KARADENİZ TEKNİK ÜNİVERSİTESİ * SOSYAL BİLİMLER ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER ANABİLİM DALI

TEZLİ YÜKSEK LİSANS PROGRAMI

SİBER ALANIN NATO GÜVENLİK MİMARİSİ ÖZELİNDE ANALİZİ

YÜKSEK LİSANS TEZİ

Sena KAYA

EYLÜL - 2024

TRABZON

KARADENİZ TEKNİK ÜNİVERSİTESİ * SOSYAL BİLİMLER ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER ANABİLİM DALI

TEZLİ YÜKSEK LİSANS PROGRAMI

SİBER ALANIN NATO GÜVENLİK MİMARİSİ ÖZELİNDE ANALİZİ

YÜKSEK LİSANS TEZİ

Sena KAYA

Tez Danışmanı: Doç. Dr. Vahit GÜNTAY

EYLÜL - 2024

TRABZON

ONAY

Sena KAYA tarafından hazırlanan "Siber Alanın NATO Güvenlik Mimarisi Özelinde Analizi" adlı bu Çalışma 04.11.2024 tarihinde yapılan savunma sınavı sonucunda oybirliği/oyçokluğu ile başarılı bulunarak jürimiz tarafından Uluslararası İlişkiler Anabilim Dalı Tezli Yüksek Lisans Programı'nda **yüksek lisans tezi** olarak kabul edilmiştir.

Jüri Üyesi		**Karar**		**İmza**
Unvanı - Adı ve Soyadı	**Görevi**	**Kabul**	**Ret**	
Doç. Dr. Vahit GÜNTAY	Başkan	☐	☐	
Doç. Dr. Bülent ŞENER	Üye	☐	☐	
Doç. Dr. Selim KURT	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.

Sena KAYA
19.09.2024

ÖNSÖZ

Dünyadaki gelişmelerin hızlı ve baş döndürücü yapısında güvenlik tarih boyunca en önemli unsurlar arasında başrolde yer almıştır. Modern toplumun güvenlik sorunları arasında siber uzayın yeri oldukça geniştir. Bu çalışmada, siber güvenlik alanında Kuzey Atlantik Antlaşması Örgütü'nün gelişmeleri incelenmiştir. Siber güvenlik konusunda yapılmış olan inceleme ile okuyuculara siber tehditlere alternatif savunma konusunda bakış açısı sağlanmaya çalışılmıştır.

Siber alanın geniş ve karmaşık doğası sebebi ile kimi zaman zorluklar ile karşılaşmış olsam da bu alanda oldukça derin tecrübe ve bilgiye sahip olan ve süreç boyunca bana ışık tutan değerli danışmanım Doç. Dr. Vahit GÜNTAY'a teşekkürlerimi sunarım.

Eylül, 2024 Sena KAYA

İÇİNDEKİLER

İKİNCİ BÖLÜM

ÜÇÜNCÜ BÖLÜM

ÖZET

Güvenliğin ne olduğu sorusu tarih boyunca birçok şekilde açıklanmaya çalışılmıştır. Uluslararası ilişkiler teorileri bağlamında birçok düşünür bu konuda çalışmalar yapmışlardır. Güvenliğin varlığının önemi bilinmekle birlikte geniş kapsamlı oluşu siber alan içerisinde de kendisini göstermesini sağlamaktadır. Bu da siber güvenlik, siber uzay, siber istikrarsızlık ve çatışma gibi birçok kavramın tartışılmasına neden olmuştur. Uluslararası ilişkiler bünyesinde devletlerin bir araya gelip çeşitli amaçlar doğrultusunda oluşturmuş olduğu birlikler bünyesinde siber güvenlik çalışmaları mevcuttur. Bu noktada önemli olan iş birliği ve ortaklıktır.

Bu çalışmada, siber savunma alanında mücadele kapsamında Kuzey Atlantik Antlaşması Örgütü (NATO)'nün rolü incelenmiştir. Uluslararası savunma alanındaki önemi vurgulanıp siber alanda benzer niteliklerde olabileceği tartışılmıştır. Bu bağlamda nitel araştırma yöntemi kullanılarak araştırmalar sonucunda bir analiz sunulması amaçlanmıştır.

Anahtar Kelimeler: Uluslararası Güvenlik, Uluslararası Örgütler, Siber Uzay, Siber Savunma, Siber Terörizm

ABSTRACT

The question of what security is has been tried to be explained in many ways throughout history. Many thinkers have worked on this issue in the context of International Relations Theories. While the importance of the existence of security is known, its wide-ranging nature enables it to manifest itself in cyberspace. This has led to the discussion of many concepts such as cyber security, cyberspace, cyber instability and conflict. Within international relations, there are cyber security studies within the unions that states have come together and formed for various purposes. What is important at this point is cooperation and partnership.

In this study, the role of the North Atlantic Treaty Organization (NATO) in the fight against cyber defense is examined. Its importance in the field of international defense was emphasized and it was discussed that it could have similar qualities in the cyber field. In this context, it is aimed to provide some clues and analysis as a result of the research by using qualitative research method.

Keywords: International Security, International Organizations, Cyberspace, Cyber Defense, Cyber Terrorism

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

GRAFİKLER LİSTESİ

KISALTMALAR LİSTESİ

AB	: Avrupa Birliği
ABD	: Amerika Birleşik Devletleri
AEA	: Uluslararası Atom Enerjisi Ajansı
APT	: Advanced Persistent Threat
BM	: Birleşmiş Milletler
BMGK	: Birleşmiş Milletler Güvenlik Konseyi
CERTs	: Bilgisayar Acil Durum Müdahale Ekipleri
CIO	: Bilgi Teknolojileri ve İletişimden Sorumlu Yetkilisini
CJTF	: Birleşik Ortak Görev Gücü
CTI	: Cyber Threat Intelligence
ÇHC	: Çin Halk Cumhuriyeti
DDoS	: Servis Dışı Bırakma Saldırısı
DNS	: Domain Name System
GCHQ	: Government Communications Headquarters
IAEA	: Uluslararası Atom Enerjisi Ajansı
INF	: Orta Menzilli Nükleer Kuvvetler Anlaşması
IOC	: Indicators of Compromise
İSS	: İnternet Servis Sağlayıcıları
NATO	: Kuzey Atlantik Antlaşması Örgütü
NICP	: NATO Endüstri Siber Ortaklığı
NSA	: Ulusal Güvenlik Ajansı
PLC	: Programlanabilir Mantıksal Denetleyicileri
RF	: Rusya Federasyonu
SB	: Sovyetler Birliği
SC-99	: 1999 Stratejik Konsepti
SIEM	: Security Information and Event Management
TTP	: Taktikler, Teknikler ve Prosedürler
US DOD	: ABD Savunma Bakanlığı
VCISC	: Sanal Siber Olay Destek Yeteneği
WAF	: Web Application Firewall

GİRİŞ

Soğuk Savaş döneminin bitmesi ile uluslararası ilişkilerde ve güvenlik dinamiklerinde birtakım değişimler ve gelişmeler yaşanmıştır. Bu değişimler uluslararası aktörlerin güvenlik politikalarını gözden geçirmelerine ve yeni tehditlerle başa çıkmak için stratejiler geliştirmelerine yol açmıştır. Bu stratejiler birtakım ortaklıklar ve iş birliği içerisinde gelişebilmektedirler. Bu bağlamda, Soğuk Savaş döneminden nispeten başarılı çıkan NATO üye devletlerin savunma kapasitelerini güçlendirmek ve ortak bir güvenlik çerçevesi oluşturmak için önemli bir rol oynamaktadır.

Gelişmekte olan siber alan, bünyesinde birtakım tehlikeleri barındırmaktadır. Örnek verilecek olursa siber terörizm gibi türleri ile kişisel veriler ve teknolojik kullanım alanları tehlikeye girmektedir. Bu durum siber savunma sistemlerinin geliştirilerek güvenli bir ortamın sağlanmasını gerekli kılmaktadır. Çünkü siber saldırılar oldukça tehlikeli ve hızlı gelişen ataklardır. Saldırganlar tek tuşla ciddi kayıplara neden olacak ataklar yapabilmektedirler. Uluslararası aktörler açısından bu saldırıların yıkıcı boyutunun bir siber savaşa dönüşmemesi için iş birliği ve ortaklıklar oldukça önemlidir.

Bu çalışmada temel olarak incelenmek istenen husus NATO'nun siber savunma bağlamında ne gibi çalışmalar yapmakta olduğudur. Bu perspektiften analiz yapıldığında belirtilmek istenen fikir, birliğin siber savunma anlamında müttefiklerine daha kapsamlı bir güvenlik çatı mimarisi oluşturabilmesi için ne tür önlemlerin etkili olabileceğinin tespitidir. Çalışmanın sonuç kısmı bu hedef doğrultusunda hazırlanmıştır.

Bu çalışmada eleştirel kaynak incelemesi ve nitel araştırma yöntemleri kullanılmıştır. Genel erişimli açık kaynaklardan elde edilen kitaplar, makaleler, tezler, haberler ve bağımsız kuruluşların raporları değerlendirilmiştir. Sonuç kısmını desteklemek amacıyla çeşitli veri, tablo ve şekiller sunulmuştur. Ayrıca tezin temel inceleme konusunda NATO'nun resmî raporlarından ve belgelerinden faydalanılmıştır. Özgün ve kesin sonuçlara ulaşılabilmesi için bu belgelerden faydalanılmış olunsa da kimi sorulara net cevaplar bulunamamıştır.

Bu çalışmanın ana araştırma soruları şu şekilde formüle edilmiştir: Siber uzay ekseninde gelişen ve değişen tehlike boyutları hangi düzeylere ulaşabilmektedir? Çalışmada incelenen NATO siber alanda ne tür çalışmalar yapmıştır? Ortaklık bağlamında siber güvenliğin daha sağlam bir zemine oturtulabilmesi için neler yapılabilir? Bu araştırma soruları temel alınarak geliştirilen ana hipotez NATO'nun siber uzay alanında güvenlik ekseninde yapmış olduğu çalışmaların yanı sıra üye

devletlerin ortak bir zeminde savunma sistemlerini geliştirebilmelerinin mümkün olabileceğidir. Bahsi geçen hipotezi kanıtlamak için NATO'nun siber alanda yapmış olduğu çalışmalar incelenmiştir.

Üç bölümden oluşan bu çalışmada, NATO'nun savunma perspektifi siber alan nezdinde incelenmiş olup, siber güvenlik çalışmalarına ilişkin analiz yapılmaya çalışılmıştır. Bu doğrultuda siber güvenliğin kapsamı ele alınarak birliğin alandaki çalışmalarını ne şekilde geliştirebileceğine dair tartışmaya açık analizler yapılmıştır.

Birinci bölüm dahilinde *Güvenlik Kavramının Analizi* başlıklı kısımda, güvenlik kavramının anlaşılmasını kolaylaştıracak kavramsal bir giriş yapılmıştır. Burada güvenlik kavramının genelden özele gidilerek uluslararası ilişkiler bağlamında ne ifade ettiği ve modern güvenlik sorunları içerisinde siber güvenliğe nasıl nüfuz ettiğinden bahsedilmiştir. Kavramın derinlemesine anlaşılması için uluslararası teorilerinden faydalanılmıştır.

İkinci bölüm dahilinde *Siber Güvenlik Kavramının Uluslararası Politika Perspektifinden Analizi* başlıklı alanda, siber alan dahilinde siber güvenliğin anlaşılmasını sağlayabilecek kavramlar incelenmiştir. Buna ek olarak siber savunma disiplininde örgütlerin stratejileri analiz edilmiştir.

Üçüncü ve son bölüm dahilinde *NATO ve Siber Güvenlik Politikaları Açısından Değerlendirme* başlıklı kısımda, NATO'nun ne olduğu anlaşılmaya çalışılıp tarihsel süreci incelenmiştir. Bu doğrultuda birliğin siber savunma bağlamında mevcut durumu yapılmış olan araştırmalar dahilinde değerlendirilmeye çalışılmıştır.

BİRİNCİ BÖLÜM

1. GÜVENLİK KAVRAMININ ANALİZİ

Güvenlik kavramının ne olduğunun anlaşılabilmesi için uluslararası ilişkiler bağlamında tarihsel süreçlere bakmak fayda sağlayabilir. Bu bağlamda güvenliğin oldukça önemli olduğu ve devletler için göz ardı edilemeyecek bir unsur olduğu söylenebilir. Geçmişten günümüze yaşanan gelişmeler doğrultusunda güvenlik algısı farklı boyutlarıyla gündeme gelmiştir. Bu durum güvenliğin ne olduğunun yorumlanmasında etkili olmuştur ve sürekli gelişen bir kavram olduğunun anlaşılmasını sağlamıştır.

Tanımsal Olarak Güvenlik Kavramı

Güvenlik kavramının tanımını yapabilmek için birçok araştırma yapılmıştır. Güvenliğin çok boyutlu bir kavram olduğu görülmektedir. Bu nedenle onu açıklamada tek ve kesin bir tanımının yapılması zordur sonucuna varılabilir. Araştırmacılar ve teorisyenler güvenliği anlamada dönemsel konulara odaklanarak açıklamalarda bulunmuşlardır.

1.1.1. Güvenlik nedir?

Geniş kapsamlı bir güvenlik anlayışını güç ve tehditlerle sınırlı bir alana indirgemeye kalkarsak güvenliği etkileyen öteki faktörleri göz ardı etmek zorunda kalabiliriz (Kolodziej, 2005: 2). Güvenlik çok boyutlu ve aynı zamanda geçmişten günümüze küresel çapta yaşanan gelişmeler ile kendisiyle ilgili yeni tanımlamalar yapılmış olan bir kavram olmuştur (Brooks, 2009: 1). Burada güvenliği sürekli gelişen cansız bir organizmaya benzetebiliriz.

Genellikle güvenlik denildiği zaman akla en başta askeri güvenlik gelmektedir. Barışçıl ortamın sağlanabilmesi için askeri güç oldukça önemli görülmektedir. Bu da uluslararası ortamın güvenlik eksenine, karakterine doğrudan etki etmektedir (Morgenthau, 1949: 8). Devletlerin anarşik yapısı dolayısı ile güvenli ortama ulaşabilmek için sürekli bir güç arayışı gerekli görülmüştür. Kenneth N. Waltz, 1979 yılında yapmış olduğu *Theory of International Politics* adlı çalışmasında bu konuyu ele almaktadır ve oldukça popüler hale getirmektedir. Yani devletler kendi güvenliklerini sağlamak için askeri gücü hedeflemekte ve bu güce dayalı denge politikası izlemektedir (Waltz, 1979). Fakat güvenlik askeri güç konularının içerisinde sınırlandırılamayacak kadar geniş bir kavramdır. Bu bağlamda Ken Booth, 2005 tarihinde *Critical Security Studies and World Politics* adlı

eserinde eleştirel bir bakış açısı ile güvenliğin çok boyutlu bir kavram olduğunu vurgulamaktadır. Neyin ve kimin güvenliği sorusunu sorduğumuzda verilecek yanıtların yelpazesi oldukça geniş olacaktır (Booth, 2005). Ekonomi, salgın hastalıklar, terörizm, sosyal toplum, adalet, insan hakları ve dijital güvenlik gibi konular bu soruya yanıt olarak verilebilmektedir. Bahsi geçen örneklerin yaşandığı durumlar tarihsel süreçte kendisini sürekli olarak yenileyen olgular oldukları için kavramın tanımının da olaylara ve zamana göre değişebilmesi mümkündür.

Güvenliğin oluşabilmesi için herhangi bir güvensizlik olgusunun ortada olmaması gereklidir. Yani güvenlik kısaca varlığı tehdit eden herhangi bir şeyin olmaması durumudur.[1] Bu nedenle güvenlik olgusu, genel anlamda güvenlik tehditleri aracılığıyla tanımlanır ve önemi bu yolla anlaşılır (Ullman, 1983). Genel olarak bir şeylerin veya bir sistemin olası tehditlere veya saldırılara karşı korunması durumuna *güvenlikli durum* denebilir. Böyle bir durum risklerin en aza indirgendiği bir haldir.

Güvenlik kavramı farklı alanlarda farklı şekillerde uygulanabilen bir kavramdır. Bilgi güvenliği bilişim sistemlerinin ve verilerin korunmasıyla ilgilenirken, fiziksel güvenlik binalar gibi somut kaynakların korunmasıyla ilgilenir. Aynı şekilde siber güvenlik dijital ortamdaki sistemlerin ve ağların korunmasıyla ilgilenir. Güvenlik bu gibi alanlarda tehlikelerin belirlenmesi, risklerin değerlendirilmesi ve uygun önlemlerin alınması sürecinde etkin rol oynamaktadır. Bahsi geçen önlemler güvenlik açıklarını azaltmak, tehditleri tespit etmek ve saldırıları engellemek için uygulanan çeşitli yöntemlerdir. Bu yöntemler arasında erişim kontrolleri, şifre oluşturma, güvenlik duvarları, kontrol ve izleme sistemleri, güvenlik protokolleri, eğitim ve farkındalık gibi yöntemler vardır. Farkındalık oluşturma adına bu gibi konularda okullarda eğitimler verilmektedir. Bunun yanında halk bilinçlendiği takdirde kişiler kendi güvenliğini sağlama adına önlemler alabilirken, kontrolleri dışında oluşabilecek tehditleri en aza indirebilmek adına dış güvenlik önlemleri üst kurumlar tarafından sağlanır. Bu güvenlik önlemleri alınırken önlemlerin sürekli olarak geliştirilmesine dikkat edilmektedir. Çünkü siber tehditler sürekli değişip gelişim göstermektedir. Hızlı ve ileri görüşlü önlemlerin alınması bu tehditlerin bertaraf edilebilmesi açısından önemlidir.

Sonuç olarak güvenlik, tehdit altına girebilecek her şeyin korunması ve bu tehditlere karşı önlem alınması sürecidir. Herhangi bir tehdit ve riskin olmadığı durum güvenlidir. Bu durum oluşturulurken riskleri en aza indirmek, kaynakları, varlıkları ve diğer şeyleri korumak ve güvenliği sağlamak temel amaçtır. Bunu yaparken de alanların genişliği göz önüne alınarak kişisel gizlilik, veri güvenliği, şirket varlıklarının korunması, kamu düzeninin sağlanması ve askeri perspektifler gibi birçok farklı alanda farklı yöntemler kullanılmaktadır. Özellikle dijital çağda siber güvenlik büyük önem taşırken aynı zamanda fiziksel güvenlik, halkın güvenliği ve ulusal güvenlik gibi alanlar da

[1] Cambridge Üniversitesi'ne ait sözlükteki açıklamaya göre güvenlik, bir kişi, bina, kuruluş veya ülkenin işlenen suçlar veya yabancı ülkelerin saldırıları gibi tehditlere karşı korunmasın durumudur (Dictionary, 2024).

büyük öneme sahiptir. Farklı yönleriyle güvenlik tanımı en çok tartışılan alanlardan biridir ve genellikle oksijene benzetilebilir çünkü değeri eksikliği fark edildiğinde anlaşılabilmektedir (Chesters, 2004). Bu eksiklik zaman içerisinde daha büyük tehlikelere yol açabilir. Bu nedenle güvenlik önlemlerinin devamlı olarak göz önüne getirilmesi ve güvensizlik durumunun oluşmaması için çabalanması önemlidir.

1.1.2. Küresel Güvenlik

Küreselleşme belirli bir zaman dilimi içinde net bir tanımı veya kesin bir başlangıcı ya da sona sahip olmayan, çok yönlü bir süreçtir (Al-Rodhan, 2006: 3). 1990 sonrasında yoğunlaşan bu kavram güvenlik anlayışında da birtakım değişimlere yol açmıştır. Bunu anlayabilmek için öncelikle küreselleşmenin ne olduğunu bilmek faydalı olacaktır. Bu noktada küreselleşme için sürekli genişleyen bir alan diyebiliriz. Bu genişleyen alanda küreselleşme dünya çapındaki aktörlerin ulusal, siyasi ve sosyal oluşumları arasındaki ortaya çıkan çelişkinin ortak bir çözümü olarak tanımlanabilir (Teeple, 2000).

Küreselleşme dünyadaki tüm gelişmelerle bağlantılı bir faktördür. Silahların yayılması, küresel sağlık sorunları, terörizm ve iklim değişikliği gibi önemli tehditlerin devletler tarafından tek taraflı olarak ele alınamaması bu tehditleri anlama ve etkili bir şekilde yanıtlama konusunda küresel bir güvenlik perspektifine ihtiyaç duyulduğunu göstermektedir (Burke vd., 2016). Yani sorunların ortak çözümü bizi *küresel güvenlik* kavramına itmektedir. Bu kavram genel olarak, uluslararası ilişkiler ve güvenlik alanlarında kullanılmaktadır. Küreselleşme boyutu içerisindeki güvenlik olgusu dünya genelinde barış, istikrar ve güvenliğin sağlanması adına alınan tedbirlerin ve politikaların bütününü kapsamaktadır. Burada bahsedilen, problemler için ortak bir çözümde iş birliğine gidilmesidir. Çözüm odaklı düşünüldüğünde dünya genelindeki küresel güvenlik sorunlarının tespiti ilk aşamadır. Bunlar arasında terörizmle mücadele, nükleer silah yayılımının kontrol altına alınması, siber güvenlik, çatışmaların önlenmesi veya hasarların en aza indirgenmesi, insani yardım ve barışı koruma gibi konular yer almaktadır.

Devletlerin iş birliği yaparak ilgilenmeleri gereken küresel konular olduğu ortadadır. Ayrıca devletlerin yanı sıra küresel güvenlik konularıyla ilgilenen uluslararası örgütler, sivil toplum kuruluşları, bölgesel örgütler ve diğer aktörler çalışmalar yapmaktadırlar. Küresel güvenlik çalışmaları yapılırken tüm aktörler arasında iş birliği önemlidir çünkü sorun küresel konular olduğunda bir bölgedeki güvenlik tehdidi diğer bölgelerdeki devletleri ve aktörleri de etkileyebilmektedir. Bu durum çeşitli uluslararası anlaşmaların ve iş birliklerinin oluşturulmasına ön ayak olmuştur. Örneğin NATO, Kuzey Amerika ve Avrupa ülkelerinin güvenlik alanında iş birliği yapmak için kurduğu askeri bir ittifaktır. Birleşmiş Milletler (BM) küresel güvenliği teşvik etmek ve korumak için uluslararası iş birliği yapmayı amaçlayan uluslararası bir örgüttür. Birleşmiş Milletler Güvenlik Konseyi (BMGK) uluslararası barış ve güvenliği sağlamak amacıyla askeri ve siyasi

önlemleri almakla sorumludur. Uluslararası Atom Enerjisi Ajansı (IAEA) nükleer enerji kullanımının barışçıl amaçlarla sınırlanması ve nükleer silah yayılmasının önlenmesi için uluslararası bir kontrol ve denetim kuruluşudur. Interpol uluslararası suçlarla mücadele etmek ve uluslararası polis iş birliğini güçlendirmek için kurulmuş bir uluslararası polis örgütüdür. Üye ülkeler arasında suçla mücadele konusunda bilgi paylaşımı ve iş birliği yapılmaktadır. Küresel terörizmle mücadele etmek için birçok ülke arasında güvenlik iş birliği yapılmıştır. Bu iş birliği istihbarat paylaşımı, terörizme finansal destek sağlayan yapıların çökertilmesi ve terörist faaliyetlere karşı ortak operasyonlar gibi çeşitli şekillerde gerçekleşmektedir. Nükleer Silahların Yayılmasının Önlenmesi Anlaşması, nükleer silah sahibi olan ve olmayan ülkeler arasında nükleer silahların yayılmasının önlenmesini hedefleyen bir anlaşmadır. Anlaşma nükleer enerji kullanımının barışçıl amaçlarla sınırlanmasını ve nükleer silah sahibi olan ülkelerin silahlarını azaltmasını teşvik etmektedir. Verilmiş olan bu örnekler küresel güvenliği sağlamak ve tehditleri önlemek için uluslararası düzeyde yapılan iş birliğinin yalnızca birkaçını temsil etmektedir. Her ne kadar küresel güvenliği sağlamak adına bu tarz girişimler mevcut olsa da uluslararası sistemde güç dağılımından memnun olmayan ve hegemonyayı elde etme arzusu taşıyan devletler mevcut olabilmektedir. Bu amacı taşıyan bir devletin gücünü artırmak için girişimleri düşünüldüğünde bir mücadeleden de bahsetmek her zaman olağan olacaktır (Mearsheimer, 2001: 17).

Küresel güvenlik anlayışı ile birçok yapı birbirine bağlı düşünülmektedir. Bu yapılar çeşitli nedenlerle etkileşim içerisindedir. Bu etkileşim esnasında uluslararası örgütler, devletler ve hükümet dışı aktörler birbiriyle iletişim kurarken belirli tehditler ortaya çıkabilmektedir. Tehdidi en aza indirmek ya da ortadan kaldırıp güvenlikli bir ortam oluşturmak küresel güvenlik için gereklidir. Küresel ısınma, terör olayları ve salgın hastalıklar gibi tehditler mevcuttur. Ayrıca ticaret, sağlık ve teknoloji gibi alanlarda karşılıklı etkileşimler gerçekleşmektedir. Bu gibi ortak alanlar da küresel sorunları tüm devletler ve aktörler için ortak güvenlik tehdidi haline getirmektedir. Yakın bir geçmişte, 2020 yılında Covid-19 virüsü ile dünya küresel bir salgın ile yüzleşmiştir. Bu hastalık tüm insanlığı ilgilendiren küresel bir güvenlik tehdidi haline gelmiştir. Hastalığın çıkış noktasının araştırılmasından alınacak önlemlere ve keşfedilip uygulanacak tedaviye kadar devletler ve uluslararası yapılar bireysel çalışmalarının yanında ortaklaşa çalışmalar da sürdürmüşlerdir. Ortadaki tehdit küresel çapta geniş bir alanı tehlikeye sokmuş olduğu için devletlerin tek başına ilerlemesi mümkün olamayacak kadar zordu. Bu da devletlerin benzer ya da ortak tedbirler alarak ilerlemesini sağladı. Bu örnekten görüldüğü üzere küresel sorunların devletleri ortak çalışmalar yapmaya teşvik edici tarafları vardır. Bu sayede aktörler uluslararası güvenlik sorunlarını azaltmaya ve hatta mümkünse bitirmeye yönelik davranış sergileyebilmektedirler.

Dijital ortamda yaşanan gelişmeler küreselleşmenin en aktif olduğu durumlardan biridir. İnternet ortamında da küresel, dijital bir dünya vardır denebilir. Tıpkı bireylerin dünyada sahip olduğu fiziksel yaşam alanları olduğu gibi dijital ortamda da kişisel yaşam alanları bulunmaktadır. Kişisel banka hesapları, sosyal medya hesapları ve tüm kişisel verilerin toplamını insanların evlerine

benzetebiliriz. Sanal ortamda insanlar ortak bir alanda etkileşim halindedirler. Sosyal medya uygulamaları, oyunlar ve iş insanlarının gerçekleştirdiği çevrimiçi toplantılar gibi birçok ortamda bireyler ortak bir sanal ortam paylaşmaktadırlar. Dünya üzerinde var olan ortak alanlarda dikkat edilmesi gereken bir takım ahlaki değerler ve kurallar olduğu gibi dijital küresel dünyada da buna benzer bir düzen olması gereklidir. Özelden genele ilerlediğimiz noktada, gerçek dünyada uluslararası alanda etkileşim halinde olan devletler, ulus ötesi aktörler ve organizasyonlar dijital küresel dünyada da etkileşim halindedir. Bu etkileşim çevrimiçi ticaret gibi pozitif gelişmeleri yaratmakla birlikte siber casusluk faaliyetleri, siber saldırılar gibi negatif durumlar da oluşturabilmektedir. Bu noktada küreselleşme baz alındığında, uluslararası toplumun siber güvenlik konusunda iş birliği yapması gereklidir. Siber saldırılar ve tehditler giderek daha karmaşık hale gelmekte ve ciddi tehlikeler oluşturabilmektedir. Tehlikenin boyutu bizi siber savaş kavramına kadar götürebilmektedir. Devletler küreselleşme kavramı ile uluslararası alanda herkesi ilgilendiren konularla uğraşmaya teşvik edilmiştir. Bu noktada siber güvenliğin yeni ve sürekli gelişen bir alan olduğunu ve tehditlerin de değişim gösterdiği görülmektedir. Tarihte yaşanan olaylar neticesinde genel bir kanıyla varılan sonuca bakıldığında devletlerin işin sonunda iş birliği içerisinde bulundukları görülmektedir. Aslında siber alanda da yapılacak uygulamalar gerçek dünyanın paralel bir evreni olarak örnek alınabilir. Nitekim bu sayede yaşanabilecek tehditlere karşı alınacak önlemler önceden düzenlenebilir. Örnek verecek olursak çevre kirliliği konusunda birçok ülke çevresel sorunları ele almak ve sınırlar arası çevre kirliliğini kontrol etmek için uluslararası anlaşmalara katılmıştır. Aynı şekilde dijital küresel dünyada da siber tehlikelerin getirmiş olduğu ortak problemler için devletler bir araya gelebilir. Uluslararası iş birliği, normlar ve politikalar siber güvenlik tehditlerinin ele alınması için önemlidir.

Sonuç olarak *küresel güvenlik* için devletleri görünmez bir bağ ile birbirine bağlayabilme gücü olan bir kavram diyebiliriz. Yani küreselleşme devletleri ben merkezci düşünce yapısından çıkarıp tüm dünyayı ilgilendiren konularla uğraşmaya teşvik etmektedir. Bu bağlamda küreselleşmenin güvenlik üzerinde dönüştürücü bir etkisinin olduğunu söylemek mümkündür. Bu da aktörleri birlikte ortak kararlar almaya ve çözümler almaya itmektedir. Yani küresel güvenlik dünya genelinde barış, istikrar ve güvenliğin korunmasını hedefleyen bir kavramdır.

1.1.3. Uluslararası Güvenlik

Uluslararası güvenliğe kapsamı açısından bakıldığında uluslararası sistem içerisinde yer edinmiş olan devletin güvenliği bu alana dahil edilebilmektedir. Her devletin ilk etapta önceliği kendi ulusal güvenliğini sağlamaktır. Uluslararası alandaki tüm aktörlerin kendi güvenliklerini sağlamalarındaki yöntemleri ve birbirleri arasındaki ilişkileri uluslararası güvenliği genel anlamda değerlendirebilmek adına önem arz etmektedir. Uluslararası güvenliğin ele aldığı konular arasında gücün nasıl tespit edileceği, tehditlere nasıl direnilebileceği ve hatta zaman zaman gücün nasıl kullanılabileceği gibi hususlar yer almaktadır (Freedman, 1998). Uluslararası sistem dediğimizde

akla birçok aktör gelmekle birlikte güvenli ortamın sağlanabilmesi için her aktörün kendisini ve sistemi düşünür şekilde davranması gerekli olabilmektedir. Uluslararası sistemin genel anlamda güvenlikli bir ortam oluşturabilmesi için kimi zaman aktörler arasında bir iş birliği görülebilmektedir. Her aktör hem kendi ulusal çıkarlarını sağlayabilmek hem de uluslararası sistemi tehlikeye sokmamak adına eşit ve kontrollü stratejiler izleme konusunda dikkatli olursa genel anlamda güvenlikli ortam sağlanabilmektedir. Nitekim uluslararası güvenlik, savaş ve barışın kavramlarının en temel bağlamına işaret etmekte ve bu yönüyle devletlerin en yüksek sorumluluklarına atıfta bulunmaktadır (Freedman, 1998).

Uluslararası sistemde tam anlamıyla güvenli bir ortamın mevcut olduğunu söylemek mümkün değildir. Sistemin daha güçlü aktörlerine bakıldığında aralarındaki nükleer silah yarışı bunun en belirgin örneğidir. Yani uluslararası sistem yeteri kadar güvenli olsaydı devletler nükleer silah geliştirme konusunda bu denli çaba göstermezlerdi. Herhangi bir tehdit algısı oluşmadığı sürece devletlerin silah geliştirme anlamında çalışmalar yapamayacakları tahmin edilebilmektedir. Fakat devletler silahlanma anlamında gelişmeler yaptıkça kendi bünyesinde güvenli hale gelirken uluslararası alanda öteki aktörler için tehdit unsuru haline gelebilmektedirler. Bu durum uluslararası alanda güvenlik düzeyini dengesiz bir hale sokmaktadır, bunun dışında birçok duruma bağlı olarak güvenlik dengesi değişim göstermektedir. Güvenlik durumu devletler arasındaki ilişkilerin karmaşıklığı, siyasi çatışmalar, terörizm, silahlanma yarışı, siber saldırılar, doğal afetler, salgın hastalıklar, ticari problemler ve ekonomik kriz gibi bir dizi küresel etkenden dolayı dengesizlik göstermektedir. Mesela siber saldırıları ele alırsak bir devlet veya aktör diğer devletlerin siber altyapısına saldırarak uluslararası alanda ilişkilere zarar verebilmektedir. Bu durum diplomatik gerginliklere yol açmakla birlikte karşıt tepki alması sonucunda siber savaş boyutuna kadar ulaşabilir. Bu nedenlerle uluslararası alanda kusursuz bir güvenlik ortamı sağlamak zor ve karmaşık bir düşünce olacaktır. Tarih boyunca uluslararası alanda ülkelerin kendi çıkarları doğrultusunda politikalar izlemesi ve bazen çatışmalar yaşaması sık sık karşılaşılan bir durum olmuştur. Hala aralarında donmuş savaş bulunan ve krizin tırmanma seviyesine ulaşma ihtimali olan istikrarsız bölgeler/sınırlar mevcuttur. Bu noktada uluslararası güvenliğin sağlanması umulan ortamda devletler arası ilişkilerde, uluslararası kuruluşlar ve aktörler arasında barış, istikrar ve güvenliğin korunmuş olması ile mümkün olacaktır.

Genel olarak uluslararası güvenlik yaşanan tehditlere karşı koruma sağlamayı hedefler niteliktedir. Yani uluslararası güvenlik bir devletin veya topluluğun bütünlüğünü ve çıkarlarını korumayı, barışı sağlamayı ve çatışma çözümüne yönelik çabalarda bulunmayı amaçlayabilmektedir. Ayrıca, uluslararası ilişkilerde karşılıklı güveni artırmayı ve iş birliğini teşvik etmek hedefleri arasındadır. Immanuel Kant (1795) uluslararası alanda ebedi barışın sağlanabilmesi için hukuk ve kurallara vurgu yapmaktadır. Bu kurallara tüm devletler uyum sağladığında düzen oluşabilmektedir. Bilhassa uluslararası alanda güvenlik, sürekli olarak değerlendirilmesi gereken aktif bir konudur. Uluslararası toplum, iş birliği, diplomasinin güçlendirilmesi ve uluslararası hukukun uygulanması

yoluyla daha iyi bir güvenlik ortamı oluşturmak devletlerin ve aktörlerin çabalarıyla mümkündür. Çünkü hiçbir ulusal güvenlik çabası, güvensiz bir uluslararası ortamda kusursuz olamayacaktır.

1.1.4. Bölgesel Güvenlik

Uluslararası ilişkilerin en önemli konularından olan güvenlik kavramı ekseninde bölgesel güvenlik tartışmaları oldukça yoğundur. Uluslararası güvensizliği en belirgin şekilde yansıtan çatışmalar ve krizler neredeyse her zaman bölgesel parametrelerle açıklanır (Buzan, 1986: 3). Devletler özellikle kendi bölgelerinde güvenliği sağlamaya yönelik çalışmalar yapmaya öncelik vermektedirler. Bunun nedenlerinden biri bölgesel anlamda güvensizlik durumunda tehlike ve tehdit boyutunun diğer boyutlara oranla daha yoğun olmasıdır.

Birçok devlet kendi çevresinde komşu ülkelerle yakın ilişkiler kurup sınırlarını güvenlikli hale getirmektedir. Devletlerin kendi bölgelerinde, yakın sınırlarda bulunan ülkeler arasında da güvensizlik ortamıyla krizler tırmanabilmektedir. Terör olaylarının varlığı ve sınır anlaşmazlıkları gibi olası örnek tehditler güvensizlik durumunu oluşturabilmekte, ülkeler arasında yaşanan bölgede güvensizlik ortamı oluşturan benzer sorunların tamamen çözüme ulaşamadığı durumlar da olmaktadır. Genelde bu tip istikrarsız bölgelerdeki olumsuz gelişmeler donmuş savaş niteliğinde olup bazı dönemlerde krizler tırmanma seviyesine ulaşabilmektedir. Kimi zaman da bu krizler savaşa dönüşebilmektedir. Bunun en yakın örneğini Rusya Federasyonu (RF) - Ukrayna Krizi'nde görebiliriz.

Bölgeselcilik küreselleşmeye bir yanıt olarak doğmuştur. Buzan bölgeselleşmenin birey, devlet ve sistem analiz düzeylerine artı olarak eklenmesinin gerektiğini analiz etmiştir. (Buzan ve Hansen, 2009: 11-12). Bölgesel güvenlik genel anlamda belirli bir coğrafi bölgede yer alan devletlerin ulusal güvenliklerini tehdit eden potansiyel tehlikelerle başa çıkma amacıyla iş birliği yapmalarını ve güvenlik önlemleri almalarını kapsar nitelikte bir kavramdır. Bu durum iş birliğini öngörmekle birlikte, tam zıttı durumda ise aynı bölgede yaşayan devletler birbirlerine zarar da verebilmektedir. Mesela devletler kendi bölgelerinde bulunan rakip devletleri takip edebilmek ya da onun gizli bilgilerine erişim sağlayıp istihbarat toplayabilmek niyeti ile siber saldırılar düzenleyebilmektedirler. Aynı zamanda rakip devlete siber saldırılarda bulunup enerji altyapısı, iletişim sistemleri veya askeri kurumlar gibi kritik altyapıları hedefleyebilmektedirler. Bu sayede onu zayıflattıktan sonra askeri birliklerle gerçekleştireceği silahlı çatışmalarda avantajlı duruma geçebilmektedirler. Genellikle devleler bu gibi durumlarla karşılaşmamak için bölgesel güvenliği sağlamak adına komşu ülkeler ile iyi ilişkiler kurarlar. Tehlikelerle karşılaşabilme olasılığı göz önüne alınarak müttefikleri ile siber güvenlik tehditleriyle başa çıkmak için iş birliği içerisine girmektedirler. Bu iş birliği, bölgesel istikrarı artırmayı hedefler ve siber tehditlere karşı daha etkili bir savunma yapılabilmeyi sağlar.

Sonuç olarak bölgesel güvenlik genellikle benzer politik, sosyal, ekonomik veya güvenlik sorunlarına sahip olan devletler arasındaki bölgesel iş birliği ve koordinasyona işaret etmektedir. Bu bağlamda bölgesel güvenlik, devletlerin kendi güvenliklerini korumak ve bölgelerinde barış ve istikrarı sağlamak için bir araya gelmelerini gerektirir. Sınırları aşan tehditlere karşı ortak savunma stratejileri geliştirmeyi, istihbarat paylaşımını artırmayı, askeri tatbikatlar düzenlemeyi, terörizm, siber saldırılar, uyuşturucu kaçakçılığı gibi sorunlarla mücadele etmeyi veya siyasi krizleri çözmeyi içeren geniş bir boyuttan söz etmekteyiz. Böylelikle bölgesel güvenlik çabaları barışı ve istikrarı sağlama ve bölgesel kalkınmayı teşvik etme amacıyla bir araya gelen devletlerin ortak çıkarlarına hizmet etmeyi amaçlamaktadır.

1.1.5. Devlet Güvenliği

Devletlerin kendi sınırları içerisinde güvenli ve barışçıl bir ortam oluşturabilmeleri sonucunda ulusal güvenliklerini korumuş olmaktadırlar. Bunu sağlamak için çeşitli yapıları ve oluşumları bulunmaktadır. Örneğin polisler, hukuk kuralları ve çeşitli yaptırımlar iç güvenlik sağlama adına kullanılmaktadır. Genellikle iç güvenliği tehdit eden unsurların başında terör eylemleri gelmektedir. Bu noktada devletlerin askeri güçlerini artırması kaçınılmaz bir seçenektir. Aynı zamanda her devletin kendisine uygun şekilde güvenlik politikası bulunmaktadır.

Devlet bireyler arasında düzenin de korunmasını sağlamaktadır. Thomas Hobbes (2020)'a göre insan doğası gereği bencil ve kaotiktir. Bu durum subjektif güvenlik ile açıklanabilmektedir. Yani birey kendisini en yüksek düzeyde ne şekilde güvende hissediyorsa bu onun güvenlik algısını oluşturur. Doğa durumunda bireyler korku ve tehdit algısı ile yaşayabilmekteydiler. Devlet bireyleri doğal haline bırakmadan güvenliği sağlayıcı bir üst konumda olmaktadır. Bu durum devletin güç kullanmasına işaret etmektedir. Daha somut önlemler ile güvenlik sağlanabilmektedir. Bu da objektif güvenlikle açıklanabilmektedir. Bireylerin güvende kalması devletin gücü ve otoritesi ile sağlanabilmektedir. Bunu sağlamak adına devletler birçok önlem almaktadırlar.

Devletler güvenliği sağlayabilmek adına askeri güçlerini geliştirebilmektedirler. İzlanda gibi ordusu bulunmayan ülkelerin yanında Amerika Birleşik Devletleri (ABD), RF, Çin Halk Cumhuriyeti (ÇHC) gibi askeri yapılanmaları güçlü olup devamlı gelişmekte olan ülkeler de bulunmaktadır. Askeri sorunlar ile bir ülkenin bağımsızlığı, egemenliği ve toprak bütünlüğü tehlike altına girerse devlet güvenliği önem kazanır. Ordular, istihbarat birimleri ve sınır kontrolü gibi unsurlar dış tehditlere karşı ülkenin savunmasını sağlamak için kullanılmaktadır. Fakat buradan yola çıkarak devletlerin yalnızca askeri olarak güvenliğinin sağlanabileceği düşüncesine sahip olmak yanlış bir düşünce olacaktır. Çünkü devlet güvenliği yalnızca askeri güvenlikle sağlanamayacağı gibi güvenlik kavramının kapsamına dahil olan sağlık, ekonomik güvenlik, siber güvenlik, sosyal ve toplumsal güvenlik gibi alanlarda da gelişime önem verilmektedir. Örneğin her devlet için çok hassas bir konu olan sağlık hakkında devletler sağlık bilgilerinin güven altında tutulması için verilerinin

korunması gibi önlemler almaktadır. Bu önlemler alınırken personellerin eğitim görmesi, bilgilerin sızdırılması konusunda yaptırım hassasiyeti ve kişisel verilerin güvenli hale getirileceği sistemler kurabilmektedir. Bir hastanenin veri tabanına erişildiğinde ciddi maddi ve manevi kayıplar yaşanabilmesi mümkündür. Aynı zamanda bunu eczaneler için de söyleyebiliriz. Hayati tehlike taşıyan bir hastayı ele alacak olursak ve siber saldırı sonucunda sistemlerin kullanılamadığı bir saldırı yaşandığı düşünüldüğünde, rapor kontrolü yapılamadığında hastanın kullanmakta olduğu ilaca erişimi mümkün olamayabilir. Bu durumu birkaç saat ya da daha fazla bir zaman dilimine ve ülkenin geneline yaydığımız zaman kelebek etkisiyle sonuçları hayati kayıplara ulaşabilecek boyutta olabilir. Bu gibi durumlar yaşandığında saldırıya uğrayan devletin, saldırıyı yapan devlete karşılık vermesi ve siber çatışma yaşanabilmesi olasılığı vardır. Tüm bunların önlenmesi için devletlerin güvenliğini gerçekleştirebilmek adına siber stratejiler oluşturması önemlidir. Tüm bu konularda devlet güvenliği iç ve dış tehditlere karşı korunmayı hedeflemektedir. Nitekim devletler bu güvenliği sağlayabilmek adına geçmişten günümüze çeşitli önlemler almışlardır. Bu önlemler uluslararası birliklerde yer almak ve güvenlik anlaşmaları yapmak gibi örneklerden oluşmaktadır.

1.2. Güvenliğin Boyutları

Güvenlik kavramının çok yönlü ve geniş bir anlam taşıdığını bilmekteyiz. Her boyutun kendi içerisinde farklı risk durumları bulunmaktadır. Bu risklerin sürekli olarak engellenmesi ve her riskin aynı yöntemle çözülmesi mümkün değildir. Bu sebeple güvenlik kendi içinde farklı alanlarda değerlendirilmiş olup her alanın tehlikesi belirlenip o tehlikenin savunması ve güvenlikli bir ortamın oluşabilmesi ilgili konuyla örtüşen yöntemlerle saptanmıştır.

1.2.1. Ekonomik Boyut Açısından Güvenlik

Ekonomik güvenlik kavramı bir ülkenin veya bir bireyin ekonomik olarak istikrarlı ve sürdürülebilir bir durumda olması anlamına gelmektedir. Ekonomik güvenlik bünyesinde ekonomik kaynakların istikrarlı bir şekilde sağlanması, gelirin sürdürülebilir olması, işsizlik oranlarının düşük olması ve ekonomik dalgalanmaların etkilerinin minimize edilmesi gibi unsurları bulundurmaktadır. Bir ülkenin ekonomik güvenliği genel olarak istikrarlı bir ekonomik büyüme, düşük enflasyon, dengeli bir bütçe, dış ticaret açığına karşı dirençli bir yapı, yatırım ortamının güvenli oluşu, işgücü piyasasının sağlamlığı ve halkın ekonomik refah içerisinde yaşaması gibi faktörlere dayandırılabilmektedir. Ayrıca, bir ülkenin para biriminin değerini ve finansal sistemini koruma yeteneği de ekonomik güvenlik için önemlidir. Bu durumda ekonomik güvenlik bir ülkenin savunma kapasitesini doğrudan etkileyen unsurlardan biri olan ticaret ve yatırımla yakından ilişkilendirilmektedir. Ayrıca silah veya ilgili teknoloji tedariki, askeri teçhizatın güvenilirliği ve potansiyel rakiplerin silah teknolojilerindeki ilerlemeler gibi faktörler ekonomik güvenliğin temel bileşenleri olarak öne çıkabilir (Cable, 1995: 306).

Ekonomik güvenliği sağlayabilmek bir ülkenin veya bir bireyin ekonomik dalgalanmalara, krizlere ve belirsizliklere karşı dayanıklılığını artırmayı hedefler nitelikte tedbirler ile mümkün olmaktadır. İstikrarlı bir ekonomik güvenlik daha iyi yaşam standartları, daha fazla istihdam imkânı, yatırımların artması ve refahın artması gibi faydalar sağlamaktadır. Bu sayede toplum refah ve ekonomik özgürlük içerisinde olduğu için teknolojik, bireysel, bilimsel alanlarda daha rahat gelişim sağlar. Ekonomik olarak gelişmiş ülkeler kendi içlerinde toplumun refahını sağladığı gibi uluslararası alanda ekonomik iş birliği ve ulus aşırı ticaret faaliyetlerinde bulunarak küresel fayda sağlayabilmektedirler. Bu bağlamda günümüz koşullarına bakıldığında ekonomik güvenliği sağlamak için genel bir koşul olarak çatışmacı değil işbirlikçi bir yaklaşımın gerekliliği önemlidir (Cable, 1995).

Gelişen teknoloji ile uluslararası ortamda artış gösteren dijital ekonomik faaliyetler bünyesinde kaynakların daha etkin kullanılabilmesi ve bunu yaparken de iş birliğinin uygulanabilmesi ekonomik güvenlik sağlamaya destektir. E-ticaret konularında alınacak güvenlik önlemleri yaşanabilecek olumsuzlukları engellemektedir. Ticaret esnasında para akışının korunması açısından dolandırıcılık gibi tehlikelerin oluşmaması adına bir dizi önlem alınmaktadır. Son yıllarda neredeyse artık tüm ödemeler çevrimiçi koşullarda gerçekleşmektedir. Bu bireysel harcamalar olduğu gibi büyük şirketler, kurum ve kuruluşlar, devletler ve örgütler gibi aktörler arasında da gerçekleşmektedir. Bahsi geçen alışverişlerde çevrimiçi ödemeler kullanıldığında şifreleme gibi siber güvenlik önlemleri ile finansal önlemler alınmaktadır. Aynı zamanda paylaşılan verilerin korunması için kötü amaçlı fidye yazılımların engellenmesi gibi konularda iyi bir siber güvenlik stratejisi oluşturularak güvenlikli ortam sağlanabilmektedir. Bunu oluşturabilmek adına devletler bazı stratejiler geliştirerek kendi aralarında anlaşmalar yaparlar. Çünkü ticaret iki taraf için de aktif olan bir eylemdir ve sonuçları iki tarafa da zarar verir ya da fayda sağlar. Yani karşılıklı ve dengeli bir etkileşim söz konusudur. Sonuç olarak devletler kendi içlerinde ekonomik güvenliklerini sağlamaya yönelik çalışmalar yaparken dış ticaret ve diğer ülkeler ile etkileşim unsurlarında iş birliği ile güvenliğin sağlamasına katkıda bulunabilmektedirler.

1.2.2. Askeri Boyut Açısından Güvenlik

Askeri güvenlik uluslararası aktörlerin fiziksel ve stratejik olarak güvende olmasını sağlamak için alınan tedbirlerin bütünüdür. Belli başlı tedbirler sayesinde bir ülkenin sınırlarını, toprak bütünlüğünü, askeri birliklerini ve diğer önemli varlıklarını koruma amacı gerçekleştirilir. Dolayısıyla askeri gücün ülkelerin sürekli varlık göstermeleri ve gelişme olasılıkları üzerinde önemli bir etkisi vardır. Bu durum ülkelerin güvenliğini doğrudan şekillendirir ve askeri güvenlik, uluslararası politika araçları arasında en önemlilerinden biridir (Szpyra, 2014). Askeri güvenlik çeşitli unsurlar içerir ve genellikle askeri liderlik, askeri istihbarat, stratejik planlama, askeri operasyonlar, lojistik, iletişim, siber güvenlik ve fiziksel güvenlik önlemleri gibi alanlarda faaliyet gösteren bir dizi uzmanlık alanını bünyesinde barındırır.

Devletler askeri güvenlikte hem iç hem de dış tehditlere karşı savunma yapmayı amaçlarlar. İç tehditler denilince akla ülke içindeki ayaklanmalar, terör eylemleri veya iç düzensizlikler gibi faktörler gelebiliyorken, dış tehditler genellikle diğer ülkelerden kaynaklanan askeri saldırılar, siber saldırılar, istihbarat faaliyetleri veya terör örgütleri tarafından gerçekleştirilen saldırılar ve tehditlerdir. Modern savunma sistemleri düşünüldüğünde iç ve dış güvenlikte siber güvenliğin sağlanması önemlidir. Siber saldırıların zaman ve mekân tanımaksızın gerçekleştirilebiliyor oluşu devletlerin siber güvenlik açısından almaları gereken önlemlerin sıkı olmasının gerekliliğini göstermektedir. Uluslararası güvenlikte ise devletin dış ülkelerden bünyesine gelen siber tarzda tüm tehlikeleri kapsar.

Günümüz teknolojik sistemleri düşünüldüğünde bir devletin askeri sistemine düzenlenebilecek herhangi bir saldırı onu ciddi şekilde yavaşlatabilmektedir. Bu bağlamda askeri birimler, siber saldırılara karşı savunma stratejileri geliştirerek askeri altyapılarını koruma altına alabilmektedirler. Birçok ülke siber savunma stratejisi içerisinde, siber tehditlere karşı erken uyarı sistemleri oluşturmuş ve siber saldırılara karşı savunma ekipleri kurmuşlardır. Askeri personellere bu konuda eğitim vermek alınan bir diğer tedbir yöntemidir. Bilgisayar virüsleri ve fidye yazılımları gibi siber tehditlere karşı nasıl korunacakları konusunda bilgili olmaları birçok tehdide karşı gelebilme konusunda faydalıdır. Ayrıca askeri birliklerin her birinde siber güvenlik birimlerinin olması kaçınılmazdır. Siber güvenlik ve askeri güvenlik günümüz dünyasındaki güvenlik tehditleriyle mücadele etmek için birbirinden bağımsız düşünülemez durumdadır. Her iki alanda da temel amaç bir devletin güvenliği ve ulusal çıkarlarını korumaktır.

Askeri güvenliği amaçlayan her ülke için bu alanın politikaları ve stratejileri, ülkelerin askeri kuvvetlerinin yeteneklerini, silahlanma programlarını, askeri eğitim ve personel eğitimlerini, istihbarat toplama ve analiz faaliyetlerini ve savunma hedeflerini belirlemektedir. Bunlar gerçekleştirilirken ülkelerin savunma yeteneklerini artırmak, potansiyel tehditleri azaltmak ve barışı korumak için çeşitli askeri doktrinler oluşturulmaktadır. Nitekim askeri güvenlik, sivil toplumu ve devleti korumak için önemli bir role sahiptir. Ayrıca bir ülkenin askeri güvenliği genellikle ordunun yanı sıra polis, gümrük ve sınır güvenliği birimleri, istihbarat teşkilatları ve diğer ilgili kurumların birlikte çalışmasıyla sağlanmaktadır. Yani askeri güvenlik, bir devletin veya bir askeri örgütün sahip olduğu koruma ve savunma önlemlerinin geniş bir yelpazesini kapsamaktadır.

1.2.3. Toplumsal Boyut Açısından Güvenlik

Bir bireyin veya toplumun sosyal yaşamında hissettiği güvenlik oldukça kapsamlıdır. Kimi zaman toplumsal anlamda güvensizlik ortamları oluşabilmektedir. Toplumsal güvensizlikler, bir toplumun kimliğinin hedef alındığını ve tehlikede olduğunu hissettiği zamanlarda meydana gelir. İnsanların kimlikleri ve devletin ideolojisi uyuşmadığında insanlar kendilerini savunmak için tepki verebilirler (Saleh, 2010: 240). Devletin buradaki sorumluluğu olası tehditleri ortadan kaldırmak ya

da en aza indirgemektir. Yani toplumsal güvenliği oluşturmak, insanların güvende hissetmelerini sağlayan çeşitli faktörleri içermekte ve insanların sağlık, ekonomik refah, adalet, eşitlik ve toplumsal istikrar gibi temel ihtiyaçlarını karşılamaya yönelik koruma ve destek sağlamayı hedeflemektedir. Bu nedenle, hükümetler, kuruluşlar ve diğer aktörler toplumsal güvenliği sağlamak için politika ve önlemler geliştirmektedirler. Aynı zamanda bu kavram bir bireyin veya topluluğun, toplumsal, ekonomik ve siyasal yaşamının korunması ve geliştirilmesiyle ilgilenmektedir.

Devletler için askeri güvenlik konuları gibi toplumsal güvenlik konuları da önemlidir. Yani ulusal güvenlik boyutu yalnızca askeri değil aynı zamanda toplumsal boyutlarla da ele alınmaktadır. Dış faktörler ve iç faktörler bu güvenlik konusunda büyük rol oynamaktadır ve askeri konular güvenliğin yalnızca bir parçası olarak görülmektedir (Buzan vd., 1983: 253). Toplumsal güvenlik boyutunda bireylerin fiziksel, sosyal ve ekonomik güvenliğinin sağlanmasına yönelik bir dizi önlem çeşidi vardır. Bunlar arasında barınma, gıda, sağlık, eğitim, iş imkanları ve sosyal hizmetler gibi temel ihtiyaçların karşılanması; suçla mücadele, terörle mücadele, sınır güvenliği, siber güvenlik ve ulusal savunma gibi güvenlik konularının ele alınması yer almaktadır. Bir toplum kendisini refah içerisinde ve güvende hissediyorsa aynı düzeyde devlet de doğru stratejileri uyguluyor demektir.

İç güvenlikte suçlarla mücadele konusunda bir dizi önlem alınmaktadır. Suçluların yargılandığı mahkemelerde uygulanan hukuk kuralları ve yaptırımlar vardır. Tüm bunlar toplumun huzurunu kaçırmak isteyen bir dizi insan ve grup için çoğu zaman caydırıcı olabilmektedir. Bu sayede toplum kendisini huzurlu hissedebilecektir. Yani sosyal güvenlik sağlandığında toplumun refaha ulaşması kolaylaşmaktadır.

Toplumun genel bir bölümü artık dijital ortamda aktif şekilde yer almaktadır. Geçiminin tümünü oradan sağlayan insanlar, yatırımcılar, oyun oynayan çocuklar, çeşitli platformlarda ekonomik amaç hedefleyerek paylaşım yapan gençler ve yaşlılar, sadece hobi olarak o ortama erişim sağlayan birçok insan bulunmaktadır. Tüm bunlar toplumun bir parçasıdır. Tıpkı iç güvenlikte asayişi sağlayan yaptırımlar ve güvenlik önlemleri olduğu gibi siber alanda da toplumun refahını ve huzurunu sağlamak onları güvende hissettirmek adına siber güvenlik stratejileri her devletin uygulaması gerekli olan stratejiler haline gelmiştir. Bunu denetlemek adına kullanım noktalarının tek bir alanda birleştirilmesi çözüm yöntemlerinden biridir.

Toplumsal bazda düşünüldüğünde, sokakta rahatsız edilen küçük bir çocuğu ele alacak olursak bu konuya müdahale edecek birçok unsur vardır. Çocuğun güvenliğinin sağlanması için sosyal kurumlar dahil güvenlikle ilgilenen diğer kurumlar devreye girecektir. Aynı şekilde çocuğun bilgisayar ortamında oyun oynarken rahatsız edildiği durumlar da mevcuttur. Siber zorba olarak adlandırabileceğimiz saldırganlar çocuğa erişim sağlayıp psikolojik şiddet de dahil olmak üzere ona fiziksel anlamda da ulaşıp zarar verebilmektedirler. Kimi uygulamalar yaş sınırı koymak, şifreler, ebeveyn kilidi gibi önlemler sunsa da bunlar her zaman yeterli olmayabilmektedir. Tüm bunlara

rağmen siber istikrarsızlık hızla devam etmektedir. Devletlerin bu noktada alabileceği önlemler konusunda tıpkı iç güvenlikteki polisler, güvenlikçiler, bekçiler olduğu gibi sanal dünyada da gözlemleyici ve müdahale edici unsurlar eklenebilir. Jeremy Bentham (2008)'ın tasarlamış olduğu Panoptikon hapishane örneği ele alındığında, gözetlenen kişilerin kurallara daha uygun yaşadığı tespit edilmiştir. Bu sanal ortamda da uygulanabilir bir yöntemdir. Çoğu zaman tehlikenin kimden geldiğinin bile tespitinin oldukça zor olduğu bir güvenlik tehdidinde, devlet o kişiyi göremediği ve kimliğini tespit edemediği halde, o kişiye henüz ele geçirilmeden olası yaptırımların uygulanmış olduğu hissini yaşatabilmektedir. Nitekim bu durum tehlikenin en aza indirilmesini sağlayabilir. Böylelikle toplum sanal ortamda da kendisini güvende hissedecektir.

Siber alanda yaşanabilecek tehlikeleri en aza indirgemek için oluşturulacak önlemlerden biri de eğitimdir. Her ne kadar bir dizi caydırıcı önlem oluşturulsa da temelde bireyleri harekete geçiren bilinç en önemli faktörlerden biridir. Sigmund Freud (2000)'un kitlesel psikoloji düşüncesine göre bireyler toplumsal normlara uyum sağlamak için davranışlarını içgüdüsel olarak değiştirebilmektedirler. Bu bağlamda toplum bilincini oluşturmada belli başlı normları öğretmek etkili bir yöntemdir. Siber alanda okullarda verilen eğitim sayesinde yetişen bilinçli toplum dijital ortamda ne şekilde hareket etmesi gerektiği konusunda en doğru kararları alacaktır. Eğitimli ve gelişmiş bir toplumda yetişen bireylerin zorbalık, terör ve tehdit gibi eylemlere yatkınlığı yoğun derecede azalacaktır. Sanal dünyada yaşanan birçok sosyal sorunun önüne geçilmesinde temel çözüm yöntemi eğitimdir.

Devletlerin toplumsal güvenliği sağlayabildiği durumlarda toplumsal kalkınma ve refah artışı yaşanmaktadır. Bireylerin güvende hissetmeleri, toplumda istikrarın sağlanmasına yardımcı olur niteliktedir. Ayrıca böyle bir durumda ülkelerin ulusal güvenliği büyük ölçüde sağlanacaktır. Anlaşıldığı üzere toplumsal güvenliği geliştirmede en büyük rol devlete düşmektedir. Çünkü herhangi bir toplumsal sorun yaşandığında devletin güvenliği de tehlikeye girecektir.

1.3. Uluslararası İlişkiler Teorilerinde Güvenlik Olgusu

Uluslararası ilişkilerde güvenlik geçmişten günümüze her dönemde önemli bir konu olmuştur. Bu bağlamda güvenlik hakkında birçok görüş ortaya atılmıştır. İdealist düşünceye göre risklerin en aza indirilmesi için toplumun birlikte hareket etmesi inşa edilmelidir. Realist düşünce ise merkeze devleti alarak güvenliği sağlayan temel unsurun güç olduğunu savunan bir görüşe sahiptir. Liberaller bunun aksine insanı temel alarak insan doğasının barışa eğilimli olduğunu varsayar. Devletler için karşılıklı iş birliği ticaret gibi unsurların barışı getirici ve güveni sağlayıcı olduğu fikrini benimser. Uluslararası ilişkiler bağlamında birçok teori güvenliği farklı şekilde yorumlamış olsa bile her biri özünde güvenliğin olmazsa olmaz bir unsur olduğu benimsemiştir. Ayrıca devletler ve bireyler için önemini göz ardı etmemişlerdir.

1.3.1. Realizm

Realizm, güvenlik de dahil olmak üzere birçok konuyu ele alan bir düşüncedir. Devletlerin temel aktörler olduğunu savunur ve uluslararası ilişkilerde güç ve çıkarlar üzerine odaklanır. Güvenlik açısından realizm, devletlerin güvenliklerini sağlama ve koruma çabalarını vurgular. Güç, korku ve anarşiye odaklanan realist teori için çatışma ve savaş konularında merkezi bir öneme sahip olduğunu söylemek mümkündür (Williams, 2008: 15). Realizm devletlerin uluslararası sistemdeki diğer aktörlerle rekabet içinde olduğunu ve güvenliklerini tehdit eden potansiyel risklere karşı savunma tedbirleri alması gerektiğini savunur. Yani realist düşünceye göre daha fazla güç arzusu insanlığın kusurlu doğasından kaynaklandığından, devletler sürekli olarak güçlerini artırma mücadelesi içindedirler (Williams, 2008: 17).

Devletlerin kendi aralarında savaş içerisinde olmaları normaldir ve bu durum doğanın yasasıdır (Karabulut ve Değer, 2015: 74). Bu teorik yaklaşıma göre uluslararası sistemde güvenlik, devletlerin kendi güç ve kaynaklarını kullanarak sağladığı bir durumdur. Realizm, devletlerin güvenliklerini sağlama çabalarını vurguladığı için güvenlik açıklarını azaltmak adına güçlü bir devlet olmanın önemini de vurgulamaktadır. Yani devletler arasında güvenliği sağlamak için güç dengesini korumak ve diğer devletlerin potansiyel saldırgan eğilimlerini engellemek için caydırıcı önlemler kullanmak önemlidir. Bu önlemler çoğu zaman askeri sistemlerin geliştirilmesi, nükleer silahlar konusunda caydırıcı yöntemler ve silah teknolojilerinin geliştirilmesi gibi hususlar olmakla birlikte özellikle Soğuk Savaş sonrası dönemde gelişen sanal ortamın yaygınlığı ile siber güvenlik önlemleri de alınmıştır.

Uluslararası arenada birçok devletin kendi siber güvenlik stratejileri bulunmaktadır. Her ne kadar realizme devletlerin iş birliği yapması konusunda yetersiz olabileceği şeklinde eleştiriler gelse de realizm farklı bir bakış açısı ile özellikle siber güvenlik alanına uygun olabilmektedir. İnternetin insanlığa sağladığı olanaklar onu artık bireylerin yaşamlarının bir parçası haline getirmiştir. Bu değişim ile devletler, şirketler, kurumlar, kuruluşlar ve bireyler kişisel verilerini sanal dünya ile paylaşmaya başlamıştır. Bu noktada karşımıza yeni bir tehdit boyutu olarak siber tehditler çıkmıştır. Siber tehditlerden korunmak için siber güvenliğin sağlanması önem arz etmektedir. Kişisel verilerin korunması, ticaret, devlet sırlarının açığa çıkmasının engellenmesi ve devletlerin güvenlik duvarlarının korunması gibi güvenlik teşkil eden durumlar açısından siber güvenlik çok önemlidir. Siber saldırıların zaman ve mekân tanımaksızın gerçekleştirilebiliyor oluşu devletlerin siber güvenlik açısından almaları gereken önlemlerin sıkı olmasının gerekliliğini göstermektedir. Siber güvenliğin realist düşünce yapısı ile bağdaştırıldığı noktada, siber alanda en önemli güvenlik konularından biri de kişisel verilerin korunmasıdır. Bunu devlet nezdinde düşünecek olursak her devletin kendisine özel verileri bulunmaktadır. Bu verilere gelebilecek herhangi bir tehdit unsuru ciddi kayıplara ve güç zayıflığına neden olabilir. Her devlet kendi kişisel çıkarını düşünür şekilde siber güvenlik stratejileri

uygulamaktadır. Bu ülkelerin gelişmişlik düzeyine ve alana yapabileceği yatırıma göre değişebilmektedir.

1.3.2. İngiliz Okulu

İngiliz Okulu II. Dünya Savaşı sonrası dönemde İngiltere'de ortaya çıkan bir uluslararası ilişkiler kuramıdır. İngiliz Okulu'nun temsilcilerinin 4 ayrı gruba ayırabiliriz (Arpalier, 2018). Birinci grupta Martin Wight, Hedley Bull, Adam Watson, John Vincent ve Alan Johnson bulunmaktadır. İkinci grupta, kuram içindeki tartışmalara direkt katkıda bulunan isimler olarak Tim Dunne, David Long, Andrew Hurrell, Nicholas Wheeler, Hidemi Suganami ve Peter Wilson vardır. Üçüncü grup ise diğer gruplar gibi İngiliz Okulu'na ve uluslararası toplum kavramına katkıda bulunmuş olmalarına rağmen diğer gruplardan bağımsız hareket etmiş isimleri içermektedir. Bu grup içinde Robert Jackson, Andrew Linklater ve Ian Clark gibi isimler bulunmaktadır. 1990'lı yıllara geldiğimizde İngiliz Okulu söylemini yeniden ele alan başta Barry Buzan ve Richard Little gibi birçok düşünür bulunmaktadır. Bu isimleri dördüncü grup olarak adlandırabiliriz (Arı, 2013: 512).

İngiliz Okulu için genel anlamda odaklandığı konular uluslararası toplum ve bu toplumdaki düzen ve devletler sistemi diyebiliriz. Bu kurama göre uluslararası toplum hem çatışma hem de iş birliği barındıran bir düzendir. İngiliz Okulu düşüncesinin temelini ortaya koyan ve en iyi şekilde ifade eden terim uluslararası toplumdur (Metkin, 2016: 240). Nitekim uluslararası toplum denildiğinde akla anarşi olgusu gelebilmektedir. Bu bağlamda İngiliz Okulu kuramı anarşik toplum içinde düzen kavramının önemli olduğunu vurgulamakla birlikte düzenin sadece güç ve güç dengesinin getirisi olarak değil, buna ek olarak devletlerin ve öteki aktörlerin kendi rasyonel çıkarları ile kuralları ve kurumsal düzenlemeleri kabul etmeleriyle oluşmuştur (Metkin, 2016). Temel anlamda İngiliz Okulu için ortaya attığı düşüncelere bakıldığında bunları dört argümanda birleştirebiliriz. İlk olarak, uluslararası ilişkilerin ilk sıradaki aktörleri egemen devletlerdir yani ulus-devletler veya şehir devletleridir. İkincisi, uluslararası ilişkiler sisteminde devletler arasındaki bağlantılar vardır. Üçüncüsü, uluslararası arenanın anarşikliği ile ilgilidir. Son olarak bu sistemde devletler varlıklarını iletişimlerine düzen sağlayan bir dizi ortak yasa ve iş birliği ile yönetilen organizasyonların kurduğu bir uluslararası toplumda sağlamaktadırlar (Devlen ve Özdamar, 2010: 48). Bu bağlamda asıl odak noktası toplum olan İngiliz Okulu için güvenlik ilgi çekici bir konu olmuştur. Klasik İngiliz Okulu yaklaşımı uluslararası ilişkileri uluslararası sistem, uluslararası toplum ve dünya toplumu olmak üzere üç bileşen olarak görerek bu unsurlar arasındaki sürekli etkileşime dayanmakta ve uluslararası ilişkilerin doğası bu unsurlar arasındaki dengeye bağlı görülmektedir. Temelde bu durum İngiliz Okulu ile uluslararası güvenlik çalışmaları arasında bir köprü oluşturur diyebiliriz. Özellikle İngiliz Okulu'nun gerçekçilik unsurunun aracılığıyla bu köprü oluşmaktadır. Ancak uygulamada İngiliz Okulu çalışmalarının büyük bir kısmı uluslararası toplum ve dünya toplumu ile ilgili konulara ve uluslararası toplumun sosyal düzenini destekleyen kurallar ve kurumlara odaklanmıştır. Çok az

İngiliz Okulu üyesi uluslararası güvenlik çalışmaları gündemini açıkça ele almış ve sonuç olarak güvenlik kavramı İngiliz Okulu düşüncesinde sınırlı bir rol oynamıştır (Cavelty ve Mauer, 2010: 34).

İngiliz Okulu güvenlik kavramını uluslararası ilişkilerde çeşitli boyutlarıyla ele alan ve analiz eden bir yaklaşım sunabilmektedir. Çünkü toplum ile ilgilenen İngiliz Okulu düşünüldüğünde sosyal sorunlarıyla da ilgileneceği düşünülebilmektedir. Toplum düşünüldüğünde ekonomik, politik, sosyal ve çevresel faktörlerin güvenliği etkileyen önemli unsurlar olduğu akla gelmektedir. Örneğin, ekonomik istikrarsızlık, çevresel sorunlar, siyasi çatışmalar ve insan hakları ihlalleri gibi faktörler güvenliği etkileyebilir ve bu konular uluslararası ilişkilerde önemli bir rol oynamaktadır. Yani İngiliz Okulu ile güvenlik alanı düşünüldüğünde güvenliğin sadece devletlerin değil aynı zamanda bireylerin, toplumların ve grupların da güvende hissetmelerini içermesi gerektiğini vurgulayabiliriz. Bu bağlamda İngiliz Okulu için güvenlik kavramını geniş bir perspektifle ele alır ve askeri tehditlerin ötesinde ekonomik, politik, çevresel ve sosyal boyutları dahil eder diyebiliriz. Bu yaklaşım ile uluslararası ilişkilerde güvenlik politikalarının ve stratejilerinin daha kapsamlı ve sürdürülebilir bir şekilde ele alınması teşvik edilmektedir.

1.3.3. Liberal Teori

Liberal teori, uluslararası ilişkiler alanında bir yaklaşımdır. Liberalizmin en belirgin niteliklerinden biri, insan aklının daha müreffeh, hür ve uzlaşmacı bir dünyayı destekleyeceği inanışıdır (Keohane, 2002: 45). Bu teori için öncelikli konular şunlardır (Pektaş, 2016: 129-130);

- Devletler ve devlet dışı uluslararası aktörler dünya siyasetinde önemli oluşumlardır.
- Devletler, uluslararası aktörler, devlet dışı oluşumlar arasında karşılıklı bağımlılık vardır.
- Uluslararası sistemde siyasi konular, askeri konularla sınırlandırılamayacak kadar geniştir.
- Devlet-toplum ve birey baz alındığında içeriden dışarıya doğru bir etki analizi görülmektedir.
- Uluslararası ortamda uzlaşmacı bir ortam söz konusu değilse karşılıklı barışın nasıl sağlanacağı konusunda çözümler üretilmelidir.

Liberalizme göre siyasi konular ve bu bağlamda güvenlik sadece askeri güç ve ulusal savunma ile sınırlı bir alan değildir. Aksine, liberal teoriye göre güvenlik daha geniş bir perspektifte ele alınmalıdır ve içerisine insanların refahını ve özgürlüğünü koruma çabalarını da eklemelidir. Anlaşıldığı üzere bu teoriye göre güvenlik, demokratikleşme, ekonomik refah, insan hakları, hukukun üstünlüğü ve uluslararası iş birliği gibi faktörlerin bir araya gelmesiyle sağlanmaktadır. Aynı zamanda liberal düşünce devletler arasındaki iş birliğini ve bağları güçlendirmeyi hedefler. Bu bağlamda liberal düşüncede güvenlik askeri oluşumların yanı sıra bir devletin diğer konularda da güvende olması, içeride demokratik kurumlarının olması, insan haklarını koruması ve hukukun üstünlüğünü sağlaması gibi unsurlara da bağlıdır. Bireylerin haklarına, özgürlüklerine ve özel

mülkiyetlerine vurgu yapan liberal düşünce siber güvenlik alanına da entegre edilir. Kişisel verilerin korunması her birey için doğal bir haktır. Ayrıca devletler bu alanda güvenliği sağlarken müdahalelerini kısıtlı tutmalıdırlar. Bireylerin özgürlüklerine eşitlik ilkelerine zarar vermeyecek şekilde bunu sağlamalıdırlar. Yani siber alandaki etik ilkeler liberal değerlere uygunluk açısından değerlendirildiğinde olumlu sonuç doğurur.

Liberalizm devletler arasında iş birliğini öngören bir düşüncedir. Ticari ilişkileri olan ve birbirleri ile etkileşim halinde bulunan devletleri düşünebiliriz. Ekonomik açıdan ciddi zararlara uğramamak için aralarında herhangi bir kriz ortamı oluşturmak istemezler. Ekonomik konular söz konusu olduğunda liberalizm serbest ticaretin ve küresel ekonomik entegrasyonun güvenlik açısından da önemli olduğunu savunur. İktisadi bağlar, devletler arasında birbirlerine bağımlılık oluşturur ve bu çatışma riskini en aza indirir. Ticaret yoluyla ekonomik büyüme ve refah artışı, devletler arasında barışın ve istikrarın sağlanmasına katkıda bulunur. Ayrıca liberal teoriye göre demokratikleşme ve insan haklarına saygı, uluslararası güvenliği artırabilen unsurlar arasındadır.

Özetle liberal teoriye göre güvenlik, askeri güç, silahsızlanma ve ulusal savunmanın ötesinde, demokratikleşme, ekonomik refah, insan hakları, hukukun üstünlüğü ve uluslararası iş birliği gibi faktörlerin bir araya gelmesiyle de sağlanabilmektedir. Devletlerin birbirleriyle iş birliği yapması, ortak çıkarları ve değerleri paylaşması, çatışma riskini azaltır ve barışı teşvik eden unsurlardır. Demokratik ülkeler halkın düşüncelerine önem verir. Gelişmiş ve demokratik ülkelerde yaşayan bireyler savaşın olası sonuçlarının bilincinde olduğu için genellikle bunu tercih etmezler. Kant'a göre savaşın ilan edilip edilmemesi konusunda karar vermek için vatandaşların onayı gereklidir, bu sebepten ötürü böylesine riskli bir teşebbüse adım atmakta bireyler ciddi şekilde kuşku yaşayan bir düzeydir. Çünkü bu karar onlara savaşın verebileceği bütün faciaları davet etmek manasına gelir (Reiss, 1970). Yani liberal düşüncede barışçıl ortam için, demokrasinin çatışmayı en aza indirdiği, uluslararası kurumların çatışmaları azalttığı ve karşılıklı bağımlılığın çatışmaları azalttığı düşüncesi vardır (Cavelty ve Mauer, 2010: 30).

Bireysel anlamda düşünüldüğünde liberalizm bireylerin hür iradeleri ile eşitlikçi yaşamalarının en doğal hakları olduğunu savunur. Bu noktada liberalizmin kurucusu olarak kabul edilen John Locke'un düşünceleri oldukça önemlidir. Locke (1690)'a göre;

> Politik gücü doğru anlamak ve onu kaynağından türetmek için, insanların doğal olarak bulunduğu durumu düşünmemiz gerekmektedir. İşte bu durum, eylemlerini düzenleme ve mülklerini ve bedenlerini istedikleri gibi kullanma özgürlüğü içinde oldukları mükemmel bir özgürlük durumudur. Bu durum, doğanın yasasının sınırları içinde, başka bir insanın iznini istemeden veya başka bir insanın isteğine bağlı olmadan gerçekleşir. Aynı zamanda, herkesin gücünün ve yargılama yetkisinin karşılıklı olduğu bir eşitlik durumudur; hiç kimsenin diğerinden daha fazla yetkisi yoktur. Aynı tür ve düzeyde yaratıkların doğaya aynı avantajlarla ve aynı yeteneklerin kullanımıyla doğduğu daha açık bir şey yoktur. Bu nedenle, birbirlerine hiyerarşi veya bağlılık olmaksızın eşit olmalıdırlar.

Sonuç olarak liberal teori uluslararası ilişkilerde iş birliğini vurgulamaktadır. Bu teori özellikle devletlerin ortak çıkarları göz önüne alınıp, çatışmalardan kaçınılıp barışçıl çözüm yöntemlerine yönelmeyi savunmaktadır.

1.3.4. Eleştirel Teori

Karl Marx düşünürlerin dünyayı değiştirebilmesi için arayışlarından vazgeçmeden dünyayı anlamalarını savunur. Bu aforizması ile onun eleştirel teorinin kökenini oluşturduğu yorumunu yapabiliriz (Cavelty ve Mauer, 2010: 45). Eleştirel teori düşünürleri genelde hangi bilgi araştırılacaksa araştırılsın bunun özgür şekilde yapılmasını benimserler. Yani özgürlük onlar için çok önemlidir ve özgürlüğün güç ile ilişkisini de tartışma konusu olarak ele alırlar. Bu görüş özellikle Frankfurt Okulu akademisyenlerinin odak noktası olmuştur. İlgilendikleri bir diğer konu ise bilgi ve kazançlar arasındaki ilişkidir. Bu noktada eleştirel teori düşünürleri, birçok akademisyenin sahiplendiği düşüncenin aynı zamanda kendi doktrinlerine uygun olduğu kanısındadır. Yani ortaya atılan düşüncelerin objektif olması konusu tartışılır bir durumdur. Görüldüğü üzere bu kuramdaki düşünürlerin niyeti, arka plandaki güçleri ve diğer simgeleri ortaya çıkarmaktır (Yılmaz, 2016: 330-333).

Ancak eleştirel teori yalnızca sosyal teori, felsefe veya sosyal bilimlerin bir alt alanı olarak değil, aynı zamanda toplumsal gerçekliği daha kapsamlı bir şekilde anlama ve toplumsal patolojileri teşhis etme amacı taşıyan daha geniş bir yöntemi öneren özgün bir teoridir. Bu yaklaşım, önceden belirlenmiş ahlaki veya siyasi değerleri ileri sürmek yerine bireysel ve toplumsal yaşamın bütününü ve bunları oluşturan toplumsal süreçleri kavrama yeteneği ile karakterizedir. Eleştirel teori bir yargılama, değerlendirme ve pratik, dönüştürücü faaliyetin tohumlarını içeren bir toplumsal eleştiri biçimidir (Thompson, 2017: 1-2). Eleştirel teoriler dünyanın geçmişte veya uzak yerlerde temelde daha iyi olduğu önermesini reddeder. Bunun yerine, şimdiki zamanın temel sosyal örgütlenmesinde değişiklikler yapmaya çalışırlar, böylece gelecekteki sosyal örgütlenme, şu anda dünyanın işleyişi tarafından ezilenleri özgürleştirir.

Eleştirel teori güvenlik konusunda ise alternatif bir bakış açısı sunar. Bu teoriye göre, bir şey oluşturulmadan harcanamaz. Aynı şekilde güvenlik oluşturulmadan önce problemin kaynağına ulaşmak gereklidir. Yani Galler Ekolü ve Frankfurt Okulu'nun güvenlik yöntemleri uluslararası güvensizlik durumunun asıl kaynağını irdeleyerek daimî ve pragmatik sonuçlara ulaşma çabası şeklindedir (Birdişli, 2010: 234). Güvenlik tehditlerinin temel noktasındaki sorun bulunursa daha kolay çözüme gidilebilir düşüncesi mevcuttur. Güvenlik sorunlarının kaynağına odaklanmak, eleştirel güvenlik çalışmalarının temel bir ilkesidir. Yani sorunların temeli düşünüldüğünde geleneksel gerçekçi veya liberal yaklaşımlardan farklı olarak eleştirel teori güvenlik kavramını politik, toplumsal ve ekonomik yapıların bir sonucu olarak ele alır diyebiliriz. Eleştirel teoriye göre

güvenlik sadece askeri tehditlerden veya devletler arasındaki ilişkilerden ibaret değildir, aynı zamanda güç ilişkileri, toplumsal eşitsizlikler ve küresel ekonomik yapılarla da ilişkilidir. Eleştirel teori güvenliğin sosyal olarak inşa edildiğini ve sürekli olarak yeniden tanımlandığını savunmaktadır.

Modern güvenlik sorunlarını ele alacak olursak eleştirel güvenlik, siber güvenlik alanını daha geniş bir perspektifte ele almamıza olanak sağlayabilir. Genel anlamda siber güvenlik dijital ortamdaki asayişi ve düzeni sağlamak için gereklidir. Bunu yaparken de bilgi sistemlerini ve dijital unsurları koruma altına almayı hedefler. Siber saldırılar düşünüldüğünde kimden ve nereden geldiği zor bulunmakla birlikte günümüzde bu saldırıları düzenleyen birçok devlet, siber casuslar, hacker toplulukları gibi aktörler bulunmaktadır. Eleştirel güvenlik, bu noktada siber saldırıların ardında yatan nedenleri ve saldırganların sosyal veya politik amaçlarını anlamaya çalışır. Bu sayede siber güvenlik konularını yalnızca teknik açıdan değil, aynı zamanda sosyal ve politik açıdan da değerlendirir.

1.4. Zaman Sürecinde Güvenlik: Kavramın Genişlemesi

Güvenlik kavramı tarih boyunca farklı şekillerde analiz edilmiş ve tanımlanmıştır. İnsanların güvenliğini sağlama ihtiyacı, insanlık tarihinin en eski dönemlerine kadar uzanmaktadır. Bireyler için öncelikli amaç ise çeşitli tehlikelerden korunma, toplum içinde huzur ve düzenin sağlanması gibi güvenlik önlemlerini içermektedir. Güvenlik bu doğrultuda zaman içerisinde gelişmiş ve toplumların ihtiyaçlarına ve yaşam koşullarına bağlı olarak farklı anlamlar kazanmıştır.

1.4.1. Tarihsel Açıdan Güvenlik Kavramının Analizi

Güvenliğin dönemsel olarak aşamaları incelendiğinde insanlığın henüz gelişmediği eski çağlar *Primitif Dönem* olarak adlandırılmıştır. Bahsi geçen çağ kendi içerisinde *Pre-Teolojik* ve *Proto-Teolojik* dönemler şeklinde iki farklı kısma bölünmüştür. *Pre–Teolojik* olarak adlandırılan zaman diliminde yaşayan insanlar, güvenliklerini sağlama açısından koruma ve savunma duygusu geliştirmişlerdir. Kendi oluşturdukları grupların dışındakilerle iş birliği haline gidilmiş olsa bile bu bağ çok ince kalmıştır. *Proto-Teolojik* zaman diliminde ise güvenlik olgusu biraz daha gelişmiş ve genişlemiştir. Din siyasi olguları açıklamada bir araç haline gelmiştir (Birdişli, 2020: 239). 1600'lü yıllara gelmeden önceki dönemde insanlık önce kendisini sonra da devleti geliştirici bir süreç yaşamıştır.

İnsanların ve oluşumların güvenlik algısı en başından beri temel ihtiyaçları olmuştur. 1648-1990 yıllarını kapsayan *Modern/Sistemik Güvenlik Dönemi* içerisinde yaşanan gelişmeler ile devletlerin dini müdahaleyi sınırlamaya ilişkin kabul gören anlaşmaları sonucunda güvenlik başka bir boyuta taşınmıştır. Dinin siyasi olguları açıklayan bir yapı olarak görüldüğü dönemlerden ziyade dinin getirmiş olduğu ayrım sebebiyle oluşan güvensizlik ortamını, toplumun ön plana alındığı yeni

bir sistemle güncellemişlerdir. Sonrasında yaşanan gelişmeler ile güvenlik kavramı genişlemiş ve 1990 sonrasında yeni güvenlik alanları dahil edilmiştir. Bu dönem ise *Postmodern Güvenlik Dönemi* olarak adlandırılmaktadır (Birdişli, 2020: 243-246).

Antik çağlarda güvenlik genellikle dış tehditlerden korunma amacıyla sınırların savunulması ve askeri güç kullanımını içermekteydi. Antik Roma İmparatorluğu'nda sınırların güvence altına alınması ve güvenliğin sağlanması için bir dizi askeri savunma önlemi alınmıştır. Benzer şekilde Çin Seddi'nin inşası Çin'in tarihi boyunca dış tehditlere karşı güvenliği sağlama amacıyla gerçekleştirilmiştir. Orta Çağ'da feodal sistemde güvenlik, derebeylerin ve soyluların sahip olduğu şatolar ve kalelerin savunulması etrafında odaklanmıştır. Feodal lordlar, topraklarını korumak ve güvende tutmak için surlar, hendekler ve diğer savunma yapıları inşa etmişlerdir.

17. yüzyıla gelindiğinde 1648 Vestfalya Anlaşması, modern ulus devlet sisteminin dinamiklerinde değişime yol açmıştır. Vestfalya terimi genellikle eşit ve egemen devletler sisteminin bir özeti olarak kullanılır, aynı zamanda Vestfalya Barış Antlaşmaları'nın modern egemen devlet kavramının temelini attığı ifade edilir (Straumann, 2008). Bu anlaşma ile Otuz Yıl Savaşları sona ermiş ve Avrupada siyasi düzeni yeniden şekillendirilmiştir. Devletlerin iç işlerinde dini müdahaleyi sınırlaması ciddi değişimlere yol açmıştır. Böylelikle iç işlerinde bağımsız olan devletler dini konularda ayrı görüşlerin getirmiş olduğu çatışma ortamından uzaklaşıp uluslararası düzeyde güvence altına alınmıştır (Gross, 1942: 22). Ulusal güvenlik konularında daha fazla yetkiye sahip olan devletler kendi güvenlik politikalarını belirleme açısından gelişme sağlamıştır. Modern devlet sisteminin temeli oluşturulmuş ve güvenlik açısından dönüşümler yaşanmıştır.

Nitekim 19. yüzyılın başlarına gelindiğinde 1815 Viyana Kongresi ile denge politikasının ilk örnekleri yaşanmıştır. Uluslararası arenada güç unsurları arasında dengeli bir siyasi ortam kurmak güvenlik sağlama bağlamında önemli bir unsurdur. Güç dengesi kavramına bakıldığında bir veya daha fazla devletin gücünün bir diğer devletin mevcut gücünü dengelemek amacıyla kullanılmasını ifade etmektedir. Bilakis güç dengesi, anarşik özelliğe sahip uluslararası sistemde bir şekilde frenleme yöntemidir. Bu da güvenlikli ve istikrarlı bir uluslararası sistemi oluşturabilmeye destekleyici bir unsurdur (Goldstein ve Pevehouse, 2013-2014: 52). Aynı şekilde 1919 yılında I. Dünya Savaşı ardından kurulan Milletler Cemiyeti barışçıl ve güvenlikli bir uluslararası ortamda iş birliği ile desteklenen uluslararası örgüt olmuştur. Bu dönemde yaygınlaşan liberalist düşünceye göre iş birliğini destekleyen olgulardan biri yeteri sayıda uluslararası kurumun bulunmasıdır. İnsanın doğası itibariyle iyi ve saldırganlığı kontrol edebilir olduğu düşüncesine sahip olan liberallerin ana varsayımları ise savaşın kaçınılmaz olmadığı ve anarşik koşulların azaltılması durumunda iş birliği potansiyelinin daha da artabileceği yönündedir (Clackson, 2011: 2). Bu sayede uluslararası ortamda aktörler arasında dengeli ve güvenlikli bir ortam oluşabilmektedir. Ortak çıkarların varlığı aktörleri iş birliği yapma konusunda teşvik etmekte ve aynı zamanda savaşın yıkıcı etkileri düşünüldüğünde aktörler hem ulusal hem de uluslararası güvenliklerini sağlayabilme amacı ile bu yönteme

başvurabilmektedirler. Bunu II. Dünya Savaşı sonrasında 1945 yılında kurulmuş olan ve ana fikri uluslararası ortamda güvenliği ve barışı korumak olan BM örgütünde de görebiliriz.

Nitekim, uluslararası ortamda savaşların getirmiş olduğu yıkıcı etkiler ve güvensizlik ortamı devletleri iş birliği yapma yoluna itmiştir. Bu sayede dağılan parçalar toparlanmış ve aktörler tekrardan güvenlikli bir ortamın oluşmasında etkili olmuşlardır. Fakat iş birliğine dahil olmayan ülkelerin üzerindeki etkisi tartışma konusu olabilmektedir. İki ya da daha fazla devlet aynı fikirdeyseler iş birliğine gidebilmektedirler. Bunların dışında görüşleri farklı olan diğer aktörlerin çatışma olasılığı düşünüldüğünde iş birliğinin kalıcı çözüm olduğu konusu realist teorisyenler için eleştiri konusu olmuştur (Clackson, 2011: 2).

Modern anlamda güvenlik kavramı yaşanan gelişmelerin beraberinde, 20. yüzyılda önemli ölçüde değişime uğramıştır. Soğuk Savaş döneminde güvenlik kavramı genellikle iki süper güç arasındaki askeri tehditleri ve nükleer savaş tehlikesini ifade etmekteydi. Bir yanda 1949 yılında kurulmuş olan NATO tarafı öte yandan 1955 yılında kurulmuş olan Varşova Paktı tarafları arasında yaşanan çekişmeler ile uluslararası ortamda güvensizlik ortamı oluşmuştur. Bu dönemde iki büyük güç arasında yaşanan gelişmelerde aktörler birbirlerinin verilerine sızarak istihbarat toplamaya çalışmışlardır. Siber alanda gelişmelerin başladığı bu dönemde uluslararası sistemdeki karar vericiler alanla ilgili çalışmalar başlatmışlardır. ABD'nin güvenlik çalışmaları siber güvenlik alanında ilklere imza atmıştır. ABD 1983 yılı Eylül ayında ilk siber güvenlik patentini yani RSA (Rivest-Shamir-Adleman) algoritmasını takdim etmiştir (Kaplan, 2020). Bu sistem verileri güvence altına almak için şifreleme yöntemi kullanmaktadır (Aryanti ve Mekongga, 2018). Yani dijital güvenlik alanında önemli fayda sağlamaktadır. Bu gibi çalışmaları yoğunlaştıran devletler ve yaygınlaşan bilgisayar kullanımı ile siber alanda yaşanan gelişmeler, sonraki süreçte güvenlik bağlamında önemli değişimlere yol açmıştır.

Süper güç çatışmasının sona ermesi ve küreselleşmenin uluslararası politikadaki öneminin giderek daha fazla anlaşılması, 20. yüzyılın sonlarından itibaren uluslararası sistemde önemli bir dönüşüme yol açmıştır. Devletlerin ulusal anlamda güvenliği sağlamaları için başvurdukları askeri güç, eskisine oranla daha az talep görmeye başlamıştır (Baldwin, 2011: 26). 1990 sonrası dönemde uluslararası ilişkilerde güvenlik, askeri tehditlerin yanı sıra ekonomik, siyasi ve sosyal tehditleri de içerecek şekilde genişlemiştir. Bu değişim, devletler arası ilişkilerde daha çok iş birliği, çok taraflılık ve ekonomik entegrasyonun vurgulanmasıyla karakterizedir. Artık güvenlik sadece askeri tehditleri değil terörizm, siber saldırılar, iklim değişikliği, enerji güvenliği, gıda güvenliği, sağlık güvenliği gibi birçok farklı alanı kapsamaktadır.

1.4.2. 11 Eylül 2001 Sonrası Temel Dinamiklerde Değişim

Güvenliğin gelişmesindeki olaylardan biri de 2001 yılında yaşanan 11 Eylül saldırılarıdır. Bu saldırılar küresel güvenliği derinden etkileyen gelişmelere yol açmıştır. Öyle ki, George W. Bush, 11 Eylül terör saldırılarının sonrasında yapmış olduğu Ulusa Sesleniş konuşmasında, Amerikan ulusunun tarih boyunca karşılaştığı hiçbir tehdide benzemeyen bir döneme giriş yaptığını ilan etmiştir. Bir diğer seslenişinde ise Bush, teröre karşı küresel savaşın sadece ABD'nin ulusal güvenliğini değil, aynı zamanda medeniyetin güvenliğini sağlama çabası olduğunu vurgulamıştır (İnaç ve Aktaş, 2013: 5). "Bu savaş dünyanın savaşı, bu medeniyetin savaşı…" ifadeleriyle, ABD'nin kendi sınırlarının ötesinde, dış politikasında küresel bir düzeyde güvenliği tesis etmeye çalıştığını belirtmiştir (Paker, 2012: 18).

11 Eylül 2001 tarihindeki saldırılar, ABD'de ve dünya genelinde güvenlik anlayışını derinden etkilemiştir. Bu saldırılar sonrasında birçok ülke ve uluslararası kuruluş güvenlik önlemlerini artırmış ve değiştirmiştir. Terörle mücadele konusunda devletler ulusal güvenlik yatırımlarını artırmışlardır. Hava sahasındaki güvenlik unsuru öncelikli olarak gündeme gelmiştir. Çünkü 11 Eylül saldırıları, uçakların teröristler tarafından kullanılmasıyla gerçekleşmiştir. Birçok ülkede havalimanlarında daha sıkı güvenlik kontrolleri uygulanmaya başlanmış, yolcuların ve bagajların daha kapsamlı bir şekilde aranması sağlanmıştır. X-ray cihazları, metal dedektörleri ve patlayıcı tespit sistemleri gibi teknolojiler gelişmeye başlamıştır. Ayrıca uçak kokpitlerine güvenlik önlemleri eklenmiş ve pilotların uçak içindeki güvenlik durumunu daha iyi kontrol etmesine olanak sağlayan önlemler alınmıştır. İleride yaşanabilecek olası terör saldırılarında uçaklara patlayıcı veya başka maddelerin getirilip getirilmeyeceği ve uçuş sırasında yaşanabilecek herhangi bir terör eylemine karşı önlemler gündeme gelmiştir (Birkland, 2004: 191).

11 Eylül saldırıları sonrası tartışılan konulardan biri istihbarat paylaşımıdır. Devletlerin güvenlik tehditleriyle ilgili istihbarat elde etmelerini sağlamak amacıyla kurulan yapılar ve süreçlere ilişkin endişeler oluşmuştur (Gill, 2006: 27). Ulusal istihbarat teşkilatları arasında daha etkili bir istihbarat paylaşımı sağlanması için çeşitli adımlar atılmıştır. ABD diğer ülkelerle daha sıkı iş birliği yapmaya başlamış ve terörizmle mücadelede bilgi akışını artırmıştır. Bununla birlikte terör saldırılarını önleme ve terör örgütlerine karşı daha etkili mücadele sağlamayı hedeflemektedir. Ayrıca bir takım yasal düzenlemeler yapılmıştır. ABD, Patriot Act olarak bilinen yasa ile terörle mücadele amacıyla daha geniş yetkilerin verilmesini sağlamıştır (Domke vd., 2007: 299). Bu yasa istihbarat toplama ve soruşturma yetkilerini genişletmiş, telekomünikasyon ve finans sektöründeki faaliyetleri daha sıkı bir şekilde denetlemeyi amaçlamıştır. Benzer şekilde diğer ülkeler de güvenlikle ilgili yasal düzenlemeler yapmış ve terörle mücadelede daha etkili olmayı hedeflemişlerdir. En önemli konulardan biri olan sınır güvenliği konusu da tekrar gündeme gelmiştir. Sınır ihlalinin gerçekleştiği bu saldırıda devletler ulusal güvenlikleri konusunda daha fazla yatırım yapma düşüncesine gitmişlerdir.

Devletlerin ulusal güvenlik mekanizmalarını güçlendirirken odaklandıkları bir diğer husus da siber güvenlik olmuştur. Terörle mücadele daha geniş bir çerçevede ele alınıyor olsa bile siber güvenlik bir devletin savunma sistemini güçlendirebilir. Kritik altyapılar ve iletişim ağlarına yönelik güvenlik önlemleri sayesinde dijital savunma yöntemleri geliştirmişlerdir. Mesela ABD'nin kritik altyapısına yönelik artan tehditlere karşı daha etkili bir iç güvenlik stratejisi oluşturmak ve bu stratejiyi desteklemek amacıyla istihbarat toplama ve analiz kapasitesini artırmaya yönelik çalışmalar için hedefler belirlenmiştir (DNI, 2005: 5). Siber altyapılara yönelik gelişmiş güvenlik yöntemleri sayesinde istihbaratın sorunsuz yapılması sağlanabilmektedir. 11 Eylül 2001 sonrası devletler ulusal güvenliklerini geliştirirken siber güvenlik alanına da yatırımlar yapmışlardır. Bu olayın öncesinde siber uzayın riskleri, güvenlik problemleri sadece kısıtlı sayıda uzmanlar arasında konuşuluyordu. Fakat saldırının gerçekleşmiş olduğu tarihten sonra, toplumlar arasında artan bağlı durum ile siber alanın önemli ölçüde tehditler barındırdığı da görülmüş oldu (Theiler, 2011).

İKİNCİ BÖLÜM

2. SİBER GÜVENLİK KAVRAMININ ULUSLARARASI POLİTİKA PERSPEKTİFİNDEN ANALİZİ

Siber güvenlik uluslararası politika bağlamında büyük bir öneme sahiptir çünkü modern toplumların ve devletlerin birçok faaliyeti dijital ortamda gerçekleşmektedir. Aynı zamanda devletlerin güvenliği, ekonomisi, ilişkileri ve insan hakları gibi konular siber alanla doğrudan ilişkili hale gelmiştir. Bu da politika yapıcıları siber güvenlik kavramıyla yakından ilgilenmeye yönlendirmiştir.

2.1. Siber Güvenlik Kavramının Analizi

Siber güvenlik kavramı gelişen küresel dünya sisteminde önemli boyutları olan bir değerdedir. Onu önemli kılan birçok faktör vardır. 1990 sonrası artan bilgisayar kullanımı ile birçok yapı dijital ortamda birbiriyle etkileşim haline girmiştir. Bireylerin kişisel verileri internet ortamıyla paylaşılmış, şahsi sosyal medya hesapları kullanımı artmış ve internet üzerinden iş kurmak gibi faaliyetleri oluşmuştur. Bankalar, hastaneler ve devlet kurumları verilerini dijital ortama geçirmişlerdir. Devletler ve uluslararası örgütler diplomatik ilişki kurmak, istihbarat toplamak, bilgi alışverişi yapmak, çevrimiçi görüşmeler ve projeler oluşturmak için interneti yoğun şekilde kullanmaya başlamışlardır.

Dijital ortam belirli nedenlerle birtakım faaliyetleri daha kolay ve hızlı uygulayabilme açısından avantaj sağlamıştır. 1990 sonrası gelişen dünya düzeyinde siber alanın sağlamış olduğu imkanlar, onun kullanım aktifliğini sürekli artan ve geniş bir alana yayılan şekilde etkilemiştir. 2019 yılında başlayan ve 2020 yılında yayılım gösteren Covid-19 salgını bireyleri sosyal mesafeyi koruyacak bir yaşantı uygulamak zorunda bırakmıştır. Birçok ülkede eğitim internet üzerinden verilmiştir. Şirketler, kurum ve kuruluşlar toplantılarını ve görüşmelerini çevrimiçi gerçekleştirmişlerdir. İnternetin getirmiş olduğu olanaklar olağanüstü durumlarda bile ilerleyişin ve düzenin aksamaması için başvurulan yardımcı bir yapı olmuştur.

Siber alanda yaşanan gelişmelerin tehlike boyutları bulunmaktadır. Virüsler, kötü amaçlı yazılımlar, siber taciz suçları, hacker faaliyetleri ile bireyler, devletler, uluslararası örgütler, kurum ve kuruluşlar tehlike altındadır. Siber ortamdaki kullanım alanlarının zayıf noktaları tespit edildiğinde saldırganların, saldırı düzenlenme imkânı bulunmaktadır. Saldırganların bunu

yapmasında birçok neden vardır. Ekonomik sebepler, dolandırıcılık, bir devletten başka bir devlete zarar verme güdüsü, iç güvenlikte devlet verilerine düzenlenen siber saldırılar, bireysel açıdan psikolojik sorunlar gibi sebepler bulunmaktadır. Kimliğin kolayca anonimleştirilebildiği ve saldırının gizlenebildiği siber ortamda, kötü niyetli aktörler hedeflerine çok daha kolay şekilde ulaşmaktadırlar. Bu durum siber güvenlik tehditlerini oldukça karmaşık hale getirmektedir. Sınırlar kolayca aşılabilir olduğu için küresel sistemlerin devletlere ve bireylere yönelik tehditlere erişimi kolaylaştırdığı gözlemlenmektedir (Aksu ve Turhan, 2012: 71).

İnternet ortamında bulunan her aktör için siber güvenlik gerekli bir olgudur. Bireylerin kişisel verilerinin ve devletlerin kritik altyapılarının korunması gibi konularda çeşitli çalışmalar yapılmıştır. Ülkeler kendi siber güvenlik stratejilerini oluşturmuş ve uygulamaya koymuşlardır. Siber güvenliğin önemi sürekli değişen ve gelişen bir olgu olmasının farkındalığı ile, devletler zaman içerisinde siber güvenlik stratejilerini geliştirmekte ve genişletmektedirler. Aynı şekilde örgütler, kurum ve kuruluşlar, şirketler de kendi siber güvenlik sistemlerini kurmuşlardır. Bu, şifreleme gibi siber yazılımlarla yapılırken aynı zamanda siber güvenlik uzmanları ile kontrol altında tutularak uygulanmıştır. Siber alanın geniş olması uygulanabilecek siber güvenlik önlemlerinin de geniş olması ile paraleldir. Bireylere düzenlenen siber tehdit yöntemleri ve devletlere düzenlenen siber tehditler birbirlerinden çok farklıdır. Siber savunma oluşturulurken asıl önemli olan saldırganın tespitidir. Saldırganların tespitinin yapılması çok güçtür bu yüzden kesin sonuçlara ulaşılabilme ihtimali düşmektedir (Güntay, 2017).

Siber güvenliğin artan güvenlik sorunları ile yaşanabilecek tehlikeli durumların çözümündeki katkısı belirgindir. Bireysel düzeyde ya da devlet düzeyinde alınabilecek tüm siber önlemleri kapsar niteliktedir. Gelişen teknoloji ve yaygınlaşan internet kullanımı ile siber güvenlik çalışmaları yoğunlaşmış ve alana yapılan yatırımlar artmıştır. Uluslararası ilişkiler bağlamında devletler ve bireyler nezdinde siber alanda yapılan çalışmalar çoğalmıştır. Bu çalışmalar siber güvenliğin ne olduğunu anlamakta, konuyu analiz etmekte ışık olmuştur. Nitekim bu sayede toplum bilinci artmakta ve eğitim ile siber güvenliğe katkı sağlanmaktadır.

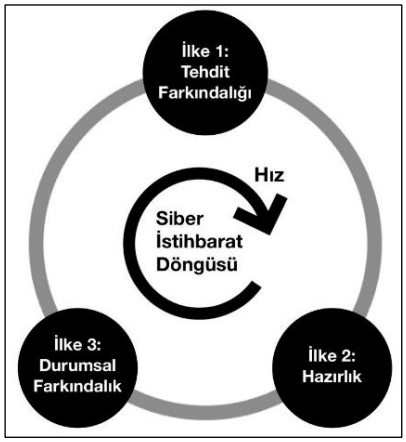
2.1.1. Siber Güvenlik Nedir?

Siber güvenlik yoğunlaşan internet kullanımı ile gelinen bilgi çağında dijital güvenlik kilidini açmakta anahtar görevini üstlenmektedir. Günümüzde teknoloji kullanımının hızla artması ve bilgisayarların insan yaşamının çeşitli alanlarını etkilemesiyle birlikte, bu alandaki tehlikeler de artmaktadır. Siber boyut içerisine birçok alanı dahil etmektedir. Bu da saldırganlar için dijital ortamı cazip kılmaktadır. Elbette ki tehditlere karşı alınabilecek önlemler de mevcuttur. Örneğin şifreleme yöntemi, güvenlik için oluşturulan yazılımlar, siber güvenlik uzmanları, siber güvenlik stratejileri savunma anlamında kullanılan siber savunma yöntemleridir. Dijital ortamda bulunan bütün sistemleri korumak siber güvenliğin alanına dahildir.

İnternet erişimin kısıtlanması, bilgilerin izinsiz kullanılması ve çalınması, kişisel verilerin kötü amaçlı elde edilmesi, devlet verilerine sızmaya çalışan terör tehlikeleri gibi kötü niyetli girişimler siber tehditlere örnektir. Bunlar dışında siber saldırılar fiziksel zarar verebilecek boyutlara ulaşabilmektedirler. Bu tarz saldırılar karmaşıktır ve tehlike boyutu oldukça büyüktür. Ayrıca siber alanda faillerin tespiti ve bu faillerin belirli devletlere hizmet edip etmediğinin açıkça belirlenebilmesi genellikle oldukça karmaşık bir süreçtir. Saldırgan taraf olaya dahil olmadığını rahatça ifade edebilmektedir (Cavelty M. D., 2015: 406). Nitekim siber güvenlik küresel çapta önemi olan bir konudur ve ulus devletler için birinci derece güvenlik sorunlarına dahil edilmiştir (Walters ve Novak, 2021: 1). Devlet yöneticileri siber güvenlik konularına söylemlerinde yer vermişlerdir. Birçok devletin kendi siber güvenlik stratejisi vardır. Alınan önlemlerin çeşitliliği günden güne artmaktadır. Ülkeler kendi bünyelerinde siber alanda eğitimler vermekte ve okullarda ders olarak anlatılmaktadır. Bunun dışında ülkelerin kendi siber güvenlik uzmanları ve tehlikeleri engelleyecek caydırıcı yöntemleri bulunmaktadır.

Dijital ortamda yaşanan tehlikelerin günden güne artması ve kimi zaman kontrol dışına çıkması devletler ve bireyler için siber güvenlik sorunu teşkil etmektedir. Devletler siber savunma sistemlerine ciddi yatırımlar yapmaktadırlar. Fakat bu alanda alınan bütün önlemlere rağmen hala güvenlik zayıflıklarının olduğu görülmektedir. Net bir sonuca ulaşabilmek için sorunların neler olduğunun tespiti önemlidir. Sorun tespitlerinden sonra çözüm üretmek kolaylaşacaktır. Siber güvenliğin tam olarak istenilen boyuta ulaşamamasının önünde dört unsur yatmaktadır. Bunlardan ilki, güvenlik konusunda karar alınırken sezgilere dayanarak önyargılı sonuçlara varılabilme durumudur. İkincisi, aktörlerin güvenlik önlemleri aldıktan sonra uygulama aşamasından hedeflenen başarıyı yakalayamamalarıdır. Üçüncüsü, virüs tarayıcıları gibi savunma yöntemleri, genellikle statik tehdit bilgisine aşırı güven duyar, ancak bu durum dinamik öğrenme ve uyum sağlama konusunda yetersiz kalmaya neden olmaktadır. Dördüncü husus ise güvenliği yönetmekte yaşanan boşlukların güvenlik açığı oluşturmasıdır (Julisch, 2013: 2207).

Şekil 1: Siber İstihbarat, Tehditleri Anlama ve Hazırlık Prensipleri



Kaynak: Julisch, 2013

Siber istihbarat erken uyarı sistemleri sayesinde olası tehlikelere karşı önlem alıp tehditlerin engellenmesini sağlayabilir. Siber güvenliği sağlamak adına en önemli ön adımlardan biri siber istihbarattır. Bu sayede saldırılar engellenebilir veya hasar en aza indirilebilir. Daha etkili bir savunma için bilgi toplanarak tehditlerin kim tarafından geldiği saptanabilir. Elde bulunan kaynakların etkin şekilde kullanımı ile potansiyel tehditlere hazırlık yapılabilir.

Siber saldırılar enerji tesisleri, iletişim ağları, ekonomik kurumları ve diğer kritik altyapıları hedef alabilmektedirler. Kritik altyapıların korunması geniş bir alana tekabül etmekle birlikte siber güvenliği sağlama açısından devletlerin üstüne düştükleri bir konudur. Şirketler ile hükümet arasında iş birliği sayesinde bu alanda yapılacak güvenlik çalışmaları daha başarılı olabilmektedir. Kritik altyapılar hem devleti hem de özel sektörü yakından ilgilendiren bir alandır (Cavelty M. D., 2015: 413). Ayrıca kritik altyapıların korunması için yeteri kadar bütçe ayırmaya ihtiyaç vardır. Bu sayede olası siber tehditlere karşı ileri teknolojik siber güvenlik önlemleri alınabilecektir.

Siber güvenlik önlemleri sayesinde olası tehditler engellenebilir ya da hasar en aza indirilebilir. Siber saldırıların karmaşık yapısı alınacak önlemleri zorlaştırsa bile gerekli yatırım ve çalışmalar ile savunma sistemleri kurulabilir. Tüm bunlara ek olarak dijital ortamda aktif olan bireylerin bilincinin geliştirilmesi önemlidir. Kritik altyapılarda çalışan bireyler, kurum ve kuruluş çalışanları ve sanal ortamda aktif olan her kullanıcının eğitim alması gerekli bir önlemdir. Bu sayede bireyler kendilerini nasıl koruyacaklarını öğrenebilir. Ayrıca olası bi saldırı durumunda sonuçların ne kadar yıkıcı olduğunun farkındalığı toplum için suç oranını düşürme açısından faydalı olacaktır.

Siber alanın yoğunlaşması ile birlikte güvenlik konularında adını sıklıkla geçiren siber alanın korunma düşüncesi, siber güvenlik olarak karşımıza çıkmaktadır. Tehlikelerin boyutları düşünüldüğünde siber güvenliğin önemi daha iyi anlaşılmaktadır. Siber tehditler finans, psikoloji, sağlık, eğitim ve kimi zaman fiziksel boyutlara ulaşabilecek düzeyde tehlike arz etmektedir. Tüm bunların kontrollü ve güvenli şekilde normal akışında düzenli boyutta ilerleyebilmesi için siber asayişin sağlanması bireyler ve devletler için gereklidir. Ulusal boyutta alınacak devlet önlemleri her devletin kendi siber güvenlik stratejisi ile planlanıp uygulanmaktadır. Bireysel düzeyde bilinçli kullanıcılar, güvenlik önlemlerine uyumlu davrandıklarında kendilerini savunma konusunda ve dünyayı tehlikeye sokmama konusunda etkili olacaktır. Siber güvenlik politikaları, dijital dünyada güvenli bir ortamın oluşturulmasına katkıda bulunmaktadır.

2.1.2. Siber Alan Kavramı

Alan kelimesi birlikte kullanıldığı kavrama göre geniş bir perspektife sahiptir. Siber kavramı, sibernetik kelimesinden gelmektedir. Sibernetik ise ilk defa Norbert Wiener'in "Cybernetics or Control and Communication in the Animal and the Machine" adlı kitabı ile duyurulmuştur. Kimi kaynaklar kavramın çok daha önce Ampere tarafından ve hatta daha da önce Platon ve Aristo

tarafından kullanıldığını belirtmektedir (Andrew, 2009: 1). Kelime kökeni olarak "kybernetes" teriminden gelmiştir. Bu terim yunanca bir terimdir ve dümendeki denetimi açıklar nitelikte kullanılmaktadır. Fransız bilim adamı Ampere ise tüm bilgilerin genel sınıflandırmasında, hükümeti tanımlamak için sibernetik terimini kullanmayı tercih etmiştir (Beer, 2002: 213). Siber kavramı genel anlamda sanal ortamda bulunan tüm dijital sistemlerle ilgilidir. Siber alan ise, dijital ortamda bulunan teknoloji, internet, yazılımlar gibi bütün uygulamaların aktifleştiği alanı ifade edebilmektedir.

Dijital çağda aktif internet kullanımı ile siber alana olan ilgi hem akademisyenlerin araştırma konusu haline gelmekte hem de bireylerin ve devletlerin üzerinde çalıştığı bir konu olmaktadır. Sürekli gelişerek ilerleyen sanal alan birçok konuyu kapsamaktadır. Dijital ortamların bünyesindeki tüm sistemler bu alana dahildir. Bu alanda fiziksel boyutlarda olmasa bile birçok eksende hem pozitif hem de negatif sonuçlar doğurabilmektedir. Etki alanı küresel çapta olup, bütün dünyayı ilgilendiren konuları barındırmaktadır. Bu sayede siber alanın sınır ötesi etkileri olmaktadır.

Uluslararası ilişkilerde siber alanın; siber güvenlik, siber çatışma, siber terörizm, siber caydırıcılık gibi siyasi boyutları bulunmaktadır. Küresel çapta var olan her aktör dijital konularda bilgi paylaşımı, ticaret, verilerin korunması gibi konularda etkileşim halindedir. Liberalizmin iş birliği odaklı yaklaşımı ile sanal alanda var olan konularda barışçıl bir süreklilik ele alınmaktadır. Bu bağlamda devletler ve diğer aktörler, uluslararası normlar ve anlaşmalar ile etik bir internet kullanımı sağlama konusunda çalışma içindedir.

Siber alanda güvenlik bağlamında iş birliği oluşturabilmek için birtakım unsurlar bulunmaktadır. İlk adım aktörlerin hangi konuda tehlikede olduklarını belirtmeleridir. Sonraki adımda tehdidin öteki aktörler tarafından da onaylanması gelir. Son adımda ise tehdit onaylandıktan sonra güvenliği sağlamak için gerekli politikalar oluşturulmaktadır. Siber güvenlik söz konusu olduğunda, siber alanın da çeşitliliği göz önüne alındığında tehdit algısı ve tehdidin boyutları aktörler tarafından farklı algılanabilmektedir. Tablo 1'de detaylı olarak görüldüğü üzere RF, ÇHC ve ABD'de siber güvenlik tehdidi algıları farklılık gösterebilmektedir.

Tablo 1: Siber Tehditlerin Ölçümünde Ortak Paydalar

İşbirliğine yönelik araçlar	Ortak alanlar			Tehditler ve tartışmalı konular
	RF	ÇHC	ABD	
				Uluslararası hukuku ihlal eden BİT kullanımı-toprak bütünlüğü ve egemenlik
				Siber uzayın askerileşmesi
				Politik siber casusluk
Tanımlanması gereken				Terör amaçlı BİT kullanımı
Soruşturma ve kanun uygulamasına ilişkin mekanizmalar + Budapeşte Sözleşmesi revizyonu				Siber suçlar (ağ saldırısı, izinsiz giriş, örneğin BİT kullanımı ile işlenen suçlar)

Tablo 1: (Devamı)

İşbirliğine yönelik araçlar	Ortak alanlar			Tehditler ve tartışmalı konular
	RF	ÇHC	ABD	
				Kamu düzeni ve toplum için zararlı bilgilerin yayılması (radikalizm dahil)
				Dijital kopukluk ve diğer ülkelerden BT teknolojisi bağımlılığı
				Dış basının ülkedeki enformasyon yayılımı ve ulusal ve uluslararası haber tablosunun çarpıtılması
İnternet Yönetişim Sistemi				Küresel ve ulusal kritik bilgi altyapılarının güvenli ve istikrarlı işleyişine yönelik tehditler
Güven Artırıcı Önlemler				Ulusal kritik altyapı ve endüstriyel kontrol sistemlerine yönelik siber saldırılar
				Fikri mülkiyet hırsızlığı (endüstriyel siber casusluk)
				İnternet özgürlüğü ve bilgi akışını tehdit eden unsurlar
	RF	ÇHC	ABD	

Kaynak: Stadnik, 2017

Tablonun renkli kutuları, ülkenin öne çıkardığı tehditleri veya tartışmalı konuları göstermektedir. Tablonun altındaki son satır, küresel iş birliği için olası politika alanlarını vurgulayarak norm oluşturma sürecine odaklanmaktadır. RF ve ÇHC, birbirlerine daha yakın tehdit algılamalarına sahiptir; ancak RF ve ÇHC siber uzayda egemenlik vurgusu yaparken, ABD ekonomik ve siyasi nedenlerle ağ güvenliği ve serbest bilgi akışına odaklanmaktadır. Her üç ülkenin ortak kabul ettiği tehlikeler arasında terör amaçlı Bilgi ve İletişim Teknolojileri (BİT)'nin kullanımı, siber suçlar, küresel ve ulusal kritik bilgi altyapılarının güvenliği ve endüstriyel kontrol sistemlerine yönelik siber saldırılar bulunmaktadır. Siber güvenlik normlarının tüm paydaşlar tarafından kabul edilmesi ile bu alanda iş birliği kolaylaşacaktır (Stadnik, 2017: 141-142).

Siber alan bireylerden devlete birçok aktörü ve dijital kullanım alanlarını içinde barındıran geniş bir kavramdır. Dijital boyutta yapılan tüm çalışmalar siber alana dahildir. Her biri internet kullanımının yaygınlaşması ile aktiflik barındıran konulardır. Alanın geniş kapsamı ve erişilebilirlik düzeyi düşünüldüğünde küresel çapta önemini görebilmekteyiz.

2.1.3. Siber Uzay Kavramı

20. yüzyıl sonrası siber alanda yaşanan gelişmeler ve dijital süreçler bizi siber uzay kavramına yaklaştırmıştır. Siber uzay kavramı çok geniş kapsamlı bir terimdir. Dijital dünyadaki çevrimiçi kullanıcıların bütün etkileşimlerini ve faaliyetlerini içerisinde dahil etmektedir. Dünya genelinde küresel çapta internet kullanımından bahsedildiğinde devletlerarası ilişkilerin de siber uzayda

diplomatik şekilde geliştiğini görmekteyiz. Bu bağlamda siber uzay diplomatik ilişkileri yeniden şekillendirmiştir. Siber uzay kapsamı çerçevesinde sınırları aşan ve iletişimi kolaylaştırıp herkesi bir araya getiren bir alandır. Bu durum internetin yoğun kullanımı ile mümkün olmuştur. ABD Savunma Bakanlığı'na göre siber uzay, bilgi teknolojisi ile yerleşik veri altyapıları arasında bağlantılar oluşturan iç içe geçmiş bir ağ üzerinde faaliyet gösteren küresel bir bilgi alanıdır; interneti, telekomünikasyon ağlarını, bilgisayar sistemlerini, gömülü işlemcileri ve denetleyicileri içermektedir (Library of Congress Congressional Research Service, 2020).

Siber uzay internet ile bağlantılı bir terimdir. İnternet kullanımı özellikle Soğuk Savaş'ın etkisiyle şekillenen Arpanet projesi ile 1969 yılında başlamıştır. Bu dönemde, Arpanet askeri bir amaca hizmet etmek üzere geliştirilmiş ve bilgisayarlar arası iletişimi sağlamak amacıyla kullanılmıştır. Ancak internet teknolojisinin yaygın kullanımı, world wide web (www)'in geliştirilmesiyle mümkün olmuştur. 1991 yılında, www'nin ortaya çıkması, internetin geniş kitlelere açılmasını sağlamış ve bu teknoloji yaygın olarak kullanılmaya başlanmıştır (Önal, 2021: 116). İnternet dünya genelinde kullanılan bir ağ sistemidir. Siber uzayın ana kaynağını oluşturan en önemli unsurlardan bir tanesidir.

Siber uzay kavramı, altı ilkeye dayanmaktadır ve bu ilkelere yapılan vurgu, bilgi teknolojileri ve internetin evrimiyle birlikte siber uzayın karmaşıklığını (Choucri, 2000: 125), hızlı gelişen yapısını (Tikk, 2010: 110), anonim karakterini, yönetilemez doğasını (Ashenden & Barnard-Willis, 2012: 116-118), asimetrik savaş üretme eğilimini (Reveron, 2012: 148; Ashenden & Barnard-Willis, 2012: 118) ve düşük maliyetli siber silah üretme kapasitesini (Kelsey, 2008: 1145) ifade eder. Siber uzay, yapısı bağlamıyla karmaşıktır. İnternetin getirdiği olanaklarla birlikte teknolojinin sürekli olarak yenilenen yapısı siber uzayın hızlı şekilde gelişmesini sağlamıştır. Siber uzayda aktif olan aktörler diledikleri zaman kimliklerini gizli tutabilmektedirler. Bu sayede kimin nasıl ne şekilde kontrol edileceğinin tespiti güçtür. Siber uzay bünyesinde devletleri, grupları, örgütleri ve bireyleri barındırmaktadır. Her yere ulaşımın daha kolay olduğu erişebilirlik düzeyinde büyük güçler ve küçük güçler kimi noktalarda eşit saldırganlıklarda bulunabilmektedirler. Bu da alanda asimetrik savaş ihtimalini canlandırabilmektedir. Yani siber uzay, sivil veya askeri kritik altyapılara karşı asimetrik bir saldırı başlatmak için ideal bir ortam olabilmektedir (Cavelty M. D., 2015: 410). Siber uzayda saldırı düzenleyebilme araçları fiziksel dünyadaki kadar maliyetli değildir. Saldırgan taraf çevrimiçi olarak zararlı yazılımlar üretebilir ve sadece internet erişimini sağlayarak amacına ulaşabilir. Nitekim küçük çapta giderler ile büyük sonuçlar elde edilebilmektedir. Bu temel ilkeler, siber tehditlerin ana kaynaklarını oluşturarak siber uzayın içinde güvenli bölgelerin olmadığı izlenimini uyandırmaktadır (Gökçer ve Gözen Ercan, 2020: 180-181).

Siber uzayın içerisinde oluşan güvensiz alanlar devletler için yeni bir güvenlik boyutunun gündeme gelmesini gerektirmiştir. Özellikle Soğuk Savaş sonrasında siber uzay faaliyetleri artış göstermiştir. 2016 yılında yapılan NATO bünyesindeki Varşova Zirvesi'nde çok önemli bir noktaya

değinilmiştir. Siber uzay; kara, deniz, hava ve uzay sahası gibi bir alan olarak tanımlanıp savaş alanına dahil edilmiştir. Ayrıca NATO'nun birçok zirvede sıklıkla üstünde durduğu gibi siber güvenlik alanında NATO ülkelerinin daha fazla iş birliği içeresinde bulunulmasına vurgu yapılmıştır (NATO, Warsaw Summit Key Decisions, 2016). NATO'nun kuruluşunda belirtilen 5. Madde kara, deniz, hava ve uzay alanlarını kapsamaktadır. Ancak 21. yüzyılın başlarından itibaren gelişen yeni dünya sistemleri ve teknolojinin getirdiği zorluklar, özellikle siber alandaki olumsuzluklar NATO'nun dikkatini çekmiş ve bu nedenle siber uzay alanı kara, deniz, hava ve uzay alanlarına ek olarak beşinci bir boyut olarak önem kazanmıştır (Polat, 2020: 149). Bu durum siber uzayın önemini ve küresel dünyayı ciddi boyutlarda etkilediğini gözler önüne sermektedir.

Sonuç olarak siber uzay kavramı dijital araçların kullanımı ve internetin yoğunlaşma süreçlerini kapsayan bir terimdir. Geniş perspektifleri ile hem olumlu hem de olumsuz sonuçları içerisinde barındırmaktadır. Bu bağlamda devletler ve bireyler siber uzay bünyesinde aktif rol oynamaktadırlar. Aktörler hem internetin olumlu getirilerinden faydalanırken hem de tehlikeli yönlerine karşı siber güvenlik önlemleri almaktadırlar.

Bilgi çağında gelinen noktada siber uzay kapsamında yaşanan tehditler dijital boyutta olup kritik alt yapılara ve sistem ağlarına zarar verebilmektedir. Bu zararlar kimi zaman fiziksel boyut tehlikesi doğuracak nitelikte olabilmektedirler. Bireyler bilinç düzeylerini geliştirip şifreleme gibi kişisel önlemler alabilmektedirler. Devletler ise ulusal güvenliklerini geliştirmek adına ihtiyaçlarına göre siber güvenlik stratejileri oluşturmaktadırlar. Elbette ki siber uzay sürekli gelişen ve ilerleyen bir alan olduğu için alınacak önlemler de aynı hızla geliştirilip takip edilmektedir. Bu bağlamda siber güvenlik uzmanlarının mümkün olduğu kadar her saat diliminde aktif savunma sistemleri izlemeleri gerekmektedir. Uluslararası alanda internet kullanımının yoğun olması küresel çapta yaşanabilecek tehditleri de barındırmaktadır. Siber uzay bünyesinde devletler iş birliği ve koordinasyonun dünya genelinde siber tehlikelerden korunabilmesi açısından önemli olduğunun bilincindedir. Bilakis NATO siber uzay kavramının öneminin altını çizip bu alanda iş birliği yapılması çağrısında bulunmuştur. Küresel düzeyde etkili bir siber güvenlik stratejisi oluşturmak, uluslararası iş birliğini güçlendirmek ve siber uzayda istikrarı sağlamak, devletlerin dış politikalarında yer edinen konular haline gelmiştir. Siber uzayın dinamikleri düşünüldüğünde kapsamının genişliği ile birbiriyle bağlantılı birçok yapıyı etkileşim halinde tuttuğu gözlemlenebilmektedir.

2.2. Siber Güvenlik ve Uluslararası Politika

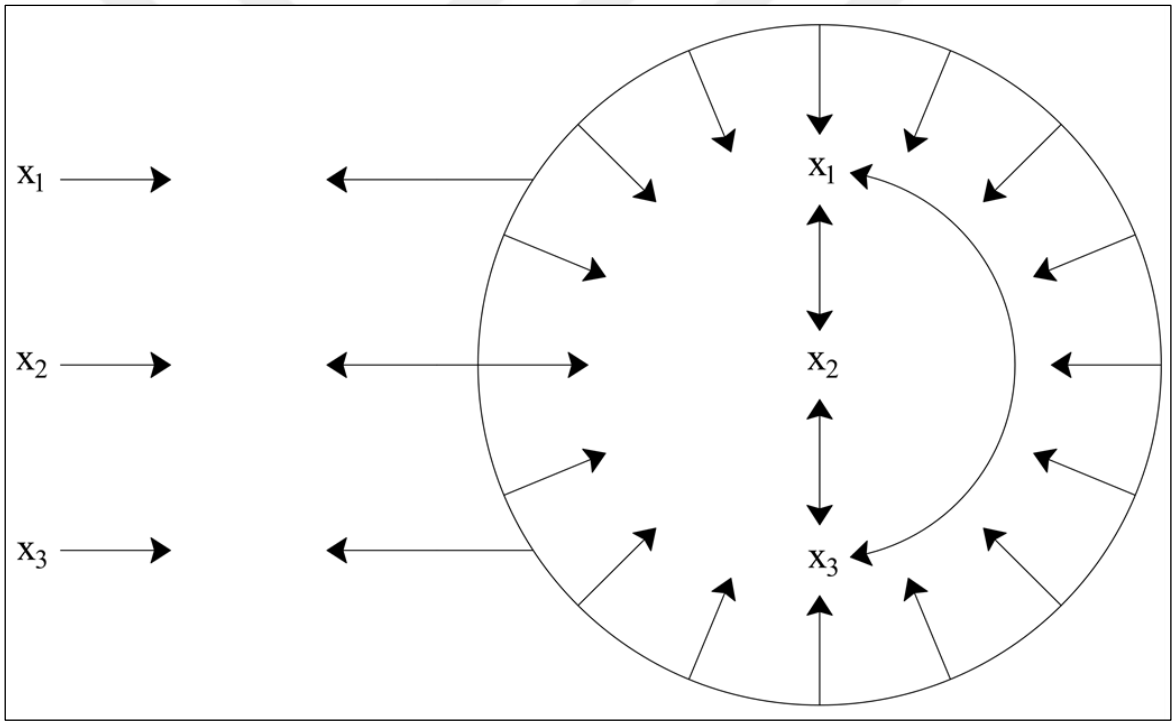
Günümüzde siber güvenlik uluslararası politikanın temel bir unsuru haline gelmiştir. Bilgi ve iletişim teknolojilerindeki hızlı ilerlemeler, uluslararası ilişkileri kökünden değiştirmekte ve devletlerin güvenlik politikalarını yeniden şekillendirmektedir. Siber güvenlik artık sadece bir devletin iç meselesi değil, aynı zamanda uluslararası politikanın merkezinde yer alan bir konudur.

Gelecekte siber güvenlik politikalarının daha da karmaşık hale gelmesi ve uluslararası politika üzerinde daha büyük bir etkiye sahip olması muhtemeldir.

2.2.1. Uluslararası Politika Kavramını Siber Alan ile İlişkilendirmek

Uluslararası politika küresel düzeydeki siyasi olayları, diplomatik ilişkileri, uluslararası aktörleri ve küresel dinamikleri kapsayan bir disiplindir. Kavram kapsamı açısından oldukça geniştir ve içerisinde birçok aktörü ilgilendiren konuları ele alır. Uluslararası alandaki her aktör siyasi olguları bağlamında bu alana dahildir. Dünya siyasetini ve çeşitli aktörler arasındaki ilişkileri anlamaya yönelik yaklaşımları içerir; bu aktörler arasında devletler, uluslararası kuruluşlar, ulusötesi ve ulusaltı gruplar yer almaktadır (Bull, 1995: 181).

Şekil 2: Sistem Değişim Dinamikleri



Kaynak: WALTZ, 1979

Kenneth Waltz (1979,100) şekil 2'de gösterilen uluslararası politika sistemindeki daireyi bir uluslararası alt yapı olarak değerlendirmiştir. Oklar, devletler arasındaki etkileşimleri ve özelliklerini göstermektedir ve bu da belirli bir ilişki içinde olduklarını işaret etmektedir. Devletlerin otonomilerini korurken birbirleriyle belirli bir ilişki içinde olması durumunu organizasyon terimiyle açıklamıştır. Devletler arasındaki kısıtlamalar ve sınırlamalar nedeniyle uluslararası politika, ilkel organizasyonel terimlerle anlaşılabilmektedir. Yapı kavramını beklenen organizasyonel etkileri açıklamak ve yapılar ile birimlerin birbirleriyle etkileşimlerini anlatmak için kullanılan bir kavram olarak belirtmiştir. Yani yapı kavramı ile devletler bir ilişki içerisindedir. Bunu ilişki içerisindeyken

de kendi özelliklerini korumaktadırlar. Daireyi, yani uluslararası alt yapıyı siber alan olarak düşünecek olursak içerisindeki oklar devletlerin etkileşimlerini göstermektedir. Yani, siber alanda da devletler uluslararası politika bağlamında etkileşim içerisine girip birbirlerini etkileyebilmektedirler. Bu etkileşim yaşanırken kendi otonomilerini koruyabilmektedirler.

Siber alan kavramı internet kullanımının dahil olduğu birçok konuyla ilgilenmektedir. Siber alan ve uluslararası politika terimleri geniş konuları bünyelerinde barındırmaları açısından benzerlik göstermektedirler. Ayrıca siber alan uluslararası politika konularına dahildir. Aynı şekilde uluslararası politika da siber alan konularıyla ilgilenmektedirler. Bu iki kavramı ortak noktada birleştiren unsurlar uluslararası sistemde bulunan devletler ve diğer aktörlerdir. Siber alan bünyesinde güvenlik siber saldırılarla mücadele, iş birliği, çevrimiçi toplantılar gibi politik konular uluslararası aktörleri dijital bağlamda etkileşime sokmaktadır. Belirli kurumsal siber güvenlik stratejilerinin oluşturulması ve bu bağlamda öngörülen iş birliği gibi çalışmalar uluslararası aktörleri siber alanda politika oluşturmaya teşvik etmektedir.

Uluslararası aktörlerin küresel boyutta siber politika yapabilmeleri için iş birliği ve ortak normlar oluşturabilmeleri önlemlidir. Bu noktada önemli olan, konuların bütün aktörleri ilgilendiren özellikler barındırmasıdır. Bu sayede ortak paydada birleşmek cezbedici olabilecektir. Kenneth Waltz (1979, 210)'a göre ortak sorunların çözümü veya etkili yönetimi için kolektif çabalara olan ihtiyaç genellikle kabul edilen bir gerçektir. Küresel sorunlar tek bir ulusun çözme kapasitesini aşar ve yalnızca bir dizi ulusun birlikte çalışmasıyla ele alınabilir.

Siber alandaki ilgili dijital konular küresel çapta devletleri ilgilendirdiği için uluslararası politika düzleminde etkileşim haline girebilmektedirler. Aynı şekilde uluslararası politikayı ilgilendiren birtakım konular vardır. Bunlar arasında askeri anlaşmalar, terörizmle mücadele, serbest piyasa ve ticari konular, insan hakları, çevre sorunları ve sağlık politikaları gibi bir dizi küresel konular bulunmaktadır. Uluslararası politikaya siber güvenlik konuları da dahil olmakla birlikte hem siber güvenlik konularının hem de öteki uluslararası politika konularının görüşülmesinde ve anlaşmalar yapılabilmesinde kimi zaman siber alanın etkisi bulunmaktadır. Çevrimiçi görüşmeler, anlaşmalar ve tüm dünyayı ilgilendiren konuların internet üzerinden kolayca göz önüne getirilebilmesi gibi örneklerle siber alanın da uluslararası politikayı etkilediği görünmektedir.

Uluslararası politika ve siber alan karşılıklı etkileşimde olan sanal dünyada yaşanan gelişmelerin yoğunlaşması ile günden güne iç içe geçen bir ilişki içerisindedir. Devletlerin uluslararası politikalarındaki en önemli stratejilerinden biri de güvenliktir. Ulusal ve uluslararası alanda asayişin sağlanması her devleti yakından ilgilendiren bir konudur. Bu bağlamda siber alanda yaşanan güvenlik sorunları da uluslararası politikanın gündeminde olan bir konudur. Siber güvenlik tehditleri devletlerin geleneksel güvenlik anlayışının ötesindedir. Bilgisayar sistemleri ve ağlara düzenlenen saldırılar ciddi tehditler oluşturabilmektedir. Bu da devletleri siber savaş kavramına ve

alınacak uluslararası politika önlemlerine götürmektedir. Siber alanın karmaşıklığı ve sürekliliği devletleri küresel çaptaki politikalarını güncellemeleri sonucuyla karşı karşıya getirebilir.

2.2.2. Siber Savaşlar Gerçek mi?

Devletler oluşumlarından bu yana çeşitli nedenlerden dolayı savaşmışlardır. Tarihin birçok döneminde savaşlar ve akabinde barışlar yaşanmıştır. Farklı zaman dilimlerinin kendisine özgü sorunları ve o sorunlardan çıkan anlaşmazlıklar sebebiyle genellikle güçlü tarafın/tarafların galip geldiği savaşlar olmuştur. Dijital çağa gelindiğinde ise siber savaşlar özellikle yakın geçmişte sıklıkla gündeme gelen bir konu haline gelmiştir. Bu saldırı tipi geleneksel saldırılardan biraz daha farklıdır. Çünkü saldırganların maliyeti düşük ve çok az çabayla ciddi sonuçlar oluşturabildikleri siber saldırılar siber savaş boyutuna ulaşabilmektedir. Sonucunda güçsüz tarafların da kazançlı çıkabilme olasılığı çok yüksektir. Ayrıca tespit edilebilmeleri güç olduğu için hiçbir bedel ödeme zorunlulukları da kalmayabilmektedir.

Siber savaş, güvenlik çalışmaları açısından önemli bir parametreyi oluşturmaktadır. Bu kavram siber alandaki çatışmaların savaş olarak nasıl ele alınacağı sorusunu beraberinde getirir niteliktedir. Eğer savaş olarak değerlendirilirse barışın sağlanması için yeni bir anlayış geliştirilmesi gerekebilmektedir. Siber savaşın devamında uluslararası ilişkilerde ve güvenlik politikalarında meydana gelebilecek değişikliklerle birlikte, barışın nasıl ortaya çıkabileceği felsefi bir düşünce konusu haline gelmektedir (Güntay, 2016: 3). Geleneksel savaş anlayışından farklı olan siber savaşlar, barış anlamında da genel anlayışın dışında getirileri sağlayabilmektedir. Dijital çağın savaş ve barış anlayışını yeniden değerlendirmek ve geleneksel normlar ve anlayışlar üzerinden düzenlemek gerekebilir. Siber alanın karmaşıklığı savaşları da tartışmaya açık konuma getirebilmektedir. Çünkü siber savaş dediğimiz kavram yeni ve çok boyutludur. Saldırılar gizli yapılabilmektedir. Fakat sonuçları ses getirecek boyutta etkileyicidir. Bunu engelleyebilmek için siber savunma oluşturmak adına tehdidin nereden ve kimden geldiğinin tespiti önemlidir. Üstelik henüz saldırının nereden geldiğinin belli olmadığı bir durumda barış için çalışmalar yürütmek de zordur.

Carr (2011); "*Siber savaş, savaşmadan savaşmanın sanatı ve bilimidir; bir rakibi kan dökmeksizin mağlup etmenin sanatıdır*." şeklinde tanımlama yapmaktadır. Robinson vd. (2015) yaptığı eleştiride siber savaşların kan dökmeyeceği kanısının kesin olmadığını vurgulamaktadır. Bu düşüncesini de elektrik şebekesi gibi kritik ulusal altyapılara yapılan bir siber saldırının yaşam kaybına neden olabilecek nitelikte olması ile desteklemektedir. Ayrıca Colarik ve Janczewski (2011) siber savaşın şiddet içeren bir boyutu olabileceğini öne sürmektedirler. Siber savaşlar genel anlamda dijital boyutlarda zararlar verebilmektedirler. Ancak gelişen teknolojik sistemler sayesinde dünya düzenindeki bazı yapıların teknoloji ile bağlantılı yapısı siber saldırıların fiziksel zarar verebilme ihtimalini doğurabilmektedir. Bir devletin hastanesindeki alt yapılara siber saldırı düzenlendiğinde,

yoğun bakım üniteleri gibi hayati önem taşıyan kısımlarda kullanılan cihazlar ve sistemler bu saldırıdan etkilenebilir. Bu saldırılar sonucunda hastaların hayatları riske atılabilir. Yani siber savaşlar doğrudan olmasa bile dolaylı yoldan can kayıplarına neden olabilme ihtimali taşıyabilmektedirler.

Siber savaş bünyesindeki saldırganlar yöntemlerini gizli tutabilmektedirler bu yüzden savunma stratejilerinin aktif şekilde geliştirilmesi önemlidir. Yapılan hızlı ve anlık saldırılar kimlik tespitini zorlaştırırken aynı şekilde siber güvenlik uzmanlarının da hızlı yanıt verme yeteneklerini geliştirmeleri gerekebilir. Siber savaşın küresel oluşu uluslararası aktörleri ve devletleri iş birliğine ve ortak normlar oluşturmaya teşvik edici olabilmektedir. Jacobsen (2014)'e göre siber savaşlar konvansiyonel savaşların yerini alamaz.

Siber savaşların gerçek olup olmadığı birçok araştırmacı tarafından farklı şekillerde yorumlanmıştır. Siber alanın karmaşıklığı onu yoruma açık bir hale getirmektedir. Siber güvenliği tehdit eden birçok saldırı çeşidi bulunmaktadır. Bu saldırılar uluslararası alanda ve ulusal bağlamda terör faaliyetleri şeklinde de gerçekleşebilmektedirler. 1990 sonrası yoğunlaşan internet kullanımı ile bu saldırıların birçok örneği görülebilmektedir. Bir savaş türüne savaş diyebilmek ya da diyememek karmaşasını yaşamak bile siber saldırıların ne kadar tehlikeli olabileceği ihtimalini gösterebilmektedir.

Tablo 2: 1991-2011 Siber Çatışma Örnekleri

Olayın Adı	Yaşandığı Yıl	Açıklama	Aktörler/Failler
Körfez Savaşı	1991	Zaferin artık yalnızca fiziksel güce bağlı olmadığı, aynı zamanda bilgi savaşını kazanma ve bilgi hakimiyetini güvence altına alma becerisine de bağlı olduğu yeni nesil çatışmaların ilki	ABD ordusu
Hollandalı hacker olayı	1991	Körfez Savaşı sırasında Pentagon bilgisayarlarına izinsiz girişler. Sınıflandırılmamış, hassas bilgilere erişim	Hollandalı gençler
Müttefik Kuvvet Harekâtı	1999	İlk "İnternet Savaşı", savaşta bilgi savaşı bileşenlerinin tüm spektrumunun kullanımını sürdürdü. Çok sayıda siber saldırı olayı yaşandı.	ABD ordusu, birçok ülkeden bilgisayar korsanı
Siber İntifada	2000-2005	İkinci İntifada sırasında hükümet ve partizan web sitelerine yönelik e-posta seli ve Hizmet Engelleme (DOS) saldırıları	Filistinli ve İsrailli bilgisayar korsanı
Siber I. Dünya Savaşı	2001	ABD keşif ve gözetleme uçağının Çin topraklarına inmeye zorlanmasının ardından Çin ve ABD web sitelerinin tahrif edilmesi ve DOS saldırı dalgaları	Birçok ülkeden bilgisayar korsanı (Suudi Arabistan, Pakistan, Hindistan, Brezilya, Arjantin, Malezya, Kore, Endonezya, Japonya)
Irak	2007	Teröristlerin yol kenarındaki bombaları yerleştirmek ve bunları patlatmak için kullandığı cep telefonları, bilgisayarlar ve diğer iletişim cihazlarına uygulanan siber saldırı	ABD ordusu
Estonya Dağıtılmış Hizmet Engelleme (DDoS) saldırıları	2007	Estonya parlamentosu, bankalar, bakanlıklar, gazeteler ve yayıncıların web sitelerine yönelik DDoS saldırıları	Rus hükümetine atfedilmiştir

Tablo 2: (Devamı)

Olayın Adı	Yaşandığı Yıl	Açıklama	Aktörler/Failler
Gürcistan DDoS saldırıları	2008	Çok sayıda Gürcü web sitesine yönelik DDoS saldırıları	Rus hükümetine atfedilmiştir
GhostNet sızıntıları	2009	Tibet sürgün gruplarına ait bilgisayarlara GhostNet bağlantılı sızmalar	Çin hükümetine atfedilmiştir
Stuxnet	2010	İran'ın nükleer programını yavaşlatmak için yayınlanmış bilgisayar solucanı	ABD hükümeti (+ İsrail)
Kore ağ Saldırıları	2011	Botnetler ve devlet web sitelerine yönelik DDoS saldırıları. Uzmanlar Kuzey Kore'nin siber silah denemelerinden şüpheleniyor	Kuzey Kore hükümetine atfedilmiştir

Kaynak: Cavelty M. D., 2015

2.2.3. Siber Terörizm Tartışması

Terörizm ulusal güvenlik, toplumsal düzen ve barışı tehdit eden bir tehlikedir. Genellikle şiddet ve korku oluşturucu unsurları kullanarak toplumun, devletlerin ve uluslararası alanın huzurunu kaçırmayı amaçlar. Terörizmin uygulanmasının kolaylığı ve hızı, özellikle terörist grupların eyleme geçmek için sabırsız olmaları terörizmin çekiciliğini artırmaktadır (Crenshaw, 2013: 396). Bu tür bir çekicilik, terörist grupların propaganda ve mobilizasyon çabalarında kullanılabilecek bir unsur olabilmektedir. Üstelik oldukça tehlikeli ve yıkıcı sonuçları vardır.

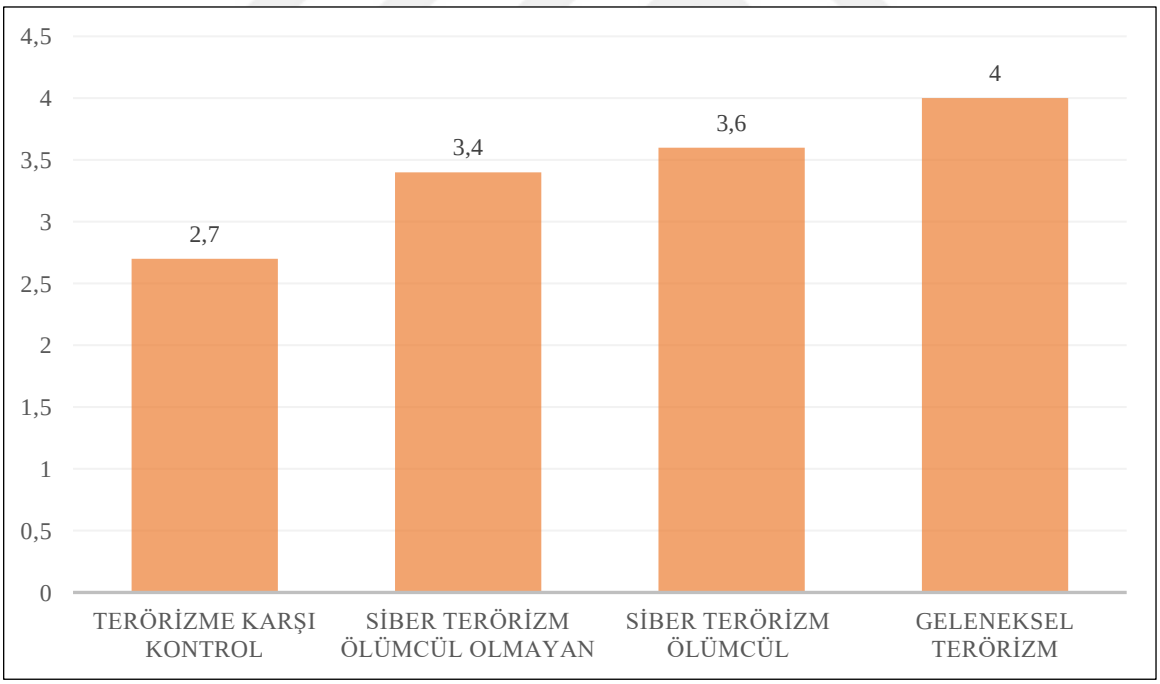
Siber terörizm geleneksel terörizm anlayışını sanal ortama taşıyarak ulusal ve uluslararası güvenliği tehdit eden bir unsur haline gelmiştir. Dijital unsurları kullanarak siyasi, dini, ideolojik amaçlar ile saldırılar düzenlenebilmektedir. Bu saldırılar bireysel olmakla birlikte kötü amaçlı örgütler tarafından da gerçekleşebilmektedir. Siber terör faaliyetleri ile siyasi ekonomik veya askeri güvenlik tehlikeye girebilmektedir. Saldırganlar dijital alanda kullanılan önemli unsurları hedef alıp ciddi sonuçlara neden olabilirler. Genel bir tanım ile, siber terörizm bilgisayar ağı araçlarının kullanılması yoluyla kritik ulusal altyapıları kapatmayı veya bir hükümeti veya sivil nüfusu zorlamak veya korkutmak amacıyla gerçekleştirilen terör eylemlerini ifade etmektedir (Lewis, 2002: 1).

Siber terörizmin beslendiği kaynaklar ve harekete geçme süreci, *siber tehditlerle* ilgilidir. Siber tehditler, internete bağlanmayı sağlayan ve çevrimiçi saldırılara maruz kalmayı mümkün kılan araçların oluşturduğu unsurlardır (Güntay, 2016: 38). Bu tehdit unsuru bireylere yönelik olduğu gibi devletlere yönelik de olabilmektedir. Saldırganlar çeşitli yöntemler kullanarak sanal alanda terör faaliyetlerini gerçekleştirmektedirler. Bilgisayar sistemlerine virüs ve kötü yazılımlar bulaştırmak, sahte web siteleri ve çeşitli uygulamalar ile kişisel verileri elde edebilmek ve izinsiz erişimler ile gizlilik ihlali oluşturmak gibi siber tehditler hem bireylere hem devlete hem de uluslararası örgütlere zarar verebilmektedir.

Siber terörizm siber uzayda siyasi, dini veya ideolojik amaçları ilerletmek amacıyla korku yaratmak için devlet, devlet dışı veya bireysel aktörler tarafından gerçekleştirilen siber saldırıları kapsar. Doğrudan ölüme neden olacak sonuçlarının olmaması onu fiziksel dünyada gerçekleşen öteki terörizm saldırılarından ayırmaktadır. Fakat dolaylı yoldan fiziksel zararlar verebilme etkileri bulunmaktadır (O'Brien, 2021). Bu yüzden siber güvenlik uzmanları ulaşım ağları, barajlar, askeri tesisler, hastaneler, bankalar ve devlet daireleri gibi kritik altyapıları siber saldırılardan koruma konusunda endişe duymaktadırlar (Lewis J. A., 2002).

Toplumun günlük yaşamını etkileyebilecek ve devletlerin düzenlerini bozabilecek her türlü terör saldırısı tehlikelidir. Siber terörizmin fiziksel boyutta zarar vermemesi konusu tartışmalı bir konudur. Fakat saldırganlar düşünüldüğünde, terörizmin nihai amacı olan korku oluşturma sonucuna siber saldırılar ile kolayca ulaşabilmektedirler. Bu da siber terörizmi yeteri kadar tehlikeli yapmaktadır. Teröristlerin amacı genellikle çok sayıda insanın ölmesini değil, bunun yerine olayın geniş bir şekilde medya ve toplum tarafından izlenmesini istemektir (Jenkins, 1975; Lerner vd., 2003). Bu tür saldırılar fiziksel zararların ötesinde, sosyal panik oluşturabilmektedirler.

Grafik 1: Risk Algısı ve Güvensizlik Duygusu



Kaynak: Gross vd., 2016

Grafik 1'de saldırıların daha ölümcül hale geldikçe stres ve kaygıların arttığını göstermektedir. Ölümcül sonuçları olan ve ölümcül olmayan siber terörizm için stres skorları arasında önemli bir fark olmaksızın tüm skorlar kontrol grubunu belirgin bir şekilde aşmaktadır. Buna rağmen ilginç olan bir nokta vardır. Bireyler, hem ölümcül hem de ölümcül olmayan siber terörizm tarafından eşit

derecede etkilenmişlerdir, yani stres açısından aralarında belirgin bir fark bulunmamaktadır. Her ikisi de önemli bir panik ve kaygıya neden olabilmektedir ve her ikisi de, ruhsal olarak iyi hissetme ve insan güvenliğinin temellerini eşit derecede etkileme potansiyeline sahiptir (Gross vd., 2016: 3).

Terörizm olgusu ve siber terörizm korku oluşturma konusunda ortak noktaları barındırsalar bile yöntemleri farklıdır. Teknolojik gelişmeler ve siber uzayın sınır ötesi olanakları sebebiyle siber terörizm modern terör faaliyetleri kapsamındadır. Burada saldırganlar klasik silahlarla savaşma geleneğini terk ederek, sofistike yüksek teknoloji kullanmaktadırlar. Onlar için küresel bilgi ağı siber terörizmi gerçekleştirmede kullanılacak modern bir silahtır. Yani saldırganlar teknolojik yöntemleri kullanarak saldırı düzenlemektedirler (Achkoski ve Dojchinovski, 2012). Sonuç olarak ulusal, bölgesel ve küresel düzeyde ciddi zararlar verebilmektedir. Görüldüğü üzere siber terörizmin kapsamı geniş bir alana yayılmakta ve onu en tehlikeli yapan unsurlardan biri de mesafe tanımaksızın dilediği yere istediği saldırıyı gerçekleştirebiliyor oluşudur.

Geleneksel terörizm ve siber terörizm benzer amaçları oluştursa bile yöntemleri birbirlerinden çok farklıdır. Etki boyutları tartışılamamakla birlikte siber terörizmin kapsamı internet ve teknoloji kullanımının bulunduğu tüm siber uzaya dahildir. Bu geniş kapsam onu oldukça tehlikeli hale getirmektedir. Dünya genelinde bilgisayar sistemlerini ve dijital alt yapıyı hedef alması ile küresel bir tehdit boyutu haline gelmiştir.

2.2.4. Siber Saldırıların Kapsamı ve Tehdit

Siber saldırılar, bireylerden devlet kurumlarına kadar birçok kuruluşu hedef alabilir ve büyük ölçekte veri kaybına, finansal kayıplara ve hatta ulusal güvenlik sorunlarına neden olabilir. Green (2015)'e göre siber saldırılar sistemleri, kuruluşları veya bireyleri hedef alır ve varlıklarını bozmaya, çalmaya yönelik bir tehdidi ifade eder. Bu varlıklar genellikle dijital formatta (veri, bilgi veya kullanıcı hesabı gibi), dijital hizmetlerde (iletişim gibi) ya da siber bir bileşeni olan fiziksel varlıklarda (binalarda, uçaklarda veya nükleer tesislerde bulunan süreç kontrol sistemleri gibi) bulunabilir.

Tehdit kavramı ise uluslararası ilişkilerde özellikle 11 Eylül 2001 saldırıları sonrasında modern boyutlar kazanmıştır. Terörizm, asimetrik tehditler, siber güvenlik tehditleri gibi unsurlar devletlerin güvenlik alanlarını geliştirmelerine neden olmuştur. Genel anlamda başkalarının güvenliğine zarar verecek potansiyele sahip olan ve hedeflerine ulaşmak için bu amacı taşıyan aktörler bulunduğunda tehdit ortaya çıkar (Wallander ve Keohane, 1999: 25).

Siber tehditler ise modern tehdit unsurları arasında internet kullanan bütün aktörlerin karşı karşıya kalabileceği bir tehdit türüdür. Aynı zamanda siber tehditlerin karmaşık ve dinamik oluşu

nedeniyle internet ağlarının bu tehditlere karşı savunma yapması oldukça zordur (Lewis J. A., 2014: 1).

Tablo 3: Siber Saldırılara Daha Yakından Bakmak

TEHDİT UNSURU	MOTİVASYONLAR	HEDEFLER	ÖRNEKLER
 **Ulus devletler Devlet destekli gruplar**	Jeopolitik, İdeolojik	Aksaklık, yıkım, hasar, hırsızlık, casusluk, mali çıkar sağlamak	Kalıcı veri tahribatı, hedeflenmiş fiziksel hasar, elektrik şebekesi kesintisi, ödeme sistemi kesintisi, sahte transferler, casusluk
 **Siber Suçlular**	Zenginleştirici	Hırsızlık, mali kazanç sağlamak	Nakit hırsızlığı, sahte transferler, kimlik hırsızlığı
 **Terörist gruplar Bilgisayar korsanları Ülke içi tehditler**	İdeolojik, Memnuniyetsizlik	Yolsuzluk	Sızıntılar, itibarsızlaştırma, dağıtım tabanlı hizmet engelleme saldırıları

Kaynak: Maurer ve Nelson, 2021

Siber saldırıların kapsamı oldukça geniştir. İnternet kullanımının aktif olduğu ve dijital araçlara bağlı olan cihazların tümü olası siber tehditler ile karşı karşıyadır. Bu saldırılar ulusal düzeyde devlete karşı siber terörizm ile gerçekleşebilirken aynı zamanda bireylerin kişisel verilerine karşı da düzenlenebilmektedir. Bireylerin ve organizasyonların çeşitli kişisel bilgileri, finansal verileri veya ticari sırları ele geçirilerek hedeflenen saldırı gerçekleştirilebilir. Saldırganlar siber saldırıları dışarıdan bir müdahale ile gerçekleştirebilecekken aynı zamanda kurum ve kuruluşların içerisinde çalışan bireyler de çeşitli bilgileri ele geçirerek siber tehdit unsuru haline gelebilmektedirler. Bunun dışında devletten başka bir devlete siber casuslar aracılığı ile de siber saldırılar gerçekleştirerek siber güvenliği tehlikeye sokabilmektedirler.

Uluslararası alanda siber saldırı boyutları çok kapsamlıdır. İnternetin küresel doğası ile siber uzayın sınırsız imkanları düzeyinde siber saldırılar sınırları aşarak coğrafi engelleri kaldırmaktadırlar. Küresel boyutta birçok aktörün yaygın şekilde internet kullandığı bilinmektedir. Bu durumda siber saldırı potansiyeli de aynı düzeyde yaygınlaşmaktadır. Bir saldırıyı önleyebilmenin en önemli yöntemlerinden bir tanesi saldırganın kim olduğunu tespit edebilmektir. Siber saldırıların kapsamının geniş olması nedeniyle, saldırgan tarafın kimliği konusunda birçok seçenek çıkmaktadır. Maurer ve Nelson (2021: 25)'a göre siber saldırıların arkasındaki aktörler

arasında, giderek daha cesur hale gelen suçluların yanı sıra farklı amaç ve motivasyonlara sahip devletler ve devlet destekli gruplar da yer almaktadır.

2.2.5. Siber Savunma Mümkün mü?

Siber uzayın getirmiş olduğu tehdit unsurlarına karşı savunma sistemi oluşturmak oldukça karmaşık bir durumdur. Çünkü siber alan karmaşıktır ve tehditlerin de çoğunlukla kimin tarafından geldiğinin tespiti zordur. Bu alanda yaşanan gelişmeler ani ve hızlı olduğu için geliştirilecek güvenlik önlemlerinin de aynı hızda ve kesintisiz şekilde uygulanması gerekmektedir. Ortada bir tehdit unsuru olduğu sürece savunma kaçınılmaz olacaktır. Çünkü siber tehditlerin çok ciddi kayıplara neden olabileceği görülmektedir. Siber savunma için devletler çalışmalar yürütmektedirler. Özellikle 1990 sonrası yaşanan gelişmeler ve yaygınlaşan internet kullanımı ile güvenlik stratejilerinde siber güvenliğe de yer vermişlerdir. Genel anlamda bu stratejiler ulusal güvenliği sağlamak, kritik altyapıları korumak, hassas bilgileri güvende tutmak ve siber tehditlere karşı etkili bir mücadele yürütmek amacını taşımaktadır.

Siber savunmanın gündeme gelmesinde siber alanda yaşanan saldırı içerikli gelişmelerin etkisi oldukça büyük olmuştur. Siber suçlar, siber casusluk ve siber çatışmalar adına örnekler bulunmaktadır. Bu tarz saldırıların yaşanmış olması ve beraberinde yaşanabilecek olmasına dair öngörüler siber savunmanın gerekliliğini göstermektedir.

Tablo 4: Siber Suç ve Siber Casusluk

Olayın Adı	Olayın Gerçekleştiği Yıl	Açıklama	Suçlular
414'lerde hırsızlık olayları	1982	ABD'de yüksek profilli bilgisayar sistemlerine izinsiz girişler	Milwaukee'den on altı yaşındaki hackerler
Hanover Hackerları (Cuckook Egg)	1986-1988	ABD'de yüksek profilli bilgisayar sistemlerine izinsiz girişler	KGB tarafından işe alınan Alman hacker
Roma Laboratuvarı olayı	1994	ABD'de yüksek profilli bilgisayar sistemlerine izinsiz girişler	İngiliz genç hackerler
Citibank olayı	1994	Citibank'tan 10 milyon dolar çalındı ve para dünyanın dört bir yanındaki banka hesaplarına aktarıldı	Rus hackerler
Güneşin Doğuşu	1998	Savunma Bakanlığı bilgisayar ağlarına bir dizi saldırı	Kaliforniya'dan iki genç hacker
Ay Işığı Labirenti	1998	Yüksek profilli bilgisayar sistemlerinin incelenmesinin patlaması	RF'ye atfedilmiştir
Titan Yağmuru	2003	ABD'deki yüksek profilli bilgisayar sistemlerine erişim	ÇHC'ye atfedilmiştir
Zeus Bot Ağı	2007	Truva atı Zeus, 196 ülkede milyonlarca makineyi etkilemiştir	Uluslararası siber suç ağında, sadece ABD'de 90'dan fazla kişi tutuklandı
GhostNet	2009	Siber casusluk operasyonu, 103 ülkedeki yüksek değerli siyasi, ekonomik ve medya merkezlerine sızma	ÇHC'ye atfedilmiştir

Tablo 4: (Devamı)

Olayın Adı	Olayın Gerçekleştiği Yıl	Açıklama	Suçlular
Aurora Operasyonu	2009	Yüksek teknoloji, güvenlik ve savunma şirketlerinin kaynak kodu havuzlarına erişim sağlamak ve potansiyel olarak bunları değiştirmek için Google ve diğer şirketlere yönelik saldırılar	ÇHC'ye atfedilmiştir
Wikileaks Cablegate	2010	28 Aralık 1966 ile 28 Şubat 2010 tarihleri arasında dünyanın dört bir yanındaki 274 ABD büyükelçiliğinden sızdırılan 251.287 gizli diplomatik yazışma	Wikileaks, kâr amacı gütmeyen aktivist kuruluş
Operasyonların İntikam ve Assange'ın İntikamı	2010	İnternet korsanlığı karşıtlarına ve Wikileaks davranışı sergilediği düşünülen şirketlere yönelik koordineli, merkezi olmayan saldırılar	Anonymous, hacker topluluğu
Sony ve şirketlerin yanı sıra hükümet saldırıları	2011	Çok ses getiren bilgisayar korsanlığı operasyonları	LuleSec, hacker kolektifi
CO2 Yayılım Belgelerinin Çalınması	2011	6,9 milyon € veya 9,3 milyon $ değerinde 475.000 karbondioksit emisyon hakkının çalınması	Organize siber suçlarla ilişkilendirildi (amaç muhtemelen kara para aklama)
NSA ifşaları	2013	ABD hükümetinin takip programlarının kapsamını gösteren gizli bilgilerin siber yollarla sızdırılması	ABD Ulusal Güvenlik Ajansı (NSA)
Sony Pictures Hacklendi	2014	Sony International'a yönelik bir dizi bilgisayar korsanlığı ve veri yayını (Kuzey Kore lideri Kim Jong Un'un vahşice ölümünü gösteren) The Interview filminin iptaliyle sonuçlandı	Kuzey Kore'ye atfedildi (Şüpheli)

Kaynak: Cavelty M. D., 2015

Dünya genelinde dijital ortamda yaşanan siber saldırılar ve olası siber savaşlar tehdit unsuru oluşturmaktadır. Tehdidin var olduğu yerde savunma sistemleri geliştirmek en makul çözümlerden biri olacaktır. Siber savunma yöntemleri dijital alandaki olası saldırılara karşı önlem alınabilir, güvenlik önlemleri uygulanabilir ve saldırıları tespit etmek ve karşı koymak için uygun teknolojiler kullanılabilir. Siber savunma stratejileri, bilgi güvenliği politikalarını oluşturma, güvenlik açıklarını tespit etme ve kapatma, zararlı yazılımları tespit etme ve engelleme gibi çeşitli alanlarda destek olabilecektir.

Siber saldırıların kesin olarak engellenmesi mümkün olmasa bile siber savunma mümkün olabilmektedir. Bilgisayarlardaki zararlı yazılımları engellemek için kullanılan antivirüs programları, kurum ve kuruluşlarda verilen eğitimler sayesinde güvenilir personeller yetiştirmek, siber istihbarat sistemleri sayesinde saldırıları kontrol altında tutabilmek, iş birliği ve çeşitli koordinasyonlar ile siber savunma etkili hale gelebilmektedir.

2.2.5.1. Ulusal Siber Savunma Stratejisi Oluşturma

İnternet kullanımında yaşanan artış ile paralel olarak siber güvenlik açısından tehditler de artış göstermiştir. Çoğalan siber saldırılar bireylerin günlük yaşantısını, kişisel verileri, devletlerin sırlarını, ekonomiyi tehdit etmektedir. Bu bağlamda dünya çapında devletler siber güvenlik konusunda önlem almak için çeşitli stratejiler geliştirmiştir. Siber güvenlik stratejileri genel anlamda siber tehditlerden, saldırılardan korunmayı amaçlamaktadır. Bu stratejiler ile siber saldırılar tespit edilip önlenebilir ve saldırılara müdahale edilebilir. Bu sayede kuruluşların bilgi varlıklarını korunabilir, güvenlik sağlanabilir ve siber saldırılara karşı dirençli hale getirilebilir.

Siber güvenlik stratejileri bilgi teknolojisi altyapısını korumak için sürekli olarak güncellenebilmektedir. Çünkü internet ortamı hızla gelişen bir yapıdadır. Bu yüzden ihtiyaçlar değişebilmektedir. Stratejiler de güncel durumlara göre tasarlanabilmektedirler. Her ülke kendi ihtiyacına göre siber güvenlik stratejilerini oluşturmuştur. Örneğin Türkiye'nin Siber Güvenlik çalışmaları 1990'lardan sonra gündeme gelmiş bir alanıdır. Ulaştırma ve Altyapı Bakanlığı tarafından yayınlamış olan üç adet Ulusal Siber Güvenlik Stratejisi ve Eylem Planı vardır. İlk Ulusal Siber Güvenlik Stratejisi ve Eylem Planı 2013-2014 yıllarını kapsamaktadır. İkinci Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ise 2016-2019 yıllarını kapsamaktadır. Üçüncü ve en son yayınlanan Ulusal Siber Güvenlik Stratejisi ve Eylem Planı ise 2020-2023 yıllarını kapsamaktadır. Ulusal Siber Güvenlik Stratejisi ve Eylem Planları ülkedeki siber güvenliği artırmaya odaklanmıştır. Planların amacı, kamusal bilgi teknolojilerinin ve sistemlerinin güvenliğini sağlamak, kamusal kritik altyapıların ve ilişkili sistemlerinin güvenliğini sağlamak ve siber saldırılar sonucunda zarar gören sistemlerin normal işleyişlerine dönmesini sağlamak için altyapı çalışmaları yapmaktır. Bu amaçlar doğrultusunda, siber saldırılara karşı önleyici tedbirler alınması, kritik altyapıların korunması ve saldırı sonrası iyileştirme çalışmalarının koordine edilmesi hedeflenmiştir (Kurnaz ve Önen, 2019). Siber güvenlik ulusal güvenlik stratejilerinin bir parçası haline gelmiş olup gerekli savunma stratejileri oluşturulmuştur.

ABD'nin siber güvenlik stratejisinin belirlenmesinde önemli bir rol oynayan başkanlık direktifleri arasında 1995 yılı temmuz ayında yayınlanan 13010 numaralı Başkanlık Direktifi bulunmaktadır. Dönemin ABD Başkanı Bill Clinton, ülkenin kritik altyapılarına yönelik potansiyel bir siber saldırıya karşı hazırlıklı olunması için başsavcılık makamını görevlendirmiştir. Bu görev doğrultusunda Kritik Altyapıları Koruma Komisyonu oluşturulmuştur. 1997 mayıs ayında yayımlanan 63 Numaralı Başkanlık Direktifi ise ABD'nin kritik altyapılarını tanımlayan ilk resmî belgedir. 2003 şubatında Siber Uzay'ın Korunmasına Yönelik Ulusal Strateji adlı belgede yine konu ABD'nin kritik alt yapılarını korumaya yönelikti (Darıcılı, 2017). 2009 yılında Başkan Barack Obama'nın isteği üzerine yayınlanan Siber Uzay Politika Revizyonu Belgesi ABD'nin siber savunma sistemindeki görevli resmi kurum ve kuruluşların federal ve yerel düzeydeki yapısını eleştirmiştir. Mayıs 2011'de ise ABD Başkanı Barack Obama'nın isteği üzerine yayınlanan Siber

Uzay İçin Uluslararası Strateji: Ağlanmış Bir Dünya'da Refah, Güvenlik ve Açıklık adlı belge, ABD'nin uluslararası alandaki siber uzay politikasını tanımlar niteliktedir. Bu belgede ABD yönetiminin gelecekte uluslararası düzeyde siber suçlarla mücadele etmek için çaba harcayacağı, internetin yaygınlaşmasını ve uluslararası iş birliğiyle yönetilmesini destekleyeceği, internet özgürlüğünü temel bir öncelik olarak benimsediği ve ekonomik refah için bilgi teknolojilerinin geliştirilmesinin önemine vurgu yapıldığı ifade edilmiştir (Office, 2011).

Siber güvenlik önlemleri yaşanan gelişmelere denk olarak geliştirilebilmektedirler. ABD'nin kritik altyapılarına yönelen siber saldırıların yoğunlaşmasının ardından Obama yönetimi 12 Şubat 2013 tarihinde Kritik Altyapı Güvenliğini İyileştirmeye Yönelik Strateji Oluşturma Başkanlık Emri'ni yayınlamıştır. Bu direktif doğrultusunda 12 Şubat 2014 tarihinde Kritik Altyapı Güvenliğini İyileştirmeye Yönelik Taslak Strateji adlı bir plan hazırlanmıştır. Bu plan özel sektör ve resmî kurumların iş birliği yaparak kritik altyapıların korunması için ortak standartlar ve metodolojiler geliştirmeyi hedeflemektedir. 2015 yılında ise ABD Savunma Bakanlığı Siber Strateji Belgesi yayınlanmıştır. Genel anlamda bu belgenin amacı siber savunma alanlarına yön göstermektir (Darıcılı, 2017). 2018 yılında yayınlanan Ülkenin Siber Güvenlik İşgücünün Büyümesini ve Sürdürülmesini Desteklemeye İlişkin Başkana Rapor: Daha Güvenli Bir Amerikan Geleceğinin Temelini Oluşturmak belgesi ile kritik altyapılar ve siber güvenlik güçlendirilmek amaçlanmıştır. Özellikle siber güvenlik iş gücünün gelişmesi ve bu alanda yapılan eğitimler konu olmuştur (U.S. Department of Commerce, 2018).

Siber tehditlerden korunmak için siber güvenliğin sağlanması önem arz etmektedir. Kişisel verilerin korunması, ticaret, devlet sırlarının açığa çıkmasının engellenmesi ve devletlerin güvenlik duvarlarının korunması gibi güvenlik teşkil eden durumlar açısından siber güvenlik çok önemlidir. Siber saldırıların zaman ve mekân tanımaksızın gerçekleştirilebiliyor oluşu, devletlerin siber güvenlik açısından almaları gereken önlemlerin sıkı olmasının gerekliliğini göstermektedir. Nitekim ulusal siber güvenlik stratejisi, bir ülkenin siber uzayda karşılaştığı tehditlere yanıt vermek, siber altyapıları korumak, siber saldırıları önlemek ve etkili bir şekilde mücadele etmek için belirlenen bir plan ve politikaların bütününü karşılamaktadır. Bu bağlamda siber uzayda yaşanan gelişmelerin hızına uyum sağlayabilecek biçimde ulusal siber güvenlik stratejisinin sürekli güncellenmesi ve yeniden değerlendirilmesi gerekebilir. Bu sayede daha başarılı olabilecektir. Ayrıca, uluslararası standartlara uyum sağlaması önemlidir, çünkü siber tehditler genellikle sınırları aşar özelliktedir. Bu noktada küresel bağlamda devletler ulusal siber güvenlik stratejilerinin dışında uluslararası örgütler bağlamında iş birliği ile siber güvenlik stratejileri sağlayabilmektedirler.

2.2.5.2. Uluslararası Örgütler Açısından Siber Strateji Tartışması

Günlük yaşamın bir gerçeği olarak kabul edilen siber uzayın önemi artmaktadır. Önemli olduğuna dair görüşler uluslararası alandaki aktörler tarafından da kabul görmektedir. Elbette siber

stratejilerin karmaşık ve sofistike niteliği uluslararası örgütler bağlamında strateji açısından ele alınması gereken bir unsur olabilmektedir. Bunun yanında uluslararası örgüt bünyesindeki üye devletlerin siber strateji bağlamında çeşitli çıkarlarının dengeli oluşu oldukça önemlidir. Bu açıdan bakıldığında uluslararası örgütlerin siber stratejileri bütün üye ülkelerin çıkarlarını göz önünde bulundurularak hazırlanmalıdır.

Teknolojideki hızlı gelişmeler ve bu teknolojilerin devletler, kuruluşlar ve bireyler arasındaki ilişkilere etkisi, siber uzaydaki uluslararası ilişkilerin karmaşıklığını ve önemini artırmaktadır. Bu alandaki sürekli değişim ve dönüşüm, uluslararası ilişkilerin dinamiklerini derinden etkilemektedir. Siber uzay artık sadece bilgi alışverişi veya ticaret platformu değil, aynı zamanda devletler arası güç mücadelelerinin ve çatışmalarının da yaşandığı bir saha haline gelmiştir. Bu nedenle siber uzayda uluslararası ilişkilerin incelenmesi ve anlaşılması her zaman ilginç ve zorlu bir konu olmaya devam edecektir.

iber uzayda stratejik hakimiyet henüz sağlanamamıştır, çünkü birçok uluslararası kuruluş siber uzayda varlığını ve hareket etme isteklerini göstermiştir. Bu durum siber uzayın çok kutuplu boyutunu ortaya koymaktadır; burada tek bir hakimiyet veya blok bölünmesi pek olası görünmemektedir. Bunun temel nedenleri, savunma sistemlerinin birbirine bağlanması durumunda karşılıklı güvensizlik ve casusluk endişeleridir. Dolayısıyla, etkili bir savunma oluşturulması için önleme, uluslararası iş birliği ve uluslararası kabul görmüş, yasal olarak bağlayıcı normların benimsenmesi kritik öneme sahiptir. Siber terörizm ve suçun artışıyla birlikte siber saldırılara karşı savunma için sistematik eğitim düzenlenmesi ve operasyonel askeri, istihbarat, polis ve sivil merkezlerin güçlendirilmesi gerekmektedir. Bu bağlamda etkili savunma stratejilerinden biri olarak uluslararası örgütler ve siber savunma stratejileri önem arz etmektedir (Duić vd., 2017).

Uluslararası örgütlere üye her ülke kendi ulusal siber güvenlik stratejisini öncelik alacaktır. Bu bağlamda etkili ve ortak bir siber savunma stratejisi için iş birliği önemlidir. Siber saldırıların her an gelişmesi ile stratejilerin de sık sık güncellenmesi gerekebilmektedir. Nitekim örgüt bünyesinde bulunan her ülkeye uygun şekilde yaşanan gelişmeler de güncellenmelidir. Bu da birtakım zorluklara yol açabilmektedir. Aynı şekilde siber stratejiler için ciddi finansal yatırımlar gereklidir. Örgüt üyelerinin ortak bir siber strateji oluşturabilmeleri için yatırım anlamında her bir devletin yeteri düzeyde bütçe ayırması gerekmektedir. Bu anlamda bakıldığında finansal düzeyde de birtakım zorluklarla karşı karşıya kalınabilir. Fakat ortak tehditlere karşı koordinasyon oluşturup önlemler alınmak isteniyorsa tüm bu sorunların ortak bir çözüme ulaşması için her ülke çaba gösterebilmektedir. Bu sayede siber stratejiler etkili olabilecek, örgütlere ve üyelerine fayda sağlayabilecektir.

ÜÇÜNCÜ BÖLÜM

3. NATO VE SİBER GÜVENLİK POLİTİKALARI AÇISINDAN DEĞERLENDİRME

Teknolojinin hızla gelişimi son yıllarda küresel çapta büyük etki oluşturmuştur. Siber alanın aktif olarak kullanımı bu alanın birtakım tehlikeler barındırmasına da neden olmuştur. Bu bağlamda bir aktör olarak NATO gelişmeleri yakından takip etmektedir. NATO siber alanda güvenlik sağlayabilmek için eğitim, tatbikatlar ve ortaklıklar gibi çalışmalar yapmaktadır. Bu sayede müttefiklerine ve birliğe güvenlik sağlayabilirken aynı zamanda uluslararası güvenliğe de katkı sağlayabileceğini düşünmektedir.

3.1. NATO ve Uluslararası Güvenlik

NATO uluslararası savunma ittifakı olarak 4 Nisan 1949'da Washington'da imzalanan Kuzey Atlantik Antlaşması ile kurulmuştur. Bahsi geçen zaman Doğu-Batı gerilimlerinin yüksek olduğu bir dönem olarak bilinmektedir. NATO da buna istinaden doğmuş bir ittifaktır. Çünkü üye ülkeler Sovyet yayılmacılığının oluşturduğu tehdide karşı ulusal güvenliklerini ve siyasi demokrasilerini korumak için birlikte hareket etmişlerdir (Miller, 1989). Kurulduğu zamanlardan günümüze kadar NATO, Sovyetler Birliği (SB)'ne karşı caydırıcı bir rol oynamış ve 1991'de SB'nin çöküşünden sonra örgüt dünya çapında birçok operasyonda yer almıştır.

Birliğin asıl amacının çatışmalardan kaçınarak güvenliği esas almak olduğu söylenebilmektedir. Aslında bu paktın düşüncesine göre müttefiklerden birine yönelik yapılan bir saldırı, herkes için yapılmış bir saldırı olarak kabul edilir ve bu saldırganlığa karşı durmayı amaçlar niteliktedir (NATO H. O., 2022). NATO kuruluşundan bu yana Soğuk Savaş, 1989'da Berlin Duvarı'nın yıkılması, Aralık 1991'de SB'nin dağılması, Varşova Paktı'nın sona ermesiyle sonuçlanan sürecin taraflarından birisi olmuştur. Ayrıca Avrupada barışı koruma operasyonları ve 11 Eylül saldırıları gibi çağdaş zamanlardaki diğer önemli olaylar da tarihsel gelişimi açısından önemli duraklardır (Weaver, 2021: 13). İlk kurulduğunda 12 ülkeden (Belçika, Kanada, Danimarka, Fransa, İzlanda, İtalya, Lüksemburg, Norveç, Portekiz, Hollanda, Birleşik Krallık ve ABD) oluşan siyasi-askeri bir ittifak olan NATO, 2024 yılında İsveç'in de katılımı ile bugün 32 üye ülkeyi bünyesinde barındırmaktadır. Aşağıdaki tabloda birliğin üye ülkeleri ve katılım yılları yer almaktadır.

Tablo 5: NATO'ya Üye Ülkeler ve Katılım Yılları

Üye Ülkeler	Katılım Yılları
Amerika Birleşik Devletleri	1949
Birleşik Krallık	1949
İzlanda	1949
Belçika	1949
Danimarka	1949
Fransa	1949
Hollanda	1949
İtalya	1949
Kanada	1949
Lüksemburg	1949
Norveç	1949
Portekiz	1949
Türkiye	1952
Yunanistan	1952
Almanya	1955
İspanya	1982
Çekya	1999
Macaristan	1999
Polonya	1999
Bulgaristan	2004
Estonya	2004
Letonya	2004
Litvanya	2004
Romanya	2004
Slovakya	2004
Slovenya	2004
Arnavutluk	2009
Hırvatistan	2009
Karadağ	2017
Kuzey Makedonya	2020
Finlandiya	2023
İsveç	2024

Kaynak: NATO, 2024

Temel hedefi üye ülkelerin savunma sistemlerini güçlendirmek, saldırganlığı caydırmak ve uluslararası barışı korumak olan NATO için uluslararası arenada güvenli ortamın sürdürülmesi önemli bir husustur. Bu bağlamda özellikle üye ülkeler arasındaki askeri iş birliği koordinesinin başarıya ulaşması NATO'nun hedeflerini gerçekleştirmesinde önemli bir adımdır. Uluslararası ortamda barışın korunması ve güvenlikli alanın istikrarı için iş birliği gerekli görülmektedir. Bu açıdan bakıldığında NATO uluslararası güvenliğe büyük ölçüde katkı sağlayan bir birliktir. Özellikle Soğuk Savaş'ın kazanan tarafı olarak nitelenen NATO, Soğuk Savaş sonrası dönemde de uluslararası alanda güvenlik temelli gelişmeleri yakından takip edip ilgi alanını buna göre genişletmiştir. Yani

NATO doğduğu andan günümüze süregelen zaman diliminde uluslararası güvenlik konuları ile yakından ilgilenmiştir. Stratejileri de bu doğrultuda güncellenmiştir.

3.1.1. NATO ve Stratejik Konseptler

NATO güvenlik ekseni etrafında yaşanan gelişmeler doğrultusunda kuruluşundan bu yana stratejik konseptler geliştirmiştir. Bu bağlamda Soğuk Savaş'ın sona ermesi ile dünya genelinde değişen ve gelişen güvenlik alanlarına uyum sağlamaya çalışmıştır. Birlik üye ülkeler arasındaki iş birliğini ön planda tutarak çeşitli güvenlik tehditlerine karşı etkili bir mücadele için sürekli gelişim sağlamaktadır. Kurulduğu tarihten günümüze NATO'nun toplamda sekiz adet stratejik konsepti bulunmaktadır.

NATO'nun birinci stratejik konseptine[2] 1 Aralık 1949 yılında imza atılmıştır. İlk stratejik konsept (DC 1/6), NATO'nun ideallerini tanımlamaktadır. Hedefleri arasında, Kuzey Atlantik Antlaşması'nın amaçlarına ulaşmak için antlaşma taraflarının siyasi, ekonomik ve psikolojik araçların yanı sıra askeri araçları da entegre etmek bulunmaktadır. Ayrıca, savaşın önlenmesi ön planda tutulup olası bir savaş durumunda ortak bir savunma koordinesi kapsamlı bir şekilde planlanmıştır. Bu kapsamlı yaklaşım coğrafi konum, endüstriyel kapasite, nüfus ve üye ülkelerinin askeri yeteneklerine dayanarak her ülkenin katkısının orantılı olması gerektiğini kabul eder niteliktedir. Amacı ise çaba, kaynak ve insan gücü ile yeterli askeri kapasiteyi sağlamaktır. Her ülkenin kendi savunmasını sağlamak ve ortak savunmaya katılmak amacıyla askeri gücünü maksimum seviyede geliştirmesi arzu edilmektedir. Bu sayede barış güvence altına alınabilecek ve saldırıya uğrama olasılığı en aza indirgenebilecektir. Bu plan 1950 ocak ayında kabul edilmiştir (NATO Strategic Concepts, 2022).

NATO tarafından 1952 Aralık ayının üçüncü gününde kabul edilen ikinci stratejik konsept, NATO'nun konvansiyonel kuvvetleri ekseninde, Sovyetlerin oluşturduğu alternatif tehditleri ele alacak şekilde hazırlanmıştır. Bu bağlamda Sovyet tehdidinin arttığı değerlendirilerek, Müttefik Kuvvetler Merkezi Komutanlığı (The Allied Forces Central Command), Müttefik Güney Komutanlığı (Allied Forces South) ve Müttefik Kuzey Komutanlığı (Allied Forces North) olarak üç adet bölgesel düzeyde yetkilendirilmiş komutanlık oluşturulmuştur (NATO Bucharest Summit Declaration, 2008).

[2] DC 6/1, mümkün olduğunca doğu coğrafyasına uzanan bir savunma gerekliliğini açıkça belli etmektedir. Her ne kadar belirsiz bir Sovyet tehdidine işaret edilse belirli roller ve sorumluluklar da betimlenmiştir. Örneğin ABD, belirgin bir şekilde nükleer savunmayı sağlama sorumluluğunu üstlenmiştir. Ancak DC 6/1'in temelinde, ekonomik istikrar ve iyileşmenin önemi de vurgulanmıştır. Dwight D. Eisenhower'ın merkezi komutası altında bütünleşmiş bir NATO askeri yapısının oluşturulması, bir sonraki stratejik kavrama şekil vermiştir (NATO Strategic Concepts, 2022).

NATO 9 Mayıs 1957 tarihine gelindiğinde üçüncü stratejik konseptini[3] kabul etmiştir. Bu konsept Batı Avrupa'ya yönelik bir saldırıyı önlemek için, nükleer silahların ilk kullanımını içeren büyük bir nükleer misilleme tehdidiyle caydırma stratejisi benimsemektedir (Davis, 2010). Bu strateji, Batı Avrupa'nın güvenliğini sağlamak ve bölgesel istikrarı korumak amacıyla bir dizi politika ve adımları içermektedir.

12 Aralık 1967 tarihinde NATO dördüncü stratejik konseptini[4] onaylamıştır. MC 14/3 Batı Avrupa'da ileri savunma pozisyonunu korurken nükleer ve konvansiyonel güçlerin dengelenmesi yoluyla sınırlı savaşa olanak tanıyan bir stratejiyi benimsemiştir. MC 14/3 tırmandırıcı tepkilere izin verecek şekilde istişareye hazır ve ileri konuşlandırılmış bir kuvvet oluşturulmasını önermiştir (NATO Strategic Concepts, 2022).

Soğuk Savaş'ın sonuna gelindiğinde ve Berlin Duvarı yıkıldıktan sonra SB, Doğu Avrupa alanından çekilmiş ve Varşova Paktı dağılmıştır. Yaşanan bu gelişmeler neticesinde güvenlik alanında değişimler gündeme gelmiştir. Doğrudan askeri saldırı riskleri azaldığı için NATO için 1991 tarihinde yeni bir stratejik konsept fikri oluşmuştur. 1991 tarihli yeni stratejik konsept ile NATO, krizlere karşı etkili mücadele ve çatışmaların önlenmesine odaklanarak görüşmeler ve iş birlikleri yolu ile ilerlemeyi teşvik etmiş ve üyelere askeri olmayan araçları kullanarak kolektif güvenlik endişelerini giderme çağrısında bulunmuştur.

Soğuk Savaş sonrası genişleyen güvenlik algısı ile yalnızca askeri güvenlik değil ticari, sağlık, eğitim, siber ve sosyal konuları kapsayan birçok güvenlik unsuru gündeme gelmiştir. Bu sayede güvenlik algısı geniş bir alana yayılmıştır. NATO, 1991 tarihli beşinci stratejik konseptinde gündeme getirdiği güvenlik yaklaşımı ile yaşanan gelişmelere entegre olduğunu göstermiştir. Daha önce onaylanan dört stratejik konsepti ile farkı gözle görülür niteliktedir. Fakat yine de askeri güvenliği göz ardı etmiş değildir. Yalnızca askeri güvenliğe ek olarak diğer güvenlik konuları ile de ilgilendiğini belli etmiştir.

Nisan 1999'da Washington'da gerçekleştirilen zirve toplantısında NATO devlet ve hükümet başkanları ittifakın yeni stratejik konseptini (SC-99) onaylamışlardır. Bu altıncı stratejik konseptin amaçları genel anlamda NATO'nun odak noktasını korur niteliktedir. Yani önceliği üye devletlerin güvenliğini kontrol altında tutmaktır. Bunun dışında, küresel olarak kitlesel göç ve organize suçlar gibi geleneksel olmayan sorunların artarak yayıldığı kabul etmiştir. Bu tehditlerin önlenmesi ve kontrol altına alınması gerekliliği açık bir şekilde gündeme gelmiştir. SC-99, Avrupa'daki

[3] ABD politikasının bir uzantısı olarak MC 14/2 sınırlı savaş kavramını reddetmiş ve caydırıcılık stratejisinde temel bir değişikliğe işaret etmiştir. Bu yaklaşım caydırıcılığın başarısız olması durumunda karşılaşılacak riskleri en aza indirgeme amacını taşır (NATO Strategic Concepts, 2022).

[4] Bu konseptin oluşturulmasında Fransa'nın NATO'nun bütünleşmiş askeri yapısından çekilmesi etkili olmuştur (NATO Strategic Concepts, 2022).

güvensizlik ve istikrarsızlık risklerinin yayılma potansiyelini kabul ederek, 5. Madde dışı durumlar ile de ilgilenmiştir. Buna neden olarak, çatışma önleme ve kriz yönetimi gibi alanlarda proaktif yaklaşımlarla güvenlik ve istikrarı artırma hedefi gösterilmiştir. Müttefiklerin topraklarının ötesinde operasyonların gerekliliğini kabul eden SC-99, Birleşik Ortak Görev Gücü (CJTF) oluşturulmasını önermiştir. Stratejik nükleer kuvvetlerin en yüksek güvenlik garantisi olarak kalması kararlaştırılmıştır. Ayrıca SC-99 çok uluslu diyalog yoluyla iş birliğine dayalı ortaklıkların kurumsallaşmasını sağlamıştır[5]. Bu Kuzey Afrika ve Ortadoğu'daki devletlerle iş birliği için forumlar oluşturulması ve NATO'ya katılmanın liberal demokrasilerin gelişimine destek sağlayacağına dair iddiaların güçlendirilmesiyle gerçekleşmiştir. İttifakın Avrupa devletlerine standart bir üyelik yol haritası sunmanın yanı sıra, Barış İçin Ortaklık Programı'nı farklı sosyal ve siyasi eğilimlere uyum sağlayacak şekilde yeniden şekillendirmiştir (NATO The Alliance's Strategic Concept, 1999).

2010 yılında Lizbon Zirvesi'nde devlet ve hükümet başkanları tarafından onaylanmış olan yedinci stratejik konsept 21. yüzyılın güvenlik sorunlarını ele alarak güncellenmiş güvenlik stratejileri barındırır özelliktedir (NATO, Strategic Concept, 2010: 35). NATO'nun üye ülkelerin güvenliğini sağlamak için aldığı çeşitli önlemler arasında şunlar bulunmaktadır;

- Nükleer ve konvansiyonel kuvvetlerin dengeli bir karışımı korunacak.
- Toplu savunma ve krizlere tepki amaçlı büyük çaplı müşterek operasyonları ve daha küçük operasyonları aynı anda yürütme yeteneğini sürdürecek.
- NATO sorumluluklarını ve NATO Mukabele Kuvveti dahil tüm alan dışı operasyonları yürütebilecek konvansiyonel kuvvetler geliştirecek.
- Savunmada eğitim, tatbikat, acil durum planlama ve bilgi alışverişini sağlayarak tüm müttefiklere destek sağlayacak.
- Mümkün olduğunca çok sayıda müttefik ülkenin toplu savunmada nükleer rollerin planlanmasına katılmasını sağlayacak.
- Balistik füze saldırılarına karşı savunma yeteneklerini geliştirecek, RF ve diğer Avrupa-Atlantik ortaklarla iş birliği yapacak.
- Kimyasal, biyolojik, radyolojik ve nükleer kitle imha silahları tehdidine karşı savunma yeteneğini artıracak.
- Siber saldırılara karşı önleme, fark etme, koruma ve toparlanma yeteneklerini geliştirecek ve NATO'nun planlama sürecinden yararlanacak.
- Uluslararası terörizmi tespit etme ve buna karşı savunma yeteneklerini güçlendirecek.

[5] İttifakın yeni üyeliklere açık olduğundan bahsetmesi ve SB'nin dağılmasından sonra ondan kopan ülkelere dolaylı olarak bu yönde çağrı yapılması ilgi çekici bir husus olmuştur. Bu çağrılar sonucunda konseptin imzalandığı 24 Nisan 2009 tarihinden günümüze dek toplam 11 ülke NATO üyesi haline gelmiştir. Bu süre zarfında NATO'nun genişlemesi bölgesel istikrarın ve güvenliğin artırılmasına önemli bir katkı sağlamıştır. 2009 yılında Bulgaristan, Estonya, Letonya, Litvanya, Romanya, Slovakya ve Slovenya, Arnavutluk ve Hırvatistan, 2017 yılında Karadağ, 2020 yılında ise Kuzey Makedonya katılım sağlamıştır (Özer, 2021: 5).

- Kritik enerji altyapısı, transit bölge ve güzergahlarının korunmasına katkıda bulunacak.
- Yeni teknolojilerin güvenlik üzerindeki etkilerini değerlendirecek ve askeri planlamada potansiyel tehditleri göz önünde bulunduracak.
- Savunma harcamalarının düzeyi korunacak ve NATO tehditlere karşı koruma konusundaki genel tutumunu sürekli gözden geçirecek (NATO, Strategic Concept, 2010: 16-19).

11 Eylül 2001 saldırıları ittifakın yapısal, stratejik ve operasyonel açıdan dönüşmesine yol açmıştır. Bunu 2010 stratejik konseptinde de açıkça görmekteyiz. Özellikle saldırı zamanında NATO'nun 5. Maddesi'nin devreye girmesi üye ülkeler arasındaki dayanışmayı güçlendirmiştir. Bu madde, bir NATO üyesine yapılan saldırının diğer üyeleri de tehdit ettiğini doğrudan kabul etmektedir.[6] 2010 yılında yayınlanan bu konseptte NATO siber güvenlik konularını gündeme getirmiştir. Yeni güvenlik anlayışında teknolojinin de gelişmesi ile siber alan yeni bir güvenlik alanı olarak ortaya çıkmıştır. NATO bu gelişmelere paralel olarak stratejilerini güncellemiştir.

NATO'nun halihazırdaki son konsepti 29 Haziran 2022 yılında Madrid'deki zirvede kabul edilmiştir. Bu konsept gelişmelerden payını almıştır. RF'nin Ukrayna'ya yapmış olduğu saldırı sonucunda bir dizi önceliği de beraberinde getirmiştir. Konseptte bu önceliklerin ana hatları çizilirken öte yandan da Çin ve Hint-Pasifik bölgesindeki gelişmelerin de göz önüne alınması gerektiği vurgulanmıştır. Madrid'deki NATO zirvesinde ittifak üyeleri tarafından RF'nin artık ortak olarak kabul edilemeyeceği vurgulanmıştır. Bu karar Avrupa topraklarında büyük çaplı ve çok yönlü bir savaşın geri dönüşünün yansıttığı jeopolitik sarsıntının somut bir şekilde anlaşılmasına neden olmuştur. Bu noktada uluslararası ilişkilerdeki dinamiklerin ve güç dengelerinin nasıl şekillendiği önemli bir rol oynamaktadır (NATO 2022 Strategic Concept, 2022: 5-11)

NATO stratejik konseptinde belirttiği üzere üç ana görevi yerine getirmeye devam edecek: caydırıcılık ve savunma, krizleri önleme, yönetim ve işbirlikçi güvenlik. Bu görevler birbirini tamamlayarak tüm müttefiklerin kolektif savunma ve güvenliğini sağlamayı amaçlamaktadırlar. Aynı şekilde bireysel ve kolektif dayanıklılığını ve teknolojik üstünlüğünü artıracağından ve bu çabaların NATO'nun temel görevlerini yerine getirmek için hayati değer taşıdığından bahsetmiştir (NATO Strategic Concept, 2022: 3).

NATO 2022 stratejik konseptinde siber güvenliğin önemini vurgulamıştır. Uzay ve siber uzayın güvenli kullanımı için ve bu alanlara sınırsız erişimin sürdürülmesi için etkili caydırıcılık ve

[6] 2010 yılında onaylanmış olan stratejik konseptte NATO, ittifakın nihai sorumluluğunun Washington Antlaşması'nın 5. Maddesi'ni uygulamak olduğu belirtilmiştir. Bu madde uyarınca bir müttefike yapılan bir saldırı, tüm müttefiklere yapılmış gibi kabul edilir. İttifak üyelerinin topraklarını ve nüfusunu korumayı ve savunmayı sağlamalıdır. Herhangi bir müttefikin güvenliğine karşı bir tehdit olması durumunda NATO'nun kararlılığından şüphe edilmemelidir. Aynı zamanda 5. Madde kapsamında yer alan sorumlulukları yerine getirirken NATO'nun Mukabele Kuvveti dahil tüm alan dışı operasyonlarını yürütebilecek sağlam, hareket esnekliği olan ve kolayca konuşlandırılabilir konvansiyonel kuvvetlerin geliştirilmesi ve idame ettirilmesi için gerekli adımları atacağından bahsetmiştir (NATO, Strategic Concept: 2010: 15-16).

savunmanın kilit öneme sahip olduğundan bahsedilmiştir. Ayrıca uzay ve siber uzayda faaliyet gösterebilmek, mevcut tüm araçları kullanarak tüm tehdit yelpazesini tespit etmek, bunlara karşı koymak ve yanıt vermek gerekli görülmüştür. Tek bir kötü niyetli siber faaliyet veya düşmanca uzay operasyonunun silahlı saldırı seviyesine ulaşabilmesi ve 5. Madde'nin uygulanmasının ön görülmesi, siber saldırıların tıpkı konvansiyonel silahlar kadar tehlikeli olduğunun ve alınacak önlemlerin ciddiyetinin vurgulandığı görülmektedir.[7] NATO bu bağlamda uzaya ve siber uzaya olan bağımlılığını artırmak için dayanıklılığını da artıracağını belirtmiştir (NATO Strategic Concept, 2022: 7). Siber uzay ve gelişen teknolojiler NATO'nun stratejik ortamını da değiştirmiştir. NATO bu değişime yanıt olarak farklı oranlarda tehditleri ele almış ve onlara uygun stratejiler geliştirmiştir.

3.1.2. NATO'nun Uluslararası Güvenliğe Katkısı

NATO'nun genel anlamda üye ülkeler arasında savunma ittifakı oluşturarak toplumsal güvenliği ve istikrarı amaçlayan bir çabası vardır. Bunu sağlarken askeri iş birliği, savunma stratejilerinin geliştirilmesi ve kriz durumlarında yardımlaşma gibi unsurlar göz önüne alınmaktadır. Elbette 5. Madde'nin önemi yadsınamaz durumdadır. Çünkü NATO'nun temel ve kalıcı amacı, tüm üyelerinin özgürlük ve güvenliğini siyasi ve askeri yollarla korumaktır. Toplu savunma, ittifakın özünü ve üyeleri arasında dayanışma ve uyum ruhu oluşturmaktadır (NATO's purpose, 2023). Bu da çatışma çözümlerinde ve güvenliğin oluşmasında ortaklık ilkesinin önemini göstermektedir.

Uluslararası ilişkiler disiplini karmaşık ve değişken doğası itibariyle devletler arasındaki iş birliğini ve güvenlik çabalarını ön plana çıkarmaktadır. Bu doğrultuda NATO uluslararası güvenlik konusunda belirleyici bir rol oynamaktadır. NATO'nun uluslararası güvenliğe katkısı savunma ittifakının temel prensipleri ve faaliyetleri aracılığıyla açıkça görülmektedir. Bu durumu NATO'nun stratejik konseptlerinde de görmekteyiz. NATO stratejik konseptlerindeki hedeflerini ve güvenlik çalışmalarını dünya genelinde yaşanan güvenlik gelişmelerine paralel olarak güncellemiştir. Bu da NATO'nun uluslararası güvenlik konularına katkısını açıkça göstermektedir. Örneğin barışı koruma, kriz yönetimi, terörle mücadele, siber güvenlik, sağlık, insan hakları ve demokratik değerlerin korunması gibi konularda geniş perspektifte uluslararası güvenlik konularıyla ilgilenmiştir.

Birliğe üye ülkeler askeri iş birliği ve savunma entegrasyonu yoluyla güvenlik elde etmeye çalışmaktadırlar. Birlik, üye ülkelerin askeri yeteneklerini birleştirerek ortak savunma stratejileri geliştirmekte ve ortak askeri tatbikatlar düzenlemektedir. Bu sayede NATO ülkelerinin savunma kapasiteleri artarken öte yandan da ortak tehditlere karşı etkili bir savunma sağlayabilmektedirler.

[7] NATO'nun 2022 tarihli stratejik konseptte bahsettiği üzere askeri ve askeri olmayan tehditlere karşı ulusal ve ittifak çapında dayanıklılığı artırmak bir sorumluluk olarak görülmüştür ve Kuzey Atlantik Antlaşması'nın 3. Maddesi'ne dayandığı belirtilmiştir. Bu bağlamda NATO kritik altyapıları, tedarik zincirleri ve sağlık sistemlerini de içeren stratejik kırılganlıkları ve bağımlılıkları tespit edip azaltmak için çaba sarf edecektir. Enerji güvenliğini artırmak ve istikrarlı bir enerji arzı sağlamak için yatırım yapmak hedefleri arasındadır (NATO Strategic Concept, 2022: 7).

Özellikle soğuk savaş sonrası SB'nin dağılması üzerine NATO, dünyanın çeşitli bölgelerindeki güvenlik konularına yönelmiştir. Üstelik alan dışı olarak görülen birtakım bölgelerdeki sorunlara da karşılık vermiştir. Aşağıdaki tabloda NATO'nun uluslararası güvenliğe katkı sağlayan bazı operasyonları yer almaktadır.

Tablo 6: NATO'nun Bazı Operasyonları

Operasyon Bölgesi	Operasyon Yılı	Operasyon Nedeni
Kosova	1999	Kosova'da Sırp güçlerine karşı hava operasyonları düzenlemiştir. Bu operasyonlar, Sırp güçlerinin Kosova'daki etnik Arnavut nüfusuna yönelik baskılarına karşı bir müdahaledir.
Afganistan	2001	NATO, ABD liderliğindeki uluslararası koalisyonun bir parçası olarak Afganistan'a askeri operasyonlar düzenlemiştir. Bu operasyonlar Taliban rejimini devirmeyi ve terörle mücadele etmeyi amaçlamıştır.
Irak	2004	NATO Irak Hükümeti'ne destek amacıyla bir eğitim misyonu başlatmıştır. Ancak NATO'nun Irak'taki rolü, üye ülkeler arasında anlaşmazlıklar nedeniyle sınırlı kalmıştır.
Libya	2011	NATO, Libya'da Muammer Kaddafi rejimine karşı askeri operasyonlar düzenlemiştir. Bu operasyonlar Kaddafi'nin sivillere yönelik saldırılarına karşı bir müdahaledir ve BM Güvenlik Konseyi'nin bir kararıyla desteklenmiştir.
Somali	2008	NATO, Somali'de korsanlıkla mücadele amacıyla bir dönem deniz operasyonları düzenlemiştir.

Kaynak: NATO, 2023

3.1.3. NATO ve Bölgesel/Uluslararası Savunma Anlayışı

NATO'nun savunma anlayışı üye ülkeler arasından herhangi birine karşı yapılan bir saldırı durumunda ortak savunma taahhüdüne dayanmaktadır. Bu ilke NATO'nun en temel ilkesidir ve üye ülkelerin içlerinden birine karşı yapılan bir saldırıya birlikte tepki vermelerini ve ortaklaşa karar almalarını sağlar niteliktedir. Bu sayede kim olduğu fark etmeksizin müttefiklerden herhangi birine yönelik potansiyel tehditlerin caydırılması ve etkili bir şekilde karşılanması hedeflenmektedir. NATO'nun bölgesel savunma anlayışı özellikle Avrupa'nın güvenliğini ve istikrarını sağlamak üzerine odaklanmıştır. Soğuk Savaş döneminde Sovyet tehdidine karşı Batı Avrupa'yı korumak amacıyla kurulan NATO, günümüzde de Avrupa'nın çeşitli güvenlik zorluklarına karşı bir kalkan görevi görmektedir. Bu durum bölgesel istikrarın ve güvenliğin sağlanması için NATO'nun önemli bir rol oynamasını sağlamaktadır.

NATO bölgesel savunmaya önem verdiği kadar uluslararası alanda savunmaya da önem vermektedir. Özellikle Soğuk Savaş sonrası dönemde uluslararası alanda etkin bir birlik olmuştur. Uluslararası alanda yapmış olduğu operasyonlar ve stratejik konseptlerinde bahsetmiş olduğu konular arasında birliğin güvenliği kadar insan hakları, kadın hakları, terörizm gibi uluslararası alanları kapsayan güvenlik konularında savunma oluşturması NATO'nun kapasitesinin genişliğini ortaya koymaktadır.

NATO'nun bölgesel ve uluslararası güvenliğe katkıları oldukça fazladır. Aslında NATO'nun savunma alanını bölgeselden başlayıp uluslararası alana ilerlettiğini ifade edebiliriz. Çünkü NATO en başta Soğuk Savaş esnasında Sovyet genişlemesini engellemek ve Batı müttefiklerini iş birliği ile savunma içerisindeydi. Fakat Soğuk Savaş'ın bitmesiyle birlikte genişleyen güvenlik olgusunun da getirdiği ortamın etkisiyle NATO savunma alanını uluslararası alana genişletmiştir. NATO başlangıçta Batı istikrarını Avrupa'nın doğu bölgelerine genişleterek *bütün, özgür ve barış içinde* bir Avrupa ortamını hedeflemiştir. Bu hedefini ise eski rakipleri ile iş birliğini artırarak ve yeni üyeleri entegre ederek gerçekleştirmiştir. NATO'nun ortaklık programı, 1991'de Kuzey Atlantik İş birliği Konseyi'nin kurulmasıyla başlamış ve daha sonra Euro-Atlantik Ortaklık Konseyi olarak adlandırılmıştır. Bu konsey NATO ile üye olmayan ülkeler arasındaki danışma ve iş birliği için başlıca forum haline gelmiştir.

1994 yılında NATO, Euro-Atlantik ortak ülkeler arasında pratik ikili iş birliği programı olan programını tanıtmıştır. Bunun aracılığıyla NATO eski Varşova Paktı ülkelerine uzanarak bağımsızlıklarına ve demokrasiye geçişlerini istikrarlı hale getirmek, NATO üyeliğine olası hazırlıklarını yapmak ve Kuzey Atlantik Antlaşması'nın 10. Maddesi uyarınca katılamayan veya katılmak istemeyenler için bir model sunmayı amaçlamıştır (Olsen, 2020). NATO burada ülkeleri hem kendi bünyesinde güvenli hale getirmeyi hem de bağımsızlıklarını korumayı amaçlamıştır.

NATO ayrıca Balkanlar'daki çatışmalara son vermek için çeşitli operasyonlar yürütmüştür. Başta Bosna-Hersek olmak üzere alan dışı operasyonlar gerçekleştirmiştir. 1995 yılında gerçekleştirilen operasyonunda NATO, ağustos ve eylül aylarında iki haftalık destek sağlamıştır. Dayton Anlaşmaları ve İcra Gücü aracılığıyla sürece daha fazla katılım sağlamış, bunu Stabilizasyon Gücü ve ardından şu anki NATO Karargâhı, Saraybosna'daki danışmanlık ekibi izlemiştir. NATO 1999'da Kosova'daki dramı durdurmak için askeri müdahalede bulunmuştur. 78 gün süren hava operasyonları devam ederken 50. yıldönümünde Çek Cumhuriyeti, Macaristan ve Polonya'yı bünyesine üye olarak kabul etmiştir (Olsen, 2020).

1990'larda NATO'nun odak noktası kriz yönetimi, işbirlikçi güvenlik gibi görevlere doğru değişmiştir. 11 Eylül 2001'deki saldırıların ardından NATO'nun Kuzey Atlantik Antlaşması'nın 5. maddesini ilk kez devreye sokmuş olması önemli bir gelişme olmuştur. NATO üyeleri ve ortak ülkeler terörizmle mücadele etmek için Afganistan'da birlikte hareket etmişlerdir. RF'nin Ukrayna'nın toprak bütünlüğünü ihlal etmesi ittifak üyelerini birbirine yakınlaştırmıştır. 2016 Varşova Zirvesi'nde müttefikler Estonya, Letonya, Litvanya ve Polonya'ya dönüşümlü olarak çok uluslu savaşa hazır birlik konuşlandırarak NATO'nun doğu kısmındaki askeri varlığını arttırmayı kabul etmişlerdir. Ayrıca, NATO Baltık Denizi'ndeki varlığını da artırmıştır. 2018 Brüksel Zirvesi'nde NATO liderleri ittifakın komuta yapısının güncellenmesini başlatmıştır. Bunun dışında NATO'nun siyasi liderleri NATO Hazırlık Girişimi 4-30'u (NRI) başlatmıştır (Olsen, 2020).

NATO Soğuk Savaş dönemi ve sonrası dönemde önemli olaylarla dönüşümler yaşamış olan bir ittifaktır. Sovyet genişlemesini durdurmak ve Avrupa'da güvenliği sağlamak amacıyla kurulan birlik zaman içerisinde kendisini ve potansiyelini genişletmiştir. Bu da birliği bölgesel savunmaya verdiği önemi uluslararası savunmaya da verir şekilde yorumlamayı sağlamıştır. NATO'nun bölgesel ve uluslararası savunma anlayışı gelecekte yaşanan gelişmeler ile bunlara nasıl uyum sağlayacağına bağlı kalacaktır.

3.1.4. Soğuk Savaş Öncesi NATO ve Uluslararası Güvenlik Gelişmeleri

Soğuk Savaş dönemi tarihin en belirgin ideolojik ve askeri kutuplaşmalarından birini temsil etmektedir. NATO bu dönemde aktif rol oynamıştır. Birliğin SB'nin oluşturduğu tehdide yanıt vermek amacıyla kurulduğu sıklıkla ifade edilmektedir. Ancak bu sadece kısmi bir doğruluk taşır. Aslında ittifakın kuruluşu daha geniş bir amaç doğrultusunda gerçekleşmiştir. NATO'nun oluşturulması üç ana hedefi gerçekleştirmeyi amaçlayan daha geniş bir çabanın parçasıydı: SB yayılmacılığını caydırmak, Avrupa'da milliyetçi militarizmin yeniden canlanmasını engellemek için güçlü bir varlığı kıtada sağlamak ve Avrupa'nın siyasi bütünleşmesini teşvik etmek. Bu nedenle, NATO'nun kuruluşu sadece SB tehdidine bir yanıt olarak değil, aynı zamanda Avrupa'nın istikrarını ve güvenliğini sağlama çabasının bir parçası olarak da görülmelidir (NATO, 2022).

Soğuk Savaş öncesi dönemde II. Dünya Savaşı'nın hemen ardından Avrupa'nın geniş bir alanı tahrip olmuştu. Üstelik SB tarafından teşvik edilen komünist rejimler Avrupa'da bölgesel olarak hükümetleri ciddi baskı altında bırakıyordu. Bu durum Avrupa için tehdit boyutu haline gelmekteydi. Bunun sonucunda ise birtakım gelişmeler yaşanmıştır. Savaşın akabinde Avrupa ülkelerinin yıkıma uğrayan ekonomilerini onarmak için ABD tarafından desteklenen Marshall Planı ve diğer yardımlar devreye girmiştir. Bu durum Avrupa'nın ekonomik istikrarını güçlendirmiştir. Ancak tam bir ekonomik iş birliği için devletler arasında güvenliğin sağlanması gerekli görülmüştür. Bu nedenle askeri iş birliği ve güvenlik önlemleri, ekonomik ve siyasi ilerlemenin yanında gelişmesi gereken gündem konuları arasındaydı. Bu düşünceyi destekleyecek biçimde Batı Avrupa'daki demokratik ülkeler daha fazla askeri iş birliği ve kolektif savunma için çeşitli projeleri hayata geçirmek için toplanmışlardır. Hemen ardından 1948'de Batı Avrupa'da Western Union kurulmuş ve sonrasında 1954'e gelindiğinde Batı Avrupa Birliği adını almıştır. 1948 tarihinde Almanya'da yaşanan gelişmeler Avrupa'da güvensizlik ortamını tetiklemiştir. Stalin, Berlin'e ulaşan demiryolu ve karayollarını keserek abluka uygulamıştır. Her ne kadar hava yoluyla yardım yapılmaya çalışılmışsa da SB'ye karşı bir ortaklık düşüncesi gerekli görülmeye başlanmıştır. Bu bağlamda Sovyet saldırganlığını caydırmak ve Avrupa militarizminin yeniden canlanmasını engellemek ve aynı zamanda siyasi entegrasyonun temelini atmaktan bahsedilirken, gerçek bir transatlantik güvenlik anlaşmasının gerekliliği üzerinde yoğun tartışmalar yaşanması üzerine nihayet tarih 4 Nisan 1949'u gösterdiğinde Kuzey Atlantik Antlaşması imzalanmıştır (A Short History of NATO, 2022).

NATO Soğuk Savaş öncesinde de uluslararası güvenlik konularına önem vermiştir. Bu konulardaki başarısını ve çabasını yaşanan gelişmeler ile göstermiştir. Avrupa'nın güvenliğini sağlarken öte yandan iş birliğinin önemini gözler önüne sermiştir. Bu bağlamda üye ülkelerin askeri kapasitelerinin güçlenmesine fayda sağlamıştır. Nitekim Soğuk Savaş dönemi başladığında güvenlik konuları genişlemiş ve üye ülkelerin entegresi sağlanarak iş birliği doğrultusunda çaba gösterilmiştir.

3.1.5. Soğuk Savaş Dönemi ve Soğuk Savaş Sonrası NATO ve Uluslararası Güvenlik Gelişmeleri

Soğuk Savaş dönemi iki kutuplu yapı ile çekişmeli bir süreci kapsamıştır. Bu dönemin başlarında Sovyetler'in 1949'da nükleer çalışmaları ve başarılı olmasının ardından 1950'de Kore Savaşı'nın[8] başlamasıyla Avrupa'da endişeler doruğa ulaşmıştır. Bunun akabinde NATO hızla Paris'in Versailles yakınlarındaki Rocquencourt banliyösünde bulunan bir askeri karargahla bütünleşmiş bir komuta yapısına geçmiştir. Sonrasında ABD'li General Dwight D. Eisenhower'ın Avrupa Müttefik Yüksek Komutanı veya SACEUR olarak atandığı Avrupa Müttefik Kuvvetler Yüksek Karargâhı veya Shape kurulmuştur. Biraz zaman geçtikten sonra üye ülkeler Paris'te daimî bir sivil sekreterlik kurmuş ve NATO'nun ilk Genel Sekreteri, Birleşik Krallık'tan Lord Ismay olmuştur. Yardımların ve güvenlik aktarımlarının desteği ile Batı Avrupa'da siyasi istikrar zamanla yerine oturmaya başlamış ve savaş sonrası ekonomik istikrar sağlanmıştır. İlerleyen süreçte ise ittifaka yeni müttefikler katılım sağlamıştır. 1952'de Yunanistan ve Türkiye, 1955'te ise Batı Almanya ittifaka katılmıştır. Batı Almanya'nın NATO'ya katılımına tepki olarak, SB ve Doğu Avrupalı ortak devletler 1955'te Varşova Paktı'nı kurmuştur (A Short History of NATO, 2022).

1959 yılında ABD'ye oldukça yakın bir bölge olan Küba'da yaşanan iç karışıklıklar Fidel Castro liderliğindeki komünistlerin devrimi ile sonuç bulmuştur. Halihazırda zaten SB komünizm rejimi ile çekişme içerisinde olan ABD için kendisine coğrafi olarak bu kadar yakın bir bölgede bu olayın yaşanması oldukça negatif bir durum olmuştur. Bu durumun karşılığı olarak ABD'nin İtalya ve Türkiye'ye füze yerleştirmesi üzerine SB Küba'ya füze rampası kurması krizi iyice tırmandıran olaylar silsilesini oluşturmuştur. Bu durum adeta bir nükleer poker oyunu haline gelmiştir. Başkan John F. Kennedy'nin krizi durdurmak için harekete geçerek Küba'yı denizden ablukaya aldırmıştır. Başkan Kennedy, Nikita Kruşçev'e haber göndererek Soğuk Savaş gerilimini azaltmaya, Beyaz Saray ile Kremlin arasında bir acil hat kurulmasına ve nükleer testlerin yasaklanmasını içeren bir anlaşmanın imzalanmasına işaret etmiştir. Bu sayede ABD ile SB arasında barış içinde bir arada yaşamanın ve uzlaşmanın desteklenmesi sağlanmıştır (Medland, 1990). Küba Füze Krizi ardından

[8] Kore Savaşı, Doğu ile Batı arasındaki Soğuk Savaş'ın belirleyici gelişmelerinden bir tanesi olmuştur. SB tarafından desteklenen Kim İl-Sung 1948 tarihinde Güney Kore'de ve Kuzey Kore'de komünist bir hükümet kurmuştur. Hemen ardından bu hükümet iki bölgeyi birleştirmek istemiştir. ABD destekli Güney Kore bu duruma karşı çıkınca 1950 yılında iki taraf arasında savaş çıkmıştır. Savaş sonunda Güney Kore'de ABD etkili, Kuzey Kore'de ise SB etkisinde uygun komünist rejim kurulmuştur. Kore Savaşı, Stalin dönemi için Soğuk Savaş'ın en tehlikeli anlarından biriydi ve Kore SB'nin çöküşüne kadar süper güçler arasındaki rekabette potansiyel bir kırılma noktası teşkil etmiştir (Grey, 2004).

kabul edilen Esnek Yanıt Doktrini, çatışma durumlarında tam bir nükleer mübadeleyi aşarak NATO'nun konvansiyonel savunma yeteneklerini güçlendirmiştir. Bu yaklaşım çatışma durumlarında NATO'nun askeri müdahale kapasitesini artırarak nükleer savaş riskini azaltmayı amaçlamaktadır (NATO, A Short History of NATO, 2022).

Şekil 3: Berlin Duvarı

Kaynak: NATO, 2022

Soğuk Savaş dönemi 1961'de Berlin Duvarı'nın inşasıyla simgelenen gergin bir çıkmaza girmiştir. Berlin Duvarı Soğuk Savaş'ın sembolü olarak iki süper güç ve iki farklı ideoloji bloğu simgelemiştir. 1955 ve 1975 yılları arasını kapsayan Vietnam Savaşı[9] da Soğuk Savaş sürecini zorlaştıran önemli olaylar arasındadır. 1979 yılına gelindiğinde SB Afganistan'ı işgal etmiştir. Bu gelişme birliğin yumuşama sürecini negatif yönde etkileyen bir durum olmuştur. İlerleyen süreçte, 1983'te birliğin üyeleri, SB ile umulan yumuşama ortamını sağlayamadıklarında iç anlaşmazlıklar yaşamışlardır. Ancak, 1985'te Mihail Gorbaçov'un Sovyet lideri olarak yükselişinin ardından, ABD ve SB arasında Orta Menzilli Nükleer Kuvvetler Anlaşması (INF) imzalanmıştır. 1987'de imzalanan bu anlaşma ile bütün nükleer ve karadan atılan orta menzilli balistik ve seyir füzelerinin ortadan

[9] Soğuk Savaş'ın ABD ve SB arasındaki ideolojik ve güç mücadelesi, Vietnam Savaşı'nın uluslararası boyut kazanmasına yol açtı. Savaş komünist ÇHC ve SB'nin desteklediği Kuzey Vietnam ile ABD'nin desteklediği Güney Vietnam arasında gerçekleşmiştir. ABD'nin nihai hedefi Güney Vietnam'da bağımsız, komünist olmayan bir hükümet kurarak komünistlerin Güneydoğu Asya'da daha fazla yayılmasını engellemekti. Başkan Johnson Vietnam'da savaşa katılma kararı aldı. Vietnam Savaşı'nın Soğuk Savaş açısından Amerikalıların öngördüğünden farklı sonuçları oldu. Domino etkisi özellikle eski Fransız Çinhindisi'nde etkili oldu ve 1975 baharında Laos ve Kamboçya komünist isyancıların kontrolüne geçti. Fakat SB'nin Vietnam'da yaşamış olduğu mali ve insani kayıplar Soğuk Savaş'ı kaybetmesinde dolaylı olarak etkili olmuştur (Herring, 2004).

kaldırılması öngörüldü. Bu anlaşma Soğuk Savaş'ın sona erdiğinin ilk belirtisi olarak kabul edilmiştir (NATO, A Short History of NATO, 2022).

9 Kasım 1989'da Berlin Duvarı'nın yıkılması ile Soğuk Savaş dönemi sona ermiştir. SB dağılmış ve Batı bloğu görece galip olarak ayrılmıştır. Fakat NATO varoluşunu aktif şekilde devam ettirmiştir. Çünkü NATO'nun kuruluş amacı yalnızca Sovyet yayılımını engellemek değildir ve çeşitli misyonları bulunmaktadır. 1991 yılında NATO genişleyerek Pan-Avrupa güvenlik mimarisinin temelini atmıştır. Avrupa-Atlantik Ortaklık Konseyi, Orta Avrupalı, Doğu Avrupa ve Orta Asyalı komşularıyla istişareler için kurulmuştur. Akdeniz Diyaloğu da bu doğrultuda oluşturulmuş oldu. İlerleyen süreçte yaşanan Yugoslav iç savaşına NATO ilk başta müdahale etmemiştir ancak sonradan doğrudan askerî harekâtlara katılarak savaş suçlarını durdurmayı amaçlamıştır. 1995'te çatışmanın sona ermesinde önemli bir rol oynamış ve 1999'da Kosova'da Sırp etnik temizliğine karşı hava saldırıları düzenlemiştir. NATO'nun çabaları sonucunda Kosova Gücü'nün konuşlandırılmasıyla bölgedeki güvenlik sağlanmıştır. 1999'da Çekya, Macaristan ve Polonya gibi ülkeler NATO'ya tam üye olmuştur. Bu süreç NATO'nun Soğuk Savaş sonrasında da Avrupa'da demokrasi ve istikrarın pekiştirilmesinde önemli bir rol oynadığını göstermiştir (NATO, A Short History of NATO, 2022).

11 Eylül 2001 tarihine gelindiğinde yaşanan terörist eylemler Dünya Ticaret Merkezi ve Pentagon'a zarar vermiştir. Küresel sistemde yaşanan siyasi karışıklıkların iç güvenlikte asayişi bozacak problemler oluşturabileceği görülmüştür. Bu durum birliğin üye ülkelerinin endişe etmelerine neden olmuştur. NATO savunma aracı olarak tarihte ilk kez 5. Maddesi'ni harekete geçirmiştir. Çünkü devlet dışı aktörlerin (El Kaide gibi) kaçırılan uçakları el yapımı kitle imha silahları olarak kullanabileceği görülmüştür. Bunun sonucunda korkunç bir tablo oluşmuş ve binlerce masum sivilin ölümüne neden olabileceği anlaşılmıştır. Tehlikenin boyutu oldukça büyük olarak görülmüştür. İlerleyen süreçte yaşanan olumsuz gelişmeler, Kasım 2003'teki İstanbul bombalamaları, 11 Mart 2004'teki Madrid banliyö treni saldırısı ve 7 Temmuz 2005'teki Londra'da toplu taşıma sistemine yapılan saldırılar gibi olaylar, şiddet yanlısı terörist grupların sivil halka zarar vermeye kararlı olduğunun kanıtıdır (NATO, A Short History of NATO, 2022).

2011 yılında NATO Libya'da yaşanan gelişmelerde etkin rol oynamıştır. Kısa bir zaman geçtikten sonra NATO'nun görevi başlangıçta sadece Kaddafi'nin hava kuvvetlerini işlevsiz bir duruma evrilmekten daha geniş bir siyasi misyona dönüşmüştür. İlerleyen aylarda birliğin desteklediği isyancılar Libya'nın genel bir bölümünü kontrol altına almış ve Kaddafi'nin iktidarını sonlandırmıştır. Fakat bu gelişme Libya iç güvenliğinde daha problemli bir karışıklığın yaşanmasına yol açmıştır. Bu beklenmeyen sonuç NATO'nun genişleyen misyonu hakkında eleştirilere neden olmuştur. Fakat NATO her ne kadar amaçladığı üzere Libya'da demokrasiyi yeniden kurmayı başaramasa da daha büyük bir hedefi olan Libya vatandaşlarını korumak ve bir katliamı önlemek konusunda başarı elde etmiştir. Bu gelişmelerden sadece birkaç yıl sonra 2014'te RF, Ukrayna'nın Kırım bölgesini ilhak etmiştir. Yaşanan bu saldırının akabinde NATO, RF'ye onla arasında olan

bütün askeri ve sivil iş birliğini askıya alarak yanıt vermiştir. Ayrıca Doğu Avrupa'daki müttefiklerine daha fazla asker gönderme konusunda garanti sağlamıştır. 2022 yılında RF'nin Ukrayna'ya yönelik saldırısının artması ve işgalci eylemleri sonucunda birliğin üye ülkeleri Ukrayna'ya mali ve askeri yardım desteği sağlamışlardır. Ayrıca Ukrayna'ya askeri eğitim sağlanmış ve NATO Genel Sekreteri Jens Stoltenberg çatışma sona erdiğinde ve tüm ülkeler yeterince güvenli olduğunda Ukrayna'nın ittifaka katılmasına izin vermeyi kabul edecekleri konusunda açıklama yapmıştır. Bu noktada genel sekreterin Ukrayna'nın birliğe katılma teklifini hemen kabul etmemesi ve özellikle güvenlikli ortamın oluşmasını beklemesi NATO'nun ana amacı olan birliğin üye ülkelerinin güvenliğini sağlaması amacı ile oldukça uyumludur (Council on Foreign Relations, 2024).

Birliğin tüm bu gelişmelere kayıtsız kalmaması Soğuk Savaş sonrası dönemde de güvenliğe ve savunmaya verdiği çabayı ortaya koymuştur. Her ne kadar birliğin misyonu değişmiş olsa da ana hedefi hala üye ülkelerin güvenliklerini sağlamaktır. Bu bağlamda NATO güvenlik kapsamındaki hiçbir konuyu göz ardı etmemektedir. Üye ülkeler arasındaki iş birliği, istihbarat paylaşımı, terörle mücadele ve bunun gibi konularda ortak operasyonlar oluşturma süreci genişleyerek ilerlemeye devam etmiştir. Bunu da yenilediği stratejik konseptlerindeki hedefleri ile açıkça belirtmektedir. NATO sadece üye ülkeler için değil, küresel dünyada diğer aktörleri de etkileyen güvenlik problemleri ile ilgilenmiştir.

3.2. NATO ve Siber Güvenlik Politikalarının Analizi

Siber uzayda yaşanan dijital gelişim sürecinin hız kazanması ile siber güvenlik konuları hızla önem kazanmaya devam etmektedir. NATO'nun Soğuk Savaş sonrası genişleyen güvenlik misyonu konularına siber güvenlik konuları da dahil olmuştur. Bilhassa böylesi geniş ve tehlikeli bir alana NATO'nun kayıtsız kalmayacağı öngörülebilmektedir. Bu bağlamda birliğin üye ülkelerinin ve uluslararası siber güvenlik politikalarının hem bireysel hem de küresel anlamda profesyonel bir şekilde uygulanması kritik bir öneme sahiptir. NATO'nun kurulduğu dönemden itibaren gelişen güvenlik sorunlarına başarılı yanıtlar vererek uyum sağlayabildiği yaşanan gelişmeler ile görülmüştür. Aynı şekilde siber güvenlik tehditlerine de uyum sağlayabilecek potansiyele sahip olabilir. Elbette bunu üye ülkelerin siber savunma kapasiteleri, alana ayırabilecekleri bütçeler ve eğitim süreçleri gibi hususlar etiketlemektedir. Sonuç olarak birliğin siber güvenlik tehditlerine savunma oluşturabileceği analiz edilebilmektedir.

3.2.1. NATO'nun Siber Güvenlik Politikalarına İhtiyacı Var mı?

Modern küresel dünyada bilgi ve iletişim teknolojileri çeşitli kolaylıklar sağlayan ve kullanılmaktan vazgeçilmesi zor bir unsur haline gelmiştir. İş hayatı, kişisel veriler, devlet verileri, ulusal bilgi alt yapısı gibi unsurlar siber uzay içerisinde barınmaktadır. Her ne kadar teknolojinin

getirdiği unsurların güvenli olduğu düşünülse de siber uzaydaki oluşumların güvenlik açıkları bulunabilmektedir. Teknolojinin hızlı ilerlemesi ile, bu hıza ayak uyduramayıp güncellenemeyen siber güvenlik ağları saldırıya açık bir tehlike ile karşı karşıya kalabilir.

Farklı ulusal siber güvenlik stratejileri ulusal egemenlik sınırlarını gözeterek, ulusal çıkarları ön planda tutabilir. Birlik alanı dahilinde başarılı bir siber savunma sistemi oluşturabilmek için en önemli unsurlardan biri iş birliğidir. Çünkü siber savunmayı sağlayabilmek için tüm aktörlerin koordine olması önemlidir. Ulusal çıkarlar uluslararası iş birliğini engellemeden ortak bir paydada buluşmayı sağlamalıdır. Tavsiye edilen güvenlik önlemleri temel haklara saygı göstermeli ve ekonomik etkileri göz önünde tutmalıdır. Bu ortaklığın siber güvenliğe entegre edildiği noktada ise ulusal siber güvenlik stratejisi taslağının hazırlanmasının karmaşık bir durum olduğu söylenebilir. Çeşitli tehdit senaryoları ve farklı aktörlerin yanı sıra, siber tehditlere karşı alınacak önlemler bir dizi farklı alanı kapsar. Bu önlemler politik, teknolojik, yasal, ekonomik, yönetimsel veya askeri nitelikte olabilir ve diğer disiplinleri de içerebilir. Üstelik bu olgular her üye ülke için farklı seviyelerde olabilmektedir. Bu bağlamda siber güvenliği güçlendiren ve tehditlere karşı birlikte direnci artırabilecek yanıtlar sunmak için iş birliği içerisinde daha belirgin bir rol veya kaynaklar için rekabet etmek yerine ortak paydada buluşmak önemlidir (Klimburg, 2012).

Siber uzayda gerçekleşen siber saldırılar bireylere, devletlere ve birliklere karşı olabilmektedir. Bu saldırılar devletlerden birliklere ya da başka devletlere yapılabildiği gibi birliklerden başka birliklere de yapılabilir. Bu noktada NATO üye ülkelerini ve birliği siber alanda savunma altına alabilmek için iş birliği ile çalışabilir. Günümüz teknolojisinde internet aracılığıyla birçok unsur gerçekleşmektedir. NATO ve üye ülkeler bu unsurları kullanmakta ve alakalı olmaktadır. Bu açıdan düşünüldüğünde zaten bir savunma birliği olan NATO'nun siber uzayla ilgilenmesi oldukça olasıdır.

Geleneksel askeri tehditler kadar siber güvenlik tehditleri de tehlikeli olabilmektedir. Günden güne yaygınlaşan siber saldırılar, kötü amaçlı yazılımlar, siber casuslar birliğe ve üye ülkelere zarar verebilir. Stratejik bilgilerin çalınması ve kritik alt yapıların zarar görmesi olasılığının sonuçları oldukça kritiktir. Halihazırda ittifakın ana amacı üye ülkelerin güvenliklerini korumaktır. Bu bağlamda siber tehditlerin NATO'yu ve üye ülkeleri zayıflatmaması için siber savunma yöntemleri koruyucu olabilir. Üstelik saldırıların hızlı ve karmaşık yapısı karşısında ülkelerin bireysel yöntemleri dışında iş birliği ile savunmaları daha etkin karşılık vermelerine fayda sağlayabilir. Giderek karmaşık ve ciddi hale gelen siber saldırılar düşünüldüğünde NATO'nun siber güvenlik politikalarına ihtiyacı olduğu görülmektedir.

3.2.2. Birliğin Yakın Geçmişi ve Siber Savunma Disiplini

Soğuk Savaş süresince NATO'nun odak noktası geleneksel askeri tehditler olmuştur. Fakat dijital çağın gelişimi ile siber güvenliğe duyulan ihtiyaçların devamında NATO'nun savunma

stratejileri de değişmiştir. Siber tehditlerin hızla artmasıyla birlikte birliğin üye ülkeleri arasında siber savunma yeteneklerini güçlendirmek ve bilgi paylaşımını teşvik etmek için daha fazla çaba öngörülmektedir. Bu çabalar ittifakın siber altyapılarını korumak ve uluslararası güvenliği sağlamak için önemli bir adımdır.

Tablo 7: Zaman Çizelgesi- NATO'nun Siber Güvenlik Çabalarındaki Önemli Aşamalar

Tarih	Olaylar
2002	Siber güvenliğin NATO'nun gündemine ilk kez Prag Zirvesi'nde girmesi.
2008	İlk kez resmi NATO Siber Savunma Politikası'nın kabul edilmesi.
2008	Estonya'nın başkenti Tallinn'de NATO İş birliği Siber Savunma Mükemmeliyet Merkezi'nin kurulması.
2010	NATO'nun Stratejik Konsepti'nin Lizbon Zirvesi'nde ilan edilmesi.
2014	NATO Siber Güvenlik Eylem Planı'nın yayınlanması.
2014	Geliştirilmiş NATO Siber Savunma Politikası'nın Galler Zirvesi'nde sunulması.
2016	Birliğin, Varşova Zirvesi'nde siber uzayı kara, deniz ve havanın yanı sıra dördüncü operasyon alanı olarak ilan etmesi.
2016	Üye devletlerin siber savunma dayanıklılıklarını güçlendirmelerini gerektiren Siber Savunma Taahhüdü'nün kabul edilmesi.
2016	Siber tehditler de dâhil olmak üzere iş birliğinin derinleştirilmesine ilişkin AB-NATO Ortak Deklarasyonu'nun imzalanması.
2017	Gözden geçirilen NATO Siber Güvenlik Eylem Planı'nın yayınlanması.
2018	Brüksel Zirvesi'nde Belçika'nın Mons kentinde bir Siber Uzay Operasyonları Merkezi kurulmasına karar verilmesi.

Kaynak: Szőke, 2019

2002 yılında NATO'nun Prag Zirvesi'nde siber savunma stratejilerini geliştirmek ve iş birliğini artırmak için deklarasyonda siber saldırılara karşı savunma yeteneklerini güçlendirmelerinin gerekliliği vurgulanmıştır (NATO, Prague Summit 2002: Selected Documents and Statements, 2002: 53). Bu karar birliğin siber saldırılara ilişkin ilk belirgin kararı olmuştur. Bu tarihten sonra siber gündem NATO nezdinde daha çok karşılaşılan bir konu olmuştur. NATO 2008 yılına gelindiğinde ilk kez resmi olarak bir siber savunma politikasını kabul etmiştir. Bu bağlamda 2008 NATO Bükreş Zirvesi önemlidir. Bu zirve ittifakın siber tehditlerle resmi olarak yüzleştiği ilk zirvedir. Ayrıca Romanya Cumhurbaşkanı Traian Băsescu zirveyle eş zamanlı olarak düzenlenen özel bir çalıştayda NATO ve siber savunma konularını içeren bir dizi belgeyi tanıtmıştır. Zirve boyunca NATO yetkilileri ve siber uzmanlar Estonya'daki deneyimlerden çıkarılan dersleri değerlendirmişlerdir. Bükreş Zirvesi Liderler Deklarasyonu'nun 47. Bölümü'nde şu önemli ifade yer almaktadır: *"NATO, ittifakın kilit bilgi sistemlerini siber saldırılara karşı güçlendirme konusundaki kararlılığını sürdürmektedir. Kısa bir süre önce bir Siber Savunma Politikası kabul ettik ve bunu uygulamak için gerekli yapı ve yetkileri geliştiriyoruz. Siber Savunma Politikamız, NATO'nun ve ulusların kilit bilgi sistemlerini kendi sorumluluklarına uygun olarak korumaları, en iyi uygulamaları paylaşmaları ve talep üzerine müttefik ülkelere bir siber saldırıya karşı koymalarında yardımcı olacak bir kabiliyet sağlamaları gereğini vurgulamaktadır. NATO'nun siber savunma yeteneklerinin geliştirilmesine*

devam edilmesini ve NATO ile ulusal birimler arasındaki bağlantıların güçlendirilmesini sabırsızlıkla beklemekteyiz." (NATO, Bucharest Summit Declaration, 2008)

20 Kasım 2010 tarihinde NATO'nun işleyişinde ciddi değişiklikler meydana getirecek olan Lizbon Zirvesi sonuçlandı ve ittifakı daha etkin, daha verimli ve daha geniş bir dünya ile daha bağlantılı hale getirecek kararlar alındı. İki gün boyunca devam eden toplantıda müttefikler balistik füze ve siber saldırılar gibi güncel tehditlere karşı savunma için yeni kapasiteler geliştirmeye karar verdiler (NATO Summit Paves Way For Renewed Alliance, 2010). 2016 yılına gelindiğinde ise birlik Varşova Zirvesi'nde siber alanda ciddi adımlar atmıştır. Müttefikler bir siber saldırının toplum için en az konvansiyonel bir saldırı kadar zararlı olabileceği konusunda farkındalık oluşturmuştur. Buna ek olarak siber savunmayı NATO'nun temel görevi olan kolektif savunmanın bir parçası olarak görmektedir. Devamında ise NATO 2016 yılında geleneksel hava, kara ve deniz alanlarının yanı sıra siber uzayı da bir harekât alanı olarak kabul etmiştir. Bu gelişme NATO'nun askeri komutanlarının, müttefiklerin ulusal siber yeteneklerinden yararlanmak da dâhil olmak üzere görevlerini ve operasyonlarını siber tehditlerden daha iyi korumalarını sağlamayı hedefler niteliktedir. Müttefikler tıpkı tanklara, gemilere ve uçaklara sahip oldukları gibi bu yeteneklere de tam olarak sahip olmaları konusunda bilinçlenmişlerdir. Diğer tüm alanlarda olduğu gibi siber alanda da NATO'nun eylemleri savunmaya yönelik, orantılı ve uluslararası hukuka uygun görülmektedir. Müttefikler kurallara dayalı, öngörülebilir, açık, özgür ve güvenli bir siber uzaydan herkesin yararlanacağı konusunda hemfikirdirler (Organization, 2020).

Haziran 2011'de NATO savunma bakanları ikinci NATO Siber Savunma Politikası'nı onaylamışlardır. Nisan 2012'de ise siber savunma NATO Savunma Planlama Süreci'ne dahil edilmiştir. 2012'deki NATO zirvesinde Chicago'da üye liderler örgütün tüm ağlarını merkezi koruma altına almayı ve siber savunma yeteneğini güncellemeyi taahhüt ederek ittifakın siber savunmasını geliştirmeye kararlı olduklarını teyit ettiler. Bunun sonucunda Temmuz 2012'de NATO ajanslarının reformu kapsamında NATO Haberleşme ve Bilgi Ajansı kurulmuştur. Şubat 2014'te müttefik savunma bakanları NATO'yu yeni bir siber savunma politikası geliştirmekle görevlendirmiştir. Nisan 2014'te Kuzey Atlantik Konseyi, Savunma Politikası ve Planlama Komitesi/Siber Savunma'nın adını Siber Savunma Komitesi olarak değiştirmeyi kabul etmiştir. Aynı yılın Eylül ayında, NATO özel sektörle siber tehditler ve zorluklar konusunda iş birliğini artırmak için bir girişim başlatmıştır. Galler Zirvesi'nde onaylanan NATO Endüstri Siber Ortaklığı (NICP) Belçika'nın Mons şehrinde düzenlenen bir siber konferansta sunulmuştur. NICP ittifakın siber savunma hedeflerine ulaşmasını sağlamak için endüstri ortaklarıyla çalışmanın önemini kabul eder niteliktedir (NATO, Cyber Defence, 2023). NATO Siber Savunma Taahhüdü'nü kabul etmiştir. Burada alt yapıları ve ağları en yüksek stratejik düzeyde savunmaktan bahsedilirken iş birliğinin önemi vurgulanmıştır. Aynı zamanda siber alandaki eğitimler konusunda kurumların geliştirilmesi kararı önem arz etmektedir. Bilinçli bir şekilde davranarak siber alanda yaşanabilecek olumsuzluklar oldukça azaltılabilir. Ayrıca birlik Washington Antlaşması'nın 3. Maddesi uyarınca ulusal altyapı ve

ağların siber savunmalarının güçlendirilmesi konusundaki ulusal sorumluluğunu ve Galler'de kabul edilen NATO'nun siber savunmaya ilişkin geliştirilmiş politikası uyarınca müttefik güvenliğinin ve kolektif savunmanın bölünmezliğine olan bağlılığını bir kez daha göstermiştir. Siber savunma için ortaklıklar da gündeme gelmiştir. NATO-AB siber savunma işbirliğinin ilerletilmesi desteklenmiştir (NATO, Cyber Defence Pledge, 2016).

Şubat 2017'de müttefik savunma bakanları güncellenmiş bir Siber Savunma Eylem Planı ve siber uzayın operasyon alanı olarak uygulanmasına yönelik bir yol haritasını onaylamışlardır. Bu da müttefiklerin birlikte çalışma, yetenek geliştirme ve bilgi paylaşma kabiliyetlerini artırmayı sağlar niteliktedir (NATO, Cyber Defence, 2023).

Brüksel'de düzenlenen 2018 NATO zirvesinde birliğin gelişen ve gittikçe tehlikeli olan siber tehditler karşısındaki uyum sürecini güçlendirme kararlılığı teyit edilmiştir. NATO burada, 3. Maddesi'nde belirtilen ve üyelerin silahlı saldırılara karşı bireysel ve kolektif kapasitelerini koruma ve geliştirmeye yönelik ulusal sorumluluk ilkesini hatırlatarak, NATO üyelerine siber alandaki faaliyetleri için net bir stratejik yön belirleme çağrısında bulunmuştur. Ayrıca bu zirvede Siber Uzay Operasyon Merkezi'nin kurulma kararı önemlidir. Bu kararı bildirinin 29. paragrafında Belçika'da kuracaklarını söyleyerek belirtmişlerdir. Bahsi geçen operasyon merkezi ittifakın siber saldırılara daha etkin ve başarılı şekilde yanıt vermesini hedeflemektedir (Cooperative Cyber Defence Centre of Excellence, 2018).

Tespit edildiğine göre NATO'nun sahip olduğu ve kullandığı ağlarda her gün şüpheli siber olaylar kaydetmekte ve müttefik ülkelerdeki hükümet ve kritik altyapı ağlarına izinsiz girişler dramatik bir şekilde artmaktadır. Bu bağlamda 13 Ekim 2019 pazar günü Londra'da STC Genel Raporu, NATO Parlamenter Asamblesi 65. Yıllık Oturumu'nda Bilim ve Teknoloji Komitesi tarafından onaylanmıştır. Bu rapor NATO'ya zarar verebilecek her türlü siber tehdide odaklanmaktadır. Müttefiklerin toprak bütünlüğünü, siyasi bağımsızlığını veya ulusal güvenliğini tehdit eden ve müttefiklerin Washington Antlaşması'nın 5. Maddesi kapsamındaki NATO'nun toplu savunma hükmünü devreye sokabilecek bütün siber saldırılar[10] buna dahildir. Ayrıca bu rapor birliğin karşı karşıya olduğu siber tehdide ilişkin bir bağlam ve NATO'nun mevcut siber stratejilerine, politikalarına genel bir bakış sunmaktadır. Bu bağlamda NATO'nun siber güvenliğini, savunmasını ve caydırıcılığını güçlendirmek için politika önerilerini barındırmaktadır (Davis, NATO Parliamentary Assembly, 2019). Aşağıdaki tabloda raporda belirtilen siber güvenliği ve savunmayı güçlendirmenin bir takım yolları bulunmaktadır.

[10] Evrensel olarak kabul görmüş bir "siber saldırı" tanımı mevcut değildir. Ancak ABD Savunma Bakanlığı (US DOD) tarafından ortaya konan tanım iyi bir başlangıç noktası sağlamaktadır. Siber saldırılar, siber uzayda fark edilebilir etkileri (yani bozulma, aksama veya yıkım) yaratan siber uzayda gerçekleştirilen eylemler veya fiziksel bir alanda görünen tahribe yol açan manipülasyon olarak anlaşılabilir (U.S. Department of Defense, 2021: 55).

Tablo 8: Siber Güvenlik ve Savunmayı Artırmaya Yönelik Bazı Yollar

Temel siber güvenlik önlemlerinin uygulanması
Durumsal farkındalığı artırma
Bilgi paylaşımının artırılması
Daha etkili tespit ve gözetim yazılımları kurmak
Yeni teknolojilerin araştırılıp geliştirilmesine yatırım yapılması
İşgücünü eğitmek, örneğin siber bakımdan yeterli hale getirmek
İşgücünün uyumluluğunu teşvik etmek
Siber eğitim ve tatbikatlar düzenlemek
Düzenli siber denetimler gerçekleştirmek
"Kırmızı takım" siber güvenlik ve savunmalar
İşbirliği ve yardım anlaşmaları imzalamak
Potansiyel saldırganları yanıltmak
Hassas dosyalarınızı şifreleyin
Ağın hassas bölümlerine duvar örün

Kaynak: Davis, NATO in the Cyber Age: Strengthenıng security ve Defence, Stabilising Deterrence: General Report, 2019

Brüksel'de gerçekleştirilen 2021 NATO zirvesinde müttefikler birliğin üç temel görevinin yanı sıra genel caydırıcılık ve savunma pozisyonunu da güçlendirecek yeni bir Geniş Kapsamlı Siber Savunma Politikası'nı onayladılar. Müttefikler ayrıca örgütü kendi arasında siyasi danışma platformu bağlamında daha çok kullanmayı, kötü niyetli siber faaliyetlerle ilgili endişeleri paylaştırmayı, ulusal tepkileri paylaşmayı ve olası toplu tepkileri değerlendirmeyi kabul etmişlerdir. Ayrıca Eylül 2021'de bilgi ve iletilişm teknolojileri sistemlerinin entegrasyonunu, hizalanmasını ve uyumunu kolaylaştırmak üzere NATO'nun ilk Bilgi Teknolojileri ve İletişimden Sorumlu Yetkilisi (CIO) atanmıştır (NATO, Cyber Defence, 2023).

9-10 Kasım 2022'de örgüt Roma'da Siber Savunma Taahhüdü Konferansı[11] gerçekleştirmiştir. Bu konferansta NATO Genel Sekreteri Jens Stoltenberg'in konuşmasında siber güvenlikten bahsetmiştir. Siber güvenliğin giderek daha etkili bir alan olduğunu belirtme konusunda çağrı yapmıştır. Siber tehkilelerin artık yalnızca devletlerden değil aynı zamanda devlet dışı aktörlerden de geldiği görülmektedir. Bu nedenle, müttefikleri siber savunmaya daha fazla önem vermeleri ve bu alanda daha fazla bütçe ayırmaları konusunda uyarmayı uygun görmüştür. Ayrıca uzmanlaşmış

[11] Konferansta NATO Genel Sekreteri Jens Stoltenberg'in konuşmaları NATO'nun siber güvenlik alanındaki misyonunu belirtir şekilde olmuştur. Stoltenberg konuşmasında şunları paylaşmıştır: "*Siber uzay mütemadiyen tartışılan bir alandır ve barış, kriz ve çatışma arasındaki çizgi belirsizleşmiştir. İşte bu nedenle NATO devletlerden ve devlet dışı aktörlerden kaynaklanan siber uzay tehdidini uzun süredir önemsemektedir. Siber saldırılara karşı korunmak için kararlı adımlar atmamızın nedeni de budur. Bu bizim ortak savunmamızın anahtarıdır. Müttefiklere siber savunmaya yeniden önem vermeleri çağrısında bulunuyorum. Daha fazla bütçe, daha fazla uzmanlaşma ve daha fazla iş birliği ile. Bu, ortak savunmamızın kritik bir parçasıdır ve bu konuda hepimiz beraber hareket ediyoruz."* (NATO Secretary General Warns of Growing Cyber Threat, 2022)

personel yetiştirmek ve uluslararası iş birliğini artırmanın önemi de vurgulanmıştır (NATO Secretary General Warns of Growing Cyber Threat, 2022).

11 Temmuz 2023'te Vilnius'ta düzenlenen Kuzey Atlantik Konseyi Toplantısı'na katılan NATO devlet ve hükümet başkanları tarafından Vilnius Zirvesi Bildirisi yayınlanmıştır. Bu bildiride siber güvenliğe vurgu yapılmıştır. NATO siber, uzay, hibrit ve diğer asimetrik tehditlerle yeni geliştirilen ve tahrip edici teknolojilerin kötü niyetli kullanılması ile karşı karşıya kalmaya devam ettiğini vurgulamıştır. Tehlikenin RF'den geldiğini belirtmiş ve NATO'ya müttefiklerine ve ortaklarına karşı hibrit eylemlerini artırdığını söylemişleridir. Bu eylemler demokratik süreçlere müdahale, siyasi ve ekonomik baskı, dezenformasyon kampanyaları, kötü niyetli siber faaliyetler ve yasa dışı istihbarat faaliyetlerini içerir şekildedir. NATO bu bağlamda hibrit saldırılara karşı koymak için araçlar geliştirdiğinin ve ittifak ile müttefiklerin savunmaya hazır olmalarını sağlayacağının üstünde durmuştur (NATO, Vilnius Summit Communiqué, 2023). NATO ayrıca önemli kötü amaç taşıyan siber faaliyetlere karşılık olarak ulusal önlem çabalarını desteklemek üzere Sanal Siber Olay Destek Yeteneği'ni (VCISC) başlattı. Liderler ayrıca siyasi, askeri ve teknik düzeylerdeki karar vericileri bir araya getirecek olan ilk kapsamlı NATO Siber Savunma Konferansı'nın Kasım 2023'te Berlin'de yapılacağını açıkladılar (NATO, Cyber Defence, 2023).

NATO siber güvenlik konusuyla yakından ilgilenmiş ve müttfefikleri ile iş birliği bağlamında uyumlu bir şekilde tehditlere karşı etkin bir savunma için stratejilerini güncellemiştir. Bunu yaparken asıl amacını ön planda tutmuş ve modern siber tehditleri klasik askeri tehdit boyutları kadar ciddiye almıştır. Ayrıca NATO'nun siber savunma anlamında bir takım ortaklıkları öngörmesi de siber savunma disiplini misyonunun genişliğini göstermektedir.

3.2.3. NATO ve Siber Alanda Mücadele

NATO modern çağın getirmiş olduğu yeni siber mücadele alanlarında etkinliğini açıkça belirtmektedir. Halihazırda örgütün kurulmuş olduğu 1949 yılından günümüze kadar geçen süreçte yenilenen ve genişleyen güvenlik olgularına uyum sağlamak adına adımlar attığı görülmektedir. Üye ülkeler bu bağlamda iş birliğini önemsemiş ve üstlerine düşenleri yapmak için hazırlanmışlardır. Aynı şekilde NATO ortaklıklar kurarak siber savunmaya katkı sağlamak için çalışmalarını sürdürmektedir. Siber uzayda güvenliği artırmak ve uluslararası barışı korumak için NATO oldukça uyumlu adımlar atmaya dikkat etmektedir.

NATO'nun siber uzayda savunma stratejisini etkileyen en önemli olaylardan biri kendi üye ülkesi olan Estonya'ya yapılan siber saldırıdır. Estonya 2007 yılının ilkbaharında üç hafta süresince bir dizi siyasi amaçlı siber saldırıya maruz kalmıştır. Siyasi mesaj içeren web tahribatları siyasi partilerin web sitelerini hedef almıştır. Hükümet ve ticari kuruluşlar farklı şekillerde hizmet engellemesi veya DDoS saldırılarına maruz kalmıştır. Hedefler arasında Estonya devlet kurumları

ve hizmetleri, okullar, bankalar, İnternet Servis Sağlayıcıları (İSS), medya kanalları ve özel web siteleri de yer almıştır. Estonya hükümetinin II. Dünya Savaşı'na ait bir Sovyet anıtını Talinn'in merkezindeki eski yerinden askeri bir mezarlığa taşıma kararı Estonya'da toplumsal ayaklanmaları, Moskova'daki Estonya Büyükelçisi'ne yönelik şiddeti, RF'nin dolaylı ekonomik yaptırımlarını ve Estonya'ya yönelik siyasi amaçlı siber saldırı girişimlerini tetiklemiştir.

28 Nisan itibariyle Estonya'ya yönelik siber saldırıların rastgele suç eylemlerinden daha fazlası olduğu resmi olarak kabul edilmiştir (Czosseck vd., 2011). Olay kısa bir süre içerisinde dünya genelinde dikkat çekmiş ve medyada saldırılar ilk *Siber Savaş* olarak adlandırılmıştır (Landler ve Markoff, 2007). Bu olayın bir sonucu olarak NATO siber saldırılara karşı ortak bir strateji geliştirmeye başlamıştır (Blomfield, 2007). 2010 yılında NATO'nun yayınlamış olduğu stratejik konseptinde siber saldırıları bir tehdit olarak algıladığını belirtmesi ve üye ülkelerin güvenliklerini bu alanda güçlendirmelerini tercih etmesi siber alanı ciddiye aldığını göstermektedir.

Siber güvenlik politika ve stratejileri oldukça başarılı olan NATO aynı zamanda siber alanda mücadele etmek için çeşitli faaliyetler de yürütmektedir. Örneğin siber tatbikatlar yapmaktadır. Bu sayede müttefiklerin ve birliğin siber tehditlerle karşı karşıya kaldıklarında nasıl başa çıkabilecekleri değerlendirilebilecektir. Siber savunma stratejileri, teknolojik alt yapıları güçlendirilip siber güvenlik boyutları sağlamlaştırılabilir. Siber alanın karmaşıklığı ve hızla yenilenen tehditlerle mücadele etme kapsamında tatbikatlar etkili bir savunma için yol haritası oluşturabilir.

Estonya'daki NATO İş birliği Siber Savunma Mükemmeliyet Merkezi tarafından her yıl düzenlenen Locked Shields tatbikatına NATO müttefikleri ve ortaklarının da aralarında bulunduğu 38 ülkeden üç binden fazla katılımcı dahil olmuştur. Locked Shields dünyanın en büyük siber savunma tatbikatı olarak bilinmektedir. Tatbikat 18 Nisan 2023 tarihinde başlamış ve bilgisayar sistemlerinin gerçek zamanlı saldırılardan korunmasını ve kritik durumlarda taktik ve stratejik kararların simüle edilmesini içerir şekilde gerçekleşmiştir (NATO Allies and Partners Take Part in World's Largest Cyber Defence Exercise, 2023).

27 Kasım – 1 Aralık 2023 tarihleri arasında deneyler uygulamak, siber uzay savaşını yönetebilmek ve siber alanda yetenek geliştirmek için Siber Koalisyon gerçekleşmiştir. Müttefik Dönüşüm Komutanlığı tarafından koordine edilen ve her yıl NATO kuruluşları, endüstri ve akademiden paydaşlarla iş birliği içinde düzenlenen Siber Koalisyon deney kampanyası, tatbikat senaryosu ve konusu ile uyumlu üç deney gerçekleştirmiştir:

- Görev Analizi ve Çözümleme Deneyi, askeri görevlerin siber faaliyetlerle uyumlu hale getirilebilecek şekilde çözümlenmesini sağlayacak bir metodoloji geliştirilmesine yardımcı olmak için yapılmıştır.

- Siber İletişim Merkezi Kabiliyeti, NATO'ya standart siber iletişim biçimlerini ve halihazırda olay örgüleri tarafından kullanılmakta olan bilgi paylaşımını ve bunlardan otomatik olarak istifade edilmesini kolaylaştıracak bir vasıta sağlamaktadır.
- Siber Durum Bilinci Platformu, iki stratejik komutanlığın konsepti, kabiliyet ihtiyaçlarını ve kullanım şekillerini kavramasının operasyonel olarak onaylanmasını mümkün kılacaktır.

Siber Koalisyon NATO'nun en önemli yıllık kolektif siber savunma uygulaması olup dünyanın en büyük tatbikatlarından biridir. Askeri Komite'nin yönetimi altında Müttefik Dönüşüm Komutanlığı tarafından planlanmakta ve yürütülmektedir (NATO's Strategic Warfare Development Command, 2023).

Sonuç olarak özellikle kendi müttefiki olan Estonya'ya yapılan siber saldırı etkisiyle de NATO, geliştirmekte olduğu siber savunma stratejilerini güçlendirme konusunda önemli adımlar atmıştır. Bu çerçevede birlik üye ülkeleri arasında bilgi paylaşımını artırmak, ortak siber tatbikatlar düzenlemek, savunma politikalarını ve misyonunu belirlemek için çaba sarf etmek gibi bir dizi önlemler almıştır. Birliğin siber alandaki mücadelesi müttefikler nezdinde iş birliği çerçevesinde günden güne gelişmektedir. Aynı şekilde birliğin siber alanda çalışmalar yapmaya başladığı ilk andan itibaren siber saldırıların hızlı ve karmaşık yapısına uygun şekilde stratejiler geliştirebildiği görülmektedir. Bu gelişme bizi örgütün siber uzaydaki geleceğinin parlak olabileceği sonucuna götürebilir.

3.2.3.1. Siber Alan Açısından NATO'nun Kurumsal Analizi

NATO sağlam bir kurumsal temele sahip çok taraflı bir güvenlik örgütüdür ve günümüzde giderek artan siber tehditlere karşı mücadele etme konusunda oldukça iyi bir konumda olduğu söylenebilir. Siber güvenliğe olan ilgisini yayınlamış olduğu stratejik konseptler ve siber güvenlik tatbikatları gibi çalışmaları ile gözler önüne sermektedir. Bahsi geçen çalışmaları ile örgüt üye ülkelerinin siber savunma ve güvenlik alanındaki uzmanlığını bir araya getirerek siber alanda iş birliği yapmakta ve savunma kapasitelerini güçlendirmek için önlemler almaktadır. Bu çerçevede birliğin ortakları arasında siber tehditlerin engellenebilmesi, tespiti ve caydırıcı unsurları için bilgi paylaşımı ve ortak politikalar gibi önlemler sıkça gerçekleştirilmektedir. Bu bağlamda NATO'yu başarılı kılan en önemli durumlardan biri de siber tehditlere karşı yanıt verme kabiliyetini artırmak için sürekli olarak siber gelişmelere ayak uyduracak hızda politika ve stratejiler geliştirmesidir. Ayrıca NATO'nun siber alandaki iş birliği kapasitesini artırmak için diğer uluslararası örgütlerle görüşmeler yapıyor oluşu siber başarısında etkili olmuştur. Bu gibi olgular birliğin siber uzayda sürekli olarak gelişimini sağlamaktadır.

NATO her ne kadar siber uzayda birtakım çalışmalar yürüterek üyelerin siber güvenliğini artırmaya çalışsa da başarılı olmasının yanı sıra birtakım sorunları da bulunmaktadır. Siber tehditleri en tehlikeli yapan unsurlarından biri saldırıların kim veya ne tarafından geldiğinin tespitinin zor olmasıdır. Bu bağlamda birliğin siber saldırıları spesifik aktörlerle net bir şekilde ilişkilendirmesi zordur. Çeşitli aktörlerin varlığına karşı mücadele etmesi ve saldırıları caydırması siber güvenliği oldukça karmaşık duruma getirebilmektedir. NATO bu gerçeğin farkında olan bir birliktir ve olaya göre değişen bir siber güvenlik duruşu sergilemiştir. Bunu da olaylara ve durumlara paralel geliştirdiği siber savunma stratejileri ile göstermektedir. NATO'nun siber güvenlik rolü giderek daha belirgin hale gelmektedir. Küresel güvenlik sorunları genellikle çok taraflı çözümler gerektirir ve NATO bu tür zorluklarla başa çıkmak için uyarlanabilir kurumsal yeteneklere sahiptir (Burton, 2015: 313-314).

NATO'nun siber güvenlik alanındaki rolü kolektif savunma, kriz yönetimi ve iş birliğine dayalı güvenlik gibi temel görevlerini destekleyerek müttefiklerin güvenliğini güçlendirebilir ve küresel istikrarı artırabilir niteliktedir. Birliğin siber savunma kapasitesi, ortakların kendi yetenekleriyle birleşerek oluşturduğu bir yapıya dayanmaktadır. Bu kapsamda NATO siber savunma yeteneklerini artırmak için çeşitli eğitim programları ve tatbikatlar yapmaktadır. Ayrıca NATO'nun diğer uluslararası kuruluşlarla da iş birliği yaparak siber güvenlik alanındaki etkinliğini artırmayı hedeflediği görülmektedir. Kollektif bir savunma örgütü olan NATO'nun siber alanda da savunma gücünün oldukça yüksek seviyede olduğu sonucuna varabiliriz.

3.2.3.2. Üye Ülkelerin Genel Olarak Siber Savunmaya Katkısı

NATO'ya üye ülkeler genel anlamda siber tehditlerle başa çıkabilmek için ortak bir düzlemde hareket etmektedirler. Bunu istihbarat paylaşımı, ortak eğitim çalışmaları, tatbikatlar düzenlemek gibi faaliyetler ile sağlarlar. Müttefikler arasındaki iş birliği desteklenerek siber savunma kapasitelerinin güçlenebilmesi için NATO üyesi ülkeler birliğe katkıda bulunmaktadırlar.

Birtakım ülkeler NATO'nun siber savunma sistemlerine daha fazla kaynak ayırabiliyorken bazı ülkeler de uzmanlık ve teknolojik katkılar ile fayda sağlamaktadır. ABD'nin siber savunmada lider rol üstlendiği söylenebilir. Bunun sebebi de ABD'nin[12] siber alanda oldukça gelişmiş strateji ve kaynaklara sahip olmasıdır. Bu bağlamda NATO'ya kaynak ayırarak destek olmakta bilgi paylaşımı ile istihbarata önemli katkılar sağlamaktadır. Ayrıca ABD'nin Ulusal Güvenlik Ajansı (NSA) ve Siber Komutanlık gibi kurumları NATO müttefikleriyle bilgi paylaşımı ve iş birliği içerisinde olarak siber savunmayı geliştirmeye yardımcı olmaktadırlar. İngiltere, Government Communications

[12] ABD bilgi güvenliği ve kritik altyapıların korunması konularında dünyanın önde gelen ülkelerindendir. Bilgi ve iletişim teknolojilerinin gelişiminde ABD ile diğer ülkeler arasında büyük bir fark olmasına rağmen, ABD bu alanda dünyaya liderlik etmek için sürekli bir gayret sergilemektedir. Bu nedenle her yıl bu alandaki araştırma, geliştirme ve yeniliklere önemli miktarda bütçe harcanmaktadır (Saeid, 2023: 115).

Headquarters (GCHQ) gibi kurumlar ile siber istihbaratı NATO üye ülkeleri ile paylaşarak ortak tehditlere karşı koymaya yardımcı olmaktadır.

NATO üyesi ülkeler uzman personeller ile siber savunmaya katkı sağlamaktadırlar. Bu bağlamda, bilgi ve deneyimler kullanılarak siber tehlikelerin analiz edilmesi ve istihbarat paylaşımı ile olası negatif gelişmelerin en aza indirilmesine fayda sağlanmaktadır. Siber güvenliğin sağlanabilmesi için en önemli katkılardan biri de eğitimdir. Siber uzayın tehlikeli hale gelmesindeki en büyük etken şüphesiz bilinçsiz kullanım ve tehlikeye neden olabilecek eğitimsizlik seviyesidir. Bu açıdan bakıldığında eğitimin önemi görülmektedir. Müttefikler hem kapasitelerini geliştirmek hem birbirlerine destek olmak hem de bilinçli personeller açısından eğitim konusunda siber güvenliğe destek vermektedirler. Almanya, Fransa ve Türkiye gibi müttefik ülkeler eğitim programlarına katılarak destek sağlamaktadırlar. Bu eğitimlerde siber tehditlerin doğasını anlamak ve olası sonuçlara karşı önlemler alabilmek için kapasiteler genişletilmektedir. Aynı şekilde üye ülkelerin ortak savunma sistemlerinin gelişmesi ve benzer potansiyellere sahip olmalarına fayda sağlamaktadır.

Sonuç olarak müttefikler giderek karmaşıklaşan siber uzayda tehlikeleri engelleyebilmek için ortak perspektifte birliğe eğitim vermek, tatbikatlara katılım sağlamak ve uzman personeller yetiştirmek şeklinde katkıda bulunmaktadırlar. Yani kaynaklarını ve uzman personellerini bir araya getirerek ortak bir paylaşım stratejisi izlemektedirler.

3.2.3.3. Örgütün Üye Ülkeler Dışındaki Aktörler ile Siber Alan İlişkisi

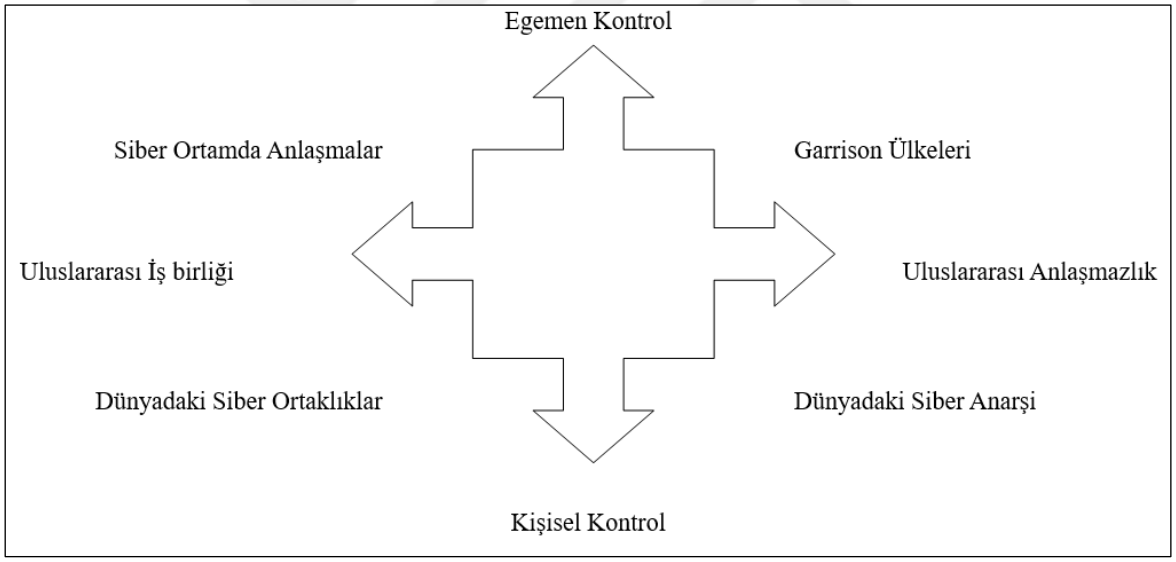
NATO, siber tehditlerin artmasıyla birlikte ortak güvenliği geliştirmek amacıyla bir dizi ülke ve uluslararası kuruluşlarla iş birliği içindedir. Bu iş birliği, ortak ülkeler arasında paylaşılan değerler ve siber savunma konusundaki ortak girişimler üzerine kurulmuştur. Bu girişimlerin amacı, siber tehditlere karşı koymak, siber altyapıları korumak ve siber saldırıların etkilerini en aza indirmektir. NATO'nun bu çabaları, uluslararası platformlarda diğer ülkeler ve kuruluşlarla koordinasyon ve iş birliği yaparak, siber güvenlik alanında bir dayanışma ve etkili bir savunma sağlamayı amaçlamaktadır (NATO, Cyber Defence, 2023).

İttifak ülkelerinin liderleri tarafından 2014 Galler Zirvesi'nde onaylanmış olan NATO Sanayi Siber Ortaklığı, siber tehditler konusunda güncel bilgi paylaşımının teşvik edilmesini ve katılımcıların durumsal farkındalıklarını artırmalarını amaçlamaktadır. NATO ve endüstri, siber alanda ortak risklerle karşı karşıya kaldığı için hem teknik seviyede hem de operasyonel seviyede karşılıklı fayda için birlikte çalışmaktadır. Girişime NATO birimleri, ulusal Bilgisayar Acil Durum Müdahale Ekipleri (CERTs) ve NATO üyesi ülkelerin endüstri temsilcileri katılmaktadır. Bu oluşum NATO ve ortaklarına yönelik siber tehditler konusunda bilinci artırmayı ve herkesin direncini ve

bilgi güvenliği konusundaki kapasitesini arttırmayı hedeflemektedir (NATO Industry Cyber Partnership, 2023).

NATO süratle değişen siber ortama uyum sağlamak adına sayıları giderek artan ortaklarıyla daha yakın bir iş birliği içine girmiştir. Bu kapsamda 2016 yılında NATO Genel Sekreteri, Avrupa Konseyi ve Avrupa Komisyonu Başkanları ile bir araya gelerek NATO-AB İş birliği üzerine Ortak Bildiri'nin yayınlanması konusunu ele almıştır. Bu bildiri çerçevesinde NATO'nun olaylara müdahale timleri ile AB arasında bir teknik anlaşma onaylanmıştır. Anlaşmanın hedefi özellikle enformasyon paylaşımı, eğitim, araştırma ve tatbikatlar gibi alanlarda iş birliğini artırmaya yöneliktir. Bu gelişmelerin her iki örgütün de stratejik hedeflerine ulaşmasına ve ortak güvenlik çıkarlarını daha etkili bir şekilde korumasına yardımcı olması beklenmektedir (Brent, 2019). Bu bağlamda NATO yakın zamanda 22 Eylül 2023 tarihinde AB ile bir görüşme[13] yapmıştır. Bu görüşmede siber uzaydaki zorlu süreç ve iş birlikleri ele alınmıştır (NATO and the European Union Meet to Discuss Deepening Cooperation on Cyber Defence, 2023).

Şekil 4: Uluslararası İş birliği ve Koordinasyona Dayanan Küresel Siber Müşterek



Kaynak: Choucri, 2013

Siber savunmada ortaklık kuruluşların güçlerini birleştirebilmeleri sonucunda hızlı ve sürekli gelişen siber tehditlere karşı güçlenebilmek açısından oldukça önemlidir. Siber uzay halihazırda

[13] 22 Eylül 2023 tarihli NATO-AB görüşmelerinde, Güvenliğin Önündeki Yeni Zorluklardan Sorumlu Genel Sekreter Yardımcısı David van Weel, siber uzayın sürekli bir rekabete sahne olduğunu ifade etmiştir. David van Weel şu ifadeleri kullanmıştır: *"Siber uzayda savunmanın etkin bir şekilde gerçekleştirilebilmesi, ortaklarla daha fazla angajmana yönelik bir anlayış değişikliği de dâhil olmak üzere daha proaktif bir yaklaşım izlenmesini gerektirmektedir. Siber uzay ancak işbirlikçi bir ruhla savunma altına alınabilir. NATO ve AB siber girişimleri arasında daha fazla sinerji oluşması kritik altyapıların korunması da dâhil olmak üzere hem vatandaşlarımızın hem ekonomilerimizin hem de siber savunmalarımızın refah ve güvenliğini arttıracaktır."* (NATO and the European Union Meet to Discuss Deepening Cooperation on Cyber Defence, 2023).

karmaşık bir alan olmakla birlikte günden güne tehlikeli bir boyuta ulaşmaktadır. Bu bağlamda NATO ve ortakları stratejilerini iş birliği içerisinde geliştirerek emin adımlar atmak doğrultusunda görüşmelerini sürdürmektedirler. Kollektif güçler saldırıların etkisini azaltıp hasarı en aza indirme konusunda başarılı olabilmektedirler.

3.2.3.4. Uluslararası Savunmadan Siber Diplomasiye Geçiş

NATO, tarihsel olarak savunma odaklı askeri bir ittifak olarak bilinmektedir. Günlük hayatta güvenlik olgusunun refahın temel taşlarından biri olduğu belirgindir. NATO'nun nihai amacı ise üyelerinin siyasi ve askeri araçlarla özgürlüğünü ve güvenliğini sağlamaktır. Siyasi olarak demokratik ilkeleri desteklemekte ve üyeler arasında savunma ve güvenlik konularında danışma ve iş birliği yaparak problemleri çözmeyi, güven oluşturmayı ve uzun vadede çatışmaları önlemeyi hedeflemektedir. Askeri olarak ise anlaşmazlıkların barışçıl çözümünü taahhüt eder. Diplomatik çabaların başarısız olması durumunda kriz yönetimi operasyonlarını gerçekleştirebilecek askeri güce sahiptir. Bu operasyonlar, NATO'nun Washington Antlaşması'nın 5. Maddesi uyarınca veya BM yetkisi altında, tek başına veya diğer ülkeler ve uluslararası örgütlerle iş birliği içinde gerçekleştirilebilir (NATO, What is NATO?, 2023).

Teknolojinin gelişim hızı ve güvenlik paradigmasındaki değişim NATO'nun siber alanda savunma sistemlerini geliştirmesine yol açmıştır. Çünkü siber alanın genişlemesi sonucunda uluslararası savunma alanı sadece askeri güç kullanımı ile sınırlı kalmayıp aynı zamanda siber güvenlikle de kavramsallaşmıştır. Bu bağlamda NATO gelişmelerin akabinde siber diplomasi ile güvenlik kapsamını genişletmiştir. Siber tehditler uluslararası alanda sınırları aşarak tehlikeli ve gerilim oluşturucu etkiye sahip olmuştur. Birliğin siber güvenliğe yönelik çalışmaları iş birliği içerisinde üye ülkelerin kapasitelerini genişletmek, uluslararası anlaşmalar yaparak ortaklık içerisinde ilerlemektedir. Halihazırda temel amaçları doğrultusunda uluslararası savunma duruşunu devam ettiren NATO aynı zamanda siber güvenlik konularında çalışmaları sürdürmektedir.

3.2.3.5. Siber Uzayın Savaş Alanı İlan Edilmesi ve Gelecek Kurgusu

Geleneksel savaş anlayışının ötesinde siber alanın bir çatışma ortamına evrilmesi olası ve araştırma alanı olan bir konu haline gelmiştir. Çünkü günümüz teknolojisinde birtakım tehditlerin varlığı yeni ve öngörülemez bir tehlike boyutu taşımaktadır. Siber casuslar kötü amaçlı yazılımlar ile saldırılar düzenleyip siber uzayda negatif gelişmelere yol açmaktadırlar. Bu durum devletler ve örgütler için uluslararası bir güvenlik açığı haline gelmekte ve siber çatışmaların yaşanabilme olasılığını ön plana çıkarmaktadır. Siber uzay içerisinde sağlık, ekonomi, askeri ve birçok kritik alanı barındırdığı için olası bir savaşın yıkıcı sonuçları endişe verici olabilmektedir.

Bilgi teknolojileri ve iletişim sistemlerinin temelinde yatan kritik altyapıların tehlikeye girmesi ve siber uzayın sonsuz döngüsünde tehlikenin kimden veya neden kaynaklı olduğunun tespitinin zor olması siber alanda savaş oluşumunu tetikleyebilir. Her ne kadar internet aracılığı ile yapılan saldırılar geleneksel savaşlar kadar yıkıcı görünmese de sonuçları fiziksel tehditler kadar tehlikeli olabilir. Uluslararası ortamda henüz bir siber savaş ilan edilmemiş olsa da devletler ve örgütler bu ihtimali önleyebilmek için siber savunma sistemlerini geliştirmektedirler.

İnternet ortamında yaşanan her negatif durumu savaş veya saldırı olarak adlandırmak yanıltıcı olacaktır. Bu durumu ayrıştırabilmek için sonuca odaklanmak faydalı olabilir. Lewis (2011: 23)'e göre negatif bir durumun en az fiziksel boyut kadar zarar verebilmiş olması onu saldırı ya da savaş olarak nitelendirme konusundaki belirsizliği ortadan kaldırabilir. Siber saldırılar bireysel eylemler ile gerçekleştirilip hedeflediği yıkım ile sonuca ulaşmayı amaçlar. Yani saldırı olabilmesi için şiddet veya şiddet tehdidi, genellikle fiziksel zarar veya fiziksel zarar tehdidi ile ilişkilidir. Savaş boyutu ise siyasi hedeflere ulaşmak için güç kullanımını içermesi ile ayrıştırılabilir. Eğer olay şiddet veya şiddet tehdidi içermiyorsa, siber saldırı olarak değerlendirilmez. Bu ayrımı yaparken güç veya şiddet kullanımını gerektiren gizli eylemler ile yasadışı bilgi toplamayı amaçlayan casusluk arasındaki farkı belirlemek önemlidir.

İlk gerçek siber savaş, ilk dijital silahın kullanıldığı ve fiziksel dünya objelerinin manipüle edilmesine yol açan Stuxnet'in keşfiyle doğrulandığı 2010 yılına kadar uzanmaktadır. Stuxnet kötü niyetli bir bilgisayar solucanı aracılığı ile özellikle İran'ın nükleer santrifüjlerinde kullanılan Programlanabilir Mantıksal Denetleyicileri (PLC) hedef almıştır. Bu özel virüs türü kendisini kopyalayabilen bir solucan olarak tanımlanmaktadır. Etkisine bakıldığında ise binlerce nükleer santrifüjün bulunduğu ortamda Stuxnet beşte birlik bir kısmı etkisiz hale getirmeyi başarmıştır. Bu olay siber savaşların fiziksel dünya sorunlarına yol açabileceğini ilk kez gösteren önemli bir dönemeç olmuştur. Bir siber saldırının devletlerin askeri güçlerini etkileyebildiği görülmüştür (Sahu vd., 2016: 70).

Birlik açısından düşünüldüğünde olası bir siber savaşta müttefiklerin ve birliğin 5. Madde'de belirtildiği şekilde bir zarar gördükleri varsayıldığında NATO'nun karşılık vermeme olasılığı oldukça düşüktür. Üye ülkelerin iş birliği içerisinde bu tarz bir saldırıya karşılık verebilmeleri için seçenekleri oldukça çeşitlidir. NATO'nun büyük bir siber saldırıya yanıtı, her bir olayın jeopolitik koşullarına bağlı olacaktır ancak, 5. Madde'nin devreye sokulabilmesi için siber saldırıların mevcudiyet alanlarında gerçekleştirilmiş olması, saldırının şiddetinin silahlı saldırı boyutuna ulaşmış olması, sibernetik yeteneklerden ödün verilmeksizin saldırının kim tarafından gerçekleştirildiğinin doğrulanabilmesi ve siber saldırının terörist ya da devlet destekli olması halinde olasıdır. Bununla birlikte, bir müttefikin büyük bir siber savaş eylemi üzerine 5. Madde'ye başvurması halinde müttefikler birbirlerinin kolektif yardımına koşacaklardır. Bu da NATO'nun ortaklık ve iş birliği ilkesiyle örtüşmektedir (Ghavam, 2016: 104).

11 Temmuz 2023 tarihinde NATO'nun Vilnius'ta gerçekleştirdiği zirvede, RF ve ÇHC'nin siber alanda kötü amaçlı faaliyetlerinin değerlendirilmesi olası bir savaş durumunda tedbirli olunacağı ve karşılık verebileceği olasılığını göstermektedir. NATO zirvede RF'nin NATO müttefiklerine ve ortaklarına karşı hibrit eylemlerini artırmış durumda olduğunu vurgulamıştır. Ayrıca bu faaliyetler içerisinde demokratik süreçlere müdahale, siyasi ve ekonomik baskı, yaygın dezenformasyon kampanyaları, kötü niyetli siber faaliyetler ve Rus istihbarat servislerinin yasadışı ve yıkıcı faaliyetleri yer aldığını belirtmiştir. Bu bağlamda RF'nin hibrit eylemlerine karşı koymak için caydırıcı ve savunmaya hazır olmaları için ortakları ve müttefiklerini hazırlayacağını açıklamıştır. ÇHC için ise benzer şekilde baskıcı politikalar ile ittifakın güvenliğini ve değer yargılarını tehlikeye soktuğunu belirtmiştir. Buna ek olarak, kötü niyetli hibrit ve siber operasyonları ile çatışmacı söylemleri ve yanıltıcı bilgileri üye ülkeleri hedef aldığını ve birliğin güvenliğine zarar verdiğini açıklamıştır. Yani ÇHC'nin stratejik bağımlılıklar yaratmak ve etkinliğini artırmak için ekonomik kaldıracını kullanarak uzay, siber ve denizcilik alanları da dâhil olmak üzere kurallara dayalı uluslararası düzeni yıkmaya çalıştığını belirtmiştir. Bu bağlamda bahsi geçen ülkeleri yapıcı olmaya davet etmekle birlikte olası negatif gelişmelere hazır olunacağı belirtilmiştir (NATO, Vilnius Summit Communiqué, 2023). NATO'nun bu zirvede iki ülkeyi açıkça tehditlerini belirtir şekilde uyarması gelecekte yaşanabilecek bir siber savaş kurgusunda olası tehdit aktörlerini ortaya koyuyor olabilir.

Gelecekte bir siber savaş olasılığı düşünüldüğünde, günümüzde siber alanda gerçekleşen olgulara ve kullanılan araçlara bakmak yardımcı olabilir. Siber alanda aktif olan birçok devletin desteklediği Advanced Persistent Threat (APT) grupları bulunmaktadır. Bu gruplar, çoğunlukla devletin çıkarlarını desteklemek, rakip ülkelerin veya kuruluşların faaliyetlerini izlemek, stratejik bilgi toplamak veya bilgi sızdırmak gibi belirli amaçlar için faaliyet göstermektedirler. Bu bağlamda devletler bir diğer siber savunma algoritması olarak Cyber Threat Intelligence (CTI) ile siber tehditler hakkında bilgi toplama, analiz etme ve yorumlama sürecini gerçekleştirmektedirler. Siber güvenlik alanında sıkça kullanılan terimlerden bir diğeri ise Taktikler, Teknikler ve Prosedürler (TTP) kavramıdır. Bu terim siber tehdit aktörlerinin nasıl hareket ettiğini, saldırıları nasıl gerçekleştirdiğini ve hedeflere nasıl ulaştığını betimlemektedir. Aynı şekilde Mıtre Attack saldırı haritası siber güvenlik alanındaki savaşçıların siber saldırganların taktiklerini, tekniklerini ve yöntemlerini anlamalarına ve savunma stratejileri geliştirmelerine yardımcı olmaktadır. Web Application Firewall (WAF) ise internet sitelerindeki uygulamalarını korumak için kullanılan bir güvenlik önlemidir. Bunu yaparken, web sunucusu ve istemcisi arasındaki trafiği izlemekte ve bu trafiği analiz ederek kötü niyetli veya istenmeyen aktiviteleri engellemektedir. Bu gibi olgular siber alanda gelecek dönemin nasıl evrileceğine dair örnekler olabilir.

SONUÇ ve ÖNERİLER

Evrende var olan her oluşum ve canlı için güvenlik önemli olabilmektedir. Güvenliğin sağladığı olumlu durumların sayısı oldukça fazladır. Refah, verimli yaşam, sağlık, sosyal etkileşim ve iletişim gibi birçok unsur güvenlikle ilişkilendirilebilir. Uluslararası ilişkiler bağlamında devletler için güvenlik hem ulusal hem de uluslararası alanda oluşumun temelini atan bir unsurdur. Özellikle bireyler için kendi varlıklarını sürdürebilmeleri adına güvensizlik olgusunun yok oluşu ya da en aza indirilmesi oldukça önemlidir.

Uluslararası ilişkiler bağlamında devletlerin güvenliği düşünüldüğünde bu alanda birçok çalışmalar yapılmıştır. Çünkü güvenlik küresel çapta dünya sorunlarının tümünü kapsar şekilde sonsuz bir döngü ile yaşamaktadır. Ayrıca bu aktif durum devletleri uluslararası arenada birbirleri ile iletişim halinde tutmaktadır. Bu durumun da iş birliği ve anlaşmalar gibi birtakım sonuçları mevcuttur. Uluslararası sistemdeki anarşi durumu göz önüne alındığında devletler için güvensiz ortamın en aza indirilmesi kendi sınırları ve bölgesel konumları için oldukça önemlidir. Bu bağlamda devletler sınır ötesi güvenlik konularına önem verirken ulusal güvenlikleri anlamında asayişi sağlamak için birçok faaliyet yürütmektedirler. Bu faaliyetler oldukça geniş kapsamlıdır, çünkü güvenlik olgusunun boyutları birçok durumu kapsar şekildedir. Güvenlik, bireysel düzeyden uluslararası konulara kadar birçok alanda referans nesnesi halindedir.

Güvenliğin geniş kapsamlı oluşu uluslararası ilişkiler teorileri bağlamında dönemsel ve olaysal gelişmelerin de etkisi ile onun hakkında farklı çıkarımlar yapılmasına neden olmuştur. Realist düşünceye göre devletler temel aktördür ve güç, çıkarlar üzerinde odaklanırlar. Uluslararası sistemdeki rekabet ortamında güvenliklerini sağlamaları için bu unsurların önemi oldukça fazladır. İngiliz Okulu düşüncesine göre ise güvenlik toplumun ilgilendiği her konuyu kapsar şekilde genişlemiştir. Liberalizm ise güvenlik konularını daha da genişleterek sadece askeri güvenlikle sınırlı kalmayıp bireysel özgürlük ve devletler nezdinde iş birliği gibi unsurlardan bahsetmiştir. Bunun dışında eleştirel teori düşüncesine göre özgürlük temel yapıtaşıdır. Aynı zamanda güvenliği tüm sosyal olgularla ilişkilendirmektedirler.

20. yüzyılın yarısına gelindiğinde güvenliğin doğası evrimleşmiştir. Klasik güvenlik anlayışı yerine birçok yeni güvenlik algıları gelişmiştir. Fakat uluslararası ilişkiler teorilerinde de görüldüğü üzere geçmişte bu yeni güvenlik algısının temelleri çoktan atılmaktaydı. Bunun dışında bu teorilerin güvenlik yorumları yaşanan gelişmeler ile ilişkilendirildiğinde birçok durumu açıklayabilecek öngörüşe sahip olabilmektedirler. Uluslararası sistemin aktörlerinin günümüzde hala süregelen çıkar

çatışmaları ile güç kullanım oranlarının artışı ve bunun yanında ulusal ve sınır dışı alanlarda asayişin sağlanabilmesi için ticaret, sağlık, siber uzay gibi alanlarda toplum güvenliği dahil edildiğinde ulaşılan iş birliği gibi sonuçları açıklamak için birçok teoriye başvurulabilir.

Tarihsel süreçte yaşanan tüm bu gelişmeler güvenliğin açıklanmasını zorlaştırmakla birlikte varlığının önemini atfeder şekilde olmuştur. Özellikle Soğuk Savaş sonrası dönemde tüm dünyayı ilgilendiren güvenlik tehditleri doğmuştur. Bu gelişme hem devletler hem de bireyler için oldukça endişe verici bir gelişmedir. Bunu 11 Eylül saldırılarında açıkça bütün dünya hissetmiştir. Korkunun ve güvensizlik durumlarının yaşandığı terörizmin sınırları aşabilen bir tehdit olduğu görülmüştür. Medeniyet temellerinin derinden sarsıldığı ve insan canına kasten zarar gelmesi amaçlanan terörün varlığı korkuya ve güvensizlik ortamına neden olmuştur. Daha da endişe verici olan ise fiziksel dünyada yaşanan saldırıların yanı sıra artık neredeyse her bireyin ve her aktörün içerisinde aktif şekilde barındığı siber uzay alanı tehlikeleridir.

Teknolojinin vazgeçilemez olanaklar sağladığı görülmektedir. Böylesi etkileyici bir alanda hızlı ve aktif şekilde faaliyetler sürdüren ve bilimsel gelişmelere dahi olanak sağlayan internet ortamının en başta yüksek boyutlarda tehlikelere ulaşabileceğini tahmin etmek zor olabilirdi. Fakat siber uzay oluşum gösterdiği ilk anlardan günümüze süregelen zaman diliminde neredeyse dünyanın alternatif bir evreni haline gelmiştir. Bu yalnızca bir benzetmedir. Siber alanda da toplum ve diğer aktörler yerleşim alanları oluşturup güvenli hale getirerek tehlikeye uğramadan aktif şekilde kullanım sağlamaya çalışmaktadırlar. Ne yazık ki terörizm faaliyetleri artık günümüzde siber alanda da yaşanmaktadır. Siber casuslar ve bilgisayar korsanları kötü amaçlı yazılımlar ile bireylere, örgütlere ve devletlere siber saldırılarda bulunabilmektedirler. Bu saldırıları tehlikeli yapan özelliklerinden biri de anonim oluşudur. Ayrıca bu tarz saldırılar hızlı ve sınır aşan şekilde yaşanmaktadır.

Dijital ortamda bireylerin ve diğer aktörlerin güvensiz hissetmesine neden olan siber tehlikelerin getirdiği yıkım oldukça endişe verici bir atmosfer oluşturmaktadır. Saldırgan tarafın hedefi ve amaçları oldukça geniş olabilir çünkü siber uzay karmaşık bir yapıdadır ve yalnızca tek tuşla yüksek finansal harcamalara ihtiyaç duyulmadan ciddi kayıplara neden olunabilir. Bu kayıplar uluslararası alanda hukuk, ticaret, diplomatik ilişkiler gibi alanları güvensiz duruma sokabilir. Bu bağlamda bir devletin ya da birliğin siber savunma geliştirmesi ulusal ve uluslararası güvenliği sağlamasına fayda sağlayabilecektir. Bunun için devletler kendi siber savunma gelişmelerini ilerletmektedirler. Aynı zamanda siber saldırılar ile mücadele edebilmek için ortaklık ve iş birliği sayesinde uluslararası ortam daha güvenli hale gelebilir.

NATO dahilinde Soğuk Savaş sonrası yaşanan güvenlik gelişmelerine kayıtsız kalmamış ve stratejilerini müttefiklerini koruyacak şekilde ortaklık ekseninde devam ettirmiştir. Birlik siber alanda mücadele edebilmek için yayınlamış olduğu stratejik konseptlerde yol haritası çizmiş ve tatbikatlar, eğitimler gibi faaliyetler ile müttefiklerini ortak zeminde hareket etmeye davet etmiştir.

Ayrıca NATO, siber uzayı öteki klasik savaş alanlarına -kara, deniz, hava ve uzay- beşinci alan olarak dahil etmiştir. Bu bağlamda siber saldırıların şiddet boyutuna göre 5. Madde'yi çekinmeden devreye sokabileceğini açıkça belirtmektedir.

Genel çerçeve ile bakıldığında NATO'nun siber savunma sistemlerini geliştirmesi, üye ülkelerin dayanışma ve ortaklık içerisinde olması ile desteklenmektedir. Zaten birliğin temel misyonu müttefiklerinin kolektif güvenliklerini sağlama temeline oturtulmuştur. Bu bağlamda Soğuk Savaş öncesi dönemde klasik güvenlik anlayışında yaptığı gibi sonrası dönemde gelişmiş olan siber tehditlere de benzer şekillerde tepkiler vereceği öngörülebilir. Fakat burada zor olan birtakım noktalar bulunmaktadır. Örneğin Soğuk Savaş dönemi düşünüldüğünde, Doğu-Batı blokları arasındaki çekişmeler ve tehlikenin nereden geldiği özellikle komünizme karşı önlemler alabilmek için hem jeopolitik hem de düşüncesel anlamda savunmanın kurulabilmesi daha kolaydı. Çünkü rakibin kim olduğu biliniyordu. Siber alan ise karmaşık ve sonsuz bir alandır, yani NATO üyelerini ne şekilde dış tehditlere karşı koruyabileceğini biliyor olsa bile kime ya da neye karşı bunu yapacağını tespit etmesi önemlidir. Siber uzay aktörlerinin kolayca gizlenebiliyor oluşu bunu oldukça zor bir hale getirmektedir.

Çalışmada, esas olarak incelenen NATO'nun savunma perspektifinde siber güvenliğin konumu sonucunda birliğin bu alana yoğun ilgisinin olduğu görülmektedir. Bu bağlamda örgütün çalışmaları aktif şekilde devam ettirdiği açıktır. Fakat müttefik olan 32 ülkenin her birinin siber alanda aynı düzeyde güvenlik boyutuna ulaşması oldukça karmaşık olacaktır. Bir siber saldırının hangi ülke için ne zararı olacağının tespiti burada önemlidir. Akabinde alınacak önlemlerin ve yeteneklerin geliştirilmesi de belirli bir bütçeye, insan kaynağına ve üretilen ürünler gibi unsurlara bağlıdır. Buradaki asıl soru birliğin ortak hareket etmeyi esas almış olmasına rağmen bu tür önlemler için her müttefikin aynı kapasiteye sahip olmaması durumudur. Bu noktada NATO müttefikleri arasında siber alanda kendisini geliştirmiş bir ülke olarak dikkat çeken ABD'dir. Bu bağlamda ABD'nin NATO'ya destek olucu bir yapıda olması fayda sağlayabilir.

NATO, müttefikleri için siber güvenlik çatı mimarisi oluşturabilir. Yani NATO üst akıl veren yapı olabilir. Bunu sağlarken de ABD gibi kendisini siber alanda geliştirmiş olan müttefiklerinin analiz ve tecrübelerinden faydalanabilir. NATO bilgi paylaşımı ile genel çerçeveye katkı sağlarken, tüm üyelere bu savunma sistemini sunabilir. Kendisini geliştirmiş üyelerin tecrübe ve analizleri NATO'ya iletilecek akabinde ise NATO bunları birleştirip genel bir çerçeve geliştirerek tüm müttefiklerine siber güvenlik sağlayabilecektir.

Birlik için en önemli olgulardan birinin istihbarat ve bilgi paylaşımı olduğu sıkça belirtilmektedir. Bu gibi paylaşımların kimi zaman siber alanda yapıldığı bilinmektedir. Siber istihbaratın tehlikeye girmesi, birlik için oldukça tehlikeli bir hal alabilir. Bunun için yalnızca birliğin değil, bir müttefikin saldırı altına girmesi öteki üye devletleri de tehlike altına sokabilmektedir.

NATO'ya üye olan 32 ülke dünya genelindeki internet kullanımının önemli bir kısmını kapsamaktadır. Bu açıdan bakıldığında her birinin hem ulusal hem de birlik nezdinde siber güvenliğinin sağlanmış olmasının önemi kritiktir. Ayrıca siber istihbarat sayesinde siber güvenlik için kurumsal bağlantılara güvenebilirler. Üye ülkeler arasındaki bilgi paylaşımı, nereden çok atak geldiğini hesaplayarak önlem almalarını sağlayabilir. Bu sayede ataklara ne şekilde cevap verileceği kolaylaşabilir. Aslında burada her şey bir döngü içerisindedir. Siber saldırıların nereden geldiğinin paylaşımı için istihbarata, istihbaratın korunabilmesi için de siber savunmaya ihtiyaç var. Her şey temelde güvenlik ile ilgilidir. Burada birlik, kendi üye ülkelerinin arasındaki bağlantıları güvenli kılmalıdır.

Bir gelecek kurgusu olarak olası bir siber savaş durumunda NATO'nun halihazırda geliştirilmiş ortak bir siber orduya ihtiyacı olabilir. Böyle bir siber ordunun kurulması müttefiklerin kendi uzman personellerini göndermeleri ve devlet destekli APT gruplarını bir araya toplamaları ile mümkün olabilir. Yani devlet destekli APT savaşçılar, NATO bünyesinde yan yana savaşabilirler. Şu an üye ülkelerden de birbirlerine siber atakların gittiği düşünüldüğünde, böyle bir siber ordunun kurulması durumunda yan yana savaşan devlet destekli APT gruplar birbirlerine atak yapmaktan vazgeçebilirler. Bu sayede 32 müttefik ülkenin birbirine yaptığı ataklar azalır ve diğer ataklar ile mücadele edebilmek için hız ve zaman kazanabilirler.

Her ne kadar şu anda NATO'nun NATO İşbirliğine Dayalı Siber Savunma Mükemmeliyet Merkezi siber savunma çalışmalarını sürdürse de açık kanallı bir siber ordu kurulması durumunda devlet denetiminde olmayan siber tehditler de engellenebilir. NATO bünyesindeki olası siber ordunun geniş kapasitesi düşünüldüğünde, hepsinin ortak hareket etmesi sonucunda tespit hızı artar ve güvenlik güçleri ile saldırılar daha kolay engellenir. Yani burada daha geniş kapsamlı bir ortaklık bahsi söz konusudur.

Siber güvenliğin oluşabilmesine katkı sağlamak için ortak bir CTI ve Indicators of Compromise (IOC) havuzu kurulabilir. Böyle bir ortak bir veri kubbesi oluşturulursa ataklar zarar vermeden engellenebilir. Müttefiklerden üç tanesine aynı anda başka bir ülkeden siber saldırı atağı geldiğini varsayacak olursak bir müttefikin, bu saldırının IP adresini incelemesi ve bilgi toplaması oldukça zaman alacaktır. Fakat bu bilgiyi elde eden ilk müttefik bunu havuza eklerse diğer tüm müttefikler bu atağı henüz gerçekleşmeden engelleyebilirler.

NATO müttefikleri siber savunmanın gelişebilmesi için ürün ve hizmetlerini birleştirebilirler. Siber güvenlik için kendi yapmış oldukları ürünleri paylaşırlarsa ortak ve daha fazla iş yapan bir ürün ortaya çıkabilir. Örneğin Mitre Attack saldırı haritası ile atakların aşamalarının kontrolü yapılmaktadır. Bu harita, güvenlik profesyonellerine, organizasyonlarının savunma stratejilerini geliştirirken hangi taktik ve tekniklerin dikkate alınması gerektiği konusunda bir rehber sağlar. Fakat elbette ki bunda birtakım eksiklikler mevcuttur. %100 oranda fayda sağladığını söylemek yanıltıcı

olacaktır. Aynı şekilde TTP sayesinde Mitre Attack içerisinde hangi durumda ne olduğu denetlenmektedir. Taktikler, hedefe ulaşma yolundaki stratejileri belirler. Teknikler, taktikleri aktive edebilmek için kullanılan yöntemlerdir. Prosedürler ise saldırganların kullandıkları taktik ve teknikleri saldırıları uyguladıkları andan sonuca kadar süregelen zaman diliminde neler yaptıklarını içerir. Aynı şekilde müttefiklerin Web Application Firewall (WAF), Domain Name System (DNS), Security Information and Event Management (SIEM) gibi bu tarz siber donanım ürünleri mevcuttur. Özellikle ABD bu çalışmalarda kendisini oldukça geliştirmiş bir ülkedir. 32 üye ülke baz alındığında NATO özelinde geliştirilen benzeri bir güvenlik çatı mimarisi ürünler geliştirilebilir. Bu ürünü farklı kılacak özelliği ise birden fazla devletin bir araya gelerek oluşturacağı ürünün kalitesi ve çok yönlü kapsamıdır. Ayrıca bireysel kullanıma oranla ortak bir ürün elde etmenin faydasının daha çok olacağını söylemek mümkündür.

Siber ordu sayesinde üye ülkeler daha az personel yardımı ile daha çok iş sağlayabilir. Aynı şekilde daha az finansal yatırım ile ortak paydada daha çok fayda sağlayabilirler. Üstelik birçok farklı insanın bir arada toplanması bilgi çeşitliliğine neden olur. Bu da ortak büyük bir akıl demektir. Farklı ülkelerden farklı bilgi düzeyinden gelen bireyler bilgi çeşitliliğini sağlarlar. Bu sayede siber savunmada gelişim artış gösterebilir. Farkı kaynaklar ve bakış açıları sayesinde daha geniş bir yelpaze ile bilinçli bilgiler elde edilebilir.

Siber güvenliği sağlamanın yanı sıra güvenilirlik olgusu da oldukça önemlidir. Olası bir siber ordu kurulması sayesinde birliğin, %80 oranda siber güvenlik sağladığı varsayılacak olunursa, 32 ülke içerisinde herhangi birinin tek bir hatası ya da olası düşmanca yaklaşımı sebebiyle bu oran %100 güvensizlik oranı ile yer değiştirebilir. Bu da risklerin en tehlikeli olanları arasında bir ihtimaldir. Fakat yine de anlaşmalar ve iş birliği esas alındığında böyle bir tehlikenin ortadan kalkması muhtemeldir. Ayrıca siber alanın karmaşık ve sonsuz sıfatları düşünüldüğünde her ülkenin bu alana ihtiyacı farklı olabilir. Bu da ortak bir paydada buluşma konusunda zorluk çıkarabilir. Öte yandan ise güvenliğin temel ihtiyaç olabileceği esas alındığında böyle bir birleşimin mantıklı yönleri baskın gelebilecektir. Bunun dışında finansal yatırım en can alıcı hususlardan bir tanesi olacaktır. Bu durumun bir sorun teşkil etmesinden ziyade daha az yatırım ile ortak paydada daha fazla pozitif dönüşüm elde edilebileceği hesaplanabilir.

NATO'nun bir müttefike yapılmış olan saldırının, tüm üye ülkelere yapılmış gibi kabul edilen bir ilkesi vardır. Bu prensip, NATO'nun kuruluş antlaşması olan Kuzey Atlantik Antlaşması'nın 5. Maddesi'nde açıkça ortaya koyulmuştur. Bu maddeye göre bir NATO üyesine yönelik bir saldırı, tüm NATO üyelerini doğrudan bir tehdit altında gördüğü için, diğer NATO üyelerinin de bu saldırıya karşı birlikte hareket etmeleri gerekmektedir. Bu madde siber saldırılar için de geçerlidir. Fakat buradaki ince çizgi siber saldırıların zarar boyutudur. Olası bir saldırı/savaş durumunda bu maddeyi siber ordusu ile devreye koyabilmesi için düşmanın kim olduğunun tespiti gereklidir.

Soğuk Savaş döneminde NATO'nun rakibi Varşova Paktı ve SB'ydi. Aralarında askeri, siyasi, ekonomik ve ideolojik rekabet bulunmaktaydı. Bunun akabinde savunmalar geliştirilmekteydi. Aynı şekilde NATO'nun belirli bir siber savunma için kendisine ve üye devletlere gelen aktif atakların dışında büyük tehlikenin nerelerden geleceğini tespit etmeye ihtiyacı olabilir. Bu tespit sayesinde doğru IP adreslerine karşı savunma gerçekleştirmesi kolaylaşabilir. 2023 tarihinde birliğin Vilnius'taki zirvesinde hibrit savaşlar ve siber saldırılar için RF ve ÇHC'yi uyardığı açıkça görülmektedir. Bu onları kesin ve net bir düşman yapmasa bile olası bir siber saldırıda akla gelebilecek isimler arasına sokmaktadır. Bu bağlamda bu iki ülkenin kurucu üyelerinden olduğu BRICS uluslararası iş birliği platformu alternatif bir bakış açısı ile olası rakipler arasında görülebilir. Her ne kadar bu birlik ekonomik ve siyasi amaçları olan ama askeri bir ittifak olmasa da siber saldırıların karmaşık ve çok katmanlı doğası göz önüne alındığında bu ihtimal düşünülebilir. Elbette burada üyelerin genel olarak neyi hedefledikleri önemlidir.

Uluslararası sistemdeki aktörlerin siber alanda varoluşları göz önüne alındığında kendi güvenliklerini kontrol altına alabilmek için iş birliği ve ortaklıklara başvurduğu ortadadır. Birçok ülke siber güvenliğin barışçıl yöntemlerle sağlanması gerektiğinin bilincindedir. Fakat çıkarlar ve kimi zaman devlet destekli ya da devlet destekli olmayan siber ataklar ile siber güvenlik tehlikeye girmektedir. Güvenliğin ihtimallere bırakılmayacak kadar önemli olduğu açıkça ortadadır. Bu yüzden ittifaklar bünyesinde siber güvenliği sağlamak için çalışmalar hızla devam etmelidir. Gerçek bir siber savaşın olmaması, gelecekte bir savaş olmayacağı sonucuna varılmasını sağlamamaktadır. Bu potansiyel tehdidin ve endişelerin ortadan kalkması için en doğru yöntemlerden biri ortaklık ve iş birliğidir.

KAYNAKÇA

Achkoski, Jugoslav ve Dojchinovski, Metodija (2012), Cyber Terrorism and Cyber-Crime – Threats for Cyber Security, MIT University, Macedonia.

Aksu, Muharrem ve Turhan, Faruk (2012), Yeni Tehditler, Güvenliğin Genişleme Boyutları ve İnsani Güvenlik, **Uluslararası Alanya İşletme Fakültesi Dergisi**.

Al-Rodhan, Dr. Nayef (2006), Definitions of Globalization: A Comprehensive Overview and a Proposed Definition, GCSP, Switzerland.

Andrew, Alex M., (2009), Cybernetics: Origins and Aims, Springer, New York.

Arı, Tayyar (2013), Uluslararası İlişkiler Teorileri, MKM Yayınları, Bursa.

Arpalier, Seçkin (2018), İngiliz Okulu ve Uluslararası Toplum Teorisi Bağlamında Uluslararası İlişkilerin Analizi, **B.U.Ü. İktisadi ve İdari Bilimler Fakültesi Dergisi**, Bursa

Aryanti, Aryanti ve Mekongga, Ikhthison (2018), Implementation of Rivest Shamir Adleman Algorithm (RSA) and Vigenere Cipher In Web Based Information System, EDP Sciences.

Ashenden, Debi ve Barnard-Willis, David (2012), Securing Virtual Space: Cyber War, Cyber Terror, and Risk, Cranfield University, Swindon, UK.

Baldwin, David A. (2011), Security Studies and the end of the Cold War, Cambridge University Press.

Beer, Stafford (2002), What is cybernetics?, MCB UP Ltd,

Bentham, Jeremy (2008), **Panoptikon Gözün İktiradarı**, Su Yayınları, İstanbul.

Birdişli, Fikret (2010), Eleştirel Güvenlik Çalışmaları Kapsamında Frankfurt Okulu ve Soğuk Savaş Sonrası Güvenlik Sorunlarına Eleştirel Bir Yaklaşım: Galler Ekolü, **Dergipark**,

_____ (2020). **Güvenlik Bilimleri Dergisi**.

Birkland, Thomas A. (2004), "The World Changed Today": Agenda-Setting and Policy Change in the Wake of the September 11 Terrorist Attacks, Review of Policy Research.

Blomfield, Adrian (2007), "Estonia calls for Nato cyber-terrorism strategy", **The Telegraphy**, https://www.telegraph.co.uk/news/worldnews/1551963/Estonia-calls-for-Nato-cyber-terrorism-strategy (17.05.2023).

Booth, Ken (2005), Critical Security Studies and World Politics, Lynne Rienner Publishers, USA.

Brent, Laura (2019), NATO'nun siber uzaydaki rolü, **NATO Review**, https://www.nato.int/docu/review/tr/articles/2019/02/12/natonun-siber-uzaydaki-rolue/index (14.06.2023).

Brooks, David Jonathan (2009), What is security: Definition through knowledge categorization, Security Research Centre (SECAU) at Edith Cowan University, Australia.

Bull, Hedley (1995), "The Theory of International Politics, 1919–1969 (1972)", International Theory Oxford University Press, London, 181-211.

Burke, Anthony vd. (2016), An Ethics of Global Securit, Journal of Global Security Studies.

Burton, Joe (2015), NATO's cyber defence: strategic challenges and institutional adaptation**,** **Defence Studies**, 297-319.

Buzan, Barry (1983), People, States and Fear, Harvester Press, London.

_____ (1986), A Framework For Regional Security Analysis, **Wheatsheaf Books**, Brighton.

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

Cable, Vincent (1995), What is international economic security?, Royal Institute of International Affairs, London

Carr, Jeffrey (2011), Inside Cyber Warfare, 2nd Edition, O'Reilly Media INC.

Cavelty, Myriam Dunn (2015), Cyber-security, Routledge.

Cavelty, Myriam Dunn ve Mauer, Victor (2010), The Routledge Handbook of Security Studies, Routledge, London and New York.

Chesters, Geoff (2004), Global Complexity and Global Civil Society, International Journal of Voluntary and Nonprofit Organizations.

Choucri, Nazli (2000), **Cyberpolitics in International Relations Context**, Connectivity and Content, International Political Science Association / SAGE Publications, London, Thousand Oaks, CA, and New Delhi.

_____ (2013), **Cyberpolitics in International Relations**, MIT Center for International Studies.

Clackson, Alexander (2011), Conflict and Cooperation in International Relations.

Colarik, Andrew M. ve Janczewski, Lech j. (2011), Developing a grand strategy for Cyber War, International Conference on Information Assurance and Security, Melacca, Malaysia.

Cooperative Cyber Defence Centre of Excellence (2018), "The NATO Cooperative Cyber Defence Centre of Excellence", Cyber defence at the 28th NATO Summit in Brussels, https://ccdcoe.org/ , (17.11.2023)

Council on Foreign Relations (2024). NATO: The World's Largest Alliance, https://education.cfr.org/learn/timeline/nato-worlds-largest-alliance , (23.11.2024)

Crenshaw, Martha (2013), The Causes of Terrorism, Ph.D. Program in Political Science of the City University of New York.

Czosseck, Christian vd. (2011). Estonia after the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security, International Journal of Cyber Warfare and Terrorism.

Darıcılı, Ali Burak (2017), **Amerika Birleşik Devletleri ve Rusya Federasyonu'nun Siber Güvenlik Stratejilerinin Karşılaştırmalı Analizi**, Uludağ Üniversitesi, Bursa.

Davis, Susan (2019). NATO ın the Cyber Age :Strengthenıng security & Defence, Stabilising Deterrence, NATO Parliamentary Assembly, https://www.nato-pa.int/document/2019-nato-cyber-age-strenghtening-security-and-defence-stabilising-deterrence, (24.02.2023).

Devlen, Balkan ve Özdamar, Özgür (2010), Uluslararası İlişkilerde İngiliz Okulu Kuramı: Kökenleri, Kavramları ve Tartışmaları, Uluslararası İlişkiler Konseyi Derneği | **Uluslararası İlişkiler Dergisi**, Ankara.

Cambridge University Press (2024), Cambridge Dictionary, Cambridge.

Defense Technical Information Center (2005), The National Intelligence Strategy of the United States of America: Transformation through Integration and Innovation, https://archive.org/details/DTIC_ADA469392/page/n1/mode/2up, (06.06.2024)

U.S. Department of Defense, (2021,) Dictionary of Military and Associated Terms, https://www.dni.gov/files/documents/CHCO/nis.pdf, (15.08.2023)

Domke, David vd. (2007), Going Public as Political Strategy: The Bush Administration, an Echoing Press, and Passage of the Patriot Act, Political Communication.

Duić, I. vd. (2017), International cyber security challenges, Faculty of Humanities and Social Sciences/Information and Communication Sciences, Zagreb, Croatia.

Freedman, Lawrence (1998), International Security: Changing Targets, Foreign Policy.

Freud, Sigmund (2000), Kitle **Psikolojisi**, Cem Yayınevi.

Ghavam, Z'hra M. (2016), NATO's Preparedness for Cyberwar, Monterey, California: Naval Postgraduate School.

Gill, Peter (2006). Policing and Society, An International Journal of Research and Policy.

Goldstein, Joshua S. ve Pevehouse, Jon C. (2013-2014), International Relations, MyPoliSciLab.

Gökçer, Onur ve Gözen Ercan, Pınar (2020), Siber Savaşlarda Jus ad Bellum ve Jus in Bello, **Alternatif Politika Dergisi.**

Green, James A. (2015), Cyber Warfare A Multidisciplinary Analysis, Routledge.

Grey, Jeffrey (2004), The Korean War, Journal of Contemporary History, London.

Gross, Leo (1942), The Peace of Westphalia, 1648-1948, The American Journal of International Law.

Gross, M., Canetti, D., & Vashdi, D. (2016). The psychological effects of cyber terrorism. *Bulletin of the Atomic Scientists.* içinde Routledge.

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

_____ (2017), Siber Uzay ve Güvenlik Politikası Üzerine Teorik Bir Yaklaşım, **Dergipark**.

Herring, George C. (2004), The Cold War and Vietnam, Oxford University Press.

Hobbes, Thomas (2020). **Leviathan**, Karbon Kitaplar, İstanbul.

İnaç, Hüsamettin ve Aktaş, Fatih (2013), 11 Eylül 2001 Terör Saldırılarının Amerikan Güvenlik Bürokrasisine Etkileri, **Akademik Bakış Dergisi**.

Jacobsen, Jeppe Teglskov (2014), The cyberwar mirage and the utility of cyberattacks in war How to make real use of Clausewitz in the age of cyberspace, DIIS - Danish Institute for International Studies, Copenhagen.

Jenkins, Brian M. (1975), **Will Terrorists Go Nuclear?,** Rand Corporation, Santa Monica, California.

Julisch, Klaus (2013), Understanding and overcoming cyber security anti-patterns, Elsevier.

Kant, Immanuel (1795), **Perpetual Peace**, Macmillan Company, London

Kaplan, Ahmet (2020), Siber Güvenlik Tarihi | Siber Güvenlik Ne Zaman Bulundu?, https://siberci.com/siber-guvenlik-tarihi/, (15.05.2024)

Karabulut, Andaç ve Değer, Filiz (2015), Uluslararası İlişkilerde Güvenlik Kavramı ve Realist Yaklaşım'a Genel Bakış, **Dergipark**.

Kelsey, Jeffrey T. (2008), Hacking into International Humanitarian Law: The Principles of Distinction and Neutrality in the Age of Cyber Warfare**, Michigan Law Review**.

Keohane, Robert O. (2002), **Power and Governance in a Partially Globalized World**, Routledge, London.

Klimburg, Alexander (2012), **National Cyber Security Framework Manual**, NATO CCD COE Publication, Tallin.

Kolodziej, Edward A. (2005), **Security and International**, Cambridge University Press.

Kurnaz, Salim ve Önen, Mustafa S. (2019), Avrupa Birliği'ne Uyum Sürecinde Türkiye'nin Siber Güvenlik Stratejileri, **Dergipark**.

Landler, M., & Markoff, J. (2007), In Estonia, What May Be the First War in Cyberspace, The New York Times https://www.nytimes.com/2007/05/28/business/worldbusiness/28iht-cyberwar.4.5901141, (17.08.2024)

Lerner, Jeniifer Vd. (2003), Effects of Fear and Anger on Perceived Risks of Terrorism A National Field Experiment, **Sage Publications**.

Lewis, James A. (2011), Cyberwar Thresholds and Effects, **IEEE Security ve Privacy**.

Lewis, James A. (2002), Assessing the Risks of Cyber Terrorism, Cyber War and Other Cyber Threats, CSIS.

_____ (2014), Cyber Threat and Response Combating Advanced Attacks and Cyber Espionage, CSIS.

Libicki, Martin C. (2009), **Cyberdeterrence and Cyberwar**, Rand Project Air Force.

Library of Congress Congressional Research Service (2020), Defense Primer: Cyberspace Operations: https://crsreports.congress.gov/product/pdf/IF/IF10537/5, (23.04.2024)

Locke, John (1690). The Second Treatise on Government. https://history.hanover.edu/courses/excerpts/163locke.html, (15.06.2023)

Maurer, Tim ve Nelson, Arthur (2021), The global cyber threat, Finance ve Development.

Mearsheimer, John J. (2001), **The Tragedy of Great Power Politics**, W. W. Norton ve Company, London.

Medland, William J. (1990), The Cuban Missile Crisis: Evolving Historical Perspectives, **Society for History Education**.

Metkin, Kısmet (2016), "İngiliz Okulu: Uluslararası Toplum ve Grotiuscu Rasyonalizm", Uluslararası İlişkiler Teorisi, Nobel Akademik Yayıncılık.

Miller, James E. (1989), A short history of NATO, Department of State Bulletin.

Morgenthau, Hans J. (1949), **Politics Among Nations**, The Struggle for Power and Peace, Alfred A. Knopf, New York.

NATO (1999), "The Alliance's Strategic Concept. National Atlantic Treaty Organization" https://www.nato.int/cps/en/natohq/official_texts_27433.htm (10.10.2023).

_____ (2002), "Prague Summit 2002: "Selected Documents and Statements" www.nato.int (15.12.2023).

_____ (2008), "Bucharest Summit Declaration. North Atlantic Treaty Organization", https://www.nato.int/cps/en/natohq/official_texts_8443.htm (02.01.2024).

_____ (2010), “NATO Summit Paves Way For Renewed Alliance”, https://www.nato.int/cps/en/natohq/news_68877.htm (20.01.2024).

_____ (2010), “Strategic Concept North Atlantic Treaty Organization” https://www.nato.int/cps/en/natohq/topics_82705.htm (10.11.2023).

_____ (2016), “Warsaw Summit Key Decisions”, https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_%202017_02/20170206_1702-factsheet-warsaw-summit-key-en.pdf (01.01.2024).

_____ (2016), “Cyber Defence Pledge”, https://www.nato.int/cps/en/natohq/official_texts_133177.htm (01.01.2024).

_____ (2022), “The History of NATO”, https://www. nato.int/cps/en/natohq/declassified_139621.htm (12.01.2023).

_____ (2022), “NATO 2022 Strategic Concept”, https://www.nato.int/cps/en/natohq/topics_210907.htm (09.04.2024).

_____ (2022), “A Short History of NATO”, https://www.nato.int/cps/en/natohq/declassified_139339.htm (07.10.2023).

_____ (2022), “NATO Secretary General Warns of Growing Cyber Threat”, https://www.nato.int/cps/en/natohq/news_208889.htm (05.04.2023).

_____ (2022), “NATO 2022 Strategic Concept. NATO leaders approve new Strategic Concept”, https://www.nato.int/cps/en/natohq/news_197281.htm (15.05.2024).

_____ (2022), “Strategic Concept. National Atlantic Treaty Organization”, https://www.nato.int/cps/en/natohq/topics_56626.htm (18.09.2024).

_____ (2023), “NATO's Strategic Warfare Development Command. NATO's Flagship Cyber Exercise Concludes in Estonia”, https://www.act.nato.int/article/cyber-coalition-23-concludes/#:~:text=Cyber%20Coalition%20is%20NATO's%20flagship,governance%20of%20the%20Military%20Committee (9.03.2023).

_____ (2023), “Cyber Defence” https://www.nato.int/cps/en/natohq/topics_78170.htm#evolution (08.02.2024).

_____ (2023), “NATO and the European Union Meet to Discuss Deepening Cooperation on Cyber Defence”, https://www.nato.int/cps/en/natohq/news_218654.htm?selectedLocale= (05.11.2024).

_____ (2023), “NATO Allies and Partners Take Part in World's Largest Cyber Defence Exercise”, https://www.nato.int/cps/en/natohq/news_214144.htm?selectedLocale (05.08.2024).

_____ (2023), “NATO Industry Cyber Partnership. NATO Communications and Information Agency”, https://www.ncia.nato.int/business/partnerships/nato-industry-cyber-partnership.html (12.01.2024).

_____ (2023), "Operations and Missions" https://www.nato.int/cps/en/natohq/68147.htm#crisis (15.04.2024).

_____ (2023), "Vilnius Summit Communiqué", https://www.nato.int/cps/en/natohq/official_texts_217320.htm (21.02.2024).

_____ (2023), "NATO's purpose", https://www.nato.int/cps/en/natohq/topics_68144.htm (18.01.2024).

_____ (2023), "What is NATO?", https://www.nato.int/nato-welcome/index_tr (17.12.2023).

_____ (2024), "NATO Member Countries", https://www.nato.int/cps/en/natohq/topics_52044.htm (13.09.2023).

O'Brien, Christopher (2021), "Small Wars Journal", What is cyber-terrorism, and is it a threat to U.S. national security?, https://smallwarsjournal.com/jrnl/art/what-cyber-terrorism-and-it-threat-us-national-security, (18.05.2024)

Office, U.S. (2011). International Strategy for Cyberspace: Prosperity, Security, and Openness in a Networked World, HSDL, https://www.hsdl.org/c/view?docid=5665, (06.06.2023)

Olsen, John Andreas (2020), Understanding NATO, The RUSI Journal.

North Atlantic Treaty Organization (2020). NATO Cyber Defence, http://www.nato.int/factsheets, (07.02.2024)

Önal, Mehmet A (2021), Siber Uzay ve Güvenlik İlişkisi Bağlamında Siber Güvenliğin Boyutları, **Hitit Ekonomi ve Politika Dergisi.**

Özer, Dr. Yusuf (2021), Stratejik Konseptler Bağlamıonda NATO'nun Stratejik Kültür Dönüşümü, **Güvenlik Yazıları**, https://trguvenlikportali.com/wp-content/uploads/2021/05/NATO StratejikKonsept_YusufOzer_v.1.pdf (02.01.2023)

Paker, Evren Balta (2012**), Küresel Güvenlik Kompleksi/Uluslararası Siyaset ve Güvenlik**, İletişim Yayınları, İstanbul.

Pektaş, Uğur (2016), Liberalizm: Karşılıklı Bağımlılık ve Küresel Yönetişim, Nobel Akademik Yayıncılık.

Polat, Doğan Şafak (2020), NATO'nun Yeni Operasyon Alanı: Siber Uzay, **Güvenlik Bilimleri Dergisi**.

Reiss, Hans (1970**), Kant's Political Writings**, Cambridge University Press, Cambridge.

Reveron, Derek S. (2012), **Cyberspace and National Security**, Georgetown University Press, Washington.

Robinson, Michael vd. (2015), Cyber warfare: Issues and challenges, Elsevier.

Saeid, Elsadig (2023), Recent Advances in Cybersecurity, University of Khartoum.

Sahu, Sachin Kumar vd. (2016), A review: Outrageous cyber warfare, **IEEE**, Hindistan.

Saleh, Alam (2010), Broadening the Concept of Security: Identity and Societal Security, Geopolitics Quarterly.

Stadnik, Ilona (2017), What Is an International Cybersecurity Regime and How We Can Achieve It?, Masarykova Univerzita Nakladatelství.

Straumann, Benjamin (2008), The Peace of Westphalia (1648) as a Secular Constitution, SSRN.

Szőke, Diana (2019), "NATO's Evolving Approach to Cybersecurity", Foreign Policy Review, Institute for Foreign Affairs and Trade, Budapest.

Szpyra, Ryszard (2014), Military Security within the Framework of Security Studies: Research Results, Partnership for Peace Consortium of Defense Academies and Security Studies.

Teeple, Gary (2000), "**What is Globalization?**", Globalization and its Discontents, Palgrave Macmillan.

Theiler, Dr Olaf (2011), Opinion, Analysis and Debate on Security Issues, New threats: the cyber-dimension, NATO Review, https://www.nato.int/docu/review/articles/2011/09/04/new-threats-the-cyber-dimension/index, (04.01.2023)

Thompson, Michael J. (2017), What Is Critical Theory?, William Paterson University.

Tikk, Eneken (2010), Global Cybersecurity-Thinking About the Niche for NATO, **SAIS Review of International Affairs**.

U.S. Department of Commerce, U. D. (2018). A Report to the President on Supporting the Growth and Sustainment of the Nation's Cybersecurity Workforce: Building the Foundation for a More Secure American Future, Computer Security Resource Center, https://csrc.nist.gov/pubs/other/2018/05/30/supporting-growth-and-sustainment-of-the-cybersecu/final, (18.10.2024)

Ullman, Richard H. (1983), **Redefining Security**, MIT Press.

Wallander, Celeste A. ve Keohane, Robert O. (1999), **Risk, threat, and security institutions**, Oxford.

Walters, Robert ve Novak, Marko (2021), Cyber Security, Artificial Intelligence, Data Protection & the Law, Springer.

Waltz, Kenneth N. (1979), **Theory of International Politics**, University of California, Berkeley.

Weaver, John Michael (2021), NATO A Brief History, and Discussion on the Methodology, Palgrave Macmillan.

Williams, Paul D. (2008), **Security Studies: An Introduction**, Routledge, London

Yılmaz, Ekrem (2016), Pozitivizm, "Eleştirel Teori ve Postmodern Anlayışlar", Uluslararası İlişkiler Teorisi, Nobel Akademik Yayıncılık.

ÖZGEÇMİŞ

İlköğrenimini 2010 yılında Gülbahar Hatun İlkokulu'nda; orta öğrenimini 2014 yılında Gülbahar Hatun Anadolu Lisesi'nde; lisans eğitimini ise 2020 yılında da Karadeniz Teknik Üniversitesi – İktisadi ve İdari Bilimler Fakültesi, Uluslararası İlişkiler Bölümü'nde tamamladı. 2020 yılında Karadeniz Teknik Üniversitesi – Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Anabilim Dalında yüksek lisans programına başladı.

KAYA, bekar olup iyi derecede İngilizce bilmektedir.