanıcı sayısının artması değişim olanaklarını kısıtlamıştır. Bu yüzden mesajı bölen ve ulaştığı adreste parçaları birleştiren Gönderim Kontrol Protokolü (Transmission Control Protocol-TCP) geliştirilmiş, iletişim ve çalışma alanında gelişim sağlanmıştır (Bıçakçı, 2014: 102).

Kullanıcı sayısı her geçen gün artmasına rağmen sisteme ulaşım sağlayan kişi sayısı sınırlı kalmıştır. Bunun en büyük nedenlerinden biri ağ sistemine ulaşım sağlayacak somut varlıkların sınırlı sayıda ve kişilerde bulunmasıdır. Yani sanal ortama ulaşım sağlayacak somut varlıklar 1970’lerde oldukça az sayıdadır. Ancak 1974 yılında H. Edward Roberts tarafından yönetilen Mikro Enstrümantasyon ve Telemetri Sistemleri (MITS) Altair 8800 tanıtılmıştır. Altair 8800 “Kişisel Bilgisayar” teriminin 1975’lerde kullanılmasına yol açmış ve o dönemde birçok kişi tarafında satın alınmıştır. Böylece ağ sistemine ulaşım olanakları çeşitlenmeye başlamıştır. Eylül 1975’de piyasaya çıkan IBM 5100, günümüz taşınabilir bilgisayarların ilk örneği olmuştur ve ağa erişebilen kişi sayısının artmasına katkıda bulunarak bir ekol yaratmıştır. Bilişim sistemlerindeki bu gibi gelişmeler ile birlikte ağa ulaşan kullanıcı sayısı her geçen gün artmaya başlamıştır. Hatta bu sivil sayının artışı sebebi ile ABD 1982 yılında MİLNET adında ayrı bir askeri ağ kurma yoluna gitmiştir. Böylece ARPANET sivil bir ağ yapısına dönüştürülmüştür.

Siber alan sadece bilgisayardan ulaşılan bir ortam değildir, birçok bilişim kaynağı ile ulaşım açık büyük bir ortamdır. Dönemin zorluklarından dolayı sadece bilgisayarlara odaklanılsa da Soğuk Savaş’ın son yılları ile birlikte teknolojik cihazların çeşitliliği hızla artmaya başlamıştır. Özellikle 21. yüzyılda akıllı telefonların orta çıkması ve kişisel bilgisayar edinmenin kolaylaşması ile birlikte ağ sistemlerine erişim kolaylaşmıştır ve siber alandaki kullanıcı sayısı her geçen gün artmıştır. Böylece siber alan günümüzdeki halini almıştır.

2.3. Siber Alanın Yapısı

Tarihsel gelişim ile birlikte günümüzde siber alan yapısı çeşitli katmanlardan oluşmaktadır (Bıçakçı, 2014: 102-111). İlk katmanı fiziksel katmandır. Bu katman somut dünyada var olan donanımları ifade etmektedir. Yani dünyada var olan donanımlar sayesinde siber alana erişim sağlanmasıdır. Donanımlardan kasıt ise teknolojik aletlerdir. Teknolojik aletler dar kalıpta tutulmamalı ve ağ sistemine ulaşım sağlayan (Ağ sisteminden faydalanmakta dâhil) teknolojik aletlerin tamamını ifade etmektedir. Bu donanımlar sayesinde dünya ile etkileşimde olan bir siber alan oluşmuştur. Fiziksel katmanın güvenlik açısından en önemli yanı ülkelerin kritik altyapılarıdır. Kritik altyapıları oluşturan teknolojik aletlere yönelik saldırılar (solucan yazılımlar gibi) güvenlik açısından önemli sonuçlar doğurmaktadır. Bu da fiziksel katmanın politik kararlara konu olabileceğini göstermektedir.

İkinci katman, kod ve yazılım katmanı olarak karşımıza çıkmaktadır. Bu katman donanımların birlikte bir bütün halinde hareket etmesine olanak sağlamaktadır. Donanımlara verilen komutların uygun şekilde gerçekleşmesi ve uyum içerisinde çalışması için gerekli yazılım komutları var olmalıdır. Bu yüzden sanal alanda gerçekleştirilmek istenen her hareket donanımlardan kodlar yardımı ile ulaşır ve gerçekleşir. Ayrıca ağ sistemleri benzer şekilde kodlar ve yazılımlar sayesinde oluşturulmaktadır. Günümüzde bu kodların ve yazılımların en bilindik örnekleri Windows, Linux, Mac Os X işletim sistemleri ile Python, Ruby, Java gibi programlardır.

Üçüncü katman, içerik katmanıdır. İlk iki katmanda meydana gelen ortam burada bir çerçeve kazanır ve içerik açısından bir ayrıma kavuşur. Bilgiler burada ayrışır, her bilgi kendi konusunun altında yer alır ve hiyerarşik yapıya kavuşur. Hiyerarşik yapıdan kastedilen ise bilgilere ulaşım bazında sınırlılık getirilebilmesidir. Ağ sisteminde bulunan herkes her bilgiye ulaşamaz, bu gizliliği sağlayan içerik katmanıdır. Aynı zamanda bu katman kurumsal bazda kişilere kurum ağında çalışma imkânı sağlamaktadır. Kısacası içerik katmanı bilgi ve kullanıcıların ayrıştırıldığı ve kimlerin hangi ağ üzerinde çalışabileceğinin ve hangi bilgilere ulaşabileceğinin belirlendiği katmandır. İçerik katmanı sayesinde kurumsal sınırlamaların dışında gündelik hayatta sivil kullanımın yaygın olduğu arama motorları (Google, Yandex, Microsoft Edge vs. gibi) bazı web sayfalarını kendi arama motorlarından kaldırabilir ve bunlara kısıtlama getirebilir (Steel, 2015: 150-158).

Son katman ise düzenleyici katmandır. Günümüz devletlerinin birçoğunda sanal dünyayı düzenleyici yazılı kurallar vardır. Bu kurallar ağ sisteminin kullanıma çeşitli kurallar ve yasaklar getirmektedir. Bazen devletler de bazı içeriklere belli dönemlerde veya sürekli olarak kısıtlama getirebilmektedir. Bunun dayanağı düzenleyici katmandaki kurallardır. Ancak bazen devlet, olağanüstü önlemler olarak düzenleyici katmanda yer almayan önlemleri ağ sistemleri için belli dönemlerde almaktadır. Bunun dışında siber alanın gelişimi ve teknolojik gelişmenin hızı ile bürokrasinin hızı bir değildir ve düzenleyici katmandaki kısıtlamalar ağ sistemlerinde çoğunlukla aşılmaktadır (Mathrani, 2010: 1588-1595).

İkinci Dünya Savaşı ile başlayan teknolojik gelişmeler ve Soğuk Savaş'ın getirdiği rekabetle birlikte siber alan meydana gelmiştir. 2023 yılı verilerine göre dünya nüfusunun %64,4'ü internete erişim sağlayabilmektedir (Alakoç-Burma ve Özdemir, 2024: 6). Bu oran yıllar geçtikçe artmış ve artmaya devam edeceği düşünülmektedir. Bu açıdan baktığımızda askeri bir sınır içinde doğan ağ sistemi dünya nüfusunun neredeyse 2/3'ünü içine alan bir ağ sistemine dönüşmüştür. Kendi içerisinde belli katmanlara ayrılıp bazı kısıtlamalara ve içerik bazında ayrımlara gidilmiş olmasına rağmen günümüzde kontrol edilebilirliği her geçen gün azalmaktadır. Bu da hızla gelişmesi ve getirdiği birçok olanağa rağmen sanal alanın güvenlik sorunlarını içerdiğini göstermektedir.

2.4. Siber Güvenlik

20. yüzyılın sonları ve 21. yüzyıl ile birlikte bilginin değeri oldukça artmıştır. Bilgi en kıymetli varlıklar arasında yerini almış ve değeri oldukça artmıştır. Siber alan ise bilginin yer aldığı ve depolandığı en önemli kaynak olmuştur. Bilginin değerli olması ve siber alanda var olması sonucunda siber alanın güvenliği tartışmaya açılmış ve siber güvenlik kavramı ortaya çıkmıştır. Yani siber güvenlik bilginin güvenliği olarak tarif edilmektedir (Goodrich ve Tamassio, 2013). Bilginin gizliliğinin, bütünlüğünün ve erişilebilirliğinin sürekli sağlanması siber güvenliğin asıl amacıdır.

Siber güvenlik, askeri güvenlik alanı dışında olan bir alandır. Yani askerler ve askeri araçlarla (Silah, uçak, vs.) korunması mümkün olmayan bir alanın korunmasını ifade etmektedir. Fiziksel alandan ayrılmış, her yerden erişilebilecek ancak hiçbir yerde varlığı olmayan bir alanın korunması anlamına gelmektedir. (L.Herrera, 2016, s. 67). Bu ortam bilginin gizlendiği, erişildiği ve korunduğu alandır.

Bilgi çağı olarak adlandırılan 21. yüzyılda siber güvenlik kavramı ulusal güvenlik, ekonomik güvenlik, çevresel güvenlik gibi güvenlik konuları arasına girmiştir. Siber güvenlik bilginin yani depolandığı ve aktarımının yapıldığı ağ sistemlerinin korunması anlamına gelmektedir. Ağ sistemlerindeki gelişim ile birlikte içerisinde barındırdığı tehlikelerde artmaya başlamıştır. Bunun sonucunda bu ağ sistemlerine yönelik yani ağ sistemlerindeki bilgilerin ve iletişimin korunması için güvenlik önemleri alınması gerekmiştir. Böylece literatüre siber güvenlik kavramı girmiştir (Kaur ve Ramkumar, 2022).

1971'de BBN Technologies'da çalışan Bob Thomas siber alanda tehlike oluşturan yazılımlardan biri olan vekendini çoğaltan (self-replicating) ilk solucan yazılımı yazmıştır. Yayılma özelliğine sahip bu program kısa sürede ARPANET ağına yayılmıştır. Yayıldığı ağ sistemine "I'M THE CREEPER: CATCH ME IF YOU CAN" mesajı göndermiştir (Hubbard ve Eunice, 2020). Creeper solucanı, bir başka yazılım olan Reaper ile ortadan kaldırılmış ve ağ güvenliği sağlanmıştır. Siber alana yönelik ilk tehdit örneği olan bu yazılım, siber alanın gelişmesi ile birlikte çeşitlilik kazanmış ve daha tehlikeli boyutlara ulaşmıştır.

2.4.1. Siber Alana Yönelik Tehditler

Creeper gibi yazılımlar zamanla ağ sistemindeki gelişimle birlikte artmış ve çeşitlenmiştir. Bu yüzden bu gibi güvenlik zafiyeti oluşturacak yazılımlar çeşitli kategorilere ayrılmış ve yarattıkları tehlike boyutuna göre derecelendirilmiştir.

Bakteriler: Bilgisayarlarda bağımsız olarak çoğalır ve daha fazla disk ve işletim zamanı işgal eder.

Solucanlar: Kendi kendine çoğalabilen bu yazılımlar hızlı bir şekilde bir ağ sisteminde yayılabilir. Bilgi akışını ele geçirerek ağ sistemlerini yavaşlatabilir.

Virüsler: Aktif olması için başka bir programın çalışmasına ihtiyaç duyar veya işletim sisteminde bazı komutların verilmesi ile çalışır ve yayılır. Verilerin zarar görmesine yol açabilir.

Mantık Bombası: Belli bir zamana ayarlanabileceği gibi bir programın çalıştırılması sonrası aktif hale gelebilir. Zararlı görülecek işlemleri yapmaya ayarlanabilir ve zamanı gelince bu işlemleri yapabilir.

Arka Kapı: Kullanıcı sistemlerine saldırganlar tarafından farklı bir yöntemle giriş yapılmasıdır. Gizli bir şekilde sisteme sızar ve sistemdeki verilere ulaşır.

Tuş Dinleyiciler: Klavye seslerini dinleyerek belli bir düzende metin oluşturur ve bu metinleri saldırganlara bildirir. Özellikle istihbarat çalışmalarında yaygın bir saldırdır.

Scriptler: Web sayfalarındaki kod topluluklarıdır. Botlarla birlikte toplu saldırılarda kullanılır.

Sahte Web Sayfaları: Günümüzde oldukça yaygın olan bu saldırı yönteminde popüler web sayfalarının çok benzerleri oluşturulur ve sayfadaki hareketler takip edilerek kişisel verilere ulaşılabilir.

Taklit E-posta Hesapları: Bazı kişi ve kurumların e-postaları taklit edilerek kişisel verilere ulaşılmaya çalışılır (Güntay, 2018: 82-84).

Bu saldırı araçları en bilindik olanlardır. Bunların haricinde sayısız saldırı aracı vardır. Bu araçlar genel anlamda kullanım amaçlarına göre seçilir. Bireylerden ülke istihbaratlarına kadar birçok kişi ve kurum bu araçları kullanmaktadır. Kişisel bilgilerden devletlerin gizli bilgilerine kadar birçok konu bu saldırıların hedefi olabilir. Bu saldırılara genel olarak siber saldırı denilmektedir. Bu saldırıları engellemek için yapılan çalışmalara ise siber savunma yani siber güvenlik denilmektedir.

2.5. Siber Güvenliği Zorlukları

Fikri mülki hırsızlıklar, veri hırsızlıkları, maddi zararlar, ağ tabanlı çalışan sistemlerin durması, casusluklar ve benzeri faaliyetler siber güvenlik alanında en çok karşılaşılan saldırılardır (Yılmaz, vd., 2021: 1149). Tek tek bakıldığında örneğin casusluk saldırıları oldukça zor olabilirken, kişisel verilerin çalınması sistemlerdeki güvenlik zafiyetleri ve kişisel bilgi eksikliklerinden dolayı oldukça kolay olabilmektedir. Ancak genel anlamda bakıldığında siber saldırı yapmak, gelen saldırıları savunmaktan oldukça kolaydır. Bunun en temel sebeplerinden biri güvenlik anlamında güçlü

yazılımlar olmasına rağmen saldırı olanaklarının oldukça geniş ve gelişmiş olmasıdır. Birden çok saldırı olanağı vardır ve aynı anda birden çok sistemden tek bir sisteme saldırı düzenlenebilir. Bu saldırıların tespit edilmesi oldukça zordur, istisnalar dışında saldırılar genelde gizli şekilde yürütülür. Sistemdeki ufak bir açık bile saldırının çıkış gibi büyümesine ve bütün sisteme yayılmasına olanak tanımaktadır.

Değinildiği gibi siber saldırılarda kullanılan araçlar otomatik şekilde hızlıca yayılabilmekte, bunlar tespit edilse bile kaynağının bulunması ve onun ortadan kaldırılması zaman alabilmektedir. Ayrıca siber saldırılar, sistemi yok etmekten çok hep belli bir hedefe yöneliktir. Yani genelde siber saldırılar bir hedefe odaklıdır ve kısa sürede ona ulaşmaya çalışır. Saldırı, çok kısa sürede gerçekleştirileceğinden bu süre zarfında tespit edilemezse başarılı olmuş olur.

Eski dönemlerde güvenlik denildiğinde devletlerin toprak bütünlüğü akıllara gelmekteyken küreselleşme ile birlikte birçok alanda güvenlik anlayışları oluşmuştur. Ekonomik güvenlik, toplumsal güvenlik gibi birçok yeni güvenlik alanları oluşmuştur. Siber alandaki entegrasyonun artması bu oluşuma benzemektedir. Siber alana her geçen gün yeni alanları bünyesine entegre etmektedir. Özellikle Soğuk Savaş sonrası küreselleşmenin büyük boyutlara ulaşması entegrasyonu hızlandıran önemli unsurlardan biri olmuştur. Bu entegrasyon belli zorlukları da beraberinde getirmiştir. Siber alan ilk çıktığında tek bir bilgisayar ve ağ sistemi vardı, askeri bir araç olarak kullanılıyordu ancak entegrasyonun her geçen gün artması ile siber alanda kendi içinde bölümlere ayrılmış ve her bölümün güvenliği ayrı ayrı ele alınmıştır. Bir bütün olarak siber güvenlik kavramı kullanılsa da siber alan içinde iletişimden bankacılık sistemine birçok kritik alan oluşmuştur. Yani siber alan için tehdit her alan için farklı şekil ve amaçlarda ortaya çıkmaktadır, bu da siber güvenliğin bir bütün olarak sağlandığını düşündüğümüzde bunu başarmanın zorluğunu ortaya koyar.

Ayrıca siber güvenlik fiziksel olmayan bir alanın güvenliği olarak bilinmektedir. Ancak siber alana erişim sağlayan, telekomünikasyon altyapılarının, eşeneksels kabloların ve fiber optik kabloların güvenliği siber güvenlik için hayatı öneme sahiptir (Ünver, 2023: 81). Yani sanal dünyadaki bilgilerin güvenliği için fiziksel âlemdeki araçların güvenliği oldukça önemlidir. Bu siber alanın güvenliği için ayrıca bir zorluk yaratmaktadır.

Siber güvenliğin sağlanması için ağın tamamen güvende olması gerekmektedir. Ağ sisteminin bütünlüğünde oluşacak bir zayıflama ağ sisteminin tamamına etki edebilmektedir. Bu dünya çapında ağ sisteminin bütünlüğünün güvenliği sağlanmalıdır anlamına gelmemelidir. Bahsedildiği üzere çevresel katmanda içerikler belli kategoriye ve sınıflara ayrılır. Ayrıca kullanıcılar siber uzayda kendi bölümlerini yaratabilirler. Bütünlüğün güvenliği bu çerçeve katmanda oluşan bölümlerin her birinin kendi bütünlük güvenliğini sağlamasıdır. Lakin bu bütünlüğün sağlanması oldukça zordur, sistemde oluşacak ufak bir güvenlik açığı tüm sistemi tehlikeye atmaktadır. Siber alan sürekli, tam kapasite güvenli şekilde tutulmalıdır, bu zor bir olasılıktır ve siber güvenliğin zorluklarından biridir. Ayrıca

bütünlüğün güvenliği sürekli sağlanırken, erişim de sürekli devam etmelidir. Güvenlik için erişimin kısıtlanması güvenliğin sağlandığı anlamına gelmemektedir. Siber güvenlik, bilginin gizliliği sağlanırken aynı zamanda erişime açık olması anlamına gelmektedir (Aldemir ve Kaya, 2020: 11).

Soğuk Savaş yıllarında meydana gelen Vesayet Savaşları'nın² benzeri niteliğinde bir yapı günümüzde oluşmuştur. Devletler üstün silah teknolojileri ve bir dünya savaşını tetikleyebileceğinden korkarak sınırlı olarak birbirlerine karşı askeri hamleler yapmakta, bunun yerine yine vesayet savaşlarına başvurumaktadırlar. Ancak gelişen teknolojinin getirdiği olanakla vesayet savaşlarının yanına siber saldırı olanağı eklenmiştir (Çelik, 2013: 143). Karşı tarafa direk olarak askeri olarak saldırmaktan Soğuk Savaş'tan beri kaçınan devletler için artık karşı tarafa vesayet savaşlarından daha çok zarar verebilme imkânı doğmuştur. Çünkü siber saldırılarda saldırganın tespit edilmesi ve bunun kanıtlanması çok zordur (Yılmaz ve Gönen, 2018). Bu zorluk siber saldırıları savaşlara kıyasla oldukça cazip kılmaktadır. Çünkü vesayet savaşlarında bile devletler sınırları içerisinde çoğu zaman olaylarla karşılaşmayıp toprak bütünlüğü olarak zarar görmemesine rağmen ekonomik olarak oldukça zarar görür. Çünkü yardım ettiği tarafa teknik, askeri ve ekonomik açıdan yardım etmelidir. Ancak siber saldırılarda bu harcanan ekonomik olanakların ve zamanın çok daha azına karşı tarafa maddi ve manevi daha büyük zarar verebilme imkânı vardır. Ayrıca siber saldırıların tespit edilmesi ve ispatlanması zor olduğundan dolayı oldukça düşük bir riske sahip bir olanaktır.

Bu olanaklar siber saldırıların cazibelerini artırırken ayrıca savunma zorluğu yaratmaktadır. Siber saldırıların yerleri tespit edilebilir ancak saldırılar genel anlamda bulunan konumdan daha farklı konum gösterilerek yapılır ve resmi olmayan araçlarla gerçekleştirildikleri için üstlenilmediği sürece kimden geldiğini kanıtlamak zordur. Lakin devletler genel anlamda sorun yaşadıkları devletleri elbette bilmektedir. Gayri resmî olmasına rağmen saldırıların kimden geldiğini tespit ederler ancak siyasi olarak kanıtlanmadığı için cevap vermekte zorluk çekerler. Saldırıya maruz kalan devletler de tıpkı askeri saldırıdan sonra meşru savunma ilkesi gereği askeri olarak cevap verme haklarına sahiplerse, siber saldırılar sonrası gayri resmi olarak bu hakkı kullanır ve karşılık olarak siber saldırı yolunu tercih edebilirler (Gümüşbaş, 2016: 186). Bu durum oluşunca karşılıklı olarak birbirine siber alanda saldırı düzenleyen iki kesim oluşur ve siber güvenliğin sağlanması oldukça zorlaşır. Hem saldırı yapmak hem de aynı anda savunma yapmak normal askeri düzende zor olduğu gibi siber alan için de oldukça zordur.

² Vesayet Savaşları, devletlerin birbirleri ile birebir savaş halinde olmadan savaş halinde olmalıdır. Vekalet savaşları olarak da bilinmekte olan bu savaşlar daha çok Soğuk Savaş yıllarında literatürde yerini almaya başlamıştır. ABD ve SSCB fiili bir savaştan kaçınmış ve savaş olan yerlerde her iki tarafta diğer tarafın desteklediğinin karşısında yer alan tarafı desteklemiştir. Böylece fiili bir savaştan kaçınarak birbirleri ile savaş halinde olmuşlardır.

Geleneksel anlamda askeri savunma oldukça zordur. Hatta birçok konuda savunma saldırıdan daha zordur. Çünkü ne zaman, hangi koşullarda gerçekleşeceği çoğu zaman belli olmayan bir saldırıya karşı bir savunma yapmak gerekir. Özellikle siber saldırıların ne zaman ve hangi koşullarda, nereye gerçekleştirileceğini bilmek oldukça zordur. Böylece birçok konuda olduğu gibi siber alanda saldırılara karşı güvende kalmak son derece zor bir süreçtir. Dünya genelinde ortalama her 39 saniyede bir siber saldırı gerçekleşmekte ve yıllık 800.000'den fazla insan bu saldırıların kurbanı olmaktadır (Martin, 2024). Ayrıca insanların toplu şekilde kullandığı altyapılara (Elektrik, telekomünikasyon, ethernet kablolarına vs.) ve dünya çapında kullanılan yazılımlara (Microsoft, Linux, vs.) yönelik saldırılar sonucu siber saldırılardan direk olmasa da etkilenen insan sayısı bu rakamın çok daha üstündedir.

Siber alan güvenliği birçok kesime konu olmaktadır. Yukarıda bahsedildiği gibi birçok insan yıllık olarak bu saldırılardan etkilenmektedir. 800.000'den fazla insan da direk olarak bu saldırılara maruz kalmaktadır. Bu açıdan bakıldığında siber alandaki güvenlik bireylerin bilgi güvenliğine kadar inmektedir. Betimleme ile anlatmak gerekirse; fiziksel toplumu oluşturan bireylerdir, sanal toplumu ise ağlara erişim sağlayan bireyler oluşturur. Fiziksel toplumun güvenliği için toplum tek bir parça kabul edilir ve dış saldırılar bireylere yönelik değil topluma yönelik olur. Güvenlik için toplumu korumak yeterlidir ve toplum güvende ise birey de güvendedir. Ancak sanal toplumda sanal toplumu korumak güvenlik için yeterli olmayacaktır. Sanal toplumda bireyler tek tek hedef alınabilecek konumdadır. Ayrıca bir bireyin hedef alınabilmesi toplumun da hedef alınabileceği anlamına gelmektedir. Buradan anlaşılacağı üzere siber güvenliğin sağlanması her bir bireyin güvende olmasını gerektirir.

Bu gibi önemli faktörlerden ötürü siber alan savunması oldukça güç bir alandır. Bilginin sürekli bir şekilde yer aldığı, erişilebilir ve gizlilik ilkesine uygun bir yapının sağlanması siber güvenliğin sağlandığı anlamına geldiği ve zorlukları göz önüne alındığında siber alan, güvenlikleştirme eylemi için oldukça uygun bir güvenlik yapısına sahip olduğu anlaşılmaktadır.

2.6. Siber Saldırıların Güvenlikleştirmeye Uygunluğu

Güvenlikleştirme bir sorunun güvenlik sorunu olmasını, beş konuyla ilgili olmasına bağlamaktadır. Bunlar askeri, siyasi, ekonomik, toplumsal ve çevresel konulardır. Kısacası bir sorunun güvenlik meselesi olabilmesi için ilk şart, bu beş konudan biri olmasıdır. Siber saldırıları ve güvenlikleştirmede yer alan konuları tek tek ele almak siber alanın hangi alana daha uygun olduğunu gösterecektir.

2.6.1. Askeri Alanda Siber Güvenlik

Geleneksel askeri anlayışta saldırılar silahlar ile gerçekleşir. Silahtan kastedilen şey yıkıcı güce sahip olan kitle imha araçlarıdır. Fiziki bir eylem söz konusudur ve geçmiş dönemlerde oldukça sık rastlanan bir durumdur. İnsanların veya insanların ürettiği makinaların birbirleri ile savaştığı bu saldırıların aksine siber uzayda, askeri alandaki siber saldırılar oldukça farklıdır. Askeri alandaki siber saldırılar devletlerin askeri altyapılarına, teknolojik alanlarına, silah sistemlerine ve teknolojik bilgilerine yönelebilir (Karakuş ve Gönen, 2022: 104-109). Günümüzde askeri sistemlerin çoğu devletlerin oluşturdukları özel altyapılara bağlı şekilde dizayn edilmiştir. Ayrıca bazı ekipmanlarda (Uçak, seyir füzeleri, navigasyon sistemleri, vs.) yazılım oldukça önemli bir unsurdur.

Hali hazırda son dönemlerde kullanılan uluslararası ilişkiler söylemlerinde sıkça değinilen hibrit savaş kavramı, bahsi geçen iki saldırı unsurunun birlikte kullanıldığını ifade eden savaş modelidir. Yani “Hibrit Savaş Modeli” ile devletler siber alanı artık savaşlarda kullanabileceği bir silah olarak görmektedir. Siber alanda uzaydan görüntüler alınması, iletişimin kesintisiz sağlanması, savaş sırasında karşı tarafın direncini halk nezdinde kırabilmeye yönelik sosyal medya propagandaları düzenlenmesi vb. gibi birçok unsur askeri düzende artık var olmuştur (Karakuş ve Gönen, 2022: 104-109).

Bu sebeplerden dolayı askeri alan da kendine siber alanda bir yer edinmiştir. Siber saldırılar ise askeri alanda bir saldırı aracı olarak kullanılmaya başlanmıştır (Güntay, 2018: 87). Askeri teknolojinin kendini siber alana entegre etmesi ve siber saldırıların da artık askeri saldırı mekanizmalarından birine dönüşmesi, siber güvenliğin askeri bir konu sayılabileceğini göstermektedir. Devletler siber alanda kendilerini güvende hissetmek için her yıl bütçelerinden daha fazla pay aktarmaktadırlar (Kışman ve Güleç, 2021: 134). Bu nedenlerden ötürü siber güvenliği askeri konulardan biri olarak sayılabilirken aynı zamanda askeri alanın da siber alana entegrasyonu hızla devam etmektedir.

2.6.2. Ekonomik Alanda Siber Güvenlik

Günümüzde tüm dünya basınında en çok konuşulan konulardan biri olan ekonomik alan, siber alana entegre edilmeye çalışılan öncelikli alanlardandır. Akıllı cihazların ortaya çıkması ile özellikle bankacılık sektörü yaratılan “App” uygulamaları sayesinde günümüzde birçok işlemi bankaya gitmeden halletme imkânı sunmaktadır. Ülke borsaları işlemleri artık sanal dünyaya entegre edilmiş bir şekilde faaliyetlerini sürdürmektedir. Her geçen gün nakit para kullanımı azalmakta ve sanal ödemelerin sayısı artmaktadır (Tarlin, 2021). Dolayısıyla ekonomik alanın entegrasyonu her geçen gün artmakta ve ekonomik alandaki faaliyetlerin çoğu artık sanal alanda yapılabilmektedir.

Ekonomik alanın sanal uzaya bu kadar entegre olması zaman ve kolaylık bakımından birçok avantajı içinde barındırmasına rağmen siber saldırılar için de odak nokta olmuştur. Özellikle banka sistemlerine yapılan saldırılar günümüzde en çok duyduğumuz siber saldırılar arasındadır. Ayrıca gönderilen sahte e-mailler ve linkler ile kişisel bilgilere çok çabuk ulaşılabilir. Ekonomik açıdan bu hırsızlık olayları dışında bir de saldırılardan korunmak ve saldırı sonucu meydana gelen etkileri ortadan kaldırmak için kişiler, kurumlar ve devletler bazı ekonomik bedellere katlanmak zorunda kalmaktadırlar (Lis ve Mendel, 2019). Bu maliyet 2023 yılı için 9 trilyon dolar iken 2024 yılı için beklenen rakam 10 trilyon dolardır (Berhtan, 2023).

Deepfake³ teknolojisi gibi teknolojilerin gelişmesi, sanal yatırım araçlarının artması ve insanların bu gibi tehlikeler hakkında yeterli bilgiye sahip olmaması gibi sebeplerden ötürü son dönemlerde ekonomik alanda siber suçlar artmıştır. Güvenlik olarak siber alanda son dönemlerde sanal paralar kullanılarak kara para aklanması gündemde yer almaktadır. Özellikle gelişmiş ülkeler bu gibi sebepler ve izi sürülemediği için vergilendirme yapılamamasına karşı özel önlemler almaktadırlar (Miynt ve Duramaz, 2013: 315-325).

Birçok nedenin birleşmesi sonucu askeri alanda olduğu gibi ekonomik alan da siber alanın içine girmiş ve ekonomik alanın güvenliği söz konusu olduğunda ekonomik anlamda siber güvenlik en önemli faktörlerden biri olmaktadır. Ekonomik alan siber uzaya her geçen gün daha fazla entegre edildiği için ekonomik güvenliğin sağlanması için siber güvenliğin sağlanması gerekmekte ve iki alan her geçen gün ayrılmaz bir bütün haline gelmektedir.

2.6.3. Siyasi Alanda Siber Güvenlik

Devletlerin kurumsal istikrarı ve bekası gibi tartışmalar siyasi alanın konularıdır. Siyasi elitler devletlerin bekasını veya istikrarını öne sürerek belli konuları güvenlikleştirme çabasına girmektedirler. Günümüzde devletler her anlamda faaliyet göstermektedirler. Bu faaliyet alanları devlet bekasına atfedilebilir. Bu atfedilme sonucu o konuya yönelik bir sorun güvenlikleştirilebilir.

Devlet kurumları, siyasi partiler, hükümetler, sivil toplum örgütleri gibi birçok aktör günümüzde siyasi sürecin içinde yer almaktadır. Siyasi süreç içerisinde oluşan tüm olay ve yaratılan bilgiler siyasi alanın bir ürünü olarak bilinmektedir. Siyasi alan, bu bilgi ve olay örgüsüyle siber alanda faaliyetlerde bulunmaktadır. Kurumsal kimlik üzerinden oluşturulan hesaplar, siyasi elitlerin oluşturdukları hesaplar, devlet bilgilerinin saklandığı ağlar, devletlerarası iletişimin sağlandığı ağ ortamları bu faaliyetlere örnek olarak verilebilir.

³ Deepfake: İnsan seslerinin analiz edilerek aynı ses tonunda konuşabilen yazılımdır.

Özellikle sosyal medya kullanımının yaygınlaşması siyasi alanın siber alanda aktif şekilde yer almasına neden olmuştur. We Are Social'ın paylaştığı rapora göre 2023 yılı için dünya çapında 4.76 milyon sosyal medya kullanıcı bulunmaktadır (We are social, 2023). Bu rakam dünya nüfusunun yarısından fazlasına eşittir. Bu seviyede bir kullanıcı sayısı siyasi süreçler için oldukça önemli bir alan yaratmaktadır. Sosyal medyanın bu gücü getirdiği avantajlarla beraber dezavantajlara da sahiptir. Sosyal medya kullanıcıları arasında bilgi oldukça hızlı yayılmakta ve bu hızlı yayılımın getirdiği avantajlar devletler için sorunlar yaratabilmektedir. Bir örnek üzerinden açıklamak gerekirse; Arap Baharı sosyal medya uygulamalarından biri olan Facebook üzerinden başlayan bir süreç olmuştur (Barr, 2016: 15). Sürecin haklı veya haksızlığı sorgulanmadan değerlendirildiğinde siber alandaki faaliyetler devletleri iç savaşa götürebilecek kadar büyük sonuçlar doğurmaktadır. Bu devletlerin isteyeceği son şeylerden biridir, bu yüzden devletler sosyal medyaya oldukça titiz ve sıkı yaklaşmaya çalışırlar. Bazı dönemlerde devletler tarafından sosyal medyaya yönelik erişim kısıtlamaları bile getirilmektedir. Bunun en temel örneği erişim yasağıdır. Bu yasaklar kısa sürmesine rağmen olağandışı bir eylem olduğu için güvenlikleştirme örneğidir (Kukulin, 2020: 177-190). Çünkü sosyal medya siyasi süreçten çıkarılmış siyaset üstü bir süreç haline getirilmiş olur.

Bu uç örneğin yanı sıra devlet kurumlarının iletişim⁴ ve bilgi ağları bulunmaktadır. Bu ağlara yönelik saldırılar, siyasi elitlerin kişisel bilgilerine yönelik saldırılar ve devlet özelinde yapılmaya çalışılan spekülasyonlar gibi durumlar siber alanda siyasi alana yönelik oluşturulan tehditlerdir. Ayrıca bazı devletler elektronik seçim sistemine geçmişlerdir. En önemli örneği ABD'dir ve birçok devlet bu yönde deneme çalışmaları yürütmektedir. Siyasi seçimlere yönelik siber saldırılar devletler için bir beka sorunu olmaktadır. 2016 yılında yapılan ABD Başkanlık seçimlerine Rusya'nın siber saldırılarla müdahale ettiği iddiası Münih Soruşturması'nın açılmasına neden olmuş ve günümüzde hâlâ tartışma konusudur.

Diğer iki alanda olduğu gibi siyasi alan da kendine siber alanda yer edinmiştir. Bu yer edinim sonrası siyasi alan içinde bahsi geçen tehlikeler ortaya çıkmıştır. Bu ve benzeri tehlikelerden ötürü siber alan siyasi alan içinde güvenlikleştirilme zeminine sahiptir.

2.6.4. Toplumsal Alanda Siber Güvenlik

Askeri ve siyasi güvenliğin yanında 20. ve 21. yüzyılda gelişen teknoloji ve gerçekleşen bazı olaylardan dolayı devletler için kimlik (Toplumsal) güvenliği sorunu ortaya çıkmıştır. İki kutuplu yapının son bulması ile artık güvenlik çalışmalarında kimlik sorunları araştırma konuları arasına girmiş, insan ve toplum güvenliği ön plana çıkmıştır (Şener, 2017: 8).

⁴ Devletler faaliyet gösterdikleri tüm alanlarda hem bilgilerin sağlıklı şekilde erişilebildiği, zamandan tasarruf edildiği ve vatandaşlara kolaylık sağlamak için birçok kurumlarının faaliyetlerini siber alana taşımış ve ağ sistemlerini bilgi depolama alanı olarak kullanmıştır. Bu kurumların ağlarının korunması devletlerin görevidir ve toplum güvenliği için oldukça önemli yere sahiptir.

Kimlik sorununun oluşumunun nedenlerinden birkaçına siber alanda yaratılacak etkilerle değinmek gerekirse; Soğuk Savaş sonrası küreselleşme ile birlikte artık devlet sınırları ortadan kalkmıştır. Teknolojik gelişim ile birlikte binlerce kilometre uzakta olan kişilerle anlık iletişim sağlayabilme ve kısa süre içerisinde ulaşım sağlama imkânına erişilmiştir.. Bu avantajlar sayesinde insanlar farklı ülkelerdeki kişilerle iletişim kurarak ve seyahat ederek kültürel etkileşimde bulunabilmektedir. Kültürel zenginlik sağlama imkânının yanında bu gibi olanaklarla devletleri ve toplumu zarara uğratacak fikirlerin yayılma olasılığı oldukça fazladır. Bunlara örnek olarak; cinsel istismar, geleneklerin yıkılması, terör propagandalarının yapılması, terör örgütlerine üye kazandırılması ve aşırı dini inançların yayılması gibi bazı toplumsal sorunlar gösterilebilir (Ağır, 2011: 118-119). Bu faaliyetlerin hepsi sanal alanda var olan ağlar üzerinden yapılabilmektedir. Dünya nüfusunun %67.1'i internete erişim sağlayabilmektedir (We are social, 2023). İnternet fikirlerin yayılmasındaki en büyük ortamlardan birini yaratmaktadır, siber alandaki bu fırsat toplumsal güvenliği etkilemektedir.

Bir diğer neden; SSCB'nin dağılması ile birlikte birçok yeni devlet bağımsızlığına kavuşmuş ve toplumsal birlik, kimlik elde etme çabalarına girişmişlerdir. Bu özellikle Avrupa Birliği'nin (AB) genişleme ve derinleşme⁵ sürecinde oldukça fazla üzerinde durulan konulardan olmuştur (Lebedeva, vd., 2021: 145). Ayrıca Soğuk Savaş döneminde ve sonrasında 11 Eylül ve Arap Baharı gibi olaylar sonucu bölgesel savaşlar meydana gelmiş ve otorite boşlukları oluşmuştur. Otorite boşlukları, bölgedeki insanların güvenliklerini ve geçimlerini sağlamak için çevre ülkelere göç etmelerine sebep olur. Ayrıca o bölgelerde birçok terör örgütünün faaliyet göstermesine olanak sağlar. Özellikle göç diğer ülkeler için son dönemlerde son derece tehlikeli hal almıştır (Korobkov ve Zaionchkovskaia, 2004: 492-493). Ülkelerin demografik yapısından ekonomik yapısına kadar birçok konuda zarar vermektedir. Sanal alanda bu göçlerin sonuçları ise toplumsal düzenin bozulması sonrası bazı taşkınlıkların örgütlenmesi ve sanal ağlar üzerinden yayılması şeklinde gerçekleşebilir. Göç eden kişileri terör örgütleri sanal âlemden ulaşarak bazı eylemlerde bulunmaya ikna edebilmektedir. Ayrıca göç çeşitli spekülasyonlara neden olur, spekülasyonlar sanal alanda hızlıca birçok kullanıcıya ulaşabilmektedir. Terörizmin ve göçün yarattığı sorunlar sanal alanlarda yer edindiği için toplumsal güvenliği sağlanması için sanal alanda güvenlik önemli yer edinmektedir.

Yukarıda yer alan nedenlerin dışında uyuşturucunun normalleştirilmesi ve satılması, insan ticareti, çeşitli zararlı eşyaların satılması gibi toplumsal güvenlik için son derece önemli olan konular günümüz de sanal alanda faaliyet göstermektedir (Alpna ve Malhotra, 2016: 145-148). Birçok devlet

⁵ AB için genişleme yeni üyelerin dâhil edilmesi anlamına gelmektedir. Özellikle SSCB'nin dağılmasından sonra Orta ve Doğu Avrupa ülkelerinin AB'ye üye olma dalgası AB'nin genişleme sürecidir. Derinleşme ise üye olan ülkelerin AB'ye adapte edilmesi ve üyeler arasında işbirliğinin geliştirilerek AB'nin yapısının her anlamda daha sağlamlaştırılma sürecidir. Yine özellikle Orta ve Doğu Avrupa ülkelerinin üye olmasından sonra AB yeni üye alımı yerine derinleşme sürecine odaklanmıştır.

bu sebeplerden dolayı siber güvenlik ekipleri kurarak sosyal medya gibi birçok ağ üzerinde denetimlerini sıkılaştırmaya çalışmaktadır.

İnternete ulaşan insan sayısının her geçen gün artması, sosyal medya kullanımının yaygınlaşması, sanal alanın propaganda aracı olarak kullanılmaya başlanması gibi unsurlardan ötürü toplum güvenliğinin sağlanması, sanal alandaki toplumsal güvenliğin de sağlanmasına bağlıdır. Bu yüzden sanal alanın güvenliği ile toplumsal güvenlik arasında sıkı bir bağ vardır.

2.6.5. Çevresel Alanda Siber Güvenlik

Çevresel alanda en çok kabul gören güvenlik anlayışı, kritik alt yapıların korunması şeklinde karşımıza çıkmaktadır (Miguel, vd., 2023: 732-735). 1996 yılından ABD’de, Kritik Altyapıların Korunması için Başkanlık Komisyonu (PCCIP) tarafından yayımlanan Marsh Raporu’nda kritik altyapı terimi kullanılmıştır (Lewis, 2015). Bu raporda kritik altyapı olarak sağlık hizmetleri, ulaşım, finans ve bankacılık, bilgi ve iletişim, su sağlama hizmetleri, acil kolluk hizmetleri, enerji ve acil durum hizmetleri sayılmıştır (The White House, 1998). Bunların dışında 2003 yılında ABD’de yayımlanan Kritik Altyapılar ve Temel Varlıkların Fiziksel Korunması için Ulusal Strateji belgesinde milli güvenlik ve çevre güvenliği için son derece kritik öneme sahip olan nükleer santraller ve baraj gibi yapıların kritik altyapılardan olduğu belirtilmiştir (The White House, 2003). Ayrıca son dönemde küresel ısınma ile birlikte ozon tabakasının delinmesi ve buzulların erimesi gibi konular da çevre güvenliğinin alt başlıkları arasına dâhil edilmiştir (Trombetta, 2010).

NATO’nun hazırlattığı Tallinn Manuelinde ise kritik altyapı, bir devletin sınırları içinde yer alan ve zarar görmesi veya yok olması durumunda o devletin güvenliğini, ekonomisini, halk sağlığını ya da çevre güvenliğini olumsuz yönde etkileyecek fiziki ya da sanal sistemler ve varlıklar şeklinde ifade edilmiştir (Schmitt, 2013). Bu altyapıların çoğu siber alana entegre bir şekilde faaliyet göstermektedir. Sanal uzaya entegre olmuş veya faaliyetlerinin belli bir kısmını buradan yürüten, kritik olarak niteleyeceğimiz ve siber alan ile çevresel alan arasındaki asıl bağı oluşturan çevresel sektörleri bir tablo şeklinde göstermek gerekirse;

Tablo 3: Siber Alandaki Kritik Çevresel Sektörler ve Faaliyet Alanları

Sektör	Faaliyet Alanı
Enerji Sektörü	Elektrik Dağıtım Sistemleri
	Petrol ve Doğal Gaz Üretim ve Dağıtım Tesisleri
	Nükleer Enerji Santralleri
Baraj ve Su Sistemleri	Su Arıtma Tesisleri
	Kanalizasyon Sistemleri
	Su Dağıtım Sistemleri
	Barajlar
	Sulama Sistemleri

Sektör	Faaliyet Alanı
Kimya Sektörü	Kimyasallar Fabrikalar vb.
İletişim Sektörü	Bilgi ve İletişim Altyapısı İnternet Altyapısı
Ulaşım Sektörü	Hava, Deniz, Kara ve Toplu Ulaşım Altyapıları

Tablo 3: (Devamı)

Tablo 3’de yer alan sektör ve faaliyet alanları siber saldırılar sonucu çevreye zarar verecek potansiyele sahip bir yapıdadır. Çevre güvenliğinde özellikle nükleer santraller, barajlar, enerji ve iletişim ağları son derece öneme sahiptir. Bu kritik altyapılara yönelik siber uzayda gerçekleştirilecek saldırılar sadece ilgili ülkede değil çevre ülkelerin çoğu için de tehlike oluşturacaktır. Örnekler vermek gerekirse, nükleer santral ağlarına yönelik saldırıda reaktörün düzenli çalışması engellenerek reaktörlerde farklı sorunlara yol açılabilir. Baraj ağlarına saldırı ile baraj kapaklarına müdahale edilebilir. Sel gibi çeşitli doğal afetlere yol açılabilir. İletişim ağlarının kesintiye uğraması ile acil durumlara müdahale edilemeyebilir. Su arıtma, kanalizasyon gibi kritik altyapılara yapılan müdahaleler sonucu halk sağlığı tehlikeye atılabilir. Ulaşım sistemlerinin durdurulması çeşitli kazalara neden olabilir. Bu örneklerle benzer birçok siber müdahale çevresel güvenliğin tehlikeye girmesine neden olabilir.

Kritik altyapıların siber uzaya entegrasyonu çevresel güvenlik ile siber güvenlik arasında sıkı bir bağ oluşmasına sebep olmuştur. Çevresel güvenliği sağlamak için aynı zamanda siber güvenliğin de sağlanması gerektiği güvenlikleştirmenin bu son başlığı için de geçerlidir.

2.6.6. Siber Alanın Güvenlikleştirmeye Uygunluk Derecesi

Kopenhag Okulu teorisyenleri bir konunun güvenlik meselesi olması için askeri, siyasi, ekonomik, toplumsal ve çevresel bir konu olması gerektiği görüşündedir. Değinilen beş alan da siber alan ile son derece ilişkilidir. Yukarıda bahsi geçtiği üzere beş ana konu içerisinde yer alan birçok olay ve olgu aslında siber güvenliğin faaliyet alanına yer almaktadır. Yani siber güvenlik, güvenlikleştirmede yer alan beş sektörün güvenliği için elzemdir.

Siber güvenliğin sağlanması değinildiği üzere oldukça zordur ve güvenlik süreklilik arz etmelidir. Tıpkı 1648 Westfalia’dan sonra devletler için sınır güvenliğinin elzem ve süreklilik arz etmesi gereken bir husus haline geldiği 21. yüzyılda da siber uzaya entegre edilmiş en küçük bir konunun dâhi güvenli hâle getirilmesi siber güvenliğin sürekli şekilde sağlanmasına bağlıdır. Siber güvenlik, sınır güvenliği ile benzer bir yapıya sahiptir ancak sınır güvenliğinden çok daha zor şekilde sağlanmaktadır.

Bireyler, kurumlar veya devletler günümüzde artık tam anlamıyla kendilerini güvende hissetmek istiyorlarsa geleneksel güvenliklerinin yanında siber güvenliklerini de sağlamak zorundadırlar. (Öğün ve Kaya, 2013: 165-170). Bu olasılık oldukça düşüktür, özellikle devletlerin

bu tür bir yapı oluşturmaları oldukça güçtür. Sınır güvenliğindeki ihlaller sonucu devletler savaşa girecek kadar olağandışı önlemler alma yetkisine sahiptir. Yani sınır güvenliği çok uzun zamandan beri güvenlikleştirilmiştir. Olağanüstü önlemler alınmasa bile yetki onayı alınmış başarılı bir güvenlikleştirme örneğidir. Sınır güvenliğine yakın bir yapıya sahip olan siber güvenlik de elzem olduğu için savunulması güç olmasına rağmen artık devletlerin gözünde bir sınır güvenliği niteliğindedir. Büyük bir siber alan ihlali için devletler karşılığını askeri enstrümanlar ile verme yoluna gitmeyi tercih edebilirler (Güler, 2018: 143-146).

Hedef kitle halk olduğunda bu söylem kulağa zor gibi gelmektedir. Çünkü insanlar bu konuda fazla bilinçli değildir ve siber suçlar için savaşa girmek gibi büyük bir sonucu onaylamak istemezler. Ancak devletler bu konuda daha bilinçlidir ve insanların aksine siber saldırıların büyük sonuçlar doğurduğunun farkındadır. Bu yüzden araştırmada örneklem olarak bir devlet değil devletlerarası bir birlik olan NATO tercih edilmiştir.

Siber güvenliğin sağlanmasının zor olması, güvenlikleştirme teorisinde yer alan beş alanın güvenliği için de ayrı ayrı tehdit oluşturmaları ve vereceği zararın boyutlarının her bir konu için epeyce büyük olacağı göz önüne alındığında, siber alanın güvenlikleştirme için oldukça uygun bir yapıya sahip olduğu ortaya çıkmaktadır.

ÜÇÜNCÜ BÖLÜM

3. KUZEY ATLANTİK ANLAŞMASI ÖRGÜTÜ VE SİBER ALAN

İlk bölümde Kopenhag Okulu ve güvenlikleştirme teorisinden ana hatları ile bahsedilmiştir. İkinci bölümde araştırmanın ilgi alanı olan siber alan ve siber güvenliğe değinilmiş ve güvenlikleştirme ile ilişkileri ele alınmıştır. Böylece iki alanın birbiri ile ilişkisi ortaya konmuştur. Bu bölümde ise bu iki konu arasındaki ilişki bir örneklem üzerinden anlatılacak ve araştırma sorusunun yanıtı ortaya çıkarılacaktır.

İlk olarak NATO'nun tarihinden, yapısından, işleyişinden bahsedilecektir. Zira NATO'nun aldığı kararlar ve siyasi elitlerinin söylemlerinin analizi için bu oldukça önemlidir. NATO'nun kuruluşu ve yapısı, Soğuk Savaş dönemindeki faaliyetleri, Soğuk Savaş sonrası varlığına yönelik eleştiriler, 21. yüzyılda kendini güncelleme çalışmaları ve siber alana yönelik çalışmaları ile aldığı kararlar üzerinde durmak konu bütünlüğü açısından gereklidir.

3.1. NATO'nun Kuruluşu

Tarih boyunca insanlar birbirleri ile savaşmışlardır. Devletlerin kurulması ile birlikte bu savaşlar devletler arasında olmuştur. Dünya genelinde neredeyse tüm devletleri ilgilendiren iki büyük savaş yaşanmıştır. Bunlardan ilki 28 Temmuz 1914 – 11 Kasım 1918 tarihleri arasında gerçekleşen I. Dünya Savaşı⁶'dır. İkincisi ise 1 Eylül 1939 – 2 Eylül 1945 tarihleri arasında gerçekleşen II. Dünya Savaşı⁷'dir. Bu iki savaş, dünyadaki neredeyse tüm ülkeleri etkilediği ve yıkıcılığı diğer savaşlara göre çok daha büyük olduğu için dünya savaşı niteliğindedir.

Devletler savaş sonrası belli şartlarda anlaşmalar imzalarlar ve bazı önlemler alırlar ve bunların barışı sağlamaya yönelik olduğunu iddia ederler. Dünya savaşları sonrası da yine barışın sağlanacağı

⁶ 28 Temmuz 1914-11 Kasım 1918 tarihi arasında dünya tarihinin o döneme kadar en büyük küresel savaşıdır. İttifak ve İtilaf olarak dünya iki kesime ayrılmıştır. 65.038.810 kişinin katıldığı savaşta, 8.556.315 kişi ölmüş, 21.219.452 kişi yaralanmış ve 7.750.945 kişi kaybolmuştur.

Ayrıntıları için bkz. NTV Tarih Dergisi Sayı:1 Şubat 2009.

⁷ 1 Eyl 1939 – 2 Eyl 1945 tarihi arasında I. Dünya Savaşı'ndan daha büyük ve yıkıcılığı daha çok olan savaştır. Mihver ve Müttefik olarak iki kesime ayrılmıştır. Yaklaşık olarak 110 milyon kişinin silahaltına alındığı savaşta, yaklaşık 80 milyon kişi ölmüştür.

Ayrıntılar için bkz. <https://www.aa.com.tr/tr/dunya/insanlik-tarihinin-en-buyuk-felaketi-2-dunya-savasi/2674182>

iddia edilerek belli anlaşmalar imzalanmış ve bazı önlemler alınmıştır. I. Dünya Savaşı sonrası imzalanan barış anlaşmaları ve alınan önlemler barışı korumaya yetmemiştir. Bunun nedeni imzalanan anlaşmaların yenilen devletler için ağır hükümler içermesidir. Savaş sonrası barışı sağlamak amacıyla kurulan Milletler Cemiyeti aldığı kararları uygulatacak bir güç mekanizmasına sahip olamamıştır. Aynı zamanda cemiyetin tarafsızlığı sorgulanmış ve kazanan devletlerin çıkarlarını koruduğu iddia edilmiştir (Polat, 2020a: 1956). Ayrıca ABD'nin savaş sonrası yeniden Monroe Doktrini'ne⁸ geri dönmesi, kazanan devletlerin savaştan kaynaklı güç kaybetmeleri, uluslararası sistemde anarşik bir yapı oluşturmuş ve kaybeden devletlerde aşırı görüşlerin⁹ oluşmasına ortam sağlamıştır. Bu sebeple I. Dünya Savaşı sonrası alınan önlemler II. Dünya Savaşı'nı önlemeye yetmemiştir.

Yetersiz önlemler sonucu başlayan II. Dünya Savaşı sırasında devletler; I. Dünya Savaşı sonrasında yapılan hataların bir daha yapılmaması için savaş sonrası kurulacak uluslararası sistemin yapısını, savaş sırasında yapılan görüşmelerle planlamaya çalışmışlardır. Bu görüşmelerden bazıları şu şekildedir;

1. Moskova Konferansı (19 Ekim-1 Kasım 1943): ABD, İngiltere, Sovyet Rusya ve Çin Dışişleri Bakanları 19 Ekim 1943'te Moskova'da son gelişmeler için toplanmışlardır. Görüşmede savaş sonrası Almanya ve İtalya'nın aşırı görüşlerden tasfiye edilmesi gerektiği kararı alınmıştır.

2. Tahran Konferansı (28 Kasım-1 Aralık 1943): Churchill, Roosvelt ve Stalin'in bir araya gelmesiyle yapılan toplantıda savaş ve savaş sonrası düzen ele alınmıştır. Tahran, savaş sonrası oluşacak uluslararası düzen hakkında ilk fikir ayrılıklarının yaşandığı yer olmuştur.

3. Dumbarton Oaks Konferansı (21 Ağustos-7 Ekim 1944) : I. Dünya Savaşı sonrası oluşan otorite boşluğunun bu savaş sonrası oluşmaması için ABD, Birleşik Krallık, Sovyetler Birliği ve Çin dünya düzeni için hamilik yapmak istemişlerdir. (Kelsen, 1945: 45). Konferansta görüşülen bu fikir sonrası Dumbarton Oaks Önerileri oluşturulmuştur. Dumbarton Oaks Önerileri ile I. Dünya Savaşı

⁸ 1823'te Başkan James Monroe tarafından Monroe Doktrini ilan edilmiştir. Avrupa'ya çalkantılı Eski dünya olarak nitelendirilmiş ve Yeni Dünya olarak nitelendirdikleri Amerika'nın bu çalkantıdan uzak kalması gerektiğini ve yalnızlık politikası yürütmesi gerektiğini savunulmuştur. I. Dünya Savaşı'na kadar bu politika ABD temel politikalarından biri olmuştur. I. Dünya Savaşı'na dâhil olduktan sonra bu politika kesintiye uğramıştır. Savaş sonrası ise dönemim ABD Başkanı Thomas Woodrow Wilson'un karşı ısrarlarına rağmen ABD politika yapıcılar tarafından Monroe Doktrini'ne geri dönmüştür.

⁹ I. Dünya Savaşı'nı kaybeden Almanya, savaş sonrası ağır barış koşulları olan Versay Barış Anlaşması'nı imzalamak zorunda kalmıştır. Anlaşmanın ağır hükümler içermesi ve Almanya'ya hareket alanı tanımaması Almanya'da aşırı görüşlerin destekçi kazanmasına sebep olmuştur ve Adolf Hitler önderliğinde Nasyonal Sosyalist Alman İşçi Partisi (Naziler) Almanya'da yönetimi ele geçirmiştir.

I. Dünya Savaşı'nın galipleri arasında yer almasına rağmen çıkar mücadelesi yüzünden istediklerini elde etmesi engellenen İtalya'da da aynı şekilde aşırı görüşler güç kazanmış ve Benito Mussolini önderliğinde Ulusal Faşist Partisi yönetimi ele geçirmiştir. Bu iki ülkenin daha sonraki yıllarda uluslararası arenada attığı adımlar II. Dünya Savaşı'nın başlamasına sebep olan en önemli nedenlerden olmuştur.

sonrası görevini yerine getiremeyen MC'nin yerine daha yaptırım gücene sahip bir örgütün kurulması gerektiği savunularak Birleşmiş Milletler'in (BM) kurucu anlaşmasının temeli oluşturulmuştur.

4. Yalta Konferansı (4-11 Şubat 1945): Üç Büyükler Konferansı olarak da anılan Yalta Konferansı, savaşın Müttefik Devletler tarafından kazanılacağı artık kesinleşmesi sonrası yeni dünya düzeninin tartışıldığı konferanstır. Konferansta özellikle Avrupa Kıtası'nın nasıl şekilleneceği gündeme alınmıştır. Taraflar arasındaki ideolojik farklılıklar giderek daha derinleşmiş, Almanya üzerinde oluşturulan işgal bölgeleri ideolojik bir çatışma ve propaganda alanı haline dönüşmüştür. Böylece Soğuk Savaş'a giden düzen tartışma ortamı başlamış ve Müttefik Devletler kendi arasında savaşıma noktasına gelmiştir (Özdemir, vd., 2018: 62-79).

Özellikle Yalta Konferansı başta olmak üzere diğer tüm konferanslarda Müttefik Devletler arasında çıkar mücadeleleri görülmüş ve konferanslar bir nevi savaş sonrası oluşacak ortamın fragmanı olmuşlardır (Özdemir, vd., 2018: 71). Müttefik Devletler açısından savaş sırasında hedeflenen ve üzerinde fikir birliğine varılmış iki ana konu vardı. Bunlardan birincisi uluslararası sistemde barışın korumasını sağlayacak bir örgütün kurulmasıdır. (Birleşmiş Milletler, 25 Nisan 1945'te 50 ülkenin temsilcileri, San Francisco Konferansı'nda bir araya gelerek 111 maddeden oluşan antlaşma ile kurulmuştur. Böylece ilk fikir gerçekleşmiştir.) İkincisi ise Almanya'nın kesin bir yenilgiye uğratılması gereken düşman olduğu ortak fikri olmuştur. Bu fikirler Müttefik Devletlerin savaş sonuna kadar birlikte hareket etmelerine sebep olmuştur.

8 Mayıs 1945'te Almanya'nın teslim olmasından sonra II. Dünya Savaşı'nda Müttefik Devletleri bir arada tutan ikinci fikir de ortadan kalkmıştır. Savaşın tamamen bitmesi sonucu artık çıkar mücadelesi başlamış ve Müttefik Devletler'in kendi içindeki fikir ayrılıkları ortaya çıkmıştır. Çıkar mücadelesinde iki devlet ön plana çıkmıştır. ABD, iki savaşa da katılmasına rağmen coğrafi açıdan uzak olduğu için sanayisi savaşlardan etkilenmemiş ve yürüttüğü politikalar sayesinde uzun vadede savaş ekonomisinden fayda görmüştür. Bu nedenlerden dolayı ön plana çıkan devletlerden ilki ABD olmuştur. İkinci devlet olan SSCB ise I. Dünya Savaşı esnasında yaşanan Bolşevik Devrimi¹⁰ ile komünist yönetime geçmiş, iki dünya savaşı arasında devrimi ihraç etmeye ve ekonomik olarak toparlanmaya çalışarak geçirmiştir. II. Dünya Savaşı'nda ise Almanya tarafından gerçekleştirilen Barbarosa Harekâtına¹¹ maruz kalmıştır. Bu saldırılar esnasında maddi ve manevi olarak çok zarara uğramasına rağmen saldırıyı durdurmayı başarmıştır. SSCB, dünya savaşlarında

¹⁰ Vladimir Lenin'in "ekmek, barış, özgürlük" sloganı altında Rus veya Ekim devrimi olarak da bilinen bir halk harekâtıdır. Fransız İhtilali'nden sonra Rusya'da gelişen sosyal, ekonomik ve siyasi olayların bir sonucu olarak ortaya çıkmıştır. Rusya'nın I. Dünya Savaşı'ndan çekilmesine ve İtilaf Devletlerine muhalif bir yönetim anlayışı ile yönetilmesine neden olmuştur. Ayrıca devrim SSCB'nin kurulmasının önünü açmıştır.

¹¹ II. Dünya Savaşı sırasında Almanya'nın SSCB'yi işgal etmek için 22 Haziran-5 Aralık 1941 tarihleri arasında yürüttüğü askeri harekâtıdır. Harekâtın başarısız olması sonrası Almanya çöküm sürecine girmiş ve savaşın galibi resmi olmasa da fiilen belli olmuştur.

yaşadığı bu olaylara rağmen II. Dünya Savaşı'ndaki Doğu ve Orta Avrupa politikaları ile etkinliğini arttırdığı ve askeri olarak güçlü kalabilmeyi başardığı için ön plana çıkan diğer devlet olmuştur.

Bu iki devletin ön plana çıkmasının bir diğer nedeni ise ikisi dışında askeri ve ekonomik olarak ayakta kalan başka devlet olmamasıdır. Savaşlarda yenilgi alan Almanya ve Japonya maddi ve manevi kayıplarını uzun yıllar gidermeye çalışacağı bir döneme girmiştir. İngiltere, iki dünya savaşında da kazanan tarafta yer almasına rağmen askeri potansiyeli bu savaşlarda verdiği kayıplar ile azaltmış, bunun yanında savaştan dolayı ekonomik olarak çökme noktasına gelmiştir. Fransa ise II. Dünya Savaşı sırasında tamamen Almanya tarafından işgal edilmiş, askeri ve ekonomik olarak son derece zayıflatılmıştır. Birleşmiş Milletler Güvenlik Konseyi üyesi olan Çin ise savaşlarda aşırı kayıplar vermemiş ancak Çin o dönemlerde ekonomik ve askeri olarak günümüz seviyesinden ve dönemin iki süper gücünün seviyesinden oldukça uzak noktada kalmıştır. Bu yüzden ABD ve SSCB, II. Dünya Savaşı sonrası öne çıkan devletler olmuşlardır.

II. Dünya Savaşı'ndan sonra İngiltere Başbakanı Winston Churchill ABD Başkanı Truman'a 12 Mayıs 1945'te yolladığı telgrafta “Bir ya da iki yıl içinde durum ne olacak? Bu tarihte Amerikan ve İngiliz orduları eriyecek, Fransızlar esaslı bir şekilde teşkilatlandırılmaktan uzak duracak, buna karşılık Rusya iki veya üç yüz tümenini ayakta tutma kararı verebilecektir... Cepheye bir demir perde inmiştir. Ardında ne olup bittiğini bilmiyoruz” (Siyasi ve Sosyal Araştırmalar Vakfı, 1997: 12-13) diyerek aslında Avrupa'da oluşan güç boşluğunu gündeme taşımış ve SSCB'nin bu boşluktan yararlanabileceğine ve etki alanını artırabileceğine değinmiştir. Churchill'in dediği şey gerçekleşmiş ve 1947'de Macaristan, Bulgaristan, Romanya ve Polonya'daki komünistler bir süre koalisyon hükümetlerinde yer almış sonra SSCB'nin desteği ile iktidarı ele geçirerek demokratik yönetimlere son vermişlerdir (İsmay, 1956: 5). Böylece SSCB, etki alanını Batı Avrupa sınırlarına kadar genişletmiştir. SSCB'nin 1948'de meydana gelen Berlin Ablukası¹² olayı ve Birleşmiş Milletler Güvenlik Konseyi'ndeki (BMGK) konumunu kullanarak BMGK'da güvenlik anlamında alınmak istenen kararları 1949'a kadar 30 kez veto etmiş olmasından dolayı ABD ve İngiltere başta olmak üzere demokratik yönetim sergileyen Avrupa ülkeleri tarafından SSCB'nin güvenlik anlamında büyük tehdit yarattığı düşünülmeye başlamıştır.

¹² Savaş sonrası Berlin dört bölgeye ayrılmıştır. 1948 yılında ABD, İngiltere ve Fransa kendi işgal bölgelerini birleştirme kararı aldı ve Trizonia'da birleştirdi. Ancak SSCB kendi işgal bölgesini bu karara dâhil etmemiş ve alınan kararı hoş karşılamamıştır. Hemen akabinde birleştirilen bölgede para reformu yapıldı ve yeni Alman Mark'ı çıkarıldı. Bunun üzerine SSCB kendi işgal bölgesinden birleştirilen bölgeye olan demiryollarını, su ve kara ulaşımını kapattı ve bölgeyi ablukaya aldı. Batılı ülkeler bölgeye ulaşması için SSCB'nin işgal bölgesinden geçmek zorundaydılar. Bu abluka ile bölgeye sadece daha maliyetli olan hava ulaşımı ile ulaşabilmişler ve bölge halkının gereksinimlerini bu yolla sağlamışlardır. Altı ay içerisinde bölgeye yüz bin uçuş yapıldığı tahmin edilmektedir. Yapılan müzakereler sonuç vermeyince Berlin Doğu ve Batı olarak ikiye ayrılmış ve Batı Almanya ve Doğu Almanya olarak iki devlet kurulmuştur. Ayrıntılar için bkz. <https://www.deutschland.de/tr/topic/politika/1948-hava-koprusu-ve-berlin-ablukasi-imdada-yetisen-kuru-uzum-bombardiman-ucaklari>

Ayrıca ABD, I. Dünya Savaşı'ndan sonra tekrar kendi coğrafyasına odaklanmış ve yalnızlık politikasına geri dönmüştür. Ancak II. Dünya Savaşı'ndan sonra ise SSCB'nin oluşturduğu tehdit, Avrupa'daki otorite boşluğundan ve savaş sonrası çöken Avrupa ekonomisinin ABD'ye muhtaç olmasından dolayı ABD bu sefer yalnızlık politikasına dönmemiş dünya siyasetinde son derece aktif rol oynamıştır. Bunun en büyük kanıtı dönemin ABD Başkanı Truman'ın 5 Nisan 1946'da Ordu Günü münasebetiyle Chicago'da yaptığı konuşmasında *“Güçlü bir devlet olmanın Birleşik Amerika'ya büyük sorumluluklar yüklediğini; bu sorumluluklardan kaçmanın uluslararası barış, istikrar ve güvene büyük bir ihanet olacağını ve geline nokta Amerikan dış politikasının evrensel olması gerektiğini, değinmiş aynı zamanda Ortadoğu'ya yönelik olarak: “Gözlerimizi Yakın ve Ortadoğu'ya çevirdiğimiz zaman, vahim meseleler arz eden bir bölge ile karşılaşırız. Bu bölgede geniş doğal kaynaklar bulunmaktadır. En işlek kara, hava ve deniz yolları buradan geçmektedir. Bu bakımdan büyük iktisadi ve stratejik öneme sahiptir. Fakat bu bölgedeki ulusların hiçbiri ne yalnız ne de beraberce kendilerine yöneltilecek bir saldırıya karşı koyabilecek kadar güçlüdürler. Böyle olunca da Yakın ve Ortadoğu'nun bu bölgenin dışındaki büyük devletlerarasında önemli bir rekabet alanı olacağını ve bu rekabetin birdenbire bir çatışmaya yol açabileceğini kestirmek güç değildir.”*(Bağcı, 2001: 5) ifadelerini kullanmasıdır.

SSCB'nin savaş döneminde ve sonrasında izlediği politikalardan çıkarım yapıldığında en önemli hedeflerinden birinin Türkiye'nin egemenliği altında olan boğazlardan ayrıcalık elde ederek, Akdeniz havzasına ulaşma isteği olduğu söylenebilir. Akdeniz havzası Başkan Truman'ın bahsettiği Ortadoğu'ya ulaşımında en önemli alandır. Buradan anlaşılacağı üzere Avrupa'da komünist-demokrasi savaşına giren ABD ve SSCB, Ortadoğu'da da bir çıkar mücadelesinin sinyallerini izledikleri politikalarla vermiştir. Bu da iki devletin askeri ve ekonomik olarak karşı karşıya geldiğini bir kez daha göstermiştir. 1946-1949 yılları arasında Yunanistan'da iç savaş yaşanması ve SSCB'nin Türkiye üzerinde baskısını artırarak savaş tehditlerinde bulunması ABD'nin Ortadoğu'ya yönelik politikalar geliştirmesini zorunlu hale getirmiş ve ABD, Truman Doktrini kapsamında bu iki devletin zorlukları aşması için 1948 yılına kadar 400 milyon yardım edileceğini açıklamıştır. Aynı şekilde Avrupa ülkeleri için de 1948 yılında ekonomik kalkınmalarını sağlamaları için Marshall Yardımları adı altında ekonomik yardım sağlamaya başlamıştır. Kısacası II. Dünya Savaşı sonrasında ABD ve SSCB güçlü kalabilen iki devlet olmuş ve aralarındaki savaş sırasında var olan fikir ayrılıkları gün yüzüne çıkmıştır. İki devlet benimsedikleri politikalar yüzünden Avrupa ve Ortadoğu başta olmak üzere dünyanın birçok noktasında karşı karşıya gelmiştir. ABD, SSCB'nin bu politikalarını engellemek için SSCB'nin etki alanının çevresindeki ülkelere ekonomik yardımlar sunmuştur.

Batı Avrupa devletlerinin ABD'nin sunduğu ekonomik yardımlara rağmen askeri olarak güçsüz olmaları SSCB'nin Avrupa'da kolayca yayılmasına olanak sağlamıştır. SSCB, II. Dünya Savaşı sırasında askeri birlikleri ile ele geçirdiği ülkeler olan, Polonya, Macaristan, Doğu Almanya, Bulgaristan, Romanya ve Arnavutluk'tan çıkmamış ve 1947-1948 yıllarında bu ülkeleri kendisine bağlı birer uydu ülke hâline getirmiştir (Gönlübol ve Ülman, 1996: 147-150). BM'nin ikazlarına

rağmen SSCB orduları doğu sınırlarında İran'ın kuzeyini terk etmemiş, Tebriz'de Azerbaycan Demokratik Cumhuriyeti ve Mehabad'da Bağımsız Kürt Cumhuriyeti kurulmasına ön ayak olmuştur. Ayrıca, çevresindeki ülkelerden askeri olarak müdahale edemediği Türkiye ve Yunanistan'a karşı da baskılarını arttırmış ve askeri tehditlerde bulunmuştur. SSCB Asya'da ise Mançurya ve Kuzey Kore'yi işgal etmiştir. 22 Şubat 1948 tarihinde gerçekleşen Prag Darbesi¹³ yayılmacılığın ne seviyeye ulaştığını gözler önüne sermiş ve Batı Avrupa ülkelerinin harekete geçmesine yol açmıştır. Batı Avrupa ülkeleri, SSCB'yi çevreleme politikasını benimsemişler ve savunma birliği çabalarına girişmişlerdir (Gül, 2015: 252). Bu kapsamda 4 Mart 1948'de savunma birliği için bir araya gelen İngiltere, Fransa ve Benelüks¹⁴ ülkeleri 17 Mart 1948'de ortak bir savunma anlaşması olan Brüksel Anlaşması'nı imzalamışlardır. Ancak ABD'nin katılmadığı bir savunma birliğinin SSCB'yi durdurmak için yeterli olmayacağı açıktır. Bunun farkında olan Başkan Truman, Brüksel Anlaşması'nın imzalandığı gün Kongre'ye konuşma yaparak "ABD'nin özgür uluslara gerekli desteği sunacağına inandığını" belirtmiş, böylece ABD hükümetinin anlaşmaya katılma politikasında olduğunu göstermiştir. Katılım politikası kapsamında Senatör Vandenberg'in hazırladığı ve 11 Haziran 1948'de Senato'da 68 oyun 64'ünü alan "Karar 239" ile BM Şartnamesi'nin 51. Maddesi gereğince ABD'nin bölgesel ittifaklara katılmasının yolu açılmıştır (Huntley, 1965: 34-35). Karar sonrası ABD ve Kanada, 15 Mart 1949'da, Portekiz, Norveç, İzlanda, İtalya ve Danimarka'yı da Brüksel Anlaşmasına katılmaya davet etmişlerdir. Böylece İngiltere, Fransa, Belçika, Hollanda, Lüksemburg, Portekiz, Norveç, İzlanda, İtalya, Danimarka, ABD ve Kanada 4 Nisan 1949'da Kuzey Atlantik İttifak Anlaşması (Washington Anlaşmasını) imzalayarak NATO'yu kurmuşlardır.

NATO, II. Dünya Savaşı'ndaki ekonomik, sosyal, askeri ve çevresel yıkımların yüksek seviyede olması, SSCB'nin Doğu ve Orta Avrupa'da yayılması, uydu devletleri vasıtasıyla Avrupa'da hakimiyet kurması ve SSCB'nin uydu devletleri ile kurduğu hakimiyeti ordusu ile Batı Avrupa'ya yayma tehlikesi sonucu kurulmuştur (Karber ve Combs, 1998: 399).

3.2. NATO'nun Soğuk Savaş Dönemindeki Stratejisi

Soğuk Savaş'ın getirdiği koşullar yüzünden kurulan NATO, Soğuk Savaş dönemi boyunca geleneksel anlayışta olduğu gibi askeri temelli güvenlik örgütü olmuştur. Anlaşmanın 5. maddesinde; "Kuzey Amerika ya da Avrupa'da bulunan üye ülkelerden herhangi birine karşı girişilecek bir silahlı saldırı tarafların tamamına yapılmış bir saldırı olarak kabul edilecektir." ifadesi yer almaktadır. Maddeden anlaşılacağı üzere sınır güvenliği en üst seviyede tutulmuş ve üye ülkelerin hepsini

¹³ Prag Darbesi ile 1948 yılında Çekoslovakya'da Komünist Partisi'nin SSCB desteğini alarak yönetimi ele geçirmiştir. Çok uluslu bir yapıdaki ve Avrupa'nın merkezindeki bir ülkenin Komünist yönetime geçmesi büyük bir infialak oluşturmuştur. Bu olay Soğuk Savaş'ın başladığının en belirgin örneği olmuştur ve SSCB'nin yayılmacılığının ne seviyede olduğunu Batı Avrupa ve Kuzey Amerika ülkelerine göstermiştir. Olay sonrası bu ülkeler tarafından bir güvenlik örgütü kurma çabalarına hız verilmiş ve sonucunda NATO kurulmuştur.

¹⁴ Benelüks; Belçika, Hollanda ve Lüksemburg'un coğrafi olarak birlikteliğini anlatan bir kavramdır.

kapsayacak topyekûn savaş sebebi olarak görülmüştür. NATO, Soğuk Savaş boyunca üye ülkelerine yönelik gerçekleşecek saldırı önleme ve caydırma politikalarını ön planda tutmuştur. Dolayısıyla NATO Soğuk Savaş döneminde askeri bir güvenlik örgütü olmuştur.

Uluslararası bir örgütün politikaları, örgüt üyesi olan en güçlü devletin veya devletlerin politikaları ile paralellik gösterir. Bu açıdan bakıldığında NATO'nun Soğuk Savaş döneminde aldığı kararların çoğu ABD politikaları ile paralel bir yapıya sahiptir (Tokatlı, 2022: 67). Bu gücün sebepleri ise; Marshall ve Truman Doktrin'lerinin gösterdiği gibi ABD'nin, ekonomik açıdan ayakta kalan tek Batı ülkesi olması ve diğer ülkelerin savaştan sonra yıkım ve ekonomik çöküntü içerisinde bulunmasıdır. Ayrıca askeri olarak atom bombası gücüne sahip olan tek devlettir. Yani SSCB'nin sahip olduğu askeri gücü önleyebilecek tek ülke olarak görülmüştür. Bu sebepler ABD'yi ülke ülkelerin en güçlüsü konumuna getirmiş ve NATO'nun izlediği politikalara benzer politikalar izlenmesini sağlamıştır.

NATO'nun Soğuk Savaş yıllarındaki ana hedefi SSCB'nin yayılmasına engel olmak olmuştur. NATO bu hedefini gerçekleştirmek için SSCB'yi çevreleme yoluna gitmiş ve üye sayısını arttırmıştır. Anlaşmanın 10. maddesine göre Kuzey Atlantik bölgesinin güvenliğine destek verecek ve anlaşmanın prensiplerinin geliştirilmesine katkı sunacak herhangi bir Avrupa ülkesine üyelik için davet yapılabilir. Bu kapsamda, 18 Şubat 1952 tarihinde Türkiye ve Yunanistan, 9 Mayıs 1955 tarihinde Federal Almanya ve 30 Mayıs 1982 tarihinde İspanya NATO üyeliğine alınmış ve kurucu üyelerle birlikte üye sayısı 16'ya yükselmiştir. Üye olarak alınan ülkeler SSCB'nin yayılma alanları olarak gördüğü yerler veya SSCB'nin uydusu altına aldığı bölgelerin sınırlarında olan yerlerdir.

NATO politikalarını etkileyen bir diğer unsur silahlanma yarışı olmuştur. II. Dünya Savaşı'nda ABD, 6 Ağustos 1945'te Uranyum-235 tipi atom bombasını (Little Boy) Hiroşima'ya ve 9 Ağustos 1945, Plütonyum-239 tipi atom bombasını (Fat Man) Nagazaki'ye atmıştır. Bu saldırılar ABD'nin dünyadaki atom bombasına sahip olan bir güç olduğunu kanıtlamıştır. Ancak 23 Ağustos 1949'da SSCB'nin ürettiği ilk atom bombasını patlatması ABD'nin nükleer güç anlamında dünyadaki tekeline son vermiştir. Bu ABD'yi harekete geçirmiş ve hidrojen bombası için çalışmalar başlatmıştır. ABD'nin ilk hidrojen bombasını 1 Kasım 1952'de patlatarak hedefine ulaşmasına rağmen SSCB de 12 Ağustos 1953'te ilk hidrojen bombasını patlatmıştır. Bu silahlanma yarışının yanında ABD politik olarak harekete geçmiş ve Nisan 1950 yılında NSC68¹⁵ raporunu kongrede kabul etmiştir. ABD silah yarışında ön plana çıkamayınca 1952 yılında Lizbon'da düzenlenen NATO Bakanlar Konseyi'nde NSC68 belgesini NATO'nun resmi stratejisi olarak kabul ettirmiştir (Gürkaynak, 2004). Aynı şekilde ABD Ulusal Güvenlik Konseyi 1953 yılında NSC162 raporunu hazırlamış ve Aralık 1954 yılındaki NATO konseyinde rapor NATO'nun yeni stratejisi olarak kabul edilerek "Topyekûn Karşılık"

¹⁵ NSC68: Amerikan Ulusal Güvenlik Konseyi (NSC) tarafından geliştirilen 68 nolu strateji belgesidir. NSC bu belge ile SSCB'nin nükleer kapasite gelişimi ve yayılmacı politikalarına karşı ABD'nin Soğuk Savaş yıllarında izlemesi gereken politikaları belirlemiştir.

benimsenmiştir. Nükleer silahlar dâhil tüm unsurların kullanılacağı ilan edilmiştir. Böylece SSCB'nin yayılma stratejisini savaş tehdidi ile durdurmuştur (Gül, 2015). Ancak 4 Ekim 1957 tarihinde SSCB, Sputnik'in uzaya fırlatılması sonrası ABD o tarihe kadar yüzleşmediği bir tehlike ile yüzleşmiştir. Sputnik ile birlikte SSCB 8000 km. mesafeye füze fırlatma kabiliyetine yani Kıtalararası Uzun Menzilli Güzümlü Füze (ICBM) teknolojisine sahip olduğunu göstermiştir. Bu Amerikan kıtasını yani ABD'yi vurabilme mesafesidir. Bu gelişme ile ABD, o güne kadar mümkün olmayan topraklarına saldırı tehlikesi ile yüzleşmiştir.

Gelişmeler sonrası literatüre yeni bir kavram kazandırılmıştır. İki tarafta yer alan devletlerin birbirlerini yok etme gücüne sahip olması sonrası "ilk vuruş üstünlüğü" kavramı ortaya çıkmıştır. İlk vuruş üstünlüğü, ilk saldıran tarafın, diğer taraf saldırmadan saldırı olanaklarını yok etme olanağı olarak bilinmektedir. Bu yüzden iki taraf da çok farklı noktalarda saldırı kapasitelerini saklı tutmuş ve bazı nükleer silahları sürekli olarak farklı noktalara hareket ettirmişler ve bir nevi önlem almaya çalışmışlardır. Alınan önlemlerin dışında ABD, NATO ülkelerine Orta Menzilli Güzümlü Füze (IRBM) yerleştirme teklifinde bulunmuştur. Bununla birlikte SSCB topraklarına yakın noktalarda vuruş kabiliyeti kazanmak hedeflenmiştir. Ancak SSCB'de aynı politikayı güderek Küba'ya füze yerleştirme girişiminde bulunmuş ve Soğuk Savaş döneminde savaşa en çok yaklaşılan olay olan 1962 Küba Krizi patlak vermiştir. Bu kriz sonrası iki taraf da işin ciddiyetine varmış ve sert politikalarından geri adım atmışlardır. ABD, Türkiye'deki Jüpiter füzelerini sökme sözü vermiştir buna karşılık SSCB'de Küba'ya füze yerleştirmekten vazgeçmiştir. Savaş noktasına gelen bu olay sonrası Soğuk Savaş dönemin içerisinde Yumuşama Dönemi olarak adlandırılan döneme girilmiştir. 20 Haziran 1963 tarihinde iki taraf arasında kriz anlarında direk iletişim sağlanabilmesi için "Sıcak Hat" olarak adlandırılan iletişim kanalı oluşturulmuştur. Bu yumuşama NATO politikalarına da yansımıştır. 1967 yılında hazırlanan Harmel Raporu ile NATO üye ülkeleri arasındaki bütünlüğün pekiştirilmesi ve SSCB ve uydu devletleri ile iyi ilişkiler geliştirme yoluna gidilmiştir.

Yumuşama döneminde nükleer silahların azaltılması da gündeme gelmiştir. Silahlanma yarışı ile birlikte çok fazla nükleer silah stoğu yapan iki taraf, dünyayı defalarca yok edecek silah gücüne kavuşmuşlardır. Bu güç ayrıca tehlikeleri de beraberinde getirmiştir. Bu silahların korunması ve saklanması iki devlet için yük olmuştur. Ayrıca meydana gelecek ufak bir kaza sonrası önüne geçilemeyecek bir felaketin fitili ateşlenmiş olacaktır. Bu yüzden iki blok Helsinki'de 17 Kasım 1969-Mayıs 1972 tarihleri arasında sürdürülen müzakereler neticesinde 26 Mayıs 1972'de R. Nixon ve Leonid Brezhnev SALT I Anlaşması'nı imzalamışlardır. Nükleer silahların kontrollü şekilde azaltılmasını içeren bu anlaşma iki blok arası ilişkide önemli bir kilometre taşı olmuştur. Oluşan ılımlı hava ile birlikte iki blok arasında siyasi diyalog gelişmiştir. 1972'te başlayan Helsinki süreci 1 Ağustos 1975'te 35 ülkenin Helsinki Nihai Senedi'ni imzalaması ve Avrupa Güvenlik ve İş Birliği Teşkilatı (AGİT) yapılanmasının kurulmasıyla neticelenmiştir. AGİT, Batı ve Doğu blokları arasından askeri, siyasi, ekonomik ve sosyal meselelerin müzakere edilmesi bağlamında önemli bir mekanizma haline gelmiş, 1972-1979 yılları arasında gerçekleşen görüşmeler neticesinde 18 Haziran

1979'da Viyana'daki Hofburg Sarayı'nda SALT II anlaşması imzalanmıştır. Stratejik nükleer silahların üretiminin ve sayısının azaltılmasını içeren bu anlaşma 24 Aralık 1979 tarihinde SSCB'nin Afganistan'ı işgal girişimi başlayınca ABD Kongresi tarafından kabul edilmemiş ve askıda kalmıştır.

Afganistan'ı işgal girişimi SSCB için on yıl sürecek çöküşün başlangıcı olmuştur (Dibb, 2010). ABD'nin 1 Kasım 1955 yılında başlattığı Vietnam Savaşına benzer bir savaş yaşanmıştır. Coğrafyanın büyüklüğü, gerilla tarzı direnişin güçlü olması ve Vietnam'da kendisinin yaptığı gibi ABD ve diğer NATO ülkelerinin direnişçilere destek vermesi ile on yıl sürecek bu savaş SSCB'nin güçlü olmayan ekonomisini paramparça etmiş ve SSCB'nin askeri olarak düşünüldüğü kadar güçlü olmadığını göstermiştir. Komünist yönetimin çökmeye başlaması, 1985 yılında Michael Gorbaçov'un SSCB'nin yeni devlet başkanı seçilmesi, glasnost ve perestroyka ¹⁶ yani açıklık/şeffaflık ve yeniden yapılanma ilkelerini açıklaması ile birlikte çöküş hızlanmıştır. Gorbaçov, Doğu Almanya'da yaptığı konuşmada "Tarih geç kalanları affetmez" diyerek Demir Perde ülkelerini değişime davet etmiştir (Gül, 2015: 256). Bu konuşma ile birlikte geri dönüşü olmayan süreç başlamıştır. 9 Kasım 1989'da Berlin Duvarı yıkılmış ve SSCB'nin uydu devletlerinde Renkli Devrimler¹⁷ başlamış ve Aralık 1989'da Çekoslovakya'da gerçekleşen Kadife Devrim ile Renkli Devrimler tamamlanmıştır. Böylece Doğu Avrupa'daki Sovyet egemenliği sona ermiştir. NATO dağılma sürecinde devrimleri hoşnutlukla karşılamış ve kansız bir şekilde gerçekleşmesi için destek olmuştur. Son olarak SSCB'nin Doğu ve Orta Avrupa'daki uydu ülkelerinin 5-6 Temmuz 1991'de Brüksel'de Avrupa ile Bütünleşme Protokolü'nü imzaları sonucunda SSCB dağılmış ve Soğuk Savaş bitmiştir.

Genel anlamda baktığımızda Soğuk Savaş döneminde NATO'nun izlediği stratejilerden bahsederken daha çok ABD'nin stratejilerinden bahsedildiği düşünülebilir. Ancak NATO'nun o dönemde hem ekonomik olarak hem de askeri olarak tek ayakta kalan ülkesi ABD'dir. SSCB'nin karşısında durabilecek tek güç de aynı şekilde ABD olarak görüldüğü için ABD'nin izlediği politikalar NATO'nun da izlediği politikalar olmuştur. Bunun en önemli örneği Küba Krizi'dir. Krize kadar NATO, ABD gibi Doğu Blokuna karşı sert tutumlar sergilerken krizden sonra yine ABD'nin izlediği ılımlı politika anlayışını benimsemiştir. Ayrıca, NSC68 ve NSC168 belgelerinin NATO stratejileri olarak benimsenmesi ile 1956 Süveyş Kanalı Krizi'nin olması diğer önemli kanıtlardır. Süveyş Kanalı Krizi aynı zamanda NATO üyelerinin ABD savunmasına ihtiyaç duyduğunun

¹⁶ Michael Gorbaçov glasnost ve perestroyka politikaları ile SSCB'de toplumsal, ekonomik, siyasi ve idari alanlarda reform yapmayı amaçlamıştır. Glasnost politikası ile kamudaki şeffaflık ve açıklık uygulamaları izlenmiş ve halkın yönetimde söz sahibi olması hedeflenmiştir. Otoriter yönetimden daha çok demokratik izler taşıyan anlayış benimsenmeye çalışılmıştır. Perestroyka politikası ise daha çok ekonomik anlamda reformlar içermiştir. Perestroyka ile birlikte merkezi üretim anlayışı yerine daha çok liberal izler taşıyan serbest piyasa ve üretim anlayışı benimsenmek istenmiştir.

¹⁷ Renkli devrimler veya çiçek devrimleri, SSCB'nin çöküşünden sonra Orta ve Doğu Avrupa ile Orta Asya'ya kadar yayılan bölgede komünist yönetimlere devirmeye yönelik hareketleri toplu olarak ifade eden isimlerdir. Şiddet içermeyen bu devrimler ile halk, yönetimleri devirerek demokratik anlayışı ülkelere kazandırmaya çalışmıştır. SSCB'nin uydu devletlerinde gerçekleşen bu devrimlerde sembol olarak genellikle belli bir renk veya bir çiçek benimsenmiştir.

göstergesi olmuştur. Kriz ile aynı dönemde o yıla kadar SSCB'nin uydu ülkelerinde karşılaştığı en büyük devrim olan Macar Devrimi gerçekleşmiştir. SSCB, krizi avantaja çevirerek dünyadaki ilgiyi o yöne çekmiştir. Krizin taraflarından olan NATO üyesi ülkeler İngiltere ve Fransa, ABD'nin uğraşlarına rağmen krizi sonuçlandıramamış ve ilgilerini Macar Devrimi'ne kaydırmamışlardır. İlginin krizde olmasından yararlanan SSCB, Kızıl Ordusu'nu 1 Kasım 1956 tarihinde başkent Budapeşte'ye sokmuştur ve devrimi sonlandırmıştır. ABD, İngiltere ve Fransa'ya bu yüzden krizin sonunda destek vermemiş ve sorunun derhal çözüme kavuşturulmadığı takdirde SSCB'nin saldırılarına karşı İngiltere ve Fransa'ya destek vermeyeceğini açıklamıştır. Bu tehdit sonrası İngiltere ve Fransa geri adım atmıştır. Bu olay ABD'nin ne kadar güçlü olduğunun ve NATO'nun o dönemde ABD olmadan bir anlam ifade etmeyeceğinin göstergesi olmuştur.

Yani Soğuk Savaş döneminde NATO, ABD ile paralel bir strateji güderek ABD'nin SSCB'ye karşı izlediği politikaları, SSCB'nin 14 Mayıs 1955 tarihinde uydu ülkeleri ile Varşova'da kurduğu NATO'nun karşı emsali olan Varşova Paktı'na karşı gütmüştür.

3.3. Soğuk Savaş Sonrası NATO

Soğuk Savaş, askeri düzenin var olduğu, iki kutbun birbirleri ile çoğunlukla vesayet savaşları yoluyla mücadeleye giriştiği ve yumuşama dönemi dışında silahlanma yarışının son derece yüksek seviyelerde olduğu dönemdir. Askeri ve siyasi konuların en üst seviyede tutulduğu bu dönemde uluslararası siyaset sürekli çatışma olasılığı üzerinde durulan bir yapıda olmuştur. Soğuk Savaş'ın bitimi tüm bu olguları ortadan kaldırmış ve yeni bir dünya düzeni oluşmuştur.

SSCB'nin dağılması ile dünya düzenindeki iki kutuplu yapı sona ermiş, yeni ilişki biçimlerinin, yeni tehditlerin ve yeni aktörlerin ortaya çıktığı bir süreç başlamıştır. Devletler, topluluklar ve uluslararası yapılar, oluşan yeni düzene ayak uydurmak için dönüşüm çabasına girişmiştir. NATO, dönüşüm içine giren uluslararası yapılardan biri olmuştur.

Soğuk Savaş'ın bitimi NATO'nun var olma nedenlerini ortadan kaldırmış ancak NATO ülkeleri birliğin dağılması taraftarı olmamışlardır. Ayrıca Varşova Paktı'ndan ayrılan ve bağımsız devlet yapılarına kavuşan eski SSCB uydu devletleri NATO'ya üye olmak istemişlerdir (Minuto-Rizzo, 2007: 3). Bunların dışında Soğuk Savaş döneminde örgütün en önemli aktörü olan ve dünya siyasetinde SSCB'nin dağılmasından sonra tek süper güç olarak kalan ABD, NATO'nun dağılmasını istememiştir. Tüm bu sebepler, NATO'nun ayakta kalmasına, genişleme ve dönüşüm sürecine girmesine neden olmuştur.

Ancak NATO, kendi içerisinde pek çok sorunla karşılaşmıştır. Bu sorunların başlıcaları şunlardır; Soğuk Savaş döneminde ABD, NATO'nun liderliğini üstlenmiştir, bu durum üye ülkeler arasında hoşnutsuzluklar yaratmasına rağmen ABD'nin varlığı örgüt üyelerinin güvenlikleri

açısından elzem olduğu için çok fazla karşı ses o dönemde çıkmamıştır. Fakat ABD'nin tek taraflı politikaları SSCB'nin dağılması sonrası tartışma konusu olmuş ve belirli bölgelerdeki üye olmayan devletlerle yapılan işbirliklerinin ABD nezdinde değil, NATO nezdinde yapılması gerektiği üye ülkeler tarafından savunulmuştur (Karaosmanoğlu, 2014: 16-20). NATO Soğuk Savaş sonrası bazı operasyonlar düzenlemiş ve bu operasyonlar üye olmayan ülkeleri korumaya yönelik olduğu gibi üye olmayan ülkelerin katıldıkları operasyonlar da olmuştur. Bazı operasyonlara üye devletler itiraz etmiştir. Bu sebepten ötürü Washington Antlaşması'nın 5. Maddesi tartışma konusu olmuştur. NATO'nun üye ülke güvenliklerini ön planda tutması gerektiği savunulmuştur. Üye ülkeler SSCB'den sonraki en büyük güç olan Rusya ile işbirliği içerisine girmiş ve Bağımsız Devletler Topluluğu (BDT) üyelerinden bazıları Rusya'nın yayılma riskine karşı NATO'dan güvenlikleri için garanti istemişlerdir. Ancak NATO'daki bazı ülkeler Rusya ile işbirliğinde oldukları için bu duruma karşı çıkmıştır. Dönüşüm noktasında bu ve buna benzer sorunlar önemli noktalar olmuş ve alınan kararlarda bu sorunlar ön planda tutulmuştur.

Değişen dünya yapısına adapte olmak ve iç sorunların çözüme kavuşturulması için yaratılan dönüşüm kavramına önce tarihsel sonra da alansal olarak bakacak olursak; ilk olarak 24 Nisan 1990'da Washington Zirvesi'nde, Soğuk Savaş sonrası ilk Stratejik Konsept kabul edilmiştir. Yeni konsept bekleneni veremeyince 1999 yılında yeni bir Stratejik Konsept kabul edilmiştir. Örgütün temel görevleri olan caydırma ve savunmanın yanına kriz yönetimi ve diyalog yoluyla işbirliği görevleri eklenmiştir. 2002 yılına gelindiğinde Transformasyon Yüksek Müttefik Komutanlığı (Supreme Allied Commander Transformation–SACT) kurulmuştur ve SACT, üyelere askeri ve siyasi tavsiye vererek dönüşümün sorunsuz ilerlemesi için çalışmalar yürütmüştür. 19 Kasım 2010'da Lizbon Zirvesinde ise o döneme kadar olan konseptler arasında en geniş ve ayrıntılı yeni Stratejik Konsept kabul edilmiştir. Kabul edilen bu belgede en önemli konu ise siber tehdidin vurgulanması ve güvenlik meselesi olarak sayılmasıdır. (NATO, 2010: 12). Ayrıca yeni teknolojilerin getirdiği güvenlik zafiyetleri, terör, istikrarsızlığın yaratacağı güvenlik açıkları ve nükleer silahların çeşitli grupların ellerine geçme riski konseptte yer almıştır. Buradan anlaşılabileceği üzere NATO, bölgesel güvenlik anlayışının yanına dünya güvenliğini tehdit edebilecek hususları ekleyerek güvenlik anlamında kendisine yeni bir boyut kazandırma çabasında olmuştur.

Siyasi tartışmalar ve yeni Stratejik Konseptler ile birlikte NATO, kendisine üç temel görev belirlemiştir. İlki, var olduğu günden beri temel dayanağı olan Washington Antlaşmasının 5. Maddesindeki ortak savunma (caydırma dâhil) görevidir. İkinci görevi, dünya çapında çıkabilecek olan çatışmaları önlemek, çıkmış olanların da tırmanmasını önlemek ve barışı koruma operasyonları ile barışı tahsis etmeyi içeren kriz yönetimi görevidir. Son görevi ise özellikle BDT başta olmak üzere dünya çapında ülkelerle güvenlik için işbirliği yapmaktır (NATO, 2010: 12).

Bu görevler dışında NATO ayrıca genişleme politikasına gitmiş ve Soğuk Savaş sonrası Orta ve Doğu Avrupa ülkelerini üye olarak bünyesine kabul etmiştir. Sırasıyla 1999 yılında Polonya, Macaristan ve Çekya, 2004 yılında Bulgaristan, Estonya, Letonya, Litvanya, Romanya, Slovakya ve

Slovenya, 2009 yılında Arnavutluk ve Hırvatistan, 2017 yılında Karadağ, 2020 yılında Kuzey Makedonya, 2023 yılında Finlandiya ve 2024 yılında İsveç örgüte üye olmuştur.

Alansal olarak baktığımızda ise, siyasi olarak sadece askeri güvenlik örgütü yaklaşımı sergilemek yerine dünyadaki birçok konuda oluşacak güvenlik zafiyetlerine yönelik çalışmalar yürütmek ve bu konuda ülkeler, uluslararası örgütler ve sivil toplum kuruluşları ile işbirliği yapmak hedeflenmiştir. Bu durum NATO'yu askeri bir güvenlik örgütü olmanın ötesine taşımıştır. Siyasi alandaki dönüşüm siber alanın ve siber güvenliğin NATO'nun ilgi alanına girmesine neden olan en önemli etken olmuştur.

NATO, askeri alanda teritoryal bir yapıdan çıkarak dünya çapında birçok soruna müdahil olan bir yapıya kavuşmuştur. Terör faaliyetleri, istikrarsız devletlerin olduğu bölgelerdeki çatışmalar, nükleer silahların yayılması ve korsanlık gibi birçok konu güvenlik alanına dâhil olmuştur. Bunlara, 1999 yılındaki Bosna ve Kosova'daki iç çatışmaları durdurmak için Balkanlara yapılan askeri müdahale, 11 Eylül saldırıları sonrası Afganistan'daki terör örgütlerine yönelik yapılan askeri müdahaleler ve 2011 yılında Libya'daki istikrarsız yapıya yönelik yapılan askeri müdahaleler örnek olarak verilebilir. Ancak askeri olarak daha aktif bir rol izlemesine rağmen askeri birlik sayısını ve karargâh sayısını azaltmıştır. Genişleme politikası ile birlikte üye sayısı 32'ye çıkmasına rağmen 5.200.000 asker sayısı 3.700.000'e, 66 adet karargâh sayısını da 11 e düşürmüştür. (Weinrod ve Barry, 2012: 8).

Ekonomik dönüşüm ise askeri dönüşümle eş zamanlı ilerletilmeye çalışılmıştır. 2010 Lizbon Zirvesi'nde yayınlanan NATO Uzmanlar Grubu Raporu'na göre ülkeler gayrisafi yurt içi hasılatlarının %2'sini savunma harcamalarına ayırmaları gerekirken, günümüzde bu sayıyı tutturabilen ülke sayısı 6'dır (Karaosmanoğlu, 2014: 23). NATO Genel Sekreteri Jens Stoltenberg, 2024 yılı 11 müttefik ülkesinin GSYH'larından en az yüzde 2'sini savunmaya ayırma hedefini tutturmasının beklendiğini belirtmiştir (Rasquinho, 2024). Ekonomik anlamda dönüşümünü tam anlamıyla başardığı söylenemez. Savunma harcamalarında ABD 2023 yılı için GSYH'nın %3.24'ünü savunma harcamalarına ayırmıştır ve bu rakam örgüte üye büyük devletler içinde en yüksek rakamlardan biridir. (Rasquinho, 2024). Miktar olarak bakıldığında ise üye ülkeler içinde en büyük rakamdır.

Kısacası NATO'nun Soğuk Savaş sonrası değişen stratejisini başlıklar halinde vermek gerekirse;

- SSCB'nin dağılmasından sonra gündeme gelen sorunlara çözüm bulacak stratejiler geliştirmek,
- Oluşan yeni düzende, yeni devletler, aktörler, siyasi yapılarla işbirlikleri geliştirmek,

- Sadece örgüt üyelerinin değil aynı zamanda yardım isteyen ve BM ile AB gibi uluslararası örgütler ile işbirliği yaparak dünya genelinde güvenlik faaliyetleri yürütmek,
- Askeri güvenlik anlayışının yanında siyasi, ekonomik, toplumsal ve çevresel konularda güvenlik faaliyetleri yürütmek,
- Yeni üyeler edinerek genişlemek,
- Kriz bölgelerinde barış ortamının oluşturulması ile devamlılığını sağlamak,
- Nükleer silahları kontrol altına alarak¹⁸ sayısının azaltılmasını sağlamak NATO'nun Soğuk Savaş sonrası stratejileri arasında en önemlileri olmuştur.

3.4. NATO'nun 5. Maddesi ve ABD ve Büyük Britanya'nın Siber Politikaları

NATO'nun siber alana yönelik geliştirdiği politikalardan önce NATO'nun kalbi olarak adlandırılan 5. maddenin incelenmesi ve yorumlanması, güvenlikleştirme eyleminin nasıl gerçekleştirildiğini anlatırken bizlere katkı sunacaktır. Ayrıca çalışmanın savlarından biri olan devletlerarası uluslararası örgütlerin politikaları ile ona üye büyük devlet olarak nitelendirilen devletlerin politikaları paralellik gösterir fikrinin, NATO'nun politikalarında nasıl işlediğini görmek için iki devletin siber alan politikasına değinilecektir.

NATO 32 üyeye sahip bir örgüttür, ancak sadece ABD ve Büyük Krallık'ın politikaları incelenecektir. Bunun birkaç nedeni vardır;

- Bu devletlerden birincisi olan ABD dünyadaki en büyük ekonomiye ve askeri kapasiteye sahip olan devlettir. Büyük Krallık ise dünyadaki en büyük altıncı ekonomiye ve askeri güce sahip olan devlettir. Hem ekonomik olarak hem de askeri olarak güçlü olan dünyadaki sayılı devletlerinden olmaları,
- Özellikle Soğuk Savaş sırasında olmak üzere NATO'nun izlediği politikalar ile bu devletlerin politikalarında paralellik olması,
- BMGK'nın 5 üyesinden biridir. Bu statü onları, izleyecekleri politikalar ile dünya siyasetini ve NATO'yu etkileyecek konuma taşıması,
- Geçmişten günümüze kadar tarihsel akışa baktığımızda iki devletin dünyadaki etki alanlarının geniş olması,
- Diğer üye devletlere göre hem aldıkları kararlar hem de ilgili ülkede yer alan aktör söylemleri siber alan için bizlere daha çok ipucu sunuyor olması bu devletlerin seçilmesinde en önemli nedenler olmuştur.

¹⁸ Özellikle SSCB'nin uydu devletlerine stokladığı ve yerleştirdiği nükleer başlıklar SSCB'nin dağılması sonrası bağımsızlık kazanan devletlerin kontrolüne geçmesi ABD başta olmak üzere tüm NATO üyelerini tedirgin etmiş ve Rusya Federasyonu ile ortak çalışmalar yürüterek bu devletlere yönelik bazı ekonomik ve siyasi tavizler vererek nükleer başlıkların Rusya Federasyonu'na sevki sağlanmıştır.

3.4.1. NATO'nun 5. Maddesi

NATO, kuruluş amacını üye devletlerinin toprak bütünlüğünü, siyasi bağımsızlığını korumak için ortak savunma yeteneklerini geliştirmek olarak belirlemiştir (Polat, 2020b). NATO bu kapsamda üye ülkelerin güvenliklerinin kapsamını çizen güvenlik parametreleri belirlemiştir. Bu parametreler kara, deniz, hava, uzay ve siber alandır. Bu parametrelerin güvenliğini sağlamak için de ortak savunma anlayışı politikası izlenmektedir. Yani NATO bir güvenlik örgütü olarak belirlediği parametreler kapsamında üye ülkelerin güvenliklerini sağlama amacındadır. Bunu kuruluş anlaşmasının 5. maddesinde açıkça belirtmektedir.

Washington Anlaşmasının 5. maddesi *“Taraflar, Kuzey Amerika’da veya Avrupa’da içlerinden birine veya daha fazlasına yöneltilecek silahlı bir saldırının hepsine yöneltilmiş bir saldırı olarak değerlendirileceği ve eğer böyle bir saldırı olursa Birleşmiş Milletler Kurucu Andlaşması’nın 51. maddesinde tanınan bireysel ya da toplu öz savunma hakkını kullanarak, Kuzey Atlantik bölgesinde güvenliği sağlamak ve korumak için bireysel olarak ve diğerleri ile birlikte, silahlı kuvvet kullanımı da dâhil olmak üzere gerekli Statü altında kurulacak olan Uluslararası Ceza Mahkemesi’nin, ulusal ceza yargı yetkisinin tamamlayıcısı olduğunu vurgulayarak”*(NATO, 1949) ayrıca atıf yapılan BM Kurucu Anlaşması’nın 51. maddesi *“Antlaşma’nın hiçbir hükmü, Birleşmiş Milletler üyelerinden birinin silahlı bir saldırıya hedef olması halinde, Güvenlik Konseyi uluslararası barış ve güvenliğin korunması için gerekli önlemleri alıncaya dek, bu üyenin doğal olan bireysel ya da ortak meşru savunma hakkına halel getirmez.”* (Birleşmiş Milletler, 1945) hükümlerini amirdir. Anlaşılabacağı üzere NATO üyelerinin güvenliklerine yönelik saldırı durumunda üyenin kendisi veya üyelerin hepsi birlikte saldırıyı gerçekleştirene yönelik meşru müdafaa haklarını kullanarak gerekli askeri cevapları verebilme hakkına sahiptir.

Bu madde için en bariz örnek, 11 Eylül saldırıları sonrası üye ülkelerin tamamının 5. maddeyi yürürlüğe sokmada kararlı olduklarını ABD’ye bildirmeleri olmuştur. ABD tarafından Afganistan’a yönelik yapılan askeri müdahaleler desteklenmiştir. İlk örneği Soğuk Savaş sonrası olsa da Soğuk Savaş dönemi boyunca NATO’nun en büyük dayanağı bu madde olmuş ve üyelerinin güvenliğini geri saldırı tehdidini ileri sürerek yani güvenlileştirme eylemi ile sağlamıştır (Sperling ve Webber, 2017: 17). Burada önemli olan NATO’nun olağan durumlarda kullanmayacağı enstrümanları ve siyasi süreç içerisinde almayacağı savaş kararını, askeri güvenliğine yönelik oluşacak tehdit sonrası alabilmesidir. Kitleli olan üye devletler tarafından bu yetki kabul edilmiştir.

Soğuk Savaş sonrası geliştirdiği stratejik güvenlik konseptleri ile birlikte hem işbirlikleri kapsamında üye olmayan ülkeler için (Kosova ve Libya Örneği) hem de geliştirilen parametreler ile üye ülkeler kapsamında 5. madde devreye sokulabilmektedir. Yani üye ülkelerin güvenlikleri için alınacak olağanüstü önlemler yetkisi günümüzde hala varlığını sürdürmektedir. Siber alan da

parametreler içinde yer aldığı için 5. maddenin ileri sürülebileceği bir güvenlik alanı olarak karşımıza çıkmaktadır.

3.4.2. ABD'nin Siber Alan Politikası

ABD için siber alanla ilgili ilk çalışmalar 1995 yılında Bill Clinton'ın Başkanlığı döneminde başlamıştır. Ancak asıl ciddi çalışmalar Başkan Barak Obama döneminde yapılmıştır. Özellikle 2009 yılında başkan Obama'nın direktifleri ile ABD'nin siber alandaki politikalarını inceleyen Siber Uzay Politika Revizyonu (Cyber Space policy review) raporu hazırlanmıştır. Başkan Obama konuşmalarında sık sık siber alanda geri kaldıklarını ileri sürmüş ve ciddi adımlar atılması gerektiğini dile getirmiştir (Rakhmanova, 2018: 53). Bunun en önemli nedenleri aşağıda ayrıntılı şekilde ele alınacak 2007 Estonya ve 2008 Gürcistan olaylarıdır. Rusya bu olaylar sırasında siber alanı aktif bir şekilde kullanmış ve bu alanda avantaj elde etmiştir.

Başkan Obama bu gelişmelerden dolayı ABD'nin siber alanda Rusya'nın gerisinde kaldığını düşünmüş ve bu yüzden 2009 yılında siber alan stratejisini esas alan bu raporun hazırlanmasını istemiştir. Hazırlanan raporda var olan politikalar eleştirilmiş, tek merkezden yürütülmeyen bir politikaya sahip olunduğunu, departmanlar arası politikaların uyumsuzluğu ve kritik altyapılardaki siber savunmaların yetersizliği hususlarına değinilmiştir (Kızılay, 2020 38-39). Raporda halkın siber alanda bilinçlendirilmesi ile birlikte kanun ve yasaların revize edilerek siber alana yönelik bireysel hakların güvence altına alınması gerektiği dile getirilmiştir (The White House, 2009). Başkan Obama rapor sonucuna yönelik çalışmaların yapılması ve politikalar geliştirilmesi için Beyaz Saray Siber Güvenlik Koordinatörü (WHCC- The White House Cyber security Coordinator) başkanlığında çalışmalar yapılması kararı almıştır.

2010 yılına ABD Ordusuna bağlı Siber Komutanlık'ın (Cyber Command) generali, 2010'da Kongre'ye verdiği konuşmasında, Amerika Silahlı Kuvvetleri'nin milyonlarca siber saldırıyla karşı karşıya olduğunu söylemiştir (Singer ve Friedman, 2014: 68). Bu konuşma ile siber saldırıların boyutunun arttığı ve dünyadaki gelişmelerden dolayı stratejik hükümetin siber politikalara öncelik vermeye başladığı anlaşılmaktadır. Bu sebeple siber alan için stratejik bir belge geliştirilmiştir. Mayıs 2011 yılında "Siber Uzay İçin Uluslararası Strateji: Ağlanmış Bir Dünya'da Refah, Güvenlik ve Açıklık" strateji belgesi yayımlanmıştır. Belgede belirtilen en önemli amaçlar; siber güvenliğin sağlanması için uluslararası normların oluşturulmasını ve siber alanın ekonomik alanda destekleyici bir yapıda kullanılmasını teşvik etmek olmuştur (The White House, 2011: 17-18). Uluslararası normlar oluşturma çabası NATO'nun bu konuda kullanılacağını sinyallerini vermiştir.

Bu iki alandaki hedefler için bazı adımlar atılmıştır. Ekonomik alan için ABD, kritik altyapılara yönelik siber saldırıları ön planda tutarak politikalar geliştirmiştir. Kritik altyapılarda ekonomik unsurlara yönelik saldırılar bunlar içerisinde ayrı bir öneme sahip olmuştur. 2013 yılında yayınlanan

Kritik Altyapı Siber Güvenliği İyileştirme Belgesi bu kapsamda hazırlanmış bir belgedir. Siber savunma anlamında güçlendirilmesi için kamu ve özel teşebbüs çalışmalarının yapılması ve devletin özel sektörle ortak çalışmalar yürüterek savunma mekanizmalarının güçlendirilmesi gerektiği belirtilmiştir. Ayrıca kritik altyapıların önem dereceleri belirlenerek, siber güvenlikte öncelikli alanların seçilmesi gerekliliğine vurgu yapılmıştır (The White House, 2013). Raporda bu noktada siber güvenliğin zorluğuna değinilmiştir. Tüm siber alanın savunulamayacağı ve öncelikli alanların var olması gerektiği savunulmuştur. Yasa çalışmalarının sonuçları ise 2014 yılında alınmış ve Siber Güvenliği Geliştirme¹⁹ ve Siber Güvenliği Koruma Yasası²⁰ kabul edilmiştir.

Ayrıca ABD’de bu belgenin yayımlanmasından sonra ordu yapısında bulunan Uzay Komutanlığı Amerika Birleşik Devletleri Stratejik Komutanlığı’na (STRATCOM) dönüştürülmüştür. Bu hamle, ABD’nin siber alanda askeri caydırıcılığını güçlü tutmaya çalışmasından kaynaklanmaktadır. Bunun asıl nedeni ise ekonomik üstünlüğünü ve ilkelerini siber alanda da koruma isteğidir (Bozkurt, 2023: 114).

2015 yılında kabul edilen Ulusal Güvenlik Stratejileri Belgesi ABD’nin siber alanda rakip ülkelere karşı geri kaldığının kabulü niteliğindedir. Soğuk Savaş sonrasında SSCB’nin en büyük mirasçısı olarak Rusya Federasyonu kabul edilmiş ve BMGK’da SSCB’nin yerini almıştır. Rusya Federasyonu ilk dönemlerdeki ekonomik zorluklar ve iç sorunlarından dolayı uluslararası politikada etkin olamamıştır. Ancak 1999 yılında Vladimir Putin başbakan olduktan sonra iç siyasette attığı adımlarla birlikte istikrarı sağlamış ve ekonomik olarak doğal kaynakların daha etkin kullanılmasıyla ekonomik açıdan rahatlama dönemine girilmiştir. Bu rahatlama ile birlikte Rusya uluslararası siyasette aktif rol oynamış ve ABD ile rekabet etme gücüne kavuşmuştur. Özellikle Rusya’nın arka bahçesi²¹ olarak literatürde tanımlanan bölgelerde ve Arap Baharı sonrası istikrarsız yapıya evrilen Orta Doğu’nun belli bölgelerinde rekabet gücü yükselmiştir. Bu gelişmelerle birlikte Rusya, siber alanda ise son derece ileriye yönelik adımlar atmış ve ABD’ye göre daha gelişmiş bir siber alan bilgisine sahip olmuştur (Nagy, 2012). Yayımlanan Ulusal Güvenlik Stratejileri belgesinde tam da bu noktaya değinilmiştir. Her anlamda rekabet içinde olduğu rakibinin siber alanda son derece aktif ve tehlikeli olmasına atıfta bulunularak tedbirlerin sıkılaştırılması gerektiği belirtilmiştir (The White House, 2015).

Raporda ayrıca Çin Halk Cumhuriyeti’nden de bahsedilmiştir. Ekonomi, ABD için siber alanda son derece önemli bir konuma sahiptir. Ekonomik olarak rekabet içinde olduğu Çin’in siber alanda son derece aktif olduğuna ve siber casusluk faaliyetlerinde bulunarak hem ekonomiye hem de siyasi

¹⁹ Ayrıntılar için bakınız: [Text - S.1353 - 113th Congress \(2013-2014\): Cybersecurity Enhancement Act of 2014 | Congress.gov | Library of Congress](#)

²⁰ Ayrıntılar için bakınız: [Text - S.2519 - 113th Congress \(2013-2014\): National Cybersecurity Protection Act of 2014 | Congress.gov | Library of Congress](#)

²¹ SSCB’nin dağılmasından sonra ortaya çıkan bağımsız devletlerin toprakları Rusya’nın kırmızı çizgisi yani arka bahçesi olarak tanımlanır. NATO’ya üye devletler dışında kalan kısımlar bu hattı oluşturan kesimlerdir.

süreçlere zarar verme ihtimali bulunduğuna vurgu yapılarak önlemlerin bu yönde de artırılması gerektiğinden bahsedilmiştir (The White House, 2015). NATO için önemli maddelerden biri bu belgede yer almıştır. “ABD’nin müttefik ülkelerin istikrarını bozmayı hedefleyen siber saldırılara karşı, ilgili ülkelere her türlü desteği vereceği” ifadesi NATO üyeleri için atılmış bir adımdır (Darıcılı, 2018: 81-82). Bu atf 2016 yılında NATO Varşova Zirvesi’nde alınacak kararlar için önemli bir ipucu olmuştur.

Ayrıca 2015 yılında ABD Savunma Bakanlığı da bir siber strateji belgesi yayımlamıştır. Söz konusu belgede, ABD’nin askeri kritik altyapılarının savunulması elzem bir alan olduğuna ve 7/24 savunulmaya hazır şekilde aktif bir yapının bulunması gerektiğine değinilmiştir. ABD’nin siber savunma alanında gücünün ve caydırıcılığının artırılması gerektiği belirtilmiştir. Operasyonlar için birimler oluşturmak, bakanlık verilerini korumak için çalışmalar yapmak ve siber saldırılardan korunmak için uluslararası ittifaklar kurmak ana hedefler olarak belirlenmiştir (Department of Defense, 2015: 4-8). Savunma Bakanlığı, ABD’nin siber alanda hem caydırıcı güce sahip olmadığını hem de savunma alanında zafiyetleri bulunduğunu belge ile bir nevi kabul etmiştir.

- 2016 yılında Ulusal Siber Güvenlik Eylem Planı ve Dışişleri Bakanlığı tarafından Uluslararası Siber Politika Stratejisi belgeleri yayınlanmıştır. İki belgede yer alan maddeler birbiri ile benzer niteliktedir. Bu belgelerde temel hedefler belirlenmiş olup bunlar; Google, Facebook, DropBox ve Microsoft gibi özel sektör kuruluşları ile ortak çalışmalar yapmak,
- Bireysel farkındalığı arttırmak için eğitim müfredatında çeşitli siber güvenlik temelli derslerin yer almasını sağlamak,
- Siber güvenliği geliştirici komisyonlar kurmak, ittifakların güçlendirilmesini sağlamak,
- Siber güvenlik kapasitesinin geliştirilmesini sağlamak
- Ekonomik alanda siber güvenlik için önlemler almaktır. (The White House, 2016).

Söz konusu belgelerde, diğer belgelerde yer alan siber güvenliğin zorluklarına, siber saldırıların sıklığına ve siber güvenliğin yetersizliklerine de ayrıca değinilmiştir.

2018 yılında yayımlanan Savunma Bakanlığı Siber Strateji belgesi ABD’nin siber alandaki uluslararası rekabet gücüne yönelik belgelerden bir diğeri olmuştur. Teknolojik gelişmelerle birlikte siber saldırı ve siber casuslukların verdiği zararın her geçen gün arttığı ve siber alanın uluslararası rekabette oyun bozucu bir alan olmaya başladığı belirtilmiştir. Çin ve Rusya Federasyonu’nun siber alandaki faaliyetlerine atıfta bulunularak ABD için tehlikeli boyutlara ulaştığını bunun için ciddi önlemler alınması gerektiği savunulmuştur. ABD’nin siber alanda çıkabilecek bir savaşta en üst seviyede savunma ve saldırı gücüne sahip olması için askeri avantajlar sağlayıcı siber operasyonlar yapılması hedeflenmiştir (U.S. Department of Homeland Security, 2018).

Yine 2018 yılında Ulusal Siber Strateji belgesi yayımlanmıştır. Belgede özellikle ekonomi ve savunma alanlarındaki siber güvenliğin öncelikli alanlardan olduğu belirtilmiştir. Strateji şöyle özetlenmiştir;

“Ağları, sistemleri, fonksiyonları ve verileri koruyarak vatani savunmak, güvenli bir ortam sağlayarak, dijital ekonomiyi geliştirerek ve yerli yenilikleri teşvik ederek Amerikan zenginliğini artırmak, ABD’nin — müttefikleri ve ortaklarıyla uyum içinde — siber araçları kötü amaçlarla kullananları caydırma ve gerekirse cezalandırma yeteneğini güçlendirerek barışı ve güvenliğini korumaktır.” (The White House, 2018: s.3).

Özetlenen bu cümlelerden ABD’nin, siber alanda öncülük etme isteği ve cezalandırma seviyesinde uluslararası alanda kabul görececek bir konumda olmayı hedeflediği anlaşılmaktadır. Ayrıca belgenin ilerleyen sayfalarında, uluslararası normların oluşturulması ve işbirliklerinin yapılmasını teşvik edilmesi ve bu anlamda öncülük edilmesi gerektiğine vurgu yapılmıştır (The White House, 2018: 6-15).

2022 yılında yayımlanan Ulusal Güvenlik Stratejileri belgesinde siber alanda kazanılacak bir üstünlüğün asimetrik bir etkisi olacağı ve diğer alanlar için de üstünlük sağlamada yarar sağlayacağı belirtilmiştir. Bu üstünlüğün sağlanması için de en iyi teknolojilere sahip olunması gerektiği vurgulanmıştır. Ayrıca siber güvenlik için kolluk kuvvetleri ile daha sıkı çalışmalar yürütülmesi gerektiği dile getirilmiştir (The White House, 2022).

2023 yılında yayımlanan Ulusal İstihbarat Stratejisi belgesinde ise ABD, siber alanı demokrasi ile otokrasinin mücadelesine sahne olan yeni bir mücadele alanı olarak tanımlamıştır. Çin, Rusya, İran ve Kuzey Kore gibi devletlerin bu alanda aktif olduğu ve siber alan sayesinde fikirlerini yaydığı belirtilmiştir. Siber saldırılar, casusluk ve dezenformasyon²² gibi faaliyetler neticesinde bölgesel ve uluslararası istikrarsızlıklara neden olmaktadır (U.S. The Director of National Intelligence, 2023). Yine aynı şekilde diğer belgelerde olduğu gibi siber savunma alanında gelişim kaydedilmesi gerektiği, ekonomik ve askeri alandaki kritik altyapıların öncelikli korunması gerektiği yer almıştır.

ABD, Soğuk Savaş’tan sonra özellikle Başkan Obama dönemi ile başlayan süreçte siber alana yönelik Savunma Bankalığı ve Dışişleri Bakanlığı dâhil birçok kurum nezdinde çalışmalar yürütmüş; stratejik belgeler ve raporlar hazırlamıştır. İçeriklerinden kısaca bahsedilen bu raporlarda özellikle üç ana temel üzerinde durulmuştur. İlk olarak, rakip olarak görülen Rusya ve Çin’in siber alanda ABD’nin çıkarlarına karşı hamleler yaptıkları belirtilmiştir. Bu yüzden ABD’nin en iyi teknolojiye sahip olması gerektiği savunulmuş ve geri kaldığına yönelik eleştiriler yapılmıştır. İkinci husus, her ne kadar en yüksek teknolojiye sahip olsan da siber alanın tam anlamı ile savunulma olasılığının yıllar geçtikçe azalmasıdır. Bu yüzden kritik altyapıları önem sırasına göre sıralamak gerektiği düşünülmüştür. Son husus ise siber alanda ekonomik ve askeri yapıların önemine atıf yapılarak

²² Dezenformasyon: Doğru bir bilginin yeniden farklı şekilde üretilerek (Yanlış olan versiyonu ile) yayılmasıdır.

uluslararası toplumda ABD'nin öncü olması gerektiği ve bu yüzden özellikle ittifakların geliştirilmesi gerektiği vurgulanmıştır.

İlk gündeme alındığı tarihin üzerinden neredeyse 30 yıl geçmesine rağmen ABD'de yayımlanan son raporda hala siber güvenlik anlamında caydırıcılığın artırılması ve savunma araçlarının güçlendirilmesi gündeme getirilmiştir. ABD için tam anlamıyla siber güvenliğin sağlanamadığı açıktır. Zaten ABD'de bunu kabul etmiş ve öncelikli alanlar seçilmesi gerektiğini, özellikle ekonomik ve askeri kritik altyapıların bu alanlar olduğunu belirtmiştir. Genel anlamda bakıldığında siber alan, güvenlik açısından ABD için son derece kritik bir yapıdadır. Çünkü uluslararası arenada rakip olarak gördüğü Rusya ve Çin gibi devletler bu alanda son derece aktiftir ve hibrit savaşlarında bu alanı verimli bir şekilde kullanmışlardır. ABD, bu alanda maruz kaldığı siber saldırılar yüzünden, dış politikadaki ilgi alanlarında ve ekonomik alanda büyük zararlarla yüzleşmektedir. Ayrıca teknolojik gelişmelerin getirdiği avantajların yanında siber saldırı olanaklarını da çeşitlendirmesi, siber alanın her geçen gün uluslararası arenada oyun bozma gücünü arttırması göz önüne alındığında, siber alanın ABD'de güvenlikleştirilebilecek konumda yer aldığını söylemek mümkündür.

Gelinen nokta siyasi elitler tarafından da gündeme taşınmış ve güvenlikleştirmede gerekli olan söylem eylemi birçok kez ABD siyasi elitleri tarafından gerçekleştirilmiştir. Bu söylem eylemine birkaç örnek vermek gerekirse;

- 2014 yılında Sony Pictures firmasının bilgisayarlarına yapılan siber saldırılar için Başkan Obama sert bir tepki vermiş ve verdiği röportajda "Orantılı ve zamanını kendimizin belirleyeceği bir yanıt vereceğiz. Bazı diktatörlerin sansür uyguladığı bir toplum olamayız" (Avcı, 2014) ifadelerini kullanmıştır. Halk tarafından saldırı büyük tepki toplamıştır. Başkan Obama bu yüzden "Bazı diktatörlerin sansür uyguladığı bir toplum olamayız" cümlesini özellikle kullanmış ve verilecek cevap için halkın desteğini almaya çalışmıştır.
- 2016 yılında Başkan Obama, ABD seçimlerinden önce patlak veren Demokrat Başkan Adayı Hillary Clinton'ın seçim kampanyası sırasında e-postalara yönelik saldırılardan sonra Rusya'yı suçlamış ve "Rusya'da Vladimir Putin'in bilgisi dışında pek bir şey olmaz. Putin'e siber saldırıları durdur" dediğini söylemiştir (Kutlu, 2016). Ayrıca açıklamalarında ABD'nin karşılık olarak Rusya'ya siber saldırılar düzenleyeceğini dile getirmiştir.
- E-posta saldırılarına maruz kalan Demokrat Aday Clinton'da yaptığı açıklamada "Başkan seçildiğim durumda siber saldırılara askeri harekâtla karşılık vereceğim" (Varlık, 2016) ifadelerini kullanmıştır.
- 2016 yılında düzenlenen ABD Başkanlığı seçimine yönelik siber saldırı iddiaları üzerine New York Times'ta "Obama Seçimlerdeki Siber Saldırı Nedeniyle Rusya'ya Misilleme Yapıyor" başlıklı bir haber yer almıştır. İlgili birimlerin direktifleri ile Başkan Obama'nın,

Rusya'ya karşı yaptırım kararı aldığı ve ABD'de görevli 35 Rus diplomatın ülkeyi terk etmesini istediği haberde yer almıştır (Kutlu, 2016).

- 2020 yılındaki bakanlık seçimlerine yönelik siber saldırı iddiaları ve 2021 yılında gerçekleşen Solar Winds Orion platformuna düzenlenen siber saldırılar sonrası ABD hükümeti, Rus diplomatik misyonundan 10 personeli sınır dışı etmiş ve ek olarak yaptırımlar arttırılmıştır (The White House, 2021).
- 2021 yılında Başkan Biden yaptığı açıklamalarda; “ABD eğer gerçek bir savaşa girecekse bu siber saldırı sonucunda olacaktır.” ifadelerini kullanmıştır (Euronews, 2021). Bu ifadeler ile Biden siber alanı savaş sebebi olarak göstermiştir.
- 2022 yılında ABD Başkanı Joe Biden, Rusya'nın ekonomik baskılara karşı siber saldırılar düzenleyebileceğini düşündüğünü dile getirmiştir. Başkan Biden yaptığı açıklamada "Yönetimim, kritik altyapılara yönelik siber saldırıları püskürtmek, engellemek ve gerekirse bunlara karşılık vermek için elindeki her aracı kullanacaktır" ifadelerini kullanmıştır (Alp, 2022). Başkan Biden'in bu ifadeleri ABD için kendisine yönelmiş siber saldırılara karşı tüm seçeneklerin masada olduğunu göstermiştir.
- 2023 yılında yukarıda bahsi geçen 2023 Ulusal Siber Güvenlik Stratejisi belgesi Başkan Joe Biden tarafından onaylanmış ve bu belge ile savunma, istihbarat ve kolluk gücüne siber saldırılara karşı misilleme yapma yetkisi tanınmıştır. Belgede, “Ulusal gücün tüm araçlarını kullanarak, kötü niyetli siber aktörleri ABD'nin ulusal güvenliğini veya kamu güvenliğini tehdit edemeyecek hale getireceğiz.” (The White House, 2023) ifadelerine yer verilmiştir. Yapılacak siber saldırılarına karşın kolluk kuvvetlerine elindeki tüm araçlarla karşılık verme yetkisi tanınmıştır. Ayrıca belge kapsamında sosyal medya uygulamalarından biri olan TikTok'a yönelik siber güvenlik nedenlerinden dolayı erişim yasağı getirilmiştir.

Belgeler ve saldırılar dışında ABD için bir olaya daha değinilmelidir. 2009 yılında İran'a karşı yapılan Stuxnet siber saldırısının ABD ve müttefikleri tarafından yapıldığı düşünülmektedir (Çelik, 2013: 144-145). Saldırıdaki hedefin İran'ın nükleer yakıt zenginleştirme tesisi Natanz olduğu iddia edilmektedir. ABD bu iddiaları yalanlamamış ve gelen soruları üstü kapalı şekilde politik olarak cevaplamıştır. ABD'nin takındığı bu tavır siber saldırıları bir saldırı aracı olarak kabul ettiğini göstermiştir (Collins ve McCombie, 2012: 83-87).

ABD siber alanda geliştirmeye çalıştığı politikaları, siber alanın ekonomi ve savunma alanında barındırdığı tehlikeleri, dünyadaki liderlik konumunu koruma için siber güvenliği sağlama zorunluluğunu, rakip ülkelerin siber alandaki tehditleri ve kritik altyapıların siber alana entegre olması hususlarını dikkate alarak geliştirmeye çalışmıştır. ABD teknolojik olarak çok üstün olmasına rağmen siber alana entegrasyonun yüksek olması ve siber saldırı olanaklarının çok fazla olmasından dolayı savunmada güçlükler çekmiş ve her büyük saldırı sonrası farklı araçlarla cevap vereceğini siyasi elitleri vasıtasıyla söyleme taşımıştır. Açıklanan son belge ile birlikte kolluk kuvvetlerine her türlü imkânı kullanma yetkisi tanınmıştır. Diğer bir ifadeyle olağanüstü önlem alma yetkisi

verilmiştir. Güvenlikleştirilmenin unsurları olan siyasi elitlerin söyleme taşıması ve kitleler tarafından onaylanması gerçekleşmiştir.

3.4.3. Birleşik Krallık'ın (BK) Siber Politikası

2009 yılında Kabine Ofisi'nin strateji belgesinde şu ifadeler yer almıştır; “*Nasıl ki 19. yüzyılda ulusal güvenliğimiz ve refahımız için denizleri, 20. yüzyılda havayı güvence altına almamız gerekiyorsa, 21. yüzyılda da siber uzaydaki konumumuzu güvence altına almamız gerekiyor.*” (Cabinet Office, 2009: 21) Bu ifadeler BK'nın siber alana nasıl yaklaştığının göstergesi olmuştur. Temel amaçları, uluslararası hukukta caydırıcılığı olmayan bu anarşik ortamda ülke güvenliğini sağlamaktır (Erkul, 2024). Soğuk Savaş döneminde Batı Almanya'daki bir bilgisayar korsanının ABD'nin ağlarından çaldığı bilgileri SSCB'nin gizli servisi olan KGB'ye sattığının ortaya çıkması BK'nın siber uzaya dikkatini vermesine sebep olmuştur. Yıllar içinde finans sektörünün siber alana entegrasyonunun artması, siber saldırılar sonucu ekonomik zararların artmasına neden olmuş ve bu durum BK'nın siber alana olan ilgisini arttırmıştır.

Krallık 20. yüzyıl sonlarında faaliyete geçmiş ve 1992 yılında ilk güvenlik ekibini Birleşik Olay Müdahale ve Uyarı Hizmeti (UNIRAS) ismiyle kurmuştur. Ancak UNIRAS'ın siber alanın yeniliklerinden dolayı iş tanım net olarak belirlenememiş ve UNIRAS işlevsiz bir hâl almıştır. Kurumun işlevsiz hâle gelmesi BK'nın siber saldırıların açık hedefi olmasına sebep olmuştur. 2000'li yıllarla birlikte kritik altyapılara yönelik saldırıların arttığı Krallık Ulusal Altyapı Güvenliği Koordinasyon Merkezi tarafından açıklanmıştır (Corera, 2015).

Krallık, siber alanı anarşinin hâkim olduğu alan olarak görmüştür (Erkul, 2024). Bu yüzden savaşın çıkma ihtimalinin çıkmama ihtimalinden daha yüksek olduğunu düşünerek stratejik planlar geliştirmiştir. İlk stratejik belge 2009 yılında yayımlanmıştır. 2011 yılında ise “Birleşik Krallık Siber Güvenlik Stratejisi: Birleşik Krallık'ı Dijital Dünyada Korumak ve Desteklemek” adlı belge yayımlanmış ve 2015 yılına kadar hedefler belirlenmiştir. Bu belgede, siber güvenlik, savunma ve caydırıcılık anlamında dünyanın önde gelen ülkeleri arasında yer almaya yönelik çalışmalar yapmak, siber alanda ekonomik bakımdan dünyanın en güvenli ülkesi olmak, siber alanda istikrarlı ve güvenli bir toplum haline gelmek ana hedefler arasında yer almıştır (Cabinet Office, 2011).

2016 yılında yayımlanan yeni belgede, savunmanın yanında saldırı araçları ile caydırıcı unsurları bünyesinde barındırmak, sektörü büyütmek ve üstün teknolojiye sahip olmak hedeflenmiştir. Bu yüzden 2011-2015 yılına kadar her yıl artarak devam eden ve toplam 650 milyon poundluk bütçe, 2016 yılındaki bu yeni belgedeki hedeflerle 1.9 milyar pounda çıkarılmıştır (Cabinet Office, 2016). Ayrıca doğru savunma, gelecek saldırılara kesin bir cevap verebilme olarak görülmüştür. Bu yüzden saldırı unsurlarının da savunma mekanizmasında yer alması kararı alınmıştır.

Soğuk Savaş'ta ülkeler karşı bloktan gelecek askeri alandaki saldırıları güvenlikleri için en önemli tehdit olarak görmüşlerdir. Ancak 21. yüzyılda ise ülkeler gizli saldırı silahları kullanmaya odaklanmış ve devletler bu saldırıları güvenlikleri için kritik olarak görmüşlerdir. Siber silahlar bu saldırıların en önemli kaynağı olmuştur (Güntay, 2019). Bu yüzden Krallık tarafından siber alan bir operasyonel alan olarak görülmüştür. Krallık, Rusya, Çin, Kuzey Kore ve İran tarafından kendisine saldırılar düzenlendiğini ve gelecekte düzenleneceğini düşünmektedir (Eren, 2020). Bu kapsamda önemler almaya odaklanmış ancak siber alanın tam anlamıyla savunulamayacağını farkına varmıştır. Çünkü gelişen teknoloji, siber saldırı olanaklarını çok fazla kolaylaştırmıştır. Bunu göz önüne alarak siber alanda savunmanın yanında hedef olarak caydırıcılık ve saldırı gücünü arttırmaya odaklanılmış ve düşmanlarına karşı bu alanı kullanarak saldırılar düzenleyebilecek seviyeye ulaşmayı hedeflemiştir (Erkul, 2024). Benimsediği yaklaşım kapsamında 2020 yılında Ulusal Siber Güç birimini kurmuştur. Ulusal Siber Güç birimi ile Krallık, siber saldırıları ve düşmanların tespit edilmesini, tespit edilenlere karşı siber saldırılar düzenlenmeyi ve en nihayetinde Krallığın siber uzayda caydırıcı bir güç olmasını hedeflemiştir (Devanny, vd., 2021). Krallık'ın 2022-2030 arası siber vizyonu stratejisine bu düşünce yansımış ve saldırı yöntemlerine dayanıklılığı artırma hedefinin yanında yüksek caydırıcılık ve saldırı gücü elde etmek de hedeflenmiştir (Cabinet Office, 2022).

İç siber saldırı tehlikelerinin boyutunun farkında olan Birleşik Krallık, siber alanda kişisel verilere erişim sağlamıştır. Yani ülke içinden gelecek siber saldırılara karşı vatandaşlarının bilgilerine erişmiştir. 2013 yılında Edward Snowden gizli servislerin kişisel verilere müdahale ettiğini ortaya çıkarmıştır. Bu gizli servislerin içinde Büyük Krallık'ın servisi de yer almaktadır (Richards, 2014). Bu olay hükümetin bu alandaki faaliyetlerini siyasi süreçten çıkardığını ve olağanüstü duruma taşıdığının göstergesi olmuştur. Bu tür durumlarda devlet çıkarlarının korunması için kurumlarda birimler kurulmuş ve avukatlar istihdam edilmiştir.

Ayrıca Birleşik Krallık, siber alanda devletlerin tek başına savunma yapamayacağını farkındadır. ABD, Krallık'ın siber savunma konusunda en önemli müttefiki olmuştur (Porpp, 2021). NATO özelinde ise ittifakın siber güvenlik yeteneklerini geliştirmeye yardım edeceğini beyan etmiş ve operasyonel bir alan olarak gördüğü siber alanda operasyonlarını nasıl planladığını ve gerçekleştireceğini NATO ile paylaşmıştır (Shea, 2017: 22-23). Bu NATO'nun operasyonel güç kazanması için oldukça önemli bir hamle olmuştur.

Bu iki önemli NATO üyesinin kısmen II. Dünya Savaşı'ndan sonra başlayan ortak politika anlayışları diğer politikalarına yansıdığı gibi siber alandaki politikalarına da yansımıştır. Bu iki devlet de siber alanı operasyonel alan olarak görmekte ve saldırılara karşı cevap verilmesi gerektiğini savunmaktadır. Savunma araçlarının yanında saldırı araçlarının da bulunması gerektiği görüşüne hâkimlerdir. İki ülke için de en önemli unsur vatandaşlarının özgürlük ve finansal durumlarıdır.

ABD'deki seçim ve ekonomik saldırılar ile İngiltere'deki ekonomik saldırılar, halkın da bu konuda hükümetin olağanüstü önemlerine ve cevap niteliğindeki saldırılarına karşı çıkmamasına sebep olmaktadır. Bu iki önemli ülkenin siber alan politikaları bahsi geçen nedenlerden dolayı NATO'nun politikaları için önemli unsurlar içerir. Üye ülke politikalarının NATO politikalarına yansımaları ve NATO'nun politikalarının üye ülkelere yansımaları hakkında ipuçları sunmaktadır.

3.5. Siber Alanın NATO Radarına Girme Süreci

Soğuk Savaş sonrası NATO'nun değişen politikaları kapsamında askeri güvenlik anlayışının yanına siyasi, ekonomik, toplumsal ve çevresel konularda güvenlik faaliyetleri yürütmek ve politikalar geliştirmek eklenmiştir. Bu stratejik hamle siber alan için de önemli gelişmelere yol açmıştır. Dünyada zamanla yaşanan gelişmelerin yeni güvenlik sorunları yaratabileceği kabul edilmiştir. Küreselleşen ve teknolojik olarak hızla gelişen dünyanın yeni güvenlik sorunları doğuracağı düşünülmüştür. Bu kapsamda uzay teknolojilerinin güvenlik konularına dâhil edilebileceği hususu 1991 Körfez Savaşı ile gündeme gelmiştir. Körfez Savaşı'nda uzay teknolojileri, istihbarat ve askeri birliklerin yerini tespit etmek amacıyla kullanılmıştır. Ayrıca savaş sırasında canlı yayın yapılarak savaşın seyri hakkında kamuoyu bilgilendirilmiştir. Bu yüzden Körfez Savaşı, İletişim Savaşı olarak da bilinmektedir. Aynı zamanda medya imkânlarının kullanılmasından dolayı hibrit savaş olarak nitelendirilmektedir (Yenal, 2015).

1994 yılında gerçekleşen Rus-Çeçen Savaşı internetin savaş üzerinde yaratacağı etkiyi gözler önüne sermiştir. Rusya, bağımsızlık hareketine giren Çeçenlere karşı bir saldırı girişiminde bulunmuştur. Çeçenistan'ın başkenti Grozni'ye saldıran Ruslara karşı Çeçenler, savaş sırasında öldürdükleri Rus askerlerinin fotoğraflarını çekerek internete yüklemişlerdir. Rus halkı bu fotoğrafları görünce savaşın durdurulması için kampanyalar başlatmıştır. Çeçenlerin bu sayede savaştan üstün çıkmaları, bilginin savaş sırasında ne kadar kıymetli olduğunu ortaya çıkarmıştır. Bu nedenle internet bir savaş aracı olarak kabul edilmiştir (Darıcılı, 2017: 140). Savaşlardaki gelişmeler NATO'nun siber uzayı dikkate almasına sebep olmuş ve yeni stratejik konsept arayışında olan NATO, siber alanın da güvenlik için önemli bir alan olabileceğine dikkat çekerek Siber Savunma ve Yönetim Kurulu (Cyber Defence and Management Board-CDMB) ve Askeri Otoriteler ve Muhabere ve Bilgi Sistemleri Ajansı (Military Authorities and Communications and Information Agency-MACIA) gibi birimleri bünyesinde kurmuştur. Ayrıca üye ülkelerin ağ yapıları ve siber uzay alanındaki askeri yeteneklerindeki farklılıklardan dolayı NATO Ağ ile Etkinleştirilmiş Güç Programı (Network-Enabled Capability/NNEC) ve Ağ Merkezli Savaş (NCW) için bilişim alt yapısının oluşturulması için gerekli çalışmalar yapılmıştır. 1 Haziran 1996 tarihinde NATO İstişare, Komuta ve Kontrol Ajansı (NATO Consultation, Command and Control Agency/NC3A) kurulmuştur. NC3A'nın en temel fonksiyonu teknolojik gelişmeleri takip etmek olarak belirlenmiştir. Ayrıca alt birimleri içerisinde siber güvenlik ve bilgi paylaşımı sağlayacak bir birim kurulmuştur.

Kurulan birimlerle birlikte, üye ülkelerin ortak savunması için müşterek planların tasarlanması, askeri kuvvetlerin görev yapabilmesi için gerekli altyapı ve tesislerinin kurulması, müşterek eğitim programları ve tatbikatların düzenlenmesi konularında daimi bir danışma ve işbirliği olanağı sunmak hedeflenmiştir (Ada ve Çakır, 2017: 639:643). Asıl hedef çıkabilecek hibrit savaşlarda siber alanın askeri alan içerisinde aktif olarak kullanılmasıdır. 1998’de düzenlenen “Harekât Sistemlerine Enformasyon Teknolojilerinin Uygulanması” ve 1999’da “21. yüzyılda NATO Enformasyon Sistemlerini Korumak” başlıklı NATO toplantıları bu hedefin yansımalarıdır.

3.6. Hibrit Savaşlar Sonrası NATO’nun Savunma Mekanizması

Kurulan birimler ve yapılan toplantılar NATO’nun siber alana verdiği önemi göstermesine rağmen NATO’nun siber güvenliğe yönelik bir stratejik eylem yaratma düşüncesi, 1999 Kosova Savaşı müdahalesi sonrası oluşmuştur. Sırp kuvvetlerine karşı girişilen bombardıman sırasında Sırp hacker grubu “Black Hand” tarafından NATO karargâhına ve üye ülkelerin askeri haberleşme sistemlerine çeşitli siber saldırılar düzenlenmiştir. Saldırıların sonucu NATO’nun operasyonlarının aksatıldığı ve önemli verilerinin silindiği iddia edilmiştir (Arquilla ve Ronfeldt, 2001: 240-248). Bu gelişme 1999 yılında düzenlenen Washington Zirvesi’nde gündeme taşınmış ve hazırlanan bildiride ittifak üyelerinin bilgi saldırılarına maruz kalabileceği bu yüzden askeri zafiyet gösterebileceği ve etkin bilgi sistemlerine sahip olunmasının İttifak’ın savunma gücünü arttıracak vurgulanmıştır. Yine zirvede kabul edilen Yeni Stratejik Konsept’te teknolojinin hızla gelişimine atıf yapılarak devletlerin yanında artık gelişen teknoloji ile devlet-dışı aktörlerin de tehdit sayılması gerektiği, devletlerin ve devlet-dışı aktörlerin ittifakın bilgi sistemlerine karşı çeşitli operasyonlar düzenleyerek zarar verebileceği dile getirilerek hibrit savaş kavramı kabul edilmiştir (NATO, 1999).

2007 yılında Estonya’nın başkenti Talinn’de bulunan Kızıl Ordu Anıtı, dikilişinin 50. yıl dönümünde Estonya hükümeti tarafından kaldırılmıştır. Bunun hemen üzerine Estonya’nın kamu sitelerine saldırılar başlamıştır. 27 Nisan 2007 tarihinde başlayan bu saldırılar sonucu internet trafiği farklı konumlardan bağlanan zombi bilgisayarlarla 400 kat artmıştır. Bu da saldırının bir plan çerçevesinde yürütüldüğünün göstergesi olmuştur (Ada ve Çakır, 2017: 639). Kamu sitelerine yönelik Hizmet Dışı Bırakma (DDoS) saldırıları sonrası ülkede kaos ortamı hâkim olmuştur. NATO için bu saldırılar üye devletlerin siber alanda ortak hareket etmesi gerektiğinin göstergesi olmuştur. Hemen ertesi yıl Bükreş’te düzenlenen NATO zirvesinde bu konu gündeme getirilmiştir. Zirvede yapılan görüşmeler sonrası NATO Siber Savunma Birleşik Politikası kabul edilmiş ve ittifak çapında siber savunma operasyonel yeteneklerini merkezileştirmek için, merkezi Brüksel’de olan Siber Savunma Yönetim Başkanlığı (CDMA) kurulmuştur. Daha sonra 2007 yılında maruz kaldığı siber saldırıların benzerlerine Mayıs 2008’de de maruz kalan Estonya’da NATO Siber Savunma Mükemmeliyet Merkezi (CCDCOE) kurulmuştur. Kurulan siber savunma merkezleri NATO’nun üyelerine ortak bir siber savunma mekanizması sunma isteğini göstermektedir.

Estonya'ya yönelik yapılan siber saldırıların benzerleri 2008 yılında Gürcistan'a yönelik gerçekleşmiştir. 8 Ağustos 2008 tarihinde Gürcü birlikleri bağımsızlık ilan eden Güney Osetya'ya operasyon düzenlemiştir. Operasyonlar sırasında iki Rus uçağı düşürülmüş bunun üzerine Rus birlikleri Güney Osetya'ya girerek Gürcü birliklere karşılık vermiştir. Başlayan Rus-Gürcü Savaşı ile birlikte Gürcistan'a yönelik siber saldırılarda eş zamanlı olarak başlamıştır. Rusların hibrit savaş stratejisini kullandığı bu olay sonrası, NATO üyeleri hibrit savaş modeline daha fazla ilgi göstermeye başlamıştır (Bıçakçı, 2012: 210). Kasım 2008'de CCDCOE tarafından "Gürcistan'a Karşı Gerçekleştirilen Siber Saldırıları: Belirlenen Yasal Dersler" isimli bir bildiri yayımlanmıştır. Bildiri, Rusya-Gürcistan Savaşı sırasında meydana gelen siber saldırılara karşı Silahlı Çatışma Hukuku'nun (Law of Armed Conflict-LOAC) uygulanabilirliğini ileri sürmüştür (Carr, 2012: 31). NATO bu hamlesi ile birlikte siber saldırıları bir silah olarak görmeye başladığını göstermiştir. Ayrıca saldırıları çatışma hukuku kapsamında değerlendirmiş karşı saldırı hakkına dikkat çekmiştir.

3.7. NATO'nun Siber Savunma Stratejileri

Kosova'daki siber saldırılar sonrası NATO zirvelerinde Siber güvenliği gündemine almaya başlamıştır. 1999 Washington Zirvesi'nde yayınlanan bildiri sonrası siber güvenlik için yapılan çalışmaların sonucu 2002 Prag Zirvesi'nde ortaya çıkmıştır ve NATO Siber Savunma Programı kabul edilmiştir. Aynı yıl program dâhilinde ilk hamle yapılmış, siber olayları tespit etmek ve siber saldırıları önlemek amacıyla NATO Bilgisayar Olaylarına Müdahale Birimi (NCIRC) kurulmuştur.

3 Nisan 2008 tarihinde Bükreş'te düzenlenen zirve sonrası yayınlanan Bükreş Zirvesi Bildirisi'nin 47'nci maddesinde siber alan stratejisine şöyle değinilmiştir;

"NATO, siber saldırılara dayanıklılığını artırmak için ittifak bilgi sistemlerini güçlendirme kararlılığını sürdürecektir. Son zamanlarda NATO siber savunma politikası kabul edildi ve ilgili birimler tarafından geliştirilmeye devam edecektir. Siber savunma politikamız NATO ve müttefik devletlerin siber savunma ihtiyaçlarını karşılamak ve kritik bilgi sistemlerini korumak üzerine yoğunlaşmaktadır. Bu amaç doğrultusunda; faydalı uygulamalar paylaşılmalı ve siber saldırıya maruz kalan devletin talep etmesi durumunda siber savunma desteği sağlanmalıdır. Biz NATO olarak, siber savunma yeteneklerimizin güçlendirilmesi için müttefik devletler ve ulusal otoriteler ile ilişkilerin geliştirilmesi konusunda istekliyiz" (NATO, 2008).

Bu fikir birliği sonucu yukarıda bahsi geçen savunma birlikleri kurulmuştur. Ayrıca 47. madde kapsamında NATO bünyesinde NATO Siber Savunma Politikası hazırlanmış ve onaylanmıştır.

2010 yılında düzenlenen Lizbon Zirvesi'nde kabul edilen NATO'nun yeni Stratejik Konsepti'ne Siber Savunma Politikası dâhil edilmiştir. Soğuk Savaş sonrası kabul edilen konseptler NATO'nun yeni güvenlik stratejilerini ortaya koymaktadır. Özellikle hangi alanlara yönelik güvenlik çalışmaları yapılacağı belirtilen bu konseptlere 2010 yılında siber alanın dâhil edilmesi NATO'nun

siber alanı güvenlik alanı olarak gördüğünün en temel göstergesi olmuştur. Siber alan artık NATO üye devletleri için ortak savunma alanı olarak görülmüştür.

2010 yılında Stratejik Konsepte dâhil edilen savunma politikası 2011 yılında revize edilerek üye ülkelerin Savunma Bakanlıkları tarafından onaylanmıştır. Gözden Geçirilmiş NATO Siber Savunma Politikası olarak adlandırılan yeni politika ile birlikte NATO üyelerinin asgari savunma sistemleri geliştirme ve ortak savunma mekanizmaları oluşturma politikaları ortaya çıkmıştır (NATO, 2011). 11 Eylül saldırısı sonrası korkulan konular arasında 11 Eylül saldırılarının benzerinin siber alanda gerçekleşme riski yer almıştır. Bunun üzerine Şubat 2012’de NCIRC’ın 2012 yılı sonuna kadar operasyonel hâle gelebilmesi için 58 milyon Euroluk bir kontrat imzalanmıştır. Yine 2012 Chicago Zirvesi’ndeki ana başlıklardan biri siber güvenlik olmuş ve bu alanda caydırıcı mücadele önlemleri alınması gerektiği kararlaştırılmıştır (NATO, 2012).

2010 yılındaki Stratejik Konsept ile birlikte NATO artık siber alanı kritik bir güvenlik alanı olarak yeni stratejik konseptlerine dâhil etmiş ve bundan sonraki tüm stratejik konseptlerinde siber güvenlik için politikalar üretmiştir. Bu yüzden 2010’da kabul edilen bu belge siber alanın NATO özelinde dönüm noktası olmuştur.

3.8. NATO’da Siber Alanın Güvenlikleştirilmesi

2012 yılındaki bir önemli gelişme de CCDCOE tarafından yayımlanan “National Cyber Security Framework Manual” dokümanı olmuştur. Üye ülkelere siber savunma için 10 farklı yöntem önerilmiştir (Klimburg, 2012: 180-188). Genel anlamda savunma sırasında yapılması gerekenler, erişim engellerinin getirilmesi ve birlikte mücadele etmek gibi yöntemleri içermesine rağmen raporun onuncu yöntemi siber savunmayı farklı bir boyuta taşımıştır. “Müttefik ülkelerin, saldırıya uğrayan müttefiki rahatlatmak ve saldırıları engellemek için siber saldırılara siber saldırılar yoluyla NATO adına cevap verebilecekleri” dile getirilmiştir (Klimburg, 2012). Bu siber savunmayı siyasi süreç dışına çıkaran ilk adım olmuş ve olağanüstü yöntemler kullanabilme olanağı barındırmaktadır.

2014 Galler Zirvesi’nde siber güvenliğin her geçen gün daha karmaşık bir yapıya kavuştuğu dile getirilmiş ve bununla daha etkin mücadele için güçlendirilmiş siber savunma politikası kabul edilmiştir. Gelişen teknoloji ile siber saldırıların yarattığı tehlikelerin ön görülemez bir hâl aldığı, siber saldırılarla mücadele için hukuki bir dayanağın varlığından söz edilemediği ve daha etkin bir siber savunma politikası üretilmesi gerektiği zirvede dile getirilmiştir (NATO, 2014). Bu nedenlerden ötürü zirvedeki liderler siber saldırıların ortak savunma ile ilgili 5. maddeyi tetikleyebileceğini düşündüklerini belirtmişlerdir.

2016 yılında düzenlenen Varşova Zirvesi’nde siber alan kara, deniz, hava ve uzay gibi bir hareket sahası olarak tanınmıştır. Siber alan güvenlik anlamında öncelikli alanlar arasında yer almış

ve siber uzay askeri operasyonel alanı olarak kabul edilmiştir (Belkin, 2016). Aynı zamanda yine siber tehlikelerin her geçen gün farklı boyutlara ulaştığı, savunmasının çok zor olduğu ve bu alanda işbirliğinin artırılması gerektiği vurgulanmıştır.

2018 yılında Brüksel Zirvesi'nde, Belçika'da bir Siber Operasyonlar Merkezi'nin (CyOC) kurulmasına karar verilmiştir. Bu merkezin siber uzayda güçlü olması için üyelerin savunmalarını güçlendirmesi hedeflenmektedir (NATO, 2018). Siber alanın operasyonel bir alan olarak görülmesi bu merkezin açılma sebebi olmuş, bu alandaki faaliyetlerde planlama ve harekete geçirme mekanizması olarak görülmüştür.

2019 yılında gerçekleştirilen Londra Zirvesinin Sonuç Bildirisi'nde, NATO'nun siber saldırılara maruz kaldığı, bu yüzden güvenliğe 360 derece yaklaşılması gerektiği, bu tehditlere karşı NATO'nun askeri kapasitesi ve planlarının uyarlanacağı belirtilmiştir (NATO, 2019). Böylelikle NATO'nun askeri gücünü de siber alanda aktif edeceği ortaya çıkmıştır.

2022 yılında düzenlenen Madrid Zirvesi'nde siber alanın hangi konularda tehdit yaratacağı gündeme taşınmıştır. Siber alanın fikri mülkiyeti, sosyal hayatın akışını, askeri faaliyetleri, ekonomik faaliyetleri, istihbarat ve siyasi faaliyetleri ve tüm kritik altyapıları tehdit eden bir saldırı potansiyeli barındırdığına değinilmiştir. Yani Kopenhag Okulu'nun değindiği güvenlik meselesi olan beş ana başlığı içinde barındırdığı NATO tarafından da gündeme taşınmıştır. Bu tür tehlikelerin önüne geçmek için savunma, caydırıcılık ve yanıt verme gücünün artırılması gerektiği kararlaştırılmıştır (NATO, 2022).

NATO düzenlediği zirveler ve yayınladığı strateji ve siber politika belgelerin hepsinde şu hususlara değinmiştir;

- Siber teknoloji her geçen gün gelişmektedir ve saldırı olanakları buna paralel olarak artmaktadır.

- Ortak savunma mekanizmaları geliştirilmelidir.
- Siber alanın yapısı gereği savunması karmaşık ve zordur.
- Siber savunma için son teknolojiye sahip olunmalıdır.
- Siber güvenliğin yanında caydırıcılık ve saldırı gücü de artırılmalıdır.
- Üyelerin kendi iç siber güvenlikleri artırılmalıdır.

Bu maddeler neredeyse tüm siber alanın gündeme geldiği belgelerde yer almıştır. Buradan anlaşılacağı üzere NATO'nun, teknolojinin sürekli gelişmesinden ve siber alanın yapısından dolayı tam anlamıyla bir siber savunma mekanizması kurduğu söylenemez. Hatta bu tüm dünyadaki aktörler için geçerlidir. Bu yüzden NATO, ABD ve Birleşik Krallık'ın izlediği politika ile benzer şekilde, siber saldırılara karşı caydırıcı cevap verme yeteneklerini ön plana çıkarmak istemiştir. NATO'nun siber saldırılara karşı cevap verme gücü 5. maddenin devreye sokulmasıdır. Bu yüzden NATO, siber

alanı diğer konvansiyonel alanlar gibi görmeye başlamıştır. Bu görüş NATO'nun siyasi elitleri olan kişilerin söylemine taşınmış ve bu kişiler siber saldırıların meşru müdafaa hakkı doğuracağını ve NATO'nun kurucu anlaşmasındaki 5. maddeyi aktif edebileceğini dile getirmişlerdir. Bunlara birkaç örnek vermek gerekirse;

- 2018 yılında Axios haber sitesine röportaj veren NATO Genel Sekreteri Jens Stoltenberg üye ülkeye yönelik bir siber saldırı durumunda 5. madde devreye sokulabilir mi sorusuna verdiği yanıtta *"Otomatik olarak devreye sokulmaz. Siber saldırının nasıl olduğuna bağlı. 5. maddeyi ne zaman devreye sokacağımız konusunda asla net olamayız"* ifadelerini kullanmıştır (Bektaş, 2018).

- 2019 yılında NATO Genel Sekreteri Stoltenberg, İngiltere'de yayımlanan Prospect dergisi için yazdığı yazıda *"Ciddi bir siber saldırı NATO için kuruluş anlaşmamızdaki 5'inci maddeyi tetikleyebilir. Bu, bir müttefikimize yönelik saldırının herkese karşı yapılmış sayılmasına yönelik ortak taahhüdümüzdür."* ifadelerine yer vermiştir (Salcı, 2019).

- 2023 yılında düzenlenen NATO Siber Savunma Konferansı'nda konuşma yapan NATO Genel Sekreteri Stoltenberg üye ülkelere yöneltilen siber saldırıların 5. maddeyi tetikleyebileceği konusunda da mutabık kaldığını *"İttifakımızın merkezinde yer alan birine yapılan saldırının herkese yapılmış sayılacağı vaadidir. Birimiz hepimiz, hepimiz birimiz için. Çünkü siber saldırılar en az kinetik saldırılar kadar zarar verici olabilir."* ifadelerini kullanmıştır (İHA, 2023).

- NATO Askeri Komitesi Başkanı Amiral Rob Bauer, 2024 Shangri-La Diyalogu forumunun "Sibernetik Savunma ve Askeri Faaliyetlerin Geleceği" bölümünde yaptığı konuşmada *"NATO'da tüm müttefiklerin ortak kararıyla, bir siber saldırının 5. maddenin uygulanmasına ilişkin karar alma sürecini başlatabileceği konusunda anlaştık. Yani, sadece fiziksel bir saldırı değil, aynı zamanda bir siber saldırı da 5. maddenin uygulanmasına ilişkin tartışmalara ve sonuç olarak daha sonraki prosedürlerin uygulanmasına temel oluşturabilir"* ifadelerini kullanmıştır (NATO, 2014).

Yıllar içinde verilen röportajlarda üyelere yöneltilen bir siber saldırı söz konusu olduğunda 5. maddenin devreye gireceği kesin bir dille ifade edilmeye başlanmıştır. Bunun en önemli nedenleri arasında, siber saldırıların boyutlarının artması, üye ülkelerin yaklaşımlarının bu yönde olması ve cevap vermede aciziyet göstermeden caydırıcılığın korunması isteği yer almaktadır. Yapılan açıklamalara, zirvelerde alınan kararlara ve stratejik belgelerde siber alan için belirlenen hedeflere bakıldığında siber alanın NATO tarafından güvenlikleştirildiği anlaşılmaktadır. Önemli olan olağanüstü önlemleri alma değil alma yetkisine sahip olunmasıdır ve bu siber alan için NATO özelinde geçerlilik kazanmıştır.

NATO siber saldırıların savaş sebebini tartışmamaktadır. Günümüzde tartıştığı konu hangi boyuttaki siber saldırıların meşru müdafaa hakkı doğuracak olduğudur. Bu tamamen NATO'nun kontrolündedir. Yani NATO siber saldırıların biri için meşru müdafaa hakkımız doğmuştur diyebileceği gibi bir başka siber saldırı da aynı kararı vermeme yetkisine sahiptir. Özellikle politikalarında paralellik gösterdiği ABD ve Büyük Krallık'ın politikalarında bu görüşe sahip olması,

bu yetkinin tanınmasının en temel nedenlerinden biri olmuştur. Yani NATO siber alanı operasyonel alan olarak görerek, 5. maddeyi aktif edecek saldırılar barındırdığını ve aktif edilebileceğini siyasi elitleri ile söyleme taşımıştır. Bu durum 2014 Galler Zirvesi'nde üye devletlerin sözcüleri yani hedef kitlesi tarafından kabul edilmiştir. Şu ana kadar olağanüstü yöntemlere başvurmaması bunun başarılı bir güvenlikleştirme eylemi olmadığını göstermez. NATO başarılı bir güvenlikleştirme yapmış ve olağanüstü önlemler alacak yetkilere sahip olduğunu göstermiştir.



SONUÇ ve ÖNERİLER

Soğuk Savaş sonrası artan eleştirilerle birlikte ortaya çıkmaya başlayan eleştirel teoriler içerisinde yer alan Kopenhag Okulunun Güvenlikleştirme teorisi, son dönemde en çok çalışılan konulardan biri olmuştur. Kopenhag Okulu'nun beş ana başlıkta incelediği güvenlik yaklaşımı için siber alanın oldukça uyumlu olduğu söylenebilir. Siber alana her geçen gün entegrasyonun artması bu uyumluluğu daha da pekiştirmektedir.

Teknolojik gelişmeler güvenlik açısından siber güvenliğin sağlanmasını oldukça zorlaştırmaktadır. Özel ve resmi birçok kurum ve kuruluş siber saldırıların hedefi hâline gelmiştir. Savunmanın zorluğu devletleri siber alanı güvenlikleştirmeye yönlendirmiştir. Rusya ve Çin gibi hatta çok fazla teknolojik gelişim göstermemiş olan İran ve Kuzey Kore gibi devletler dâhi siber saldırı tehdidi altındadır. Siber saldırı, ABD ve Birleşik Krallık için de tehlike arz etmektedir. NATO'nun en büyük iki devleti olarak kabul edilebilecek bu iki devlet NATO politikalarının da ilgi odağı olmaktadır. Savunmanın zorluğu ve maliyeti sebebiyle devletlerin tek başına savunma yapmasının zorlaştırtığının ABD ve Birleşik Krallık farkındadır. Bu farkındalık nedeniyle NATO'nun Soğuk Savaş sonrası değişen ve gelişen yapısına adapte ederek siber alanda NATO'nun faaliyetlerini arttırmaya çalışmaktadırlar.

Büyük devletler için saldırıların savunulmasından çok daha önemlisi saldırılara karşılık verme gücüne sahip olmaktır. Bu durum bir güvenlik örgütü olan NATO için de oldukça önemlidir. Yani NATO'nun üyelerine karşı yapılacak saldırı sonrası NATO net bir cevap vermek zorundadır zira bunu taahhüt etmektedir. Siber saldırılarda bu minvalde olmuştur ve NATO'nun cevap verme zorunluluğunu ortaya çıkarmıştır. NATO bunu siber veya askeri saldırı veyahut ambargo uygulaması ile yapabilir. Önemli olan bunu yapması değil, yapma yetkisine sahip olmasıdır. Normal siyasi durumlarda bu yetkiye sahip değilken bu alanda sahip olması NATO'nun güvenlikleştirme eylemini gerçekleştirdiğini bizlere gösterir.

Çalışmada asıl dikkat çekilmek istenen bir diğer husus siber alana her geçen gün birçok konunun dâhil olması ve siber saldırı gücünün teknolojik gelişmeler ve entegrasyon ile artmasıdır. Bu durum siber güvenliği her geçen gün imkânsız hâle getirmektedir. Saldırıların büyüklüğü ve hedeflerine bakıldığında birçok devlet için artık siber saldırılar savaş sebebi sayılma boyutuna gelmiştir.

Elde ettiğimiz veriler, siber alanın güvenlikleştirmeye ile uyumlu olduğu, siber alanın güvenlikleştirmeye yatkın olduğu, siber güvenliğin her geçen gün zorlaştığı, büyük devletlerin siber alanı savaş alanı olarak görmesi, uluslararası örgütlerin politikalarının üye büyük devletlerin politikaları ile paralel olması ve NATO'nun Soğuk Savaş sonrası gelişen güvenlik yapısı ile çok boyutlu yapıya kavuşmasıdır. Siber alan için yapılan çıkarımlar tek bir örneklem yani NATO üzerinden anlatılmış, NATO ve uluslararası örgüt çıkarımları ise siber alan üzerinden anlatılmıştır. Böylece hem Soğuk Savaş sonrası NATO'nun yapısına yönelik çıkarımlara hem de NATO'nun siber alana bakış açısına yönelik çıkarımlara ulaşılmaktadır.

Soğuk Savaş sonrası varlığı sorgulanan ancak güvenlik yaklaşımındaki güncellemeler ve stratejik belgelerindeki belirlediği hedefler sayesinde varlığını güçlendiren NATO için siber alan ilerleyen yıllarda oldukça gündemde olacak bir konudur. NATO için önemli olan bu konu tüm dünya devletleri için de önemli olacaktır. Devletlerin birbiri ile gizlenerek savaşacağı önemli bir alan doğmuştur. Bu savaşlar olağanüstü durumları da beraberinde getirecektir. NATO, 32 üyeye sahiptir ve bu üyeler dünya çapında en büyük ekonomiye ve askeri güce sahip olan ülkeler arasındadır. Bu ülkelerin hiçbiri NATO'nun siber alandaki politikalarını eleştirmemiş aksine desteklerini dile getirmişlerdir. Bu durum hedef kitlenin iknasının yanında bu ülkelerin siber alana bakış açılarını da gözler önüne sermektedir.

NATO için siber alan sonraki yıllarda çıkaracağı stratejik konseptlerde ve zirve bildirilerinde önemli yer tutacağı açıktır. Bu kritik öneme sahiptir çünkü NATO için siber alan dinamik bir yapıda olacak ve sürekli yeni çıkarımlar sunacaktır. Bu sadece NATO özelinde değil uluslararası arena boyutunda geçerlidir. Dünyanın her yerinde artık siber alan varlığını hissettirmeye başlamıştır ve her geçen gün varlığını derinleştirmektedir. Siber güvenlik artık dünya sorunu olmuştur.

Araştırmada ana belirlenen sorulara odaklanmış olsa bile araştırma sırasında birçok yeni soru akıllara gelmektedir. Özellikle bu kadar çok sorun barındırmasına rağmen siber alana entegrasyonun her geçen gün artmasının sebebi nedir? Şuan mevcut sorunların boyutu büyüktür ancak ileride daha büyük sorunlar yaratma potansiyeli siber alana bakışı değiştirecek midir? Benzeri birçok soru bizim için siber alanın geleceğini tartışmaya açmamıza olanak tanımaktadır.

Çalışmada NATO üyesi iki ülkenin siber savunma politikalarına değinilmiştir. Ancak araştırma sırasında diğer ülkelerin özellikle Almanya, Fransa ve Türkiye'nin de NATO kapsamında siber politikalar üzerine yoğunlaştığı görülmüştür. Bu ülkelerin siber alan politikalarında ve aktör söylemlerinde NATO'nun siber politikasını ortaya çıkarmaya yarayacak birçok bilgi söz konudur. İlgili ülkeler sonraki çalışmalar için oldukça zengin bir alandır.

Siber alan uzun yıllar boyunca araştırmalar için ilgi odağı olacağı gözükmemektedir. Türkiye'deki literatür taramamızda son dönemlerde artan araştırma sayısına rağmen yetersiz bir literatürümüz

olduğu açıktır. Bu yönde yapılacak çalışmalar ile literatür zenginleştirilebilir ve siber alan konusunda yapılan çalışmalarda öncü bir literatüre kavuşulabilir. Siber alan yapısı gereği birçok konu ile ilişkilendirilebilir bu yüzden yapılacak sonraki çalışmalarla spesifik örnekler ortaya konabilir.

Özellikle araştırma sırasında dikkat çeken bir diğer unsur siber alanın gelecekte hangi devletlere daha çok avantaj sağlayabileceği sorusu olmuştur. Dünya siyasi tarihi boyunca bazı gelişmeler bazı devletlerin ön plana çıkmasına yol açmıştır. Siber alana entegrasyonun bu hızda devam etmesi gelecek adına hangi ülkeye

Soğuk Savaş'tan sonra uluslararası güvenlik örgütlere ihtiyaç kalmadığı iddiası son derece yanıltıcıdır. Daha çok siber alana odaklanılmış olmasına rağmen siber alanda hatırı sayılır sorun mevcuttur ve bu sorunların çoğu ülkelerin tek başlarına üstesinde gelemeyecek ve işbirliği gereken sorunlardır. Siber güvenlik gibi birçok güvenlik konusu Soğuk Savaş sonrası uluslararası siyasette gündemdedir. Bu sorunların çoğunun çözümü işbirliği gerektirmektedir. Buda uluslararası güvenlik örgütlerinin gerekliliğini gözler önüne sermektedir. Son dönemlerde azalan uluslararası örgüt çalışmaları farklı şekilde ele alınarak canlandırılabilir.

Genel itibari ile baktığımızda siber dünya artık günlük hayatın tüm alanlarına sirayet etmiştir. Güvenlikleştirme ile arasındaki bağ ve siber güvenliğin zorlukları sorunun güvenlikleştirilmesine olanak sunmaktadır. Ancak araştırma sadece bu unsurları bir örnek üzerinden anlatma çalışmamış gelecek adına teori, siber alan ve uluslararası örgütler nezdinde bir yol göstermeye çalışmıştır.

KAYNAKÇA

- Ada, Mehmet ve Çakır, Hüseyin (2017), “Kuzey Atlantik Antlaşma Örgütü' nün (NATO) Siber Güvenlik Stratejilerinin İncelenmesi”, **Düzce Üniversitesi Bilim ve Teknoloji Dergisi**, 5(2), 632-656.
- Ağır, Burak (2011), “Güvenlik Kavramını Yeniden Düşünmek: Küreselleşme, Kimlik ve Değişen Güvenlik Anlayış”, **Güvenlik Stratejileri Dergisi**, 11(22), 97-131.
- Akgül Açıkçeşme, Sinem (2011), “Algı mı? Söylem mi? Kopenhag Okulu ve Yeni Klasik Gerçekçilikte Güvenlik Tehditleri”, **Uluslararası İlişkiler Dergisi**, 8(30), 43-73.
- Alakoç Burma, Zehra ve Özdemir, Asena (2024), “Ülkelerin Gelir Düzeyleri ve Ağa Hazırlık Endeksi Bileşenlerinin: Dijital Göçmen Yaşlı Bireylerin İnternet ve Sosyal Medya Kullanımlarına Etkileri”, **Dünya İnsan Bilimleri Dergisi**, 2024(1), 1-31.
- Aldemir, Ceray ve Kaya, Merve (2020), “Bilgi Toplumu, Siber Güvenlik ve Türkiye Uygulamaları”, **Kamu Yönetimi ve Politikaları Dergisi**, 1(6), 6-27.
- Alp, Şahin (2022), “ABD'den Rusya'ya 'Siber Saldırı' Resti! Biden: Gerekirse Cevap Vereceğiz”, <https://www.mynet.com/abd-den-rusya-ya-siber-saldiri-resti-biden-gerekirse-cevap-verecegiz-110106931534> (21.03.2022)
- Alpna ve Malhotra, Sona (2016), “Cyber Crime-Its Types, Analysis and Prevention Techniques” **International Journal of Advanced Research in Computer Science and Software Engineering**, 6(5), 145-150.
- Arquilla, John ve Ronfeldt, David (2001), **Networks and Netwars: The Future of Terror, Crime and Militancy**, RAND Corporation, Santa Monica.
- Arends, Frederik J. (2009), “Homeros’dan Hobbes ve Ötesine: “Güvenlik” Kavramının Avrupa Geleneğindeki Boyutları”, **Uluslararası İlişkiler Akademik Dergi**, 6(22), 3-33.
- Arslanel, Nazan ve Eryücel, Ertuğrul (2011), “Modern Devlet Anlayışının Felsefi Temelleri”, **Atatürk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi**, 15(2), 1-20.
- Atmaca, Ayşe Ö. ve Ercan Gözen, Pınar (2018), “Uluslararası Güvenliği Yeniden Düşünmek”, **Uluslararası İlişkiler Disiplininde Feminist Eleştiriler**, 15(19), 19-31.
- Austin, John L. (1955), **How To Do Things With Words**, Oxford University Press, London.
- Avci, Erkan (2014), “Kuzey Kore'nin Siber Saldırısına Yanıt Vereceğiz”, <https://www.aa.com.tr/tr/dunya/kuzey-korenin-siber-saldirisina-yanit-verecegiz/91153> (19.12.2014)
- Bağcı, Hüseyin. (2001). **Türk Dış Politikasında 1950'li Yıllar**, ODTÜ Geliştirme Vakfı Yayınları, Ankara.

- Balzacq, Thierry (2005), "The Three Faces of Securitization: Political Agency, Audience and Context", **European Journal of International Relations**, 11(2), 171-201.
- Baran, Paul (1962), **On Distributed Communications Networks**, Rand Corporation, Santa Monica.
- Barr, James (2016), **Kırmızı Çizgi Paylaşılmayan Toprakların Yakın Tarihi**, (Çev. Ekin Can Göksoy), Pegasus Yayınları, İstanbul.
- Baylis, John (2008), "Uluslararası İlişkilerde Güvenlik Kavramı", **Uluslararası İlişkiler Dergisi**, 5(18), 69-85.
- Baysal, Başar, ve Lüleci, Çağla (2015), "Kopenhagen Okulu ve Güvenlikleştirme Teorisi", **Güvenlik Stratejileri Dergisi**, 11(22), 61-96.
- Bektaş, Ümit (2018), "Stoltenberg: Rusya'ya karşı 5. maddeyi uygulayabiliriz." <https://anlatilaninotesi.com.tr/20180917/stoltenberg-rusya-madde-1035235740.html> (17.09.2018)
- Belkin, Paul (2016), "NATO' Warsaw Summit: In Brief", **Congressional Research Service**, <https://sgp.fas.org/crs/row/R44550.pdf> (14.11.2016)
- Berktaş, Hande (2023), "Siber Saldırı Faturasının 10 Trilyon Dolara Çıkması Bekleniyor", <https://bloomberght.com/siber-saldiri-faturasinin-10-trilyon-dolara-cikmasi-bekleniyor-2348517> (01.03.2024)
- Bıçakçı, Salih (2012), "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu", **Uluslararası İlişkiler Dergisi**, 9(34), 205-226.
- Bıçakçı, Salih (2014), "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", **Uluslararası İlişkiler Dergisi**, 10(40), 100-130.
- Birleşmiş Milletler (1945), "Birleşmiş Milletler Antlaşması", https://turkiye.un.org/sites/default/files/2020-02/UN-charter-turkish_0.pdf?afd_azwaf_tok=eyJhbGciOiJSUzI1NiJ9.eyJhdWQiOiJ0dXJraXIIIjLnVuLm9yZyIsImV4cCI6MTcyNTU2MzE2NCwiaWF0IjoxNzI1NTYyODY0LCJpc3MiOiJ0aWVyMS04NDhkNWM3OTQ5LTdqY3R3Iiwic3ViIjoiMTg4LjExOS42Mi4y (29.10.2024).
- Brendon, Laura (2010), "Arpanet: An Efficient Machine as Social Discipline", **Science as Culture**, 10(1), 73-95.
- Bozkurt, Gaye (2023), **Kuzey Atlantik Antlaşması Örgütü'nün (NATO) Siber Güvenlik Politikası**, Yayınlanmamış Yüksek Lisans Tezi, Çanakkale Onsekiz Mart Üniversitesi – Eğitim Enstitüsü.
- Buzan, Barry (2015), **İnsanlar, Devletler, Korku**, (Çev. Emre Çıtak), 2. Basım, Uluslararası İlişkiler Kütüphanesi, İstanbul.
- Buzan, Barry vd. (1997), "Security: A New Framework For Analysis", Lynne Rienner Publishers Inc., Colorado.
- Cabinet Office (2009), **Cyber Security Strategy of the United Kingdom**, HM Government, London, <https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf> (09.06.2024)

- Cabinet Office (2011), **The UK Cyber Security Strategy Protecting and Promoting The UK in a Digital World**, TSO, London, <https://assets.publishing.service.gov.uk/media/5a7c69fb40f0b62aff6c17fc/7642.pdf> (12.06.2024).
- Cabinet Office (2016), **The UK Cyber Security Strategy 2011-2016**, TSO, London, https://assets.publishing.service.gov.uk/media/5a81bae5e5274a2e8ab558ca/UK_Cyber_Security_Strategy_Annual_Report_2016.pdf (12.06.2024).
- Cabinet Office (2022), “Government Cyber Security Strategy”, HM Government, London, <https://assets.publishing.service.gov.uk/media/61f0169de90e070375c230a8/government-cyber-security-strategy.pdf> (09.06.2024).
- Carr, Jeffrey (2012), **Inside Cyber Warfare: Mapping the Cyber Underworld**, 2. Baskı, O'Reilly Media, Sebastopol.
- Cohen, Cohen (1996), **Communism, Fascism, and Democracy: The Theoretical Foundations**, 3. Baskı, McGraw-Hill Companies, Boston.
- Collins, Sean ve McCombie, Stephen (2012), “Stuxnet: The Emergence of A New Cyber Weapon and Its Implications”, **Journal of Policing, Intelligence and Counter Terrorism**, 7(1), 80-91.
- Corera, Gordon (2015), **Intercept: The Secret History of Computers and Spies**, Weidenfeld and Nicolson, London.
- Cybersecurity ve Infrastructure (2020), “2009 Cyberspace policy review” <https://www.cisa.gov/resources-tools/resources/2009-cyberspace-policy-review> (21.07.2023).
- Çelebi, Vedat (2014), “Gündelik Dil Felsefesi ve Austin’in Söz Edimleri Kuramı”, **Beytulhikme An International Journal of Philosophy**, 4(1), 73-89.
- Çelik, Şener (2013), “Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme”, **Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi**, 15(1), 137-175.
- Çokbıdık, Anıl, C. (2018), “Siber Uzay ve İnsan Hakları”, **Cyberpolitik Journal**, 3(5), s. 133-157.
- Darıcı, Ali B. (2017), **Amerika Birleşik Devletleri ve Rusya Federasyonu’nun Siber Güvenlik Stratejilerinin Karşılaştırmalı**, Yayınlanmamış Doktora Tezi, Uludağ Üniversitesi - Sosyal Bilimler Enstitüsü.
- Darıcı, Ali. B. (2018), **Siber Uzay ve Siber Güvenlik: ABD ve Rusya Federasyonu' nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi**, Dora Yayıncılık, Bursa.
- Department of Defense (2015), “Department of Defense, The DOD Cyber Strategy”, <https://dod.defense.gov/Portals/1/Documents/pubs/OSD011517-15-RES-Final.pdf>.
- Devanny, Joe vd., (2021), **The National Cyber Force That Britain Needs?** King's College, London.
- Dibb, Paul (2010), The Soviet Experience in Afghanistan: Lessons To Be Learned? **Australian Journal of International Affairs**, 64(5), 495-509.
- Doğan, Zehra (2019), “Kopenhag Okulu’nun Güvenlikleştirme Teorisi Bağlamında Güvenlik-Medya İlişkisi”, **İletişim Kuram ve Araştırma Dergisi**, (49), 170-186.

- Elmer, Philip (1996), "Thinking locally, acting globally", <https://www.eff.org/pages/thinking-locally-acting-globally> (08.02.2024)
- Emmers, Ralf (2017), "Güvenlikleştirme" **Çağdaş Güvenlikleştirme Çalışmaları**, (Çev. Nasuh Uslu), 3. Baskı, Uluslararası İlişkiler Kütüphanesi, İstanbul.
- Eren, Mehmet. (2020), "İngiltere'nin Siber Güvenlik Politikası", **Yeni küresel tehdit: Siber Saldırıları Siber Güvenlik ve Politika Uygulamalar**, içinde (109-136), Nobel Yayınları, Ankara.
- Ergüven, Nasih S. (2016), Uluslararası Hukuk Açısından Güvenlik Kavramının Teorik Temelleri, **Ankara Üniversitesi Hukuk Fakültesi Dergisi**, 65(3), 771-836.
- Erkul, İbrahim Çağrı (2024), Birleşik Krallık'ın Siber Güvenlik Politikasını Güç ve Caydırıcılık Üzerinden Anlamlandırmak, **Journal Information Systems And Management Research**, 6(1), 26-39.
- Euronews (2021), "Biden: ABD Gerçek Bir Savaşa Girse Bu Siber Saldırıları Nedeniyle Olur", <https://tr.euronews.com/2021/07/28/biden-abd-gercek-bir-savasa-girerse-bu-siber-sald-r-lar-nedeniyle-olur> (08.07.2021).
- Euronews (2022), "Küresel Nükleer Silah Sayısı Soğuk Savaş'tan Bu Yana İlk Kez Artacak", <https://tr.euronews.com/2022/06/13/rusya-n-n-ukrayna-y-iskali-nedeniyle-nukleer-silahlanma-yar-s-h-z-kazanacak-rapor> (13.06.2022).
- Goodrich, Michael ve Tamassia, Roberto (2013), **Introduction To Computer Security**, 1. Baskı Pearson, London.
- Gönlübol, Mehmet ve Ülman, Haluk (1996), "Türk Dış Politikasının Yirmi Yılı (1945-1965)", **Olaylarla Türk Dış Politikası**, içinde (143-182), Siyasal Kitapevi, Ankara.
- Gül, Murat (2015), "Kuruluşundan 21. Yüzyıla: 1990'larda NATO'da Devamlılık ve Dönüşüm", **Akademik İncelemeler Dergisi**, 10(1), 247-265.
- Güler, Ayşegül (2018), "İnsani Müdahale Aracı Olarak Siber Uzay", **Medeniyet Araştırmaları Dergisi**, 2(4), 139-149.
- Gümüşbaş, Ahmet (2016) "Siber Savaş Hukukunda Meşru Müdafaa Hakkı ve İsnat Edilebilirlik: Stuxnet ve Aramco Saldırıları", **TASAM yayınları uluslararası ilişkiler Serisi**, 181-194.
- Güntay, Vahit (2018), "Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler", **Güvenlik Stratejileri Dergisi**, 14(27), s. 79-111.
- Güntay, Vahit (2019), "21. Yüzyıl Paradoksu Olarak Siber Uzay ve Uluslararası Hukuk", **Novus Orbis: Siyaset Bilimi ve Uluslararası İlişkiler Dergisi**, 1(2), 87-109.
- Gürkaynak, Muharrem (2004), **Avrupa'da Savunma ve Güvenlik**, Asil Yayın Dağıtım, Ankara.
- Hubbard, Gregory, ve Eunice, Matthew (2020), "Topical Review of Vulnerability Management for Local Hampton Roads Industry", **OUR Journal: ODU Undergraduate Research Journal**, 7(1), 1-14.
- Huntley, James R. (1965), **The NATO Story**, Manhattan Publishing Company, New York.
- Huysmans, Jeff (1998), "Revisiting Copenhagen: Or, On the Creative Development of a Security Studies Agenda in Europe", **European Journal of International Relations**, 4(4), 479-505.

- İHA. (2023), “NATO ilk kez siber savunma konferansı düzenledi”, https://www.ntv.com.tr/dunya/nato-ilk-kez-siber-savunma-konferansi-duzenledi_8dEVmhINUqmd9Z7kCYc6A (10.11.2023).
- Ismay, Lord (1956), **NATO The First Five Years 1949-1954**, Secretary General of The North, Paris.
- Ji, Qiang vd. (2019). “The Impact of OPEC on East Asian Oil Import Security: A Multidimensional Analysis”, **Energy Policy**, 126, 99-107.
- Karakuş, Güzide ve Gönen, İbrahim (2022), “Askeri Alanda Endüstri 4.0 Uygulamaları”, **Avrupa Bilim ve Teknoloji Dergisi** (43), 104-109.
- Karaosmanoğlu, Ali L. (2014), “NATO' nun Dönüşümü”, **Uluslararası İlişkiler Dergisi**, 10(40), 3-38.
- Karber, Phillip ve Combs, Jerald (1998), “The United States, NATO and the Soviet Threat to Western Europe: Military Estimates and Policy Options, 1945–1963”, **Oxford University Press**, 22(3), 399-429.
- Kaur, Jagpreet ve Ramkumar, Kasinathan (2022), “The Recent Trends in Cyber Security: A Review”, **Journal of King Saud University-Computer and Information Sciences**, 34(8), 5766-5781.
- Kelsen, Hans (1945), “The Old the New League: The Covenant and The Dumbarton Oaks Proposals”, **The American Journal of International Law**, 39(1), 45-83.
- Kişman, Zülfükar ve Güleç, Özge (2021), “Uluslararası İlişkiler Açısından Siber Güvenlik ve NATO'nun Siber Güvenlik Stratejileri”, **Akademik Açı**, 1(1), s. 127-154.
- Kızıışay, Şeyma (2020), “Soğuk Savaş Sonrası ABD'nin Siber Güvenlik Politikası”, **International Journal of Economics Administrative And Social Sciences**, 3(1), 33-44.
- Klimburg, Alexander (2012), **National Cyber Security Framework Manual**, NATO Cooperative Cyber Defence Centre of Excellence, London.
- Korobkov, Andrei ve Zaionchkovskaia, Zhanna (2004), “The Changes in the Migration Patterns in the Post-Soviet States: The First Decade” **Communist and Post-Communist Studies**, 37(4), 481-508.
- Kukulin, Ilya (2020), “The Culture of Ban: Pop Culture, Social Media and Securitization of Youth Politics in Today's Russia”, **International Journal of Cultural Policy**, 27(2), s. 177-190.
- Kurt, Selim (2020), Güvenlikleştirme Kuramı Açısından Rusya Federasyonu- Ukrayna Çatışmasını Anlamak. **Ankara Üniversitesi SBF Dergisi**, 75(1), 1-30.
- Kutlu, Övünç (2016), “New York Times: ABD' ye Yönelik Siber Saldırıya En Güçlü Yanıt Verildi”, <https://www.aa.com.tr/tr/dunya/new-york-times-abdye-yonelik-siber-saldiriya-en-guclu-yanit-verildi/716845> (30.12.2016).
- Lebedeva, Nadezhda vd., (2021), “Multiple Social Identities İn The Post-Soviet Sontext. Non-Western Identity”, **Pragmatics**, içinde (131-150) Cambridge University Press, İsveç.
- Lewis, Ted (2015), **Critical İnfrastructure Protection İn Homeland Security: Defending A Networked Nation**, 3. Baskı, Wiley-Interscience, New Jersey.
- Lis, Piotr ve Mendel, Jacob (2019), “Cyberattacks On Critical İnfrastructure: An Economic Perspective”, **Economics And Business Review**, 5(19), 24-47.

- Loader, Brian (1997), **The Governance Of Cyberspace: Politics, Technology And Global Restructuring**, 1. Baskı, Routledge, New York.
- Mathrani, Anuradha ve Alipour, Massoud (2010), “Website Blocking Across Ten Countries: A Snapshot”, **PACIS 2010**, 1588-1595.
- McDonald, Matt (2008), “Securitization And The Construction Of Security”, **European Journal of International Relations**, 14(4), 563-587.
- McSweeney, Bill, (1999), **Security, Identity And Interests; A Sociology Of International**, Cambridge University Press, New York.
- Migueluez, Cristina V. (2023), “Guidelines For Renewal And Securitization Of A Critical Infrastructure Based On Iot Networks”, **Smart Cities**, (2), 728-743.
- Minuto-Rizzo, Alessandro (2007), “NATO's Transformation And New Partnerships: The Mediterranean”, **Duke University Press**, 18(3), 1-13.
- Miş, Nebi (2014), “Güvenlikleştirme Teorisi ve Siyasal Olanın Güvenlikleştirilmesi”, **Akademik İncelemeler Dergisi**, 6(2), 345-381.
- Miynat, Mustafa ve Duramaz, Selim (2013), “Karapara Aklama Aracı Olarak Yeni Bir Mali Suç: Siber- Aklama”, **Yönetim ve Ekonomi Dergisi**, 20(1), s. 315-325.
- Nagy, Viktor (2012), “The Geostrategic Struggle İn Cyberspace Between The United States, China And Russia”, **National University of Public Service**, 11(1), 13-26.
- NATO (1949), “*Kuzey Atlantik Antlaşması*”,
https://www.nato.int/cps/fr/natohq/official_texts_17120.htm?selectedLocale=en (09.04.1949).
- NATO (1999), “The alliance's strategic concept (1999)”,
https://www.nato.int/cps/en/natohq/official_texts_27433.htm (24.04.1999).
- NATO (2008), “Bucharest Summit Declaration”,
https://www.nato.int/cps/en/natolive/official_texts_8443.htm (03.04.2008).
- NATO (2010), “Strategic Concept For The Defence And Security Of The Members Of The North Atlantic Treaty Organization (2010)”,
https://www.nato.int/cps/en/natohq/topics_82705.htm (19.11.2010).
- NATO (2011), “Cyber Defence”
https://www.nato.int/cps/en/natohq/topics_78170.htm?selectedLocale=en (30.07.2024).
- NATO (2012), “Chicago Summit Declaration”, North Atlantic Treaty Organization:
https://www.nato.int/cps/en/natohq/official_texts_87593.htm (20.05.2012).
- NATO (2014), “NATO wales summit 2014: Outcomes.”,
<https://researchbriefings.files.parliament.uk/documents/SN06981/SN06981.pdf> (12.09.2014).
- NATO (2018), “Press Conference By NATO Secretary General Jens Stoltenberg At The Conclusion Of The Brussels Summit”, https://www.nato.int/cps/en/natohq/opinions_156738.htm (12.07.2018).
- NATO (2019), “London Declaration”,
https://www.nato.int/cps/en/natohq/official_texts_171584.htm (04.12.2019).

- NATO (2022), “NATO 2022 Strategic Concept”, https://www.nato.int/nato_static_fl2014/assets/pdf/2022/6/pdf/290622-strategic-concept.pdf (29.06.2022).
- Ortaç, Tuğrul (2019), “İkinci Dünya Savaşında Müttefik Konferansları ve Türkiye İçin Önemi”, **Genel Türk Tarihi Araştırmaları Dergisi**, 1(1), 97-126.
- Öğün, Mehmet vd., (2013), Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler. **Güvenlik Stratejileri Dergisi**, 9(18), 145-181.
- Özdemir, Musa. vd., (2018), Yalta Konferansı: Soğuk Savaşa Giden Yol Yalta Conference: The Road To Cold War. **Barış Araştırmaları ve Çatışma Çözümleri Dergisi**, 5(2), 62- 79.
- Polat, Doğan Ş. (2020a), “Kuruluşundan Çöküşüne Milletler Cemiyeti Sistemi”, **Elektronik Sosyal Bilimler Dergisi**, 19(76), 1950-1967.
- Polat, Doğan Ş. (2020 b), “NATO'nun Yeni Operasyon Alanı: Siber Uzay”, **Güvenlik Bilimleri Dergisi**, Şubat Özel Sayısı, 135-158.
- Propp, Kenneth (2021), **International Legal Materials**, Cambridge University Press, New York.
- Rakhmanova, Upagül (2018), “Siber Uzayın Güvenlikleştirilmesi: ABD Örneği”, **Cyberpolitik Journal**, 3(5), 45-61.
- Rasquinho, Selen V. (2024), “Stoltenberg: Bu Yıl NATO Ülkelerinin Üçte İki Savunma Harcamalarında Yüzde 2 Hedefini Tutturacak”, <https://www.aa.com.tr/tr/dunya/stoltenberg-bu-yil-nato-ulkelerinin-ucte-ikisi-savunma-harcamalarinda-yuzde-2-hedefini-tutturacak/3164512> (14.03.2024).
- Richards, Julian (2014), **Cyber-War The Anatomy Of The Global Security Threat**, Palgrave Pivot, New York.
- Salcı, Tayfun (2019), “NATO Genel Sekreteri Stoltenberg: Siber Saldırı NATO'nun 5. Maddesini Tetikleyebilir”, <https://www.aa.com.tr/tr/dunya/nato-genel-sekreteri-stoltenberg-siber-saldiri-natonun-5-maddesini-tetikleyebilir/1566941> (28.08.2019).
- Schmitt, Michael N. (2013), **Tallin Manual On The International Law Applicable To Cyber Warfare**, 2. Baskı, Cambridge University Press, New York.
- Schneider, Anne ve Ingram, Helen (1993), “Social Construction of Target Populations: Implications for Politics and Policy”, **The American Political Science Review**, 87(2), 334-347.
- Shea, Jamie (2017), “How is NATO Meeting the Challenge of Cyberspace?” **Prism**, 7(2), 18-29.
- Sheehan, Michael (2005), **International Security: An Analytical Survey**, Lynne Rienner Publishers. London.
- Singer, Peter W. ve Friedman, Allan (2014), **Cybersecurity And Cyberwar: What Everyone Needs To Know**, Oxford University Press, New York.
- Siyasi ve Sosyal Araştırmalar Vakfı (1997), **NATO'nun Genişlemesi ve Türkiye**, SİSAV, Ankara.
- Sperling, James ve Webber, Mark (2017), “NATO and the Ukraine Crisis: Collective Securitisation”, **European journal of international security**, 2(1), 19-46.
- Steel, Chad (2015), “Web-Based Child Pornography: The Global Impact Of Deterrence Efforts and Its Consumption on Mobile Platforms”, **Child Abuse&Neglect**, 44, 150-158.

- Şener, Bülent. (2017), “Soğuk Savaş Sonrası Dönemde Uluslararası Göç Olgusu ve Ulusal Güvenlik Üzerindeki Etkileri Üzerine Bir Değerlendirme”, **Güvenlik Bilimleri Dergisi**, 6(1), s. 1-30.
- Tarlin, Solomon (2021), “The Future of Cash”, **Consumer Finance İnstitute**, <https://www.philadelphiafed.org/-/media/frbp/assets/consumer-finance/discussion-papers/dp21-03.pdf> (20.09.2021).
- The White House (1998), “Presidential Decision Directive 63”, <https://irp.fas.org/offdocs/pdd/pdd-63.htm> (22.05.1998).
- The White House (2003), “National Strategy For The Physical Protection Of Critical İnfrastructures And Key Assets”, https://www.dhs.gov/xlibrary/assets/Physical_Strategy.pdf (23.02.2003).
- The White House (2008), “National Security Presidential Directive/Nspd54”, <https://irp.fas.org/offdocs/nspd/nspd-54.pdf> (08.01.2008).
- The White House (2009), “Cyberspace Policy Review”, <https://irp.fas.org/eprint/cyber-review.pdf> (15.06.2023).
- The White House (2011), “International Strategy for Cyberspace”, https://obamawhitehouse.archives.gov/sites/default/files/rss_viewer/international_strategy_for_cyberspace.pdf (03.06.2011).
- The White House (2013), “Improving Critical İnfrastructure Cybersecurity”, <https://www.govinfo.gov/content/pkg/FR-2013-02-19/pdf/2013-03915.pdf> (12.02.2013).
- The White House (2015), “National Security Strategy”, https://obamawhitehouse.archives.gov/sites/default/files/docs/2015_national_security_strategy_2.pdf (23.02.2015).
- The White House (2016), “Factsheet: Cybersecurity National Action Plan”, <https://obamawhitehouse.archives.gov/the-press-office/2016/02/09/fact-sheet-cybersecurity-national-action-plan> (09.02.2016).
- The White House (2018) “National Cyber Strategy”, <https://trumpwhitehouse.archives.gov/wp-content/uploads/2018/09/National-Cyber-Strategy.pdf> (09.09.2022).
- The White House (2021), “Fact Sheet: Imposing Costs For Harmful Foreign Activities by The Russian Government”, <https://www.whitehouse.gov/briefing-room/statements-releases/2021/04/15/fact-sheet-imposing-costs-for-harmful-foreign-activities-by-the-russian-government/> (15.04.2021).
- The White House (2022), “National Security Strategy”, <https://www.whitehouse.gov/wp-content/uploads/2022/10/Biden-Harris-Administrations-National-Security-Strategy-10.2022.pdf> (31.01.2022).
- The White House (2023), “National Cybersecurity Strategy”, <https://www.whitehouse.gov/wp-content/uploads/2023/03/National-Cybersecurity-Strategy-2023.pdf> (31.03.2023).
- Thucydides (2015), **The History of the Peloponnesian War**, (Çev. Richard Crawley), CreateSpace Independent Publishing Platform, Washington.
- Tokatlı, Seda G. (2022), “NATO'nun Sistem İçerisindeki Dönüşümü ve Geleceği”, **UPA Strategic Affairs**, 3(2), 61-84.

- Trombetta, Maria J. (2010), "Rethinking The Securitization Of The Environment: Old Beliefs, New Insights", **Securization Theory How Security Problems Emerge And Dissolve**, içinde (135-149), Routledge, New York.
- U.S. Department of State. (2005). "Report of the Working Group on İnternet Governance", <https://digitallibrary.un.org/record/542570?v=pdf> (15.10.2023).
- U.S. Department of Homeland Security (2018), "Cybersecurity Strategy", https://www.dhs.gov/sites/default/files/publications/DHS-Cybersecurity-Strategy_1.pdf (15.05.2018).
- Ünver, Gül N. (2023), **Siber Güvenlik Politikalarının Karşılaştırmalı Bir Analizi: Türkiye ve İngiltere Örneği**, Livre de Lyon, Lyon.
- Varlık, Ergün (2016), "Clinton: Siber Saldırlara Askeri Harekatla Karşılık Vereceğim", <https://siberbulten.com/uluslararası-iliskiler/clinton-siber-saldırlara-askeri-harekatla-karsilik-verecem/> (10.09.2016).
- Waever, Ole (1995), "Securitization and Desecuritization", **On Security**, içinde (46-86), Columbia Universty Press, New York.
- Walt, Stephen (2017), "Realism and Security", <https://oxfordre.com/internationalstudies/display/10.1093/acrefore/9780190846626.001.0001/acrefore-9780190846626-e-286;jsessionid=53BE2AE9467FDB1F963C0252C6B88C81?rskey=YurqLt&result=1> (22.12.2017).
- We are Social (2023), "Digital 2023", <https://wearesocial.com/wp-content/uploads/2023/03/Digital-2023-Global-Overview-Report.pdf> (17.05.2024).
- Weinrod, Bruce ve Barry, Charles (2012), **NATO Command Structure Considerations For The Future**, CreateSpace İndependent Publishing Platform, Washington.
- Wohlforth, William (2009), "Realism and Security Studies", **The Routledge Handbook of Security Studies**, 1. Baskı, içinde (9-20) Routledge, New York.
- Yılmaz, Ercan N. ve Gönen, Serkan (2018), "Attack Detection/Prevention System Against Cyber Attack in İndustrial Control Systems", **Computer&Security**, 77, 94-105.
- Yılmaz, Ercan N. vd., (2021), "Endüstri 4.0'ın Gelişim Sürecinde Unutulan Bileşen: Siber Güvenlik" **Düzce Üniversitesi Bilim ve Teknoloji Dergisi**, 9(4), s. 1142-1158.

ÖZGEÇMİŞ

2017 yılında Atatürk Üniversitesi Uluslararası ilişkiler bölümü kazandı ve 2020 yılında mezun oldu. Aynı yıl Karadeniz Teknik Üniversitesi'nde Uluslararası İlişkiler Tezli Yüksek Lisans programını kazandı.

KAYA nişanlıdır, İngilizce bilmektedir ve aktif olarak çalışmaktadır.

