T.C.

TRAKYA ÜNİVERSİTESİ

SOSYAL BİLİMLER ENSTİTÜSÜ

ULUSLARARASI İLİŞKİLER ANABİLİM DALI

YÜKSEK LİSANS TEZİ

2000'Lİ YILLARDA NATO'NUN SİBER GÜVENLİK POLİTİKALARI

BURAK BULUT

TEZ DANIŞMANI

DOÇ. DR. SİBEL KAVUNCU

EDİRNE 2022

Tezin Adı: 2000'li Yıllarda NATO'nun Siber Güvenlik Politikaları

Hazırlayan: Burak BULUT

ÖZET

21. yüzyılın başından itibaren teknolojinin öngörülemez hızda gelişim ve dönüşümünü sürdürmesi ile internetin her alanda kullanımını artırması, coğrafi mesafelerin önemini yitirmesini ve küreselleşmenin etkilerinin en üst seviyede hissedilmesini sağlamıştır. İçerisinde bulunulan dönem itibarıyla küreselleşmenin bu denli baskın hissedilmeye başlanması sonucu ülkelerin sınırları artık neredeyse yapay bir hal almış ve bunun sonucunda, modern toplumların siber alana bağımlılığının giderek artış göstermesinin önü açılmıştır. Teknoloji ve bilginin büyük bir hızla gelişip, küreselleşmesinin de etkisiyle dünyanın her bir bölgesine yayılması, siber alanın olumlu etkilerinin yanı sıra tehdit oluşturmanın bir yolu olarak da kullanılmaya başlanmasına neden olmuştur. Böylece, üyelerinin savunmalarını ve güvenliklerini öncelik ekseni olarak belirleyen NATO'nun stratejik doktrinlerinde, siber ön ekli terimler yaygın olarak yer almaya başlamıştır. Sanal dünyanın gittikçe gerçek dünya ile iç içe geçmesiyle beraber NATO'nun güvenlik anlayışında, siber güvenlik tehditleriyle mücadele için ortak durumsal farkındalık, kesintisiz bilgi paylaşımı, kolektif karar alma, erken müdahale ve siber savunma konularına yer verildiği görülmektedir. Bu bağlamda çalışmada, 2000'li yıllarda NATO'nun güvenlik anlayışının gelişimi ve dönüşümünde siber güvenlik politikalarının yeri ve önemi analiz edilecektir.

Anahtar Kelimeler: Güvenlik, Siber Güvenlik, Siber Uzay, Siber Savunma, NATO

Title of the Thesis: NATO's Cybersecurity Policies in the 2000s

Prepared by: Burak BULUT

ABSTRACT

Since the beginning of the 21st century, the development and transformation of technology at unpredictable speed has increased the use of the internet in all areas, ensuring that geographical distances lose their importance and the effects of globalization are felt at the highest level. As of the current period, with globalization feeling so dominant, the borders of countries have now become almost artificial and, as a result, the dependence of modern societies on cyberspace has gradually opened the way for an increase. The rapid expansion of technology and information to all regions of the world due to effect of globalization, which has led to the positive effects of cyberspace as well as its use as a way to pose a threat. Thus, it can be mentioned that the terms with cyber prefixes are widely included in NATO's strategic doctrines, which set the defenses and security of its members as a priority axis. As the virtual world becomes more intertwined with the real world, it is seen that NATO's understanding of security appears to include common situational awareness, uninterrupted information sharing, collective decision-making, early intervention and cyber defense issues to combat cybersecurity threats. In this context, the place and importance of cybersecurity policies in the development and transformation of NATO's understanding of security in the 2000s will be analyzed in the study.

Keywords: Security, Cybersecurity, Cyberspace, Cyber Defence, NATO

ÖNSÖZ

"2000'li Yıllarda NATO'nun Siber Güvenlik Politikaları" başlığını taşıyan tez çalışmasında, Bilgi ve İletişim Teknolojileri'nde yaşanan hızlı gelişmelerin, NATO'nun güvenlik anlayışında yarattığı değişimler ve bu değişim sürecinde siber güvenlik politikalarının rolü ve etkinliği incelenmeye çalışılmıştır.

Tüm yazım sürecinde kıymetli bilgi, birikim ve tecrübeleriyle bana rehberlik eden ve oldukça anlayışlı bir şekilde ileriye dönük gelişimimi sağlayacak yönlendirmeleri yapan danışman hocam Sayın Doç. Dr. Sibel KAVUNCU'ya en içten teşekkürlerimi ve şükranlarımı sunuyorum. Yüksek lisans eğitimim boyunca değerli bilgi ve birikimlerini paylaşan ve çeşitli konularda desteğini ve yol göstericiliğini hiç esirgemeyen başta bölüm başkanımız Sayın Prof. Dr. Sibel TURAN hocam olmak üzere, Sayın Prof. Dr. Fahri TÜRK, Sayın Doç. Dr. İbrahim KAMİL, Sayın Dr. Öğr. Üyesi Emre AYKOÇ, Sayın Dr. Öğr. Üyesi Serap YOLCU YAVUZ hocalarıma ve Sayın Arş. Gör. Dr. Tolga ERDEM hocama ayrı ayrı teşekkürlerimi iletiyorum. Son olarak ise, daima yanımda olan ve desteklerini hiç esirgemeyen sevgili aileme verdikleri kıymetli destekleri ve sonsuz sabırları için saygılarımı ve teşekkürlerimi sunarım.

Ocak, 2022 / EDİRNE

İÇİNDEKİLER

ÖZET……i

ABSTRACT……ii

ÖNSÖZ……..…..iii

İÇİNDEKİLER……....iv

KISALTMALAR……vi

GİRİŞ……1

BİRİNCİ BÖLÜM……...5

1. ULUSLARARASI İLİŞKİLER BAĞLAMINDA SİBER GÜVENLİK……...5

1.1. Siber Güvenliğin Tanımı ve Gelişimi ……..……5

1.2. Siber Güvenliğin Tarihsel Analizi ……11

1.2.1. Soğuk Savaş Dönemi İnternetin Gelişimi …….....12

1.2.2. Soğuk Savaş Sonrası Siber Güvenliğin Gelişimi …..……..14

1.3. Siber Güvenlik Kapsamındaki Kavramlar……...……...17

1.3.1. Siber Uzay……...……18

1.3.2. Siber Saldırı ve Siber Tehdit……20

1.3.3. Siber İstihbarat ve Siber Casusluk……...…24

1.3.4. Siber Diplomasi……...27

1.3.5. Siber Savunma……29

1.3.6. Siber Caydırıcılık……31

İKİNCİ BÖLÜM……...……35

2. DEĞİŞEN GÜVENLİK ANLAYIŞI PERSPEKTİFİNDE NATO'NUN GÜVENLİK ANLAYIŞI…… ……...35

2.1. Güvenliğin Tanımı ve Dönüşümü …….……36

2.1.1. Soğuk Savaş Dönemi Geleneksel Güvenlik Anlayışı ……..……40

2.1.2. Soğuk Savaş Sonrası Yeni Güvenlik Anlayışı ……45

2.1.3. 11 Eylül Sonrası Güvenlik Anlayışı……48

2.2. Geçmişten Günümüze NATO'nun Güvenlik Anlayışının Dönüşümü…….…...51

2.2.1. NATO'nun Kuruluşu ve Soğuk Savaş Dönemi Güvenlik Anlayışı..…....52

2.2.2. NATO'nun Soğuk Savaş Sonrası Güvenlik Anlayışı ……..60

ÜÇÜNCÜ BÖLÜM……...72

3. NATO'NUN SİBER GÜVENLİK ANLAYIŞININ DEĞERLENDİRİLMESİ: FIRSATLAR VE ZORLUKLAR…..……..……72

3.1. NATO'nun Siber Güvenlik Algısı ……...……..73

3.1.1. 2000-2010 Yılları Arası Siber Güvenlik Algısı……...…74

3.1.2. 2010-2020 Yılları Arası Siber Güvenlik Algısı……...…85

3.2. NATO'nun Siber Tehditlerle Mücadelede Karşılaştığı Zorluklar, Kurumsallaşma ve İş birliği Çabaları ……..……...97

3.2.1. Kurumlar ve Tatbikatlar……..98

3.2.2. Avrupa Birliği ile İş birliği Girişimleri……..107

3.2.3. Sanayi, Özel Sektör ve Akademiyle İş birliği Faaliyetleri……..…...114

3.2.4. Kuzey Atlantik Antlaşması'nın 5. Maddesi Kapsamında Yetki Sınırı ve Atıf Sorunu……..……..…….117

SONUÇ…….122

KAYNAKÇA……..……..……127

KISALTMALAR

ABD: Amerika Birleşik Devletleri

ABM: Anti-Ballistic Missile - Anti Balistik Füze

ACT: The Allied Command Transformation - Müttefik Dönüşüm Komutanlığı

AGİT: Avrupa Güvenlik ve İşbirliği Teşkilatı

AGSK: Avrupa Güvenlik ve Savunma Kimliği

ARPA: Advanced Research Projects Agency - Gelişmiş Araştırma Projeleri Ajansı

ARPANET: The Advanced Research Projects Agency Network - Gelişmiş Araştırma Projeleri Ajansı Ağı

AWACS: Airborne Warning and Control System - Havadan Erken Uyarı ve Kontrol Sistemi

BAB: Batı Avrupa Birliği

BİO: Barış İçin Ortaklık

BİT: Bilgi ve İletişim Teknolojileri

BM: Birleşmiş Milletler

CCDCOE: Cooperative Cyber Defence Centre of Excellence - Müşterek Siber Savunma Mükemmeliyet Merkezi

CDMA: The NATO Cyber Defence Management Authority – NATO Siber Savunma Yönetim Otoritesi

CDMB: The NATO Cyber Defence Management Board - NATO Siber Savunma Yönetim Kurulu

CERT-EU: The Computer Emergency Response Team for the EU - Avrupa Birliği Bilgisayar Acil Müdahale Ekibi

CIA: The Central Intelligence Agency - Amerikan Merkezi İstihbarat Teşkilatı

CyCon: International Conference on Cyber Conflict - Uluslararası Siber Çatışma Konferansı

DARPA: Defense Advanced Research Projects Agency - Savunma İleri Araştırma Projeleri Ajansı

DDoS: Distributed Denial of Service - Dağıtılmış Hizmet Reddi

DoD: U.S. Department of Defense - ABD Savunma Bakanlığı

DPPC: The Defence Policy and Planning Committee - Savunma Politikası ve Planlama Komitesi

EDA: The European Defence Agency - Avrupa Savunma Ajansı

EEAS: The European External Action Service – AB Dış İlişkiler Servisi

ENISA: The European Union Agency for Cybersecurity - Avrupa Ağ ve Bilgi Güvenliği Ajansı

FBI: The Federal Bureau of Investigation - ABD Federal Soruşturma Bürosu

FFCI: The Framework For Collaborative Interaction - İşbirliğine Dayalı Etkileşim Çerçevesi

FOC: The Full Operational Capability - Tam Harekat Kabiliyeti

IP: Internet Protocol - İnternet Protokolü

ITU: International Telecomunication Union - Uluslararası Telekomünikasyon Birliği

KAİK: Kuzey Atlantik İşbirliği Konseyi

MAD: Mutual Assured Destruction - Karşılıklı Kesin Mahvolma

MN CD2: Multinational Cyber Defence Capability Development - Çokuluslu Siber Savunma Yeteneği Geliştirme Projesi

NATO: The North Atlantic Treaty Organization - Kuzey Atlantik Antlaşması Örgütü

NATO MC: The North Atlantic Treaty Organisation Military Committee - NATO Askeri Komitesi

NCIA: The NATO Communications and Information Agency - NATO İletişim ve Bilgi Ajansı

NCIRC: The NATO Computer Incident Response Capability - NATO Bilgisayar Olaylarına Müdahale Yeteneği

NCISG: The NATO Communications and Information Systems Group - NATO İletişim ve Bilgi Sistemleri Grubu

NICP: The NATO-Industry Cyber Partnership – NATO-Sanayi Siber Ortaklığı

NICE: National Initiative for Cybersecurity Education - Siber Güvenlik Eğitimi Ulusal Girişimi

NNEC: The NATO Network Enabled Capability - NATO Ağ Destekli Yetenek Programı

NRF: NATO Response Force – NATO Acil Mukabele Gücü

NSA: The National Security Agency – ABD Ulusal Güvenlik Ajansı

RRT: Rapid Reaction Team - Hızlı Tepki Ekibi

SALT: The Strategic Arms Limitation Talks - Stratejik Saldırı Silahlarının Sınırlandırılmasına İlişkin Tedbirler Antlaşması

SHAPE: The Supreme Headquarters Allied Powers Europe - Avrupa Müttefik Kuvvetleri Yüksek Karargahı

SSCB: Sovyet Sosyalist Cumhuriyetler Birliği

TDK: Türk Dil Kurumu

VJTF: The Very High Readiness Joint Task Force - Çok Yüksek Hazırlıklı Müşterek Görev Gücü

WEF: The World Economic Forum - Dünya Ekonomik Forumu

Wi-Fi: Wireless Fidelity - Kablosuz Bağlantı Alanı

WP: The Warsaw Pact - Varşova Paktı

WUDO: The Western Union Defence Organisation - Batı Birliği Savunma Örgütü

GİRİŞ

Yirmi birinci yüzyılın ilk yirmi yılında, Bilgi ve İletişim Teknolojileri'nde (BİT) yaşanan öngörülemez hızda teknolojik gelişmelerle bireylerin; ticari faaliyetlerini, iletişimlerini, sosyal etkileşimlerini, kültürel ve siyasi ilişkilerini dijital alana taşıdıkları görülmüştür. Uluslararası İlişkiler açısından dijitalleşmenin birçok alanda kullanımını artırması, güvenlik araçlarını ve yöntemlerini kapsayacak biçimde uluslararası sistemin bütününe etki edebilecek kadar önemli değişimleri beraberinde getirmiştir. Enerji, ulaştırma, savunma sanayii ve bankacılık hizmetleri gibi kritik altyapı sistemlerinden sağlık hizmetlerine kadar devletlerin olağan işleyişleri üzerinde oldukça büyük öneme sahip alanlarda dijital ortamdan yararlanılmaktadır.

Soğuk Savaş döneminde güç mücadelelerinde makineli tüfekler, uçak gemileri, tanklar, denizaltılar ve savaş uçakları gibi askeri saldırı ve savunma araçlarının ve silahlarının kullanımı ön planda iken, günümüzde bu araçların internet tabanlı teknolojiler ile iç içe geçerek hibrit çatışma modelini açığa çıkardığı görülmektedir. Devletlerin yanı sıra organize suç örgütleri, aşırılık yanlısı gruplar ve bireyler de zaman ve mekân sınırlaması olmaksızın internet destekli yazılım ve donanım yardımı ile siber alanda suç kapsamına girecek faaliyetler yürütebilmektedir. Böylece bazı bilim insanları tarafından, siber uzayın devletlerin, uluslararası örgütlerin, özel sektör kuruluşlarının ve bireylerin çıkarlarını ilerletmek için kullanıldığı politik bir alan olarak yorumlandığı görülmektedir. Hızlı teknolojik gelişmeler ve siber ortamı devletlerle ve toplumlarla daha fazla ilişkilendirmeye yönelik devam eden bu süreç, siber güvenlik ve Uluslararası İlişkiler disiplinini birbirine bağlayan bir dizi yeni güvenlik sorununu ortaya çıkarmıştır. Siber güvenlik, kritik ulusal altyapıların ve donanımların fiziksel güvenliğinden, belirli bilgisayar yazılım programları veya sosyal medya platformlarını kullanmanın toplumsal etkilerine kadar uzanan çok yönlü bir alandır. Siber tehditlerin çok merkezli ve asimetrik bir yapıya sahip olması, bu tehditlerle mücadele edebilmek için ulusal, bölgesel ve küresel düzeyde siber güvenlik çalışmalarının yürütülmesini gerektirmiştir.

21. yüzyıl itibarıyla asimetrik bir yapıya sahip siber tehditlerin devlet ve devlet dışı aktörler tarafından gerçekleştirilebiliyor olması, küresel düzeyde bir kolektif güvenlik örgütü olma hedefiyle politikalar faaliyete geçiren Kuzey Atlantik Antlaşması Örgütü (*The North Atlantic Treaty Organization*, NATO) için de en önemli güvenlik sorunları arasında yer almıştır. 2002 yılında NATO'nun Prag Zirvesi'nde ele alınan yeni güvenlik tehditleri arasında siber uzay yoluyla gelebilecek tehditlere de yer verilmiş ve siber güvenlik konusu resmi olarak ilk kez bir politik kaygı olarak ele alınmıştır. NATO'nun, siber güvenlik üzerine ilk büyük endişesi, 2007 yılında Estonya'nın kamu kurumlarını ve özel sektör işletmelerini hedef alan Dağıtılmış Hizmet Reddi (*Distributed Denial of Service,* DDoS) saldırıları ve 2008 yılında Gürcistan'a yönelik düzenlenen silahlı saldırılara siber saldırıların eşlik etmesi sonucunda yaşanmıştır. Bu gelişmeler sonrasında, siber tehditlerle mücadelede erken müdahalenin gerçekleştirilmesi, savunma sistemlerinin geliştirilmesi ve uluslararası iş birliğinin artırılmasına yönelik NATO bünyesinde birçok kurumun faaliyete geçirilmesinin yanı sıra 2008, 2011, 2014 ve 2021 yıllarında siber savunma politikaları onaylanmıştır. Ayrıca, 2010 yılında açıklanan NATO Stratejik Konsepti'nde, siber güvenlik kavramına ilk kez yer verilerek, siber saldırıların ulusal güvenliğe olumsuz etkisine ve de Avrupa-Atlantik bölgesinin bütününe tehdit oluşturma potansiyeline sahip olduğuna değinilmiştir. Bu gelişme, İttifak'ın geleceğine yönelik önemli birer yapı taşı oluşturmasının yanı sıra NATO üyelerinin siber güvenliği temel odak noktası olarak kabul ettiğinin de bir göstergesini oluşturmaktadır.

2011, 2014 ve 2017 yıllarında NATO'nun, gelişen siber tehdit ortamıyla etkin mücadele edilebilmesi için siber güvenlik kapsamında üye devletlerin birlikte çalışmalarını sağlama, yeteneklerini geliştirme ve bilgi paylaşma becerilerini artırma temelli eylem planları açıklanmıştır. 2016 yılındaki NATO Varşova Zirvesi Sonuç Bildirisi'nde, hava, kara, deniz ve uzay alanlarında olduğu gibi siber uzayın da etkili savunulması gerekli bir operasyon alanı olarak tanınması gerektiği belirtilmiştir. NATO'nun, öncelikli olarak siber tehditlerle mücadelede kendi ağlarının güvenliğine önem verirken, İttifak'ın siber güvenlik politikalarında hükümetler arası örgütler, özel sektör kuruluşları, akademik kurumlar ile siber güvenlik alanındaki ortaklığın ve iş birliğinin önemine de sık sık vurgu yaptığı görülmektedir.

Yine NATO'nun, siber güvenlik çalışmalarında, üye ülkeler arasındaki anlaşmazlıklar, üye ülkelerin siber savunma kapasitelerindeki kayda değer gelişmişlik farkları, siber saldırılara yanıt verme ve saldırıyı gerçekleştiren aktöre atfetme konularında bazı zorluklarla da mücadele etmesini gerektirmiştir.

"2000'li Yıllarda NATO'nun Siber Güvenlik Politikaları" isimli çalışmada; NATO'nun siber güvenlik politikalarının gelişiminde hangi olayların etkili olduğu, NATO'nun siber güvenlik politikalarında ön plana çıkan konuların hangileri olduğu, NATO'yu hedef alan veya hedef alma potansiyeline sahip siber tehditlere yanıt vermek için mevcut NATO siber politikalarının ne kadar yeterli olduğu, siber alandaki tehdit ve risk ortamıyla mücadelenin NATO'nun ikili ve çok taraflı ilişkilerini ne yönde etkilediği, NATO'nun güvenlik anlayışında siber güvenliğin yeri ve öneminin nasıl bir değişim gösterdiği sorularına temel olarak yanıt aranmaya çalışılacaktır. Bu sorular kapsamında, siber güvenlik kavramının detaylı analizi, NATO'nun güvenlik anlayışının yıllar içerisinde değişim ve dönüşümü, siber güvenliğin gelişimine yönelik NATO bünyesinde faaliyete geçirilen kurumlar, İttifak'ın siber güvenlik yeteneklerinin gelişimi üzerine NATO zirvelerinde ele alınan konular, antlaşmalar ve iş birliği girişimleri, teknolojik gelişmelerden kaynaklanan zorlukların NATO'nun güvenlik anlayışı üzerindeki etkileri ve bu zorluklarla mücadelede çözüm önerileri konularının incelenmesi amaçlanmıştır.

Çalışmada, NATO'nun siber güvenlik politikaları kapsamında İttifak'ın güvenlik gündeminde "siber" kavramının ilk kez yer aldığı 2002 yılından, çalışmanın tamamlandığı 2021 yılına kadar olan süreç ele alınmakla beraber, NATO'nun güvenlik anlayışının genişlemesinin ve siber güvenlik kavramının gelişiminin daha iyi anlaşılabilmesi adına 20. yüzyıl ortalarından itibaren bazı örnek olaylara da yer verilmiştir. Ayrıca, oldukça geniş kapsam alanına sahip olan siber uzay ve siber güvenlik temelli konuların araştırılmasında, Uluslararası İlişkiler disiplini kapsamına giren kavramlara ve tanımlamalara yer verilerek, siber güvenlik kavramı, Uluslararası İlişkiler disiplini kapsamında değerlendirilmeye çalışılmıştır.

Çalışmanın ilk bölümünde, Uluslararası İlişkiler disiplini bağlamında siber güvenlik kavramının gelişimi değerlendirilerek kuramsal analiz yapılacak, siber

güvenliğin tarihsel gelişimi incelenecek ve siber güvenlik kavramıyla bağlantısı bulunan "siber" ön ekli kavramlar ele alınacaktır. İkinci bölümde, Soğuk Savaş döneminden günümüze kadar olan süreçte Uluslararası İlişkiler disiplini bağlamında güvenlik kavramının dönüşümü çeşitli Uluslararası İlişkiler kuramlarıyla ve örnek olaylarıyla desteklenerek incelenecek ve NATO'nun kuruluşundan günümüze güvenlik anlayışındaki dönüşüm irdelenecektir.

Çalışmanın üçüncü bölümünde ise, NATO'nun siber savunma politikaları ve siber güvenlik anlayışı analiz edilecektir. İlk olarak, tarihsel perspektifte NATO'nun siber güvenlik anlayışının gelişimi incelenecektir. Bu bağlamda, siber güvenlik konusunun yer aldığı çeşitli NATO zirvelerine ve İttifak'ın siber güvenlik politikalarına öncelikli olarak yer verilecektir. Ayrıca, siber tehditlerle mücadele için NATO'nun faaliyete geçirdiği kurumsal reformlar, siber güvenlik eğitimleri ve tatbikatları, Avrupa Birliği (AB), özel sektör kuruluşları ve akademik kurumlar ile iş birliğinin derinleştirilmesine yönelik adımlar ele alınacaktır. Son olarak ise, NATO'nun kolektif savunma ilkesi çerçevesinde siber tehditlerle mücadelede iki güncel sorun olarak değerlendirilebilecek yetki sınırı ve saldırıyı gerçekleştiren aktöre yönelik atıf sorunları analiz edilecektir.

BİRİNCİ BÖLÜM

1. ULUSLARARASI İLİŞKİLER BAĞLAMINDA SİBER GÜVENLİK

Teknoloji alanındaki gelişim ve dönüşümlerin bir sonucu olarak internet ağına bağlı aletlerin sayılarının artmış olması, insanoğlunun yaşamı üzerinde olumlu ve olumsuz etki doğurabilmektedir. Her yeni teknolojik ilerleme sayesinde bilgiyi analiz etme düzeyi ve dünya ile etkileşim şekli günden güne değişiklik göstermiştir.[1] Soğuk Savaş sonrası dönemde bazı araştırmacıların dünyayı küresel bir köy olarak tanımlama girişimlerinin yerini günümüz dünyasında küresel bir apartman olarak ifade edilişlerin aldığı görülmektedir.[2] Uluslararası politika açısından bu denli gelişim ve dönüşümün avantajlı yönleriyle birlikte dezavantajlı yönleri de kendini en etkili biçimde hissettirebilmektedir. Teknolojinin olumsuz yönleriyle mücadele edilebilmesi adına yeni güvenlik tanımlamalarına ve önlemlerine ihtiyaç duyulması sonucunda, Uluslararası İlişkiler disiplini içerisinde güvenlik kavramının ayrılmaz parçalarından biri olarak ifade edilen siber güvenlik kavramının etkisini göstermeye başladığı görülmektedir.

1.1. Siber Güvenliğin Tanımı ve Gelişimi

Siber güvenlik kavramı, 1960'lı yıllarda internetin askeri amaçlı kullanılmaya başlanmasından yirmi yıla yakın bir süre geçtikten sonra ortaya çıkmıştır. İnternetin tasarlandığı dönem içerisinde öncelikli hedef olarak belirli alanlarda kullanım kolaylığı oluşturması, düşük maliyetli olması ve birden fazla ağ üzerinde iletişim sağlanabilmesi amaçlanmış, ancak kullanıcıların zamanla güvenlik tehditleri oluşturabileceği tahmin edilememiştir.[3] Alexander Klimburg'a göre siber kavramı,

---

[1] Robert Reardon ve Nazli Choucri, "The Role of Cyberspace in International Relations: A View of the Literature", *ISA Annual Convention*, Cilt 1, Nisan 2012, ss. 2-3.

[2] Nezir Akyeşilmen, *Disiplinlerarası Bir Yaklaşım ile Siber Politika ve Siber Güvenlik*, Orion Kitabevi, Ekim 2018, s. 107.

[3] Seymour E. Goodman, "Critical Information Infrastructure Protection", *Responses To Cyber Terrorism NATO Science For Piece and Security*, Derleyen: Centre Of Excellence Defence Against Terrorism, IOS Press, Cilt 34, Ankara 2008, ss. 25-26.

bilgisayar ve bilgisayar ağlarının bulunduğu her ortamı veya cihazı tanımlamak amacıyla kullanılmaktadır.[4] Siber alanda yaşanan teknolojik gelişmeler ve tehditler sonucu siber güvenlik kavramı zamanla uluslararası siyasi sistem içerisinde adından söz ettirmeye başlamıştır. Siber güvenlik aracılığıyla yakın zamanda keşfedilmiş olunan sanal gerçeklik kavramı, bugün itibarıyla hayatımızın ayrılmaz bir parçası haline gelmiştir. Siber güvenlik; siber saldırı ve tehditlerin verebilecekleri potansiyel zararları gitgide artırmaları sonucu uluslararası sistem içerisinde hayati önem taşıyan bilgi işlem alanı halini almıştır.[5] Siber saldırılar aracılığıyla devletlerin kritik altyapılarına tahribat oluşturulabilmesi, askeri sistem ve operasyonlarının olumsuz yönde etkilenebilmesi, devlet kurumlarına ve ekonomilerine saldırı düzenlenerek maddi kayba uğratılabilmesi, bireylerin güvenlik ve özgürlük alanlarının işgal edilebilmesi gibi eylemler sonucunda Uluslararası İlişkiler disiplininde siber güvenlik kavramı önemli bir konuma sahip olmuştur.[6]

Siber güvenlik uygulamaları, yalnızca devletler tarafından kullanılmamakta, bunun yanında politikacılar, bilgisayar uzmanları, bilgi ve iletişim teknolojileri yöneticileri, sağlık çalışanları ve ulusal güvenlik uzmanları gibi çok çeşitli sahalardaki aktörün kullanım alanı içerisine girebilmektedir. Bunun sonucunda, oldukça geniş bir kapsamı olan siber güvenlik kavramının tek bir tanım üzerinden ifade edilmesi neredeyse imkânsız hale gelmektedir. Bu nedenle siber güvenlik kavramının yorumlama ve tanımlama girişimi, Soğuk Savaş'ın sona ermesini takip eden yıllardan bu yana birçok araştırmacı ve kurum tarafından yapılmaya çalışılmaktadır.

Siber Güvenlik Eğitimi Ulusal Girişimi (*National Initiative for Cybersecurity Education,* NICE); bilgi ve iletişim ağlarındaki verilerin herhangi bir saldırı aracılığıyla değiştirilmesine ya da istismar edilmesine karşı korunduğu eylemler bütünü olarak bir siber güvenlik tanımı yapmıştır.[7] Bilgi, teknoloji ve haberleşme

---

[4] Alexander Klimburg, *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn 2012, s. 2.

[5] Jangirala Srinivas, Ashok Kumar Das ve Neeraj Kumar "Government Regulations in Cyber Security: Framework, Standards And Recommendations", *Future Generation Computer Systems*, Cilt 92, Mart 2019, ss. 178-179.

[6] Mehmet Eren, *Avrupa Birliği'nin Siber Güvenlik Politikası*, Beta Yayınları, İstanbul 2017, s. 25.

[7] Douwe Korff, "Cyber Security Definitions", *Associate of the Oxford Martin School of the University of Oxford's Global Cybersecurity Capacity Centre*, Oxford 2011, s. 1.

teknolojileri üzerine daimî olarak araştırma ve çalışmalar yürüten Uluslararası Telekomünikasyon Birliği (*International Telecomunication Union,* ITU) ise, siber güvenliği; siber ortamda kurumların ve bireylerin bilgi varlıklarını koruyabilmek adına kullanabilecek araçlar, politikalar, güvenlik önlemleri, risk yönetimi yaklaşımları, eylemler, eğitimler ve teknolojilerin toplamı olarak ifade etmektedir.[8] Bir başka tanıma göre de siber güvenlik; siber ortam içerisindeki kullanıcı ve aktörlerin güvenliğini sağlayabilmek amacıyla her türlü siber tehdit ve saldırılara karşı alınan önlemler bütününü yansıtmaktadır.[9] Siber uzay alanında önemli araştırmacılardan biri olan Nazli Choucri ise siber güvenlik kavramını devlet temelli bir yaklaşımla ele almıştır. Choucri'ye göre siber güvenlik; bir devletin kendisini ve kurumlarını tehditlere, casusluğa, sabotaja, kimlik hırsızlığına ve e-işlemlere karşı koruma durumunu ifade etmektedir.[10] Nezir Akyeşilmen, siber güvenlik kavramına dair güvenliğin bütün boyutlarını ve aktörlerini kapsayacak şekilde geniş bir tanımlama yapmıştır. Akyeşilmen'e göre siber güvenlik; bütün siber uzay bileşenleri, bilgisayar sistemleri, bilgi ve iletişim ağları kapsamında bilginin gizliliğine, bütünlüğüne ve erişilebilirliğine yönelik gerçekleştirilen her türlü saldırılara yönelik hukuk ve insan hakları çerçevesinde mücadele edebilmek amacıyla ortaya konan önlem, politika, mekanizma ve yapıların bütünüdür.[11]

Yukarıdaki tanımlamaların ortak yanlarından yola çıkılarak bir siber güvenlik tanımlaması yapılacak olunursa; donanım, yazılım ve ilgili altyapı sistemleriyle birlikte bu sistemlerin içerisinde yer alan verilerin ve hizmetlerin saldırganlar tarafından yasa dışı yollarla erişilip zarar verilmesinden korunması olarak ifade edilebilir.[12] Bu bağlamda siber güvenlik, gerekli tüm koruma ve engelleme faaliyetlerini gerçekleştirmek için tasarlanmış teknolojiler, süreçler ve uygulamalardan oluşmakta ve ağların, programların ve verilerin bütünlüğünü saldırı,

---

[8] ITU-T X.1208, "Series X: Data Networks, Open System Communıcations and Security: Telecommunations Security – Overview of Cybersecurity", *International Telecommunication Union,* Nisan 2008, s. 2.
[9] Hakan Şentürk, Celal Z. Çil ve Şeref Sağıroğlu, "Cyber Security Analysis of Turkey", *International Journal Of Information Security Science,* Cilt 1, Sayı 4, Ankara 2012, s. 112.
[10] Nazli Choucri, *Cyberpolitics in International Relations,* The MIT Press, Londra 2012, s. 39.
[11] Nezir Akyeşilmen, *a.g.e.*, s. 116.
[12] Mustafa Ünver, Cafer Canbay ve Ayşe Gül Mirzaoğlu, *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler,* Bilgi Teknolojileri ve İletişim Kurumu, Nisan 2011, s. 3.

hasar veya yetkisiz erişime karşı korumak için kullanılan bir dizi teknik veya önlemler bütününü temel almaktadır.[13] Birçok araştırmacının ve kurumun tanımlama girişiminden görüldüğü üzere aktörler, ilgili olduğu alanlar çerçevesinde siber güvenlik kavramını ele almış, böylelikle küresel sistem içerisinde kabul görmüş genel bir tanımlama henüz yapılamamıştır. Aktörlerin yapmış olduğu tanımlama girişimlerinin farklılığına odaklanmak yerine; değişen ve dönüşen güvenlik gündemi içerisinde siber güvenliğin, kimin güvenliğini sağlayacağı ya da ne için güvenlik oluşturacağına dair tüm aktör, yapı ve sistemi kapsayan bir çerçeve ortaya koyabilmenin siber güvenlik kavramının anlaşılmasında daha faydalı olacağı düşünülmektedir.

Siber güvenlik alanı içerisinde, saldırı ve tehditlerden korunmanın yanı sıra bilginin güvence altına alınması da ciddi önem taşımaktadır. Siber güvenliğin; bilgi güvenliğinin sağlanması ve korunması hususunda 7 önemli prensibi bulunmaktadır. Siber güvenlik kavramının daha iyi anlaşılabilmesi konusunda kritik önem düzeyine sahip bu prensipler, genel özellikleriyle şu şekilde değerlendirilir;

Gizlilik: Bilgi ve iletişim ağlarındaki verilerin içerisinde önem derecesi yüksek bilgiler yer alabileceğinden, verilere yalnızca erişim yetkisi olan kişilerin ulaşabilmesi anlayışı olarak ifade edilmektedir.[14]

Bütünlük: Göndericiden çıkan verinin hiçbir koşulda ağdaki yetkisiz saldırgan tarafından değiştirilmemesi ya da zarar verilmemesi durumu olarak tanımlanmıştır.[15]

Erişilebilirlik: Yetkili kişilerin ihtiyacı olduğu her an verilere erişebilmesi, işlemlerinin sürdürülebilirliği açısından büyük önem arz etmektedir. Bilgi ve iletişim ağlarında gerçekleşecek kesintinin kritik altyapı sistemlerinin hizmet vermesini de

[13] Dan Craigen, Nadia Diakun-Thibault ve Randy Purse, "Defining Cybersecurity", *Technology Innovation Management Review,* Cilt 4, Sayı 10, Ekim 2014, s. 13.
[14] P.W. Singer ve Allan Friedman, *Siber Güvenlik ve Siber Savaş*, Çev. Ali Atav, 2. Baskı, Buzdağı Yayınevi, Şubat 2008, s. 57.
[15] Mustafa Ünver, Cafer Canbay ve Ayşe Gül Mirzaoğlu, *a.g.e.*, s. 4.

etkileyebileceği için erişimin kaliteli şekilde sürdürülebilmesi ve oluşabilecek tüm kayıpların önlenmesi, siber güvenlik alanında öncelikli hedeflerden biri olmuştur.[16]

Kimlik Doğrulama: Kullanıcıların kimliğinin doğrulandığı bir mekanizma yoluyla sadece yetkili hesap sahibinin verilere erişebilmesi sağlanabilmektedir.[17] Kimlik doğrulamasında kullanılan faktörlerin sayısına bağlı olarak tek faktörlü, iki faktörlü veya çok faktörlü kimlik doğrulaması uygulanabilmektedir.[18]

Yetkilendirme: Kullanıcının sistemdeki tanımlanmış rolüne bağlı olarak yalnızca izin verilmiş olunan verilere erişebilmesiyle siber alanda bilgi güvenliği korunmaya çalışılmaktadır.[19]

İnkâr Edememe: Sistemde iletişim kuran gönderici ve alıcının, göndermiş oldukları verileri inkâr edemeyeceklerine dair güvence anlamına gelmektedir.[20]

Kayıt Tutma ve İzlenebilirlik: Sistem içerisindeki verilerin, istenildiği zaman incelenebilmesi amacıyla kaydedilmesi durumu olarak ifade edilmiştir.[21]

Devletlerin, kurumları aracılığıyla sağlanan eğitim, enerji, ulaştırma, sağlık, savunma, elektronik haberleşme, bankacılık ve finans sistemleri gibi kritik altyapı hizmetlerinin büyük kısmının kontrolü ve işletilmesinde bilişim sistemlerinden yararlanılabilmektedir. Altyapı sistemlerinin sürekli olarak birbirleri ile etkileşim içerisinde olması nedeniyle herhangi birine yönelik gerçekleştirilebilecek siber saldırı faaliyeti sonucu diğerlerinin de hizmetlerinin aksamasına sebebiyet verilebilmesinin yanı sıra bu sistemlerden biri veya birkaçının hasar görmesi halinde kamu güvenliğinin, ekonomik refahın ve toplumsal huzurun olumsuz yönde etkilenmesi de

---

[16] Şeref Sağıroğlu, "Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemler", *Siber Güvenlik ve Savunma- Farkındalık ve Caydırıcılık,* Derleyen: Şeref Sağıroğlu ve Mustafa Alkan, Grafiker Yayınları, Ankara 2018, s. 42.

[17] Ahmet Naci Ünal, *Siber Güvenlik ve Elektronik Bileşenleri*, Nobel Akademik Yayıncılık Eğitim Danışmanlık Tic.Ltd.Şti, Eylül 2015, ss. 111-112.

[18] ITU, "ITU-T X.1205 – Supplement on framework of security information sharing negotiation", SERIES X: DATA NETWORKS, OPEN SYSTEM COMMUNICATIONS AND SECURITY, *International Telecommunication Union,* Nisan 2013, s. 5.

[19] Gürol Canbek ve Şeref Sağıroğlu, "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", *Politeknik Dergisi*, Cilt 9, Sayı 3, 2006, s. 170.

[20] Sait Yılmaz ve Olcay Salcan, *Siber Uzay'da Güvenlik ve Türkiye*, Milenyum Yayınları, İstanbul 2008, s. 86.

[21] Gürol Canbek ve Şeref Sağıroğlu, *a.g.m.*, ss. 171-172.

olasılık dahilindedir. Örneğin, bir ülkenin enerji sistemlerine düzenlenen kapsamlı bir siber saldırı ile binlerce veya milyonlarca vatandaşın hesabının bulunduğu bankacılık ve finans sistemlerinde ciddi maddi kayıplar yaşanmasına yol açılabilmektedir. Bu bakımdan, altyapı sistemlerinin güvenliğinin sağlanması için hem alanında uzman kişilerin çalıştırılması hem de güncel, güçlü ve doğru planlanmış siber güvenlik stratejisinin faaliyete geçirilmesinin devletler ve özel şirketler açısından büyük önemi bulunmaktadır.[22]

Siber güvenlik, sanal dünyada gerçekleştirilen saldırı ve tehditlerin etkilerinin birey, toplum ve devlet gibi fiziksel dünyada yer alan aktörlere yansıması sonucu ortaya çıkmıştır.[23] Devletlerin, askeri yönden güçlü ordu ve ekipmanlara sahip olsalar dahi teknolojik yenilikler ile desteklenmediği sürece ciddi güvenlik tehditleriyle karşı karşıya kalabilecekleri düşüncesiyle, ABD'nin ilk siber diplomatı Christopher Painter tarafından dile getirilen siber güvenliğe ciddi derecede finansal destek sağlanmadığı durumda devletlerin daha fazla askeri gücüne yatırım yapmak zorunda kalacakları ifadesi, bu savı destekleyen bir açıklama olarak değerlendirilebilir.[24] Bu çerçevede, 2000'li yılların başından beri devletlerin, güvenliklerini etkin bir şekilde sağlayabilmek adına askeri güvenlik unsurlarını siber savunma ve siber saldırı stratejileri ile destekleyerek yeniden organize etmesi gerektiği anlayışı, ulusal siber güvenlik stratejilerinde sıklıkla ifade edilmektedir.[25] Siber güvenlik kavramı özellikle 21. yüzyılın başlarına kadar "*alçak politika*" alanı içerisinde değerlendirilmesine rağmen, 2007 yılında Estonya'ya yönelik siber saldırılar, 2010'da İran'a yönelik Stuxnet Saldırısı, Arap Baharı sürecinde teknolojinin etkin rolü ve Wikileaks skandalı gibi ulusal güvenliğe yönelik büyük tehdit oluşturan siber saldırı niteliğindeki

---

[22] Mustafa Meral, *Siber Güvenlik Kapsamında Kritik Altyapıların Korunmasının Önemi*, (Harp Akademileri Stratejik Araştırmalar Enstitüsü, Savunma Kaynakları Yönetimi Ana Bilim Dalı, Yüksek Lisans Tezi), İstanbul 2015, ss. 30-31.

[23] Salih Bıçakcı, "Siber Güvenlik ve Savunma", Güvenlik Yazıları Serisi, No 42, Kasım 2019, https://trguvenlikportali.com/wp-content/uploads/2019/11/SiberGuvenlik_SalihBicakci_v.1.pdf, (Erişim tarihi: 22.04.2021), s. 2.

[24] A. Burak Darıcılı ve Barış Özdal, "Rusya Federasyonu'nun Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi", *Ahmet Yesevi Üniversitesi Türk Dünyası Sosyal Bilimler Dergisi* (BİLİG), Avrasya'nın Siyasal İktisadı Özel Sayısı, Sayı 83, Güz 2017, ss. 139-140; Betül Çatal, "Diplomaside Değişim ve Dönüşüm: Siber Diplomasi", *Medeniyet Araştırmaları Dergisi,* Cilt 2, Sayı 3, İstanbul 2015, s. 47.

[25] Eneken Tikk, Kadri Kaska ve Liis Vihul, *International Cyber Incidents: Legal Considerations*, NATO CCDCOE Publication, Tallinn 2010, s. 29.

eylemler sonucu karar alıcılar tarafından kavramın, "*yüksek politika*" alanı içerisinde değerlendirilmesinin gerekliliği anlaşılmıştır.[26] Bu bağlamda, güvenlik gündeminin genişleme sürecinde siber güvenliğin artan öneminin anlaşılabilmesi için siber güvenlik kavramının tarihsel perspektifte gelişiminin incelenmesi gereklilik oluşturmaktadır.

1.2. Siber Güvenliğin Tarihsel Analizi

İnternet, çeşitli veri türlerini değiş tokuş etmek üzere kurulmuş, birbirine bağlı dijital ağlardan oluşan küresel bir sistem olarak tanımlanmakta, bu çok merkezli yapı aracılığıyla coğrafi mesafe tanımaksızın milyonlarca teknolojik cihazın birbirleriyle bağlantısı sağlanabilmektedir. İnternetin, iş dünyası için küresel bir altyapı sağlaması, siyaset ve askeri faaliyetlerin yanı sıra casusluk gibi faaliyetler için de yeni bir araç olarak gelişmesi sonucu siber güvenliğin yerelden küresele güvenlik disiplininin ana kavramlarından biri halini aldığı görülmüştür.[27]

İnternet'in günümüzdeki versiyonunun ilk aşamaları, 1960'lı yılların ortalarında yürütülen çalışmalara dayanmakta ve Amerika Birleşik Devletleri Savunma Bakanlığı'nın (*U.S. Department of Defense*, DoD) Savunma İleri Araştırma Projeleri Ajansı (*Defense Advanced Research Projects Agency*, DARPA) tarafından finanse edilen Gelişmiş Araştırma Projeleri Ajansı Ağı'nın (*The Advanced Research Projects Agency Network,* ARPANET) dinamik bir evrimi olarak değerlendirilmektedir.[28] Soğuk Savaş döneminin sonlarına doğru siber alan içerisinde yer alan kritik bilgi altyapısının korunması veya bilgi güvenliği gibi kavramlar, uzman çevreler içerisinde çoğunlukla teknik yönleri ele alınarak tartışılmıştır. 1990'lı yılların başında ise siber güvenlik kavramı ilk olarak bilgisayar teknisyenleri tarafından internet ağlarının ve bunlara bağlı bilgisayarların güvenlik sorunlarını ifade etmek için kullanılmaya başlanmıştır.[29] 21. yüzyıla girilmesiyle beraber küreselleşmenin

[26] Nazli Choucri, *a.g.e.,* s. 3; David D. Clark ve Nazli Choucri, "Who Controls the Cyberspace?" *Bulltein of the Atomic Scientists*, Cilt 69, Sayı 5, Eylül 2013, s. 21.
[27] Nezir Akyeşilmen, *a.g.e.,* ss. 23-32.
[28] Murat Güngör, "Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma", *T.C. Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı*, Yayın No: 2919, Uzmanlık Tezi, Mart 2015, s. 27.
[29] Mehmet N. Öğün ve Adem Kaya, "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", *Güvenlik Stratejileri Dergisi*, Cilt 9, Sayı 18, Temmuz 2013, s. 163.

yaygınlaşması ve teknolojinin öngörülemez gelişimi sonucu siber tehditlerin hem bireyler hem devletler hem de organize suç örgütleri tarafından gerçekleştirilebileceği gerçeği ortaya çıkmıştır. Bunun sonucunda da siber güvenlik kavramı, devletlerin ulusal güvenlik stratejileri içerisinde yer almaya ve ulusal güvenlik sorunu olarak görülmeye başlanmıştır.[30]

1.2.1. Soğuk Savaş Döneminde İnternetin Gelişimi

Birinci Dünya Savaşı ve İkinci Dünya Savaşı yılları, teknolojinin savaş alanında kullanımının net bir şekilde gözlemlendiği yıllar olmuştur. Birinci Dünya Savaşı süresince telsizlerin haberleşme aracı olarak kullanımı, telsiz haberleşme üslerinin yerinin tespit edilmesi, haberleşme faaliyetlerinin dinlenmesi ve aldatılması şeklinde teknolojinin kullanıma girdiği görülmüştür.[31] İkinci Dünya Savaşı boyunca ise elektronik gelişmeler dahilinde uçak seyrüsefer sistemlerinde oynamalar, radar ikaz sistemlerinin yaygın olarak kullanılması ve radar sistemlerine karıştırıcıların uygulanması gibi teknolojik yenilikler, ülkelerin harekat planlarında yer almıştır.[32] İkinci Dünya Savaşı'nın sona ermesiyle birlikte teknolojinin gelişimi açısından yepyeni bir çağın başladığı görülmektedir. Her iki savaş dönemlerinde savaş alanlarında teknolojik araçlarla gerçekleştirilen faaliyetlerin, Soğuk Savaş dönemi içerisinde teknolojinin hızla değişim ve gelişimine aracılık etmesindeki itici gücü oluşturduğu düşünülmektedir.[33]

19. yüzyılda iletişim ve haberleşmeyi sağlamak amacıyla devrim niteliğinde iki buluş olan telefon ve telgraf, internetin de icat edilmesinin en büyük öncüsü olarak kabul görmektedir.[34] İnternetin, Soğuk Savaş döneminde ABD ve SSCB arasında cereyan eden askeri, ekonomik ve ideolojik rekabet sonucu ortaya çıkmış olduğu, bir diğer ifadeyle internetin ortaya çıkışının eğlence, bilim ya da ticari amaca dayanmaktan ziyade, Soğuk Savaş dönemindeki rekabet ortamının bir ürünü olduğu

[30] Marie Baezner ve Patrice Robin, "Hotspot Analysis: Cyber-Conflict Between The United States Of America And Russia", *Center for Security Studies* (CSS), Haziran 2017, s. 14.
[31] Ahmet Naci Ünal, *a.g.e.*, s. 9.
[32] Ahmet Naci Ünal, *a.g.e.*, s. 10.
[33] Ahmet Naci Ünal, *a.g.e.*, s. 16.
[34] Mustafa Ünver ve Cafer Canbay, "Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik", *Elektrik Mühendisliği Dergisi*, Sayı 438, Mart 2010, s. 94.

değerlendirilmektedir.[35] SSCB, yürütmüş olduğu çalışmalar kapsamında 4 Ekim 1957'de dünyanın ilk yapay uydusu olan Sputnik-1'i hemen ardından 4 Kasım'da Sputnik-2'yi uzaya göndermiştir.[36] SSCB'nin aya uydu göndererek ikili rekabet ortamında öne geçmesi, ABD ve müttefikleri arasında korku ve güven eksikliğinin doğmasına sebep olmuştur. ABD, ikili rekabet ortamını lehine çevirebilmek amacıyla 1958 yılında "Gelişmiş Araştırma Projeleri Ajansı" (*Advanced Research Projects Agency*, ARPA) adında bir birim kurarak, olası bir savaş durumunda haberleşme sistemlerinin önemli bölümü kesintiye uğrasa dahi iletişimin kesintisiz olarak sürdürülebileceği bir ağ yaratmak üzerine ilk adımı atmıştır.[37] Bu proje, 1962 yılında birimin araştırma alanı genişletilerek ARPANET adını aldığı görülmektedir.[38] Günümüzde, hemen hepimizin hayatının vazgeçilmez unsuru haline gelen internetin ortaya çıkışının temelinde bu gelişmelerin bulunduğu söylenebilir. Bilindiği üzere, Soğuk Savaş dönemi içerisinde ABD'nin en önemli tehdit kaygısının kaynağı, Doğu Bloğu olarak görüldüğünden SSCB tarafından herhangi bir ağ merkezli saldırıyla karşı karşıya kalınsa dahi iletişim ve haberleşmenin problemsiz devam etmesinin ABD'ye büyük fayda sağlayacağı düşünülmüş, böylelikle nihai amacı birden çok merkez ve komuta yapısına sahip olan ARPANET'in kurulma kararı alınmıştır.[39] Ancak, Akyeşilmen'in de vurguladığı gibi; sistemin herhangi bir yönetim veya kontrol mekanizması olmadan yalnız tehdit odaklı olarak geliştirilmesi, internetin zamanla çok merkezli ve asimetrik bir tehdit aracına dönüşmesine sebebiyet vermiştir.[40]

Siber saldırıların tarihsel kökleri değerlendirildiğinde, bu alanda çalışmalar yapan birçok araştırmacı, ABD tarafından siber teknoloji kullanılarak tarihteki ilk siber saldırının 1982 yılında gerçekleştirildiğini belirtmektedir. Bu araştırmacılardan biri olarak Thomas Rid; siber saldırının, Amerikan Merkezi İstihbarat Teşkilatı'nın (

---

[35] Nezir Akyeşilmen, *a.g.e.*, s. 25.
[36] Zuhal Demirci, "İnsanoğlunun Uzay Macerası 61 Yıl Önce Başladı", (03.10.2018), *https://www.aa.com.tr/tr/bilim-teknoloji/insanoglunun-uzay-macerasi-61-yil-once-basladi/1271438*, (Erişim tarihi: 27.07.2020).
[37] Gabriel Weimann, *Terror On The Internet: The New Arena The New Challenges*, United States Institute of Peace Press, Mart 2006, s. 5.
[38] Mahruze Kara, *Siber Saldırılar- Siber Savaşlar ve Etkileri*, (İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü, Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, Yayımlanmış Yüksek Lisans Tezi), İstanbul 2013, s. 7.
[39] Myriam Dunn Cavelty, "Cyber-Security", *Contemporary Security Studies*, Derleyen: Alan Collins, Oxford University Press, Mayıs 2012, s. 363.
[40] Nezir Akyeşilmen, *a.g.e.*, s. 26.

The Central Intelligence Agency, CIA) Sibirya'daki doğalgaz boru hattının yazılımına Truva atı virüsü yerleştirilmesi sonucu meydana geldiğini ve virüsün bir süre sonra boru hattındaki gaz akışını aşırı derecede artırarak borunun patlamasına sebebiyet vermiş olduğunu ileri sürmektedir.[41] 1988 yılında ise siber saldırılara örnek olarak gösterilebilecek Morris solucanının, dünyanın bilgisayar ve internet altyapısını tehdit eden ilk solucan olmasının yanı sıra ABD'deki bilgisayarlara sızarak işlevsiz hale getirene kadar yavaşlamasına neden olduğu belirtilmektedir.[42]

1.2.2. Soğuk Savaş Sonrası Siber Güvenliğin Gelişimi

1990'lı yıllar itibarıyla internetin; iletişimi, bilgi paylaşımını ve ağlar arasındaki transferi sağlaması nedeniyle tüm dünyada kullanıcı sayısı gittikçe artış göstermiştir. Bilişim teknolojisinde yaşanan öngörülemez gelişim sayesinde yaygınlaşan internet kullanımı; devlet kurumlarında, şirketlerde, sivil toplum kuruluşlarında, okullarda ve bireyler arasında hayatın vazgeçilmez bir parçası haline gelmiştir.[43] 1990'lı yıllarda kişisel bilgisayarların boyutlarında ve işlemcilerinde yapılan düzenlemeler sonrası neredeyse tüm işletmeler içerisinde en az bir bilgisayar bulunur olmuştur. Bilişim sistemlerinin ve internet ağlarının bu kadar hızlı yayılması bir yandan kullanıcılara geniş bir hareket sahası ve etkileşim olanağı sağlarken, diğer yandan da bilişim sistemlerinin kötüye kullanılarak ulusal ve uluslararası güvenlik sorunlarının yaşanmasına neden olmuştur.[44]

Siber güvenlik kavramı, ilk kez 1990'lı yılların başında bilgisayar teknisyenleri tarafından internete bağlı bilgisayarlardaki güvenlik sorunlarına yönelik olarak kullanılmıştır. 1991 senesinde Tim Berneis Lee isminde bir araştırmacının, "World Wide Web" (www) sistemini bularak ilk web sitesini kullanıma açmasıyla kullanıcılar arasında internet aracılığıyla bilgi paylaşımında ciddi ilerleme

---

[41] Thomas Rid, "Think Again: Cyberwar", (27.02.2012), *https://foreignpolicy.com/2012/02/27/think-again-cyberwar/,* (Erişim tarihi: 12.07.2020).
[42] Hasan Çifci, *Her Yönüyle Siber Savaş*, 2. Baskı, TÜBİTAK Bilim Kitapları, Temmuz 2017, s. 169.
[43] Neil F. Doherty, Leonidas Anastasakis ve Heather Fulford, "The Information Security Policy Unpacked: A Critical Study of the Content of University Policies", *International Journal of Information Management*, Cilt 29, Sayı 6, Aralık 2009, s. 450.
[44] Cihan Daban, "Siber Güvenlik ve Uluslararası Güvenlik İlişkisi" *Siber Politikalar Dergisi*, Cilt 1, Sayı 1, Kış 2016, s. 88.

kaydedildiği görülmüştür.[45] Ancak bilgi paylaşım sistemlerindeki geliştirmeler, dezavantajları da beraberinde getirmiş ve internet ortamı karşı taraflar üzerinde tehdit oluşturmak amaçlı da kullanılır olmuştur.[46]

1999 yılında NATO'nun, Kosova Harekâtı sırasında Sırp hedeflerini bombalaması üzerine Sırp ve Rus bilgisayar korsanları tarafından İttifak'ın askeri haberleşme sistemleri ve merkez karargahındaki sunucular kapsamlı siber saldırıların hedefi olmuştur.[47] Bunun üzerine NATO'nun hem kendi içerisinde hem de üye devletlerle olan çevrim içi koordinasyonu sekteye uğramıştır. Bu saldırı sonucu siber güvenlik, uluslararası sistemin aktörleri tarafından önem derecesi artan bir kavram halini almıştır.[48]

2000'li yılların ortalarında siber güvenliğe, ulusal güvenlik stratejileri içerisinde yer verilmesine sebep olarak iki önemli siber saldırı örneği gösterilmektedir. Birinde Estonya'nın diğerinde ise Gürcistan'ın hedef alındığı, saldırıların arkasında Rusya'nın olduğunun iddia edildiği bu saldırılardan; Estonya'ya yönelik siber saldırılar 3 haftaya yakın bir süre etkisini devam ettirmiştir.[49] Aynı zamanda Estonya'da, internet kullanım oranının yüksek olması sebebiyle bu süre boyunca kritik altyapı hizmetlerinin çoğu ciddi derecede etkilenmiştir. Gürcistan ise internet kullanım oranının düşüklüğü sebebiyle saldırılar karşısında nispeten daha az zarar görmüştür.[50] 2009-2010 yılları içerisinde İran nükleer tesislerine yönelik gerçekleştirilen Stuxnet isimli siber saldırı ise; siber güvenlik kavramının gelişim ve dönüşümüne sebebiyet veren ana olaylardan birini temsil etmiştir. Bu saldırı sonucu, İran'ın yüksek koruma altında işletilen nükleer santrifüjlerinin büyük zarar görmesinin yanı sıra hem İran'a hem de nükleer programına azımsanmayacak miktarda maddi zarar verildiği

---

[45]Alper Kaya, "World Wide Web (WWW) Nedir?" (28.04.2016), *https://www.tech-worm.com/world-wide-web-www-nedir*/, (Erişim tarihi: 14.07.2020).

[46] Salih Bıçakcı, "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu" *Uluslararası İlişkiler*, Cilt 9, Sayı 34, Yaz 2012, s. 209.

[47] Kenneth Geers, "Cyperspace and the Changing Nature of Cyber Space", *NATO CCD COE Publication,* Tallinn 2008, *https://www.ccdcoe.org/uploads/2018/10/Geers2008_CyberspaceAndTheChangingNatureOfWarfare.pdf*, (Erişim tarihi: 14.07.2020), s. 6.

[48] A. Burak Darıcılı, "NATO'nun Siber Güvenlik Stratejisi'nin Analizi", *Uluslararası Sistemde Yeni Düzen Arayışları,* Derleyen: Tayyar Arı ve Barış Özdal, Dora Basım, Bursa 2015, ss. 411-412.

[49] Şirin Duygulu, *Dönüşen Savaşların Değişen Araçları*, SETA Yayınları, Temmuz 2019, ss. 89-90.

[50] Salih Bıçakcı, "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", *Uluslararası İlişkiler*, Cilt 10, Sayı 40, Kış 2014, ss. 119-122.

anlaşılmıştır. Ayrıca, siber alanın devletlerin nükleer programlarına karşı kullanılıp çeşitli zararlara sebep olabileceği ve nükleer istikrar için tehdit oluşturabilecek bir alan haline geldiği görülmüştür.[51]

Uluslararası İlişkiler disiplini çalışmalarını derinden etkisi altına alan olaylardan bir diğeri de 2010 yılında gerçekleşen Wikileaks sızıntılarıdır. Wikileaks; hükümetler, istihbarat örgütleri ve siyasi liderler hakkındaki önemli bilgi ve haberleri kamuoyu ile paylaşan uluslararası bir kâr amacı gütmeyen kuruluş olarak kendini tanıtmaktadır.[52] Bu bağlamda, ABD Dışişleri Bakanlığı'nın 1966-2010 yılları arasındaki gizli yazışmalarını ve ABD Büyükelçilikleri tarafından gönderilen 250.000'e yakın diplomatik belgeyi internet sitesi üzerinden yayımlamıştır.[53] Ayrıca, konuyla ilgili yapılan araştırmalarda Wikileaks tarafından bugüne kadar çeşitli hükümetler temsilcilerine, kamu çalışanlarına ve kamu kurumlarına ait 10 milyonun üzerinde belgenin ele geçirildiğinin tahmin edildiği belirtilmektedir.[54] Bu saldırı, siber güvenliğin en önemli prensiplerinden olan bilginin gizliliğinin ve bütünlüğünün korunmasının ne kadar önemli olduğunu göstermiştir. Aynı zamanda devletler veya organize suç örgütlerinden ziyade tek bir bireyin bile devletin ulusal güvenliğine ciddi zararlar oluşturabileceği anlaşılmıştır. 2013 yılında Edward Snowden isimli eski CIA ve Ulusal Güvenlik Ajansı (*The National Security Agency*, NSA) çalışanının ABD hakkındaki bazı gizli bilgileri ortaya çıkarması sonucu NSA'nın, siyasi liderleri ve büyükelçilikleri elektronik takibe aldığı, milyonlarca ABD vatandaşının telefon kayıtlarını dinlediği ve kişisel bilgilerin erişilerek kayıt altına alındığı ortaya çıkmıştır.[55] Snowden Olayı sonrası bir yandan bireysel özgürlükler, insan hakları ve özel hayatın gizliliği kavramları diğer yandan da siber güvenlik-hukuk ilişkisi sorgulanır hale gelmiştir.

---

[51] Şirin Duygulu, *a.g.e.*, s. 91.

[52] Arzu Turgut, *Wikileaks Belgelerinde Türkiye ve Yakın Çevresi- Türkiye, Rusya, Güney Kafkasya ve Ortadoğu ile İlgili Belgeler*, Uluslararası Stratejik Araştırmalar Kurumu Yayınları, Rapor No: 11-03, Nisan 2011, s. 7.

[53] Francis Whittaker, "What Is WikiLeaks? Everything you need to know", (30.04.2018), *https://www.nbcnews.com/storyline/smart-facts/what-wikileaks-everything-you-need-know-n869556*, (Erişim tarihi: 25.07.2020).

[54] Susan Miller, "What is WikiLeaks?", (07.03.2017), *https://www.usatoday.com/story/news/2017/03/07/what-wikileaks/98853896/*, (Erişim tarhi: 17.07.2020).

[55] BBC News, *Edward Snowden: Leaks That Exposed US Spy Programme*, (17.01.2014), https://www.bbc.com/news/world-us-canada-23123964, (Erişim tarihi: 19.07.2020).

Sonuç olarak; özellikle son 20 yıldaki gelişmelerden anlaşılacağı üzere siber güvenlik kavramının yerel, bölgesel ve küresel düzeyde büyük bir gelişim ve dönüşüm geçirdiğine yönelik çıkarım yapmak mümkündür. Günümüzde, yaşanan bu olaylar sonucunda hükümetler, uluslararası örgütler, kurumlar ve şirketler bilgi güvenliğini daha iyi sağlayabilmek için yeni eylem ve politikalar geliştirmişlerdir. Siber tehditlerin asimetrik yapısı nedeniyle ulusal güvenlik stratejileri içerisinde askeri güvenliğe yakın derecede önem önceliğine sahip bir siber güvenlik kavramının ön plana çıktığı dikkat çekmektedir. Bununla birlikte, siber saldırıların yol açtığı maddi hasarın yıldan yıla yükselmesi üzerine bazı devletlerin ve özel sektör kuruluşlarının siber savunmaya yönelik ayırdığı bütçelerinde büyük artışlar gerçekleştirdikleri görülmüştür.[56] Siber güvenliğe yönelik henüz kapsamlı hukuk normları ve uluslararası iş birliği ortamı sağlanamamış olsa dahi gelecek yıllarda siber tehditlerle mücadele edebilmek adına bu alanlarda önemli adımların atılacağına yönelik beklentiler bulunmaktadır.

1.3. Siber Güvenlik Kapsamındaki Kavramlar

Siber uzay, neredeyse kırk yıla yakın bir süredir devletleri ve toplumları derinden etkilemeyi sürdürmektedir. Bu kapsamda, günlük yaşamımızı devam ettirmemizde yarar sağlayan teknolojik hizmetleri sunmasının yanı sıra saldırı ve tehdit unsurlarını da içerisinde barındırmaktadır. Siber saldırı ve tehditlerin birçoğu ulusal güvenlik üzerinde ciddi etkileri olabilecek çeşitli siyasi ve askeri amaçların bir aracı olarak kullanılabilmektedir. Siber saldırılar sadece devletleri etkilememekte; bunun yanı sıra özel sektör işletmeleri, toplumlar, bireyler, kurum ve kuruluşlar da ekonomik, sosyal ve kültürel açıdan zarar görebilmektedir. Özellikle devletler ve özel şirketler tarafından, bu tür saldırı ve tehditler ile mücadele edebilmek için siber savunma ve siber caydırıcılık üzerine önemli çalışmalar yürütülmekte ve stratejiler geliştirilmektedir. Buna ek olarak devletler, siber alandaki diplomatik işlerinin yerine getirilebilmesi için günümüz itibarıyla nispeten yeni bir kavram olan siber diplomasi alanına yatırım yapmaya başlamışlardır. Ayrıca, siber uzayın anonim yapısı sayesinde saldırı ve tehditlerin kaynağının zaman zaman devletler olduğuna ilişkin görüşler de

[56] Mutlu Çavuş, "Kurumların Siber Güvenlik Için Ayırdığı Bütçe Artacak", (08.11.2018), *https://www.btgunlugu.com/kurumlar-siber-guvenlik-butce/*, (Erişim tarihi: 19.07.2020).

ortaya atılabilmektedir. Ortaya atılan iddialarda, saldırıların nedeni olarak bazı devletlerin tehdit olarak gördüğü diğer devletlerle ilgili stratejik veri ve bilgileri ele geçirebilmek için istihbarat ve casusluk faaliyetlerine yönelmeleri olduğu ileri sürülmektedir.[57]

1.3.1. Siber Uzay

Bilişim teknolojilerinin ve internetin kullanımındaki artış, günlük yaşamın akışı içerisinde gerçekleştirilen faaliyetlerin büyük kısmının bilgi ve iletişim teknolojileri ile iç içe geçmesini sağlamıştır. 1990'lar itibarıyla internetin bireyler tarafından kullanılmaya başlanması üzerine insanlar, toplumlar ve devletler arasındaki coğrafi mesafeler önemini yitirmiş ve bilgi paylaşımı kademeli olarak artış göstermiştir. Teknolojik gelişmelerin insanların hayatını bu kadar hızlı geliştirmesi ve dönüştürmesi, siber uzay olarak tanımlanan yeni bir alanın doğmasını sağlamıştır.[58] Siber uzay kavramı ilk olarak 1984 yılında bilim kurgu yazarı William Gibson tarafından yayınlanan "*Neuromancer*" adlı eserde kullanılmıştır.[59] Bu eserin ortaya çıkmasından birkaç yıl sonra ise, siber uzay kavramı bilişim teknolojileri alanı ile ilişkilendirilmiştir.[60] Siber güvenlik kavramında olduğu gibi, siber uzayın da değişken bir yapıya sahip olması sebebiyle net bir tanımı ortaya konulamamıştır. Bu bağlamda siber uzay, en çok kabul görmüş tanımlamalardan biri olarak bilgisayarlar ve onların operatörleri arasında iletişim ve bilgi alışverişini sağlayan küresel bir araç olarak belirtilmektedir.[61] Aynı zamanda siber uzay kavramı; bilginin bir ortamdan diğerine dolaştığı, işlendiği, çoğaltıldığı ve depolandığı bir alanı ifade etmektedir.[62]

Amerikalı siyaset bilimci Joseph S. Nye, siber uzayı; sadece ağa bağlı bilgisayarların interneti değil, aynı zamanda intranetler, hücresel teknolojiler, fiber

---

[57] Vahit Güntay, "Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler", *Güvenlik Stratejileri Dergisi*, Cilt 14, Sayı 27, 2018, ss. 87-89.
[58] Jason Whittaker, *The Cyberspace Handbook,* Routledge, Şubat 2004, s. 3.
[59] William Gibson, *Neuromancer*, Özel 20. Yıl dönümü Baskısı, ACE Book, New York 2004, s. 4.
[60] Güzin Ulutaş, "Siber Güvenlik", *Siber Güvenlik ve Savunma- Farkındalık ve Caydırıcılık,* Derleyen: Şeref Sağıroğlu ve Mustafa Alkan, Grafiker Yayınları, Ankara 2018, s. 88.
[61] Paul Cornish, "Governing Cyberspace Through Constructive Ambiguity", *Survival,* Cilt 57, Sayı 3, Haziran-Temmuz 2015, s. 153.
[62] P.W. Singer ve Allan Friedman, *a.g.e.*, s. 29.

optik kablolar ve uzay tabanlı iletişim bütünü olarak açıklamaktadır.[63] ABD Savunma Bakanlığı'na göre siber uzay; bilgi ortamı dahilinde internet, telekomünikasyon ağları, bilgisayar sistemleri, gömülü işlemciler ve denetleyiciler dahil olmak üzere birbirine bağlı bilgi teknolojileri ağından oluşan küresel bir alanı tanımlamaktadır.[64]

Siber alan, dünyadaki tüm bilgisayar ağlarına ilaveten iletişim ağları, askeri ağlar, enerji aktarım ağları, elektronik komuta sistemleri, mobil cihazlar, telsizler, uydu sistemleri, insanlı ve insansız hava araçları gibi çeşitli sistemlerin ve donanımların bütününü kapsamaktadır.[65] Kısacası; dijital sinyallerin gönderilmesi, alınması ve işlenmesinin mümkün olduğu her alan siber uzayın kapsamı içerisine girebilmektedir. Bu ortam, kişiler arasında yaygın bir şekilde internet olarak tanımlanmasına rağmen, siber uzayı sadece internet olarak tanımlamak eksik kalacaktır. Bunun en önemli sebebi, gerçek dünyada gerçekleşmeyen her tür işlem veya olayın siber alanda gerçekleşebilme ihtimalinden kaynaklanmaktadır. Bir bakıma, herhangi bir bilgisayar sistemi aracılığıyla işlenen ve gerçek dünya tarafından görülemeyen veri veya bilgiler de siber alanın parçası olabilmektedir. Aynı zamanda, veri ve bilgilerin yerel ağlar, kablosuz bağlantı alanı (Wi-Fi) veya Bluetooth gibi internet dışı yöntemlerle paylaşılması da siber uzayın kapsam alanına girmektedir.[66]

İnsanlar tarafından denizcilik alanı binlerce yıldır, havacılık neredeyse yüz yıldır, uzay ise altmış yıldır kullanılmaktadır. Bunun sonucunda siber uzay, evrensel ortak alanlar içerisinde en yenisi olmakla birlikte en az diğerleri kadar önemli bir yere sahip olduğu düşünülmektedir. Siber uzay, uluslararası sistem içerisinde yaklaşık kırk yıldır yer almasına rağmen, günümüz itibarıyla dünya nüfusunun dörtte birinden fazlası tarafından her gün kullanılmakta ve bu sayı gün geçtikçe artmaya devam etmektedir.[67] Böylece siber uzay, küreselleşmiş dünyanın ve ulusların kullanım

---

[63] Joseph S. Nye, "Nuclear Lessons for Cyber Security?", *Strategic Studies Quarterly*, Cilt 5, Sayı 4, Kış 2011, s. 19.
[64] US Department of Defence, *Cyberspace Operations*, Joint Publication 3-12, Haziran 2018, s. 1.
[65] Hasan Çifçi, *a.g.e.*, s. 5.
[66] David Clark, Thomas Berson ve Herbert S. Lin, *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*, Washington DC: The National Academies Press, Temmuz 2014, s. 8.
[67]Mark Barrett, Dick Bedfort, Elizabeth Skinner ve Eva Vergles "Assured Access to the Global Commons", *Supreme Allied Command Transformation, North Atlantic Treaty Organisation*, Virginia 2011, *https://meerverstehen.net/wp-content/uploads/2012/05/global-commons.pdf*, (Erişim tarihi: 11.08.2020), ss. 33-34.

alanının ağırlık merkezi halini almıştır. Siber uzay; 2016 yılındaki Varşova Zirvesi'nde, NATO ve müttefikleri tarafından askeri operasyonların bir alanı olarak kabul edilmiş ve ulusal altyapıların güvenliği için önemli kurumlar faaliyete geçirilmiştir.[68] Bu gelişme, siber uzayın devletlerin askeri operasyon ve politikaları içerisinde yer alan en önemli bileşenlerinden biri haline gelmekte olduğunun en büyük göstergesini oluşturmuştur.[69] Siber uzay sadece askeri alan içerisinde değil, aynı zamanda ekonomik, finansal, diplomatik ve toplumsal alanlar da dahil olmak üzere ulusal faaliyetlerin tüm yönleri açısından etkili bir güç aracı olarak kabul edilmektedir.[70]

Sonuç olarak; siber uzay, günümüz dünyasında enerji, ulaştırma, bilişim ve iletişim dahil olmak üzere her kritik altyapıyı birbirine bağlayan bir araç olması sebebiyle ulusal ve küresel güvenlik paradigmasının hayati bileşeni haline gelmiştir. Siber uzay; diplomasi, istihbarat, ekonomi ve askeri gibi tüm ulusal güç unsurlarının veri ve ağ geçiş kontrollerinin sağlanabildiği tek alandır. Halihazırda siber uzayın bu kadar etkin ve yaygın şekilde kullanılması, devletlere sağladığı büyük imkanların yanı sıra güvenlik zafiyetlerini de doğurmuştur.[71] Bu nedenle siber uzay; devletlerin, devlet dışı örgütlerin hatta bireylerin kimliklerini gizleyerek rakibe saldırı veya tehdit oluşturabileceği anarşik bir alan özelliği de taşıyabilmektedir.[72] Gelecek yıllarda gerçekleşecek siber saldırıların ciddi maddi ve manevi kayıplara yol açmasını önleyebilmek için devletlerin hem kendi aralarında hem de özel şirketlerle konu kapsamında iş birliği içerisinde olma gereksinimine ihtiyaç duyulmaktadır.

1.3.2. Siber Saldırı ve Siber Tehdit

Teknolojinin hızla gelişiminin güvenlik sistemleri üzerinde olumlu etkileri olmasına rağmen bilgisayarların ve teknolojik aletlerin sayılarında yaşanan olağanüstü

---

[68]NATO, *Warsaw Summit Communiqué*, (29.03.2017), https://www.nato.int/cps/en/natohq/official_texts_133169.htm, (Erişim tarihi: 11.08.2020).
[69]Laura Brent, "NATO's Role in Cyberspace", (12.02.2019), *https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html*, (Erişim tarihi: 11.08.2020).
[70]Salih Bıçakcı, "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda…", s. 103.
[71]Fred Schreier, "On Cyberwarfare", DCAF Horizon 2015, Araştırma Makalesi, *The Geneva Centre for the Democratic Control of Armed Forces* (DCAF), Sayı 7, Cenevre 2013, s. 13.
[72]Nazli Choucri, "Introduction: CyberPolitics in International Relations", *International Political Science Review*, Cilt 21, Sayı 3, 2000, s. 257.

artış, siber saldırı ve tehditlerin günden güne kapasitelerini ve etkilerini artırmalarını da beraberinde getirmiştir. Andress ve Winterfeld'e göre siber saldırı; bilgisayar sistemlerindeki veya ağlardaki verilere, yazılımlara veya donanımlara karşı kasıtlı eylemler bütününü ifade etmektedir. Bu doğrultuda, hükümetler veya özel şirketler, internet ve dijital altyapılara ne kadar bağımlı olursa, saldırıları gerçekleştirenler tarafından o derece önemli birer hedef haline gelebilmektedirler.[73] Geçmiş yıllarda tecrübe edilen siber saldırıların altyapı sistemleri üzerinde açabileceği tahribatın farkında olunması sebebiyle günümüzde pek çok hükümet tarafından siber saldırıları caydırabilmek ve engelleyebilmek için gerekli faaliyetlerin yürütülmesine çalışılmakta olduğu görülmektedir.

Siber saldırı kavramının mevcut tanımlamaları, her ülkenin ve her uluslararası aktörün kendine has tehdit öncelikleri bulunması sebebiyle farklılık gösterebilmektedir. Avrupa Ağ ve Bilgi Güvenliği Ajansı'na (*The European Union Agency for Cybersecurity*, ENISA) göre siber saldırı; bilgisayar veya ağlar aracılığıyla rakibin kritik sistemlerine zarar vermeye veya yok etmeye neden olan olaylar bütününü tanımlamaktadır.[74] NATO Müşterek Siber Savunma Mükemmeliyet Merkezi (*The NATO Cooperative Cyber Defence Centre of Excellence*, NATO CCDCOE) koordinatörlüğünde ve Uluslararası Bağımsız Uzmanlar Grubu'nun katılımıyla hazırlanan "Talinn El Kitabı" içerisinde ise siber saldırı kavramı; saldırı ya da savunma amaçlı yapıldığı fark edilmeksizin kişiler veya nesneler üzerinde yaralanmaya, yıkıma ya da tahribata yol açan siber faaliyetler olarak ele alınmıştır.[75] Aynı kaynakta, bir eylemin siber saldırı olarak kabul edilebilmesi için kesinlikle düşmana karşı şiddet unsurları içermesi gerektiği vurgulanmaktadır. Bunun

[73] Jason Andress ve Steve Winterfeld, *Cyber Warfare: Techniques, Tactics And Tools For Security Practitioners*, 2. Baskı, Syngress, Ekim 2013, ss. 20-21.
[74] The European Union Agency for Cybersecurity, "Overview Of Cybersecurity And Related Terminology", *European Union Agency For Network and Information Security*, Versiyon 1, Eylül 2017, *https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology*, (Erişim tarihi: 12.08.2020), s. 7.
[75] Michael N. Schmitt, *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, New York 2013, s. 105.

sonucunda, psikolojik siber operasyonlar veya siber casusluk gibi şiddet içermeyen eylemlerin siber saldırı olarak nitelendirilemeyeceği belirtilmiştir.[76]

Siber tehdit kavramı, bilişim sistemlerinin birer araç olarak kullanılması yoluyla bir devletin veya kurumun ekonomik, toplumsal veya politik değerlerine şüphe ve korku aşılamak amacıyla gerçekleştirilen faaliyetler olarak tanımlanmaktadır.[77] Herhangi bir saldırının siber tehdit olarak nitelendirilebilmesi için saldırıyı kimin gerçekleştirdiğinin ve neleri hedef aldığının belirlenmesine gerek duyulabilmektedir. Siber tehditler, sadece bir kişinin ya da bir ulusun güvenlik ve finansal yapısını tehdit etmekle kalmamakta, aynı zamanda sosyal itibarına da büyük tahribat verebilmektedir.[78] Fulya Aslay'a göre siber tehdit ve saldırıların temel hedefleri arasında; sisteme izinsiz erişim, bilginin gizliliğine ve bütünlüğüne zarar verilmesi, ifşa edilmesi ve sistemi hizmet veremez hale getirmesi yer almaktadır.[79]

Siber saldırıların gerçekleşmesi sonucu ağ erişiminin kesilmesi, engellenmesi, bozulması veya tamamen yok olması gibi sonuçlar ile karşı karşıya kalınmasının yanı sıra nükleer santrifüjler, hava savunma sistemleri, elektrik şebekeleri, ulaşım altyapıları, sağlık sektörü, acil servisler, barajlar, bankacılık ve finans, tarım, kimya ve savunma altyapıları gibi kritik hedeflere düzenlenen siber saldırılar yoluyla bir ülkenin ulusal güvenliği ciddi zararlar görebilmektedir. 2009 yılında, ABD'nin 44. Devlet Başkanı Barack Obama tarafından siber saldırı ve tehditlerin ulus olarak karşı karşıya kalınan en ciddi ekonomik ve ulusal güvenlik sorunlarından biri olunduğu ve bu saldırılara karşı henüz olması gerektiği kadar hazırlıklı olunmadığı ifade edilmiştir.[80] Dolayısıyla Kello'nun da belirttiği gibi;

---

[76] Michael N. Schmitt, *Tallinn Manual on the International Law…*, s. 106.
[77] Sam Berner, "Cyber-Terrorism: Reality or Paranoia?", *South African Journal of Information Management*, Cilt 5, Sayı 1, Mart 2003, s. 4.
[78] Steve Morgan, "Cyber Crime Costs Projected To Reach $2 Trillion by 2019", (17.01.2016), *https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#479eef553a91*, (Erişim tarihi: 13.08.2020).
[79] Fulya Aslay, "Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi", *International Journal of Multidisciplinary Studies and Innovative Technologies*, Cilt 1, Sayı 1, Kasım 2017, s. 26.
[80] The New York Times, *Text: Obama's Remarks on Cyber-Security,* (29.05.2009), https://www.nytimes.com/2009/05/29/us/politics/29obama.text.html, (Erişim tarihi: 13.08.2020).

devletlerin, çeşitli tehditler ile mücadele edebilmek için saldırı, savunma, strateji ve istihbarat kapasitelerini devamlı geliştirmeleri gerektiği sonucuna varılmaktadır.[81]

Günümüzde, bilişim teknolojilerinin sağlamış olduğu imkanlar sayesinde yüz binlerce siber saldırı aracı bulunmasıyla birlikte, bu sayıya her yıl binlercesi daha eklenmeye devam etmektedir.[82] Siber saldırı araçları içerisinde en çok kullanılanları ise; virüs, kimlik avı saldırısı, truva atı, solucan ve casus yazılımlar oluşturmaktadır. Aon ve Financial Times'ın ortaklaşa hazırladığı C-Suite Siber Risk Raporu'nda, siber saldırı kaynaklı maddi kayıpların 2021 yılı itibarıyla 6 trilyon doları aşarak dünyanın en büyük üçüncü ekonomisi halini alacağı beklentisine ek olarak, 2017-2021 yılları arasında siber güvenliğe yönelik harcamaların ise 1 milyon doları aşacağı belirtilmiştir.[83] Kayda değer büyüklükte finansal hasar potansiyeline sahip olan bu saldırılar, siber güvenlik alanının ne kadar ciddiye alınması gerektiğini tüm yönleriyle gözler önüne serebilmektedir.

Murugesan Uma ve Ganesan Padmavathi, genel olarak siber saldırıları ve tehditlerin türlerini, özelliklerini ve potansiyel etkilerini anlama eksikliği olduğunu ve bu nedenle bilgi güvenliğini sağlamada büyük sorunlarla karşı karşıya kalındığını belirtmektedirler.[84] Dolayısıyla, siber dünyada neler olduğuna dair bireysel düzeyden küresel düzeye kadar dünya çapında bir farkındalık oluşturulmasıyla siber saldırı ve tehditlerin üstesinden gelinebilmesi için adımlar atılabilir. Atılabilecek adımlar arasında; siber saldırılara karşı uluslararası geçerliliği olan yasal çerçevenin oluşturulması, bu anlamda en ağırlıklı katkıyı sağlayabilecek bir adım olarak değerlendirilebilir. Netice itibarıyla, siber saldırı ve tehditlerin dinamik ve asimetrik olarak ifade edebileceğimiz bir yapıya sahip olması nedeniyle gelecek yıllarda devletlere, toplumlara ve özel şirketlere vereceği zararların devam edeceği öngörülmektedir. Bu bağlamda yerel, bölgesel ve küresel düzeyde iş birliği ve yasal

---

[81] Lucas Kello, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", *International Security*, Cilt 38, Sayı 2, Güz 2013, s. 17.
[82] Şeref Sağıroğlu, *a.g.e.*, s. 38.
[83] AON*, Siber Saldırı Kayıplarının Toplam Maliyeti Yıllık 6 Trilyon Dolara Ulaşacak*, (16.03.2020), https://www.aon.com/turkey/tr/about-aon/newsroom-2020/Siber-Saldırı-Kayıplarının-Toplam-Maliyeti-Yıllık, (Erişim tarihi: 10.08.2020).
[84] Murugesan Uma ve Ganapathi Padmavathi, "A Survey On Various Cyber-Attacks And Their Classification", *International Journal of Network Security*, Cilt 15, Sayı 5, Eylül 2013, s. 395.

çerçevenin oturtulması amacıyla birlikte çalışan uluslararası topluma ihtiyaç duyulmaktadır.

1.3.3. Siber İstihbarat ve Siber Casusluk

Uluslararası İlişkiler disiplinindeki çeşitli araştırmacıların tanımlarından yola çıkılarak istihbarat kavramı; devletlerin çıkar ve politikaları çerçevesinde çeşitli koşullara veya durumlara makul bir algı sağlanması ve ilgili yerlere iletilmesi sonucu karar verme sürecine sağladığı veriler ile önemli derecede katkı yapılması olarak ifade edilebilir.[85] Günümüzde, teknolojik sistemlerin ve internet ağlarının kullanımındaki artışla bağlantılı olarak istihbarat yöntemleri siber alan içerisinde etkili olmaya başlamıştır.[86] Siber istihbarat ise; siber organizasyon yapıları, potansiyel siber gücü, ağ sistemi, donanım, yazılım, veri, tehdit, güvenlik açıkları ve benzeri konularda mevcut verilerin toplanması, işlenmesi, analizi, entegrasyonu, değerlendirilmesi ve yorumlanması sürecini kapsamaktadır.[87]

Matthew Hurley'e göre siber istihbarat; stratejik, operasyonel ve taktiksel olmak üzere üç düzeyde gerçekleşmektedir.[88] Stratejik siber istihbarat; operasyondan sorumlu kişiye doğru kararları verebilmesi ve savaş amacına ulaşabilmesi için tüm bilgileri sağlayan, askeri temelli siber operasyonları destekleyen, mevcut siber uzay ortamını değerlendiren ve ulusal siber güvenliğe tehdit oluşturabilecek düşmanların güç ve niyetleri hakkında bilgi toplayan istihbarat olarak tanımlanmaktadır. Operasyonel siber istihbarat; siber uzay içerisindeki stratejik hedeflere ulaşabilmek amacıyla büyük siber operasyonların planlanması ve yürütülmesi için gerekli olan istihbarat olarak ifade edilmiştir. Taktiksel operasyonların angajmanı ve manevrası için gerekli olan istihbarat bütünü ise taktiksel siber istihbarat olarak

---

[85] Sait Yılmaz, *21. Yüzyılda Güvenlik ve İstihbarat*, Milenyum Yayınları, İstanbul 2007, s. 77; Amos Kovacs, "Using Intelligence", *Intelligence and National Security*, Cilt 12, Sayı 4, 1997, ss. 144-145; Emre Çıtak, *Güvenlik ve İstihbarat: Yeni Güvenlik Politikaları Bağlamında Türkiye'de İstihbaratın Dönüşümü*, Yeniyüzyıl Yayınları, İstanbul 2017, s. 62.

[86] Gökhan Bayraktar, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, Yeniyüzyıl Yayınları, İstanbul 2015, s. 53.

[87] Jung ho Eom, "Roles and Responsibilities of Cyber Intelligence for Cyber Operations in Cyberspace", *International Journal of Software Engineering and Its Applications,* Cilt 8, Sayı 9, Ocak 2014, s. 138.

[88] Matthew M. Hurley, "For and from Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance", *Air & Space Power Journal*, Kasım- Aralık 2012, s. 15.

nitelendirilmektedir.[89] Siber istihbaratın en önemli görevlerinin başında, siber alanı kapsayan görevlerin yerine getirilmesini kolaylaştırmak için gerekli verilerin ve bilgilerin istihbari yöntemlerle elde edilmesi gelmektedir.[90] Bir diğer ifadeyle, siber operasyon planlanırken veya düşman bir hedefin altyapısına saldırı düzenlenirken önemli stratejik hedeflere ulaşabilmek için siber yöneticilere veya birimlere gerekli tüm veri ve bilgilerin ulaştırılması hedeflenmektedir.

Bir devletin, başka bir devletin özel bilgilerini ele geçirmek amacıyla casuslarını onun topraklarına göndermesi durumuyla askeri anlamda casusluk ifade edilmektedir.[91] Casusluk; Birleşmiş Milletler Şartı uyarınca bir tehdit veya güç kullanımı olarak görülmemektedir. Bu nedenle bir bakıma, ulus devletlerin askeri gücünü casusluğa karşı nefsi müdafaa olarak kullanamayacağı anlamı doğmaktadır.[92] Buna karşın, yabancı ülkede faaliyet gösteren casusların, o ülkenin toprak bütünlüğünü ihlal ettiği görüşünün uluslararası alanda kabul gören bir anlayış olması sebebiyle çoğu ülkede casusluk, ceza gerektiren bir suç olarak kabul edilmektedir.[93] Bununla birlikte, devletlerin jeopolitik ve ekonomik avantajlar sağlayacak bilgiler elde etmeleri sebebiyle casusluk operasyonlarına ciddi destekler verdiği de belirtilmektedir.[94] Casusluk eylemleri sadece devletler arasında gerçekleşmemekte bununla birlikte, şirketler arasında rakiplerinin ticari sırlarını ele geçirmek ve ekonomik kar elde etmek için casusluk operasyonlarının desteklendiğinden de bahsedilmektedir.[95]

Singer ve Friedman'a göre siber casusluk, devlet kontrolündeki veya yönlendirilmiş siber saldırganların ticari, siyasi ya da askeri kazanç elde etmek amacıyla rakibin hassas bilgilerini çalması durumu olarak tanımlanmaktadır.[96] Bilgi ve iletişim teknolojilerindeki yeniliklerle birlikte çok büyük depolama alanlarına sahip

[89] Matthew M. Hurley, *a.g.m.*, ss. 16-17.
[90] Nezir Akyeşilmen, *a.g.e.*, s. 231.
[91] Hasan Çifci, *a.g.e.*, s. 327.
[92] Anna Wortham, "Should Cyber Exploitation Ever Constitute A Demonstration Of Hostile Intent That May Violate UN Charter Provisions Prohibiting The Threat Or Use Of Force?", *Federal Communications Law Journal*, Cilt 64, Sayı 3, Güz 2012, s. 652.
[93] Herbert S. Lin, "Offensive Cyber Operations and the Use of Force" *Journal Of Natıonal Securıty Law & Polıcy*, Cilt 4, Sayı 63, Ağustos 2010, s. 78.
[94] Janine Kremling ve Amanda M. Sharp Parker, *Cyberspace, Cybersecurity, and Cybercrime*, SAGE Publications, 2017, s. 219.
[95] Janine Kremling ve Amanda M. Sharp Parker, *a.g.e.*, ss. 220-221.
[96] P.W. Singer ve Allan Friedman, *a.g.e.*, ss. 130-131.

cihazların ortaya çıkması, siber casusluk faaliyetlerinin kolaylaşmasının önünü açmışken, bu gelişme bir diğer yönden de verilerin gizliliğinin ve bütünlüğünün ciddi tehdit altında kalmasına sebep olmuştur. Yabancı topraklara casus göndermek zorunda kalınmadan internet üzerinden gerekli tüm veri ve bilgileri ele geçirme imkânı sağlanması sebebiyle siber casusluk, ulus devletler için son yirmi yıl içerisinde oldukça çekici bir nitelik kazanmıştır.[97] Bu durumla bağlantılı olarak 1998-2001 yılları arasında ABD Güvenlik ve Terörle Mücadele Ulusal Koordinatörlük görevini yürüten Richard A. Clarke, geleneksel casusluğa göre Washington'daki bir SSCB Devlet Güvenlik Komitesi (KGB) ajanının ABD Federal Soruşturma Bürosu'ndan (*The Federal Bureau of Investigation,* FBI) veya CIA'den veri çalabilmesinin çok riskli ve uğraş isteyen bir iş olduğunu ancak, günümüzde terabaytlarca büyüklüğünde bilginin düşük risk ile bir gecede çalınabileceğini belirterek siber casusluğun önemine dikkat çekmiştir.[98]

Melnitzky gibi bazı düşünürler tarafından yabancı ülke topraklarında devlet destekli casusluk faaliyeti yürüten kişileri riske atmak zorunda kalmadan daha büyük miktarda bilgiyi gizlice ele geçirme imkânı bulunabilmesi sebebiyle siber casusluğun geleneksel casusluğa göre gizliliğinin daha ön planda olduğu ve daha geniş kapsamlı müdahale gücünün bulunduğu savunulmaktadır.[99] Melnitzky, bu nedenlerden dolayı siber casusluğun bazı durumlarda Birleşmiş Milletler Sözleşmesi'ne göre güç kullanımı ya da silahlı saldırı olarak ele alınması gerektiğini belirtmektedir.[100] Weissbrodt gibi bazı düşünürler ise bu konu üzerine farklı fikirler ortaya koymaktadırlar. Weissbrodt, eğer bir operasyon sonucu sadece bilgi toplanıyorsa, bu durumun siber casusluk faaliyeti kapsamında değerlendirilebileceğini ancak, operasyon sırasında bilgi toplamanın yanı sıra farklı eylemler de gerçekleştiriliyorsa, bu durumun siber saldırı veya güç kullanma olarak görülmesi gerektiğini ifade

---

[97] Richard A. Clarke ve Robert K. Knake, *Cyber War – The Next Threat to National Security and What to Do About It*, HarperCollins, Nisan 2010, s. 123.

[98] James F. Smith, "Richard Clarke on Cyber Threats: Defense is Key", (21.09.2010), *https://www.belfercenter.org/publication/richard-clarke-cyber-threats-defense-key*, (Erişim tarihi: 07.08.2020).

[99] Alexander Melnitzky, "Defending America Against Chinese Cyber Espionage Through The Use Of Active Defenses" *Cardozo Journal of International & Comparative Law*, Cilt 20, Sayı 2, Kış 2012, s. 565.

[100] Alexander Melnitzky, *a.g.m.*, s. 567.

etmektedir.[101] Weissbrodt'un savunmuş olduğu düşünceye karşılık günümüzde bir siber saldırının bile ortaya çıkarılması oldukça zor iken, siber casusluk ile siber saldırı arasında ayrım yapabilmek bazen imkânsız olabilmektedir.

1.3.4. Siber Diplomasi

Diplomasi kavramı, İngiliz Okulu kuramına göre uluslararası politikanın özü olarak görülmekle birlikte uluslararası toplumun tanımlanması ve sürdürülmesinde merkezi bir kurum olduğu ifade edilmektedir.[102] Kuramın en önemli temsilcilerinden Hedley Bull'a göre diplomasi kavramı, uluslararası toplum fikrinin koruyucusu olarak kabul edilmektedir.[103] Amacker'e göre de diplomasi, genellikle devletler tarafından kendi çıkarlarını sağlamak için yürütülen bir araç gibi gözükse de uluslararası sistem içerisinde küresel sorunları ele almak, çok yönlü ticaret akışını sağlamak, savaş ve şiddeti önlemek gibi olumlu yanları da mevcuttur.[104]

Siber diplomasi henüz çok yeni bir kavram olması sebebiyle, literatürde fikir birliğine varılan bir tanımı bulunmamaktadır. Genel kabul görmüş bir tanımının bulunmayışının bir diğer sebebi ise, akademisyenler tarafından "*siber diplomasi*" isminin yanı sıra "*dijital diplomasi*", "*e-diplomasi*", "*Twiplomasi*" gibi çeşitli isimlerle de kullanılıyor olmasından kaynaklanabilmektedir.[105] Manor ve Segev'e göre siber diplomasi kavramı, bir ülkenin dış politika hedeflerine ulaşmak ve itibarını proaktif olarak yönetmek için internet veya modern iletişim teknolojisinin kullanımı olarak tanımlanmaktadır.[106] Siber diplomasinin başlangıç noktasını, 2011 yılında dünya çapında siber sorunların uluslararası yönlerine odaklanan ilk hükümet belgesi olan "ABD Uluslararası Siber Uzay Stratejisi'nin" yayımlanması oluşturmaktadır. Strateji

---

[101] David Weissbrodt, "Cyber-Conflict, Cyber-Crime and Cyber-Espionage", *Mınnesota Journal Of International Law*, Cilt 22, Sayı 2, 2013, s. 372.
[102] Martin Wight, *Systems Of States*, Leicester University Press, Leicester 1979, s. 89.
[103] Hedley Bull, *The Anarchical Society: A Study Of Order in World Politics*, 3. Baskı, Columbia University Press, Ekim 2002, s. 176.
[104] Christopher Amacker, "The Functions of Diplomacy,", (20.07.2011), *http://www.e-ir.info/2011/07/20/the-functions-of-diplomacy/*, (Erişim tarihi: 15.08.2020).
[105] DiploFoundation, *Digital diplomacy, E-diplomacy, Cyber diplomacy*, https://www.diplomacy.edu/e-diplomacy, (Erişim tarihi: 15.08.2020).
[106] Ilan Manor ve Elad Segev, "America's Selfie: How The US Portrays Itself On Its Social Media Accounts", *Digital Diplomacy Theory and Practice*, Derleyen: Corneliu Bjola ve Marcus Holmes, Routledge, New York 2015, s. 91.

içerisinde ağ koruması, hukuksal yaptırım, internet yönetişimi ve internet özgürlüğü gibi birtakım öncelikler tanımlanırken; bu hedefleri gerçekleştirmenin ancak üç sütunlu bir yapı olan diplomasi, savunma ve kalkınma ile mümkün olduğu vurgulanmıştır.[107] Bu stratejiyle birlikte ilk defa siber amaçlar doğrultusunda diplomatik araç ve kaynakların kullanımı konusunda net bir tavır ortaya koyulduğu görülmektedir.

Günümüz Uluslararası İlişkiler aktörleri arasında siber diplomasinin kullanım alanının gitgide artmasının getirdiği bazı avantajlar ve dezavantajlar bulunmaktadır. İlk olarak avantajlı tarafları değerlendirilecek olunursa; siber diplomasinin en dikkat çekici yönlerinden biri çift yönlü ve çok yönlü iletişime katkı sağlayabilmesidir. Sosyal medyanın popülerliğini artırması sonucu diplomatların ve hükümet liderlerinin hem diplomatik ağlarını kolayca genişlettiği hem de etkili stratejik ilişkiler kurmaya başladıkları görülmüştür. Bu konuyla ilgili olarak 2012 yılında Hollanda'nın ABD Büyükelçisi olarak görevini yürüten Rudolf Bekink, dijital arenanın birebir görüşmelerden toplumlarla iletişime kadar birçok alanda yeni olanaklar sağladığını belirtmiştir.[108] Bir diğer yönden, teknolojinin gelişmesiyle birlikte hükümet temsilcilerinin toplantı yapmak için sürekli olarak uçağa binip uzak bir ülkeye gitmek yerine çevrim içi ortamda diyalogların yürütülebilmesine olanak sağlayarak, aynı zamanda finansal ve çevresel maliyetlerden tasarruf edilmesinin önünü açacağı düşünülmektedir.[109] Dolayısıyla, hükümetlerin uluslararası ilişkiler ve dış politika alanındaki çalışmalarını daha hızlı ve daha uygun maliyetler ile yürütmelerine de olanak sağladığı ifade edilebilir.

Siber diplomasi faaliyetlerinin devletlere bazı kolaylıklar sağlaması üzerine oluşan fikir birliğine rağmen, bir dizi zorluğu da beraberinde getirdiği siber alanda diplomatik faaliyetlerin uygulanmasındaki artışla beraber gözlenmiştir. Siber diplomasi alanındaki en büyük olumsuzluklardan biri olarak hükümet yetkililerinin

---

[107] Andre Barrinha ve Thomas Renard, "Cyber-Diplomacy: The Making of an International Society In The Digital Age", *Global Affairs*, Cilt 3, Sayı 4-5, Aralık 2017, s. 359.
[108] Brian Hocking ve Jan Melissen, "Diplomacy in the Digital Age", *Clingendael Institute*, Temmuz 2015, s. 25.
[109] Andre Barrinha ve Thomas Renard, "Power and diplomacy in the post-liberal cyberspace", *International Affairs*, Cilt 96, Sayı 3, 2020, ss. 760-761.

veya diplomatların sosyal medya üzerinden yaptıkları bazı paylaşımlarının yanlış anlaşılabildiği veya provokasyon amaçlı kullanılabildiği görülebilmektedir.[110] Bu nedenle, sosyal medya üzerinden kamuoyuna yapılan bir paylaşımın diplomatik dil kullanımından uzaklaşılması, çeşitli provokatörler veya protestocular aracılığıyla gerçeğinden farklı bir şekilde yansıtıldığı durumlar ile karşı karşıya kalınabilmektedir. Bunun sonucunda, paylaşımı yapan yetkilinin hem mesleki itibarı zedelenebilmekte hem de ufak çaplı diplomatik krizler yaşanabilme olasılığı bulunmaktadır.[111] Siber diplomasi alanındaki bir diğer tehdit ise hesapların saldırıya uğraması veya ele geçirilmesi sonucunda ortaya çıkmaktadır.[112] Hükümet yetkililerinin yürütmüş oldukları gizli diplomatik yazışmaların veya belgelerin ele geçirilmesi sonucu devletlerin ulusal güvenlik stratejileri tehdit altında kalabilmektedir.[113]

1.3.5. Siber Savunma

Siber alanda faaliyet gösteren bilişim teknolojilerinin, internet ağlarının ve bu ağlar ile etkileşime geçen yazılım, donanım ve sistemlerin herhangi bir saldırı veya tehdit eylemine karşı korunması durumu siber savunma olarak tanımlanmaktadır. Bilgi sistemlerinin gizliliğinin ve bütünlüğünün korunması, siber savunma içerisindeki en temel amaçların başında gelmektedir.[114] Siber savunma faaliyeti kapsamında her türlü bilişim teknolojilerinin ve altyapı sistemlerinin zarar görmemesi için saldırıların veya tehditlerin önlenmesine, tespit edilmesine ve zamanında yanıt verilmesine odaklanılmaktadır.[115]

---

[110] Bridget Verrekia, "Digital Diplomacy and Its Effect on International Relations*", Independent Study Project Collection,* Bahar 2017, *https://digitalcollections.sit.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com.tr/&httpsredir=1&article=3619&context=isp_collection*, (Erişim tarihi: 17.08.2020), s. 22.

[111] Emma L. Briant ve Alicia Wanless, "A Digital Ménage à Trois- Strategic Leaks, Propaganda and Journalism", *Countering Online Propaganda and Extremism- The Dark Side of Digital Diplomacy,* Derleyen: Corneliu Bjola ve James Pamment, New York 2019, ss. 49-51.

[112] Olubukola S. Adesina, "Foreign Policy In An Era Of Digital Diplomacy", *Cogent Social Sciences,* Cilt 3, Sayı 1, Mart 2017, s. 11.

[113] Emma L. Briant ve Alicia Wanless, *a.g.e.,* ss. 45-46.

[114] Atalay Keleştemur, *Siber İstihbarat*, Yazın Basın Yayınevi Matbaacılık Trz.Tic.Ltd.Şti, İstanbul 2015, s. 316.

[115] Vahit Güntay, "Uluslararası Sistem ve Güvenlik Açısından Değişen Savaş Kurgusu; Siber Savaş Örneği", *Güvenlik Bilimleri Dergisi*, Cilt 6, Sayı 2, Kasım 2017, s. 92.

Siber uzayda gerçekleştirilen saldırı ve tehditlerin yol açtığı maddi ve manevi zararların gün geçtikçe artış göstermesi; devletlerin, özel şirketlerin, kurumların, kuruluşların ve bireylerin çeşitli savunma sistemlerini uygulamaya geçirmelerini sağlamıştır. Siber savunma sistemleri içerisinde en dikkat çekenler arasında zafiyet tarayıcı, kimlik doğrulama, güvenlik duvarı, saldırı tespit ve önleme, antivirüs, veri kaçağı önleme, ağ erişimi kontrol, içerik filtreleyici, balküpü, şifreleme ve sayısal imza yazılımları bulunmaktadır.[116] Devletler ve uluslararası örgütler, siber saldırı ve tehditlerden en çok zarar gören aktörler olması sebebiyle yukarıdaki yazılımların yanı sıra siber güvenlik stratejilerini de faaliyete geçirmektedirler. Bu stratejiler kapsamında siber savunmanın güçlü bir şekilde sağlanabilmesi, erken tespitin yapılabilmesi ve saldırılara anında müdahale edilebilmesi için çeşitli kurum ve ekipler kurulmaktadır.[117]

Siber saldırıların coğrafi mesafe tanımaksızın saniyeler içerisinde gerçekleştirilebilmesi nedeniyle, bu saldırılar ile mücadele edebilmenin en iyi yollarından birinin siber savunma olduğu düşünülmektedir.[118] Siber alan içerisinde ülkeler teknolojiye ne kadar çok bağımlıysa, saldırılardan etkilenmemek için siber savunmaya o kadar çok yatırım yapması gerekmektedir. Caydırıcı etkiye sahip siber savunma sistem ve kurumlarının faaliyete geçirilmesinin son derece maliyetli olduğu bilinmesine rağmen, saldırıların yol açtığı finansal zarar çoğu zaman açık ara fazla olabilmektedir. Bununla birlikte, gizli kalması gereken verilerin ve bilgilerin saldırganların eline geçmesi sonucu ciddi manevi kayıplar ile karşı karşıya kalındığı görülmektedir. Siber güvenliğin en zayıf halkasının insan olması sebebiyle, siber alan ile etkileşime geçen bir iş ağına sahip çalışanların hem alanlarında uzman kişilerden seçilmeleri hem de güvenlik tehdidi ile karşılaşıldığında ne yapılması gerektiği bilmelerinin siber savunmanın sağlanmasında öncelik alanlarından birini oluşturduğu düşünülmektedir.[119]

---

[116] Hasan Çifci, *a.g.e.*, ss. 226-238.
[117] Mustafa Ünver, Cafer Canbay ve Ayşe Gül Mirzaoğlu, *a.g.e.*, s. 35.
[118] Sico van der Meer, "Defence, Deterrence, and Diplomacy: Foreign Policy Instruments to Increase Future Cybersecurity," *Securing Cyberspace: International and Asian Perspectives*, Derleyen: Cherian Samuel ve Munish Sharma, Pentagon Press, Hindistan 2016, s. 100.
[119] Hasan Çifci, *a.g.e.*, s. 225.

Sonuç olarak, günümüzde siber saldırıların etkisini ve hızlarını giderek artırması sebebiyle, siber savunmanın önemi birkaç yıl öncesine göre büyük ölçüde yükseliş göstermektedir.[120] Siber savunmanın temel özelliği yalnızca acil durumlarda ve kriz durumlarında aktif olması değil, aynı zamanda günlük durumlarda bile tutarlı bir şekilde tespit ve korumayı sürdürebilmesidir. Devletlerin siber savunma altyapısının güçlü olması halinde bir yandan temel hizmetlerin ve toplumsal işlevlerinin engellenmeden sürdürülmesi sağlanırken diğer yandan saldırganın siber saldırılar yoluyla vereceği zararın önüne geçilebilmektedir. Diğer bir ifadeyle, siber savunma gücü; bir devletin saldırılara karşı direncini artırabilmekte, siber saldırı sonrası oluşabilecek olumsuz sonuçları azaltabilmekte ve saldırganın siber uzay yoluyla devleti tehdit etme gücünü sınırlayabilmekte veya ortadan kaldırabilmektedir.[121] Bu doğrultuda devletlerin, ülkenin savunmasını kırabilecek her türlü siber saldırıya direnmek için kendi kapasite ve yeteneklerini geliştirmesi, siber saldırıların yol açtığı maddi ve manevi hasarları azaltmada katkı sağlayabilecektir.

1.3.6. Siber Caydırıcılık

Caydırıcılık kavramı genel olarak; bir aktörün gerçekleştireceği eylem sonrasında elde edeceği faydaların, maliyet ve risklerden daha az olacağına ikna edilip amaçlarından vazgeçirilmesi olarak ifade edilmektedir.[122] Askeri anlamda caydırıcılık ise; askeri güç, yaptırım ve tehditler aracılığıyla düşmanın ağır bedeller ödeyeceğine inandırılarak saldırganlığı önleme veya saldırganı korkutarak uzaklaştırma durumu olarak tanımlanabilmektedir.[123] Bir ülkenin veya bir uluslararası örgütün tehdit değerlendirmesini anlamak, onun stratejik tepkisinin öngörülmesine katkı sağlayabilmekte, bunun yanı sıra etkili bir ulusal strateji geliştirilmesiyle ve caydırıcılık teorisinin uygulanmasıyla bir tehdidin niteliği, kullanılan teknik araçlar ve

---

[120]Neil Robinson, "NATO: Siber Savunmada Vites Değiştiriyor", (08.06.2016), *https://www.nato.int/docu/review/tr/articles/2016/06/08/nato-siber-savunmada-vites-degistiriyor/index.html*, (Erişim tarihi: 15.08.2020).

[121] Dorothy E. Denning, "Framework and principles for active cyber defense", *Computers & Security*, Cilt 40, Şubat 2014, ss. 109-110.

[122] Eric T. Jensen, "Cyber Deterrence", *Emory Internatıonal Law Revıew*, Cilt 26, Mayıs 2012, s. 779.

[123] Mehmet T. Akad, *Modern Savaşın Temel Kavramları*, Kitap Yayınevi, Ankara 2011, s. 98; Richard K. Betts, "The Lost Logic of Deterrence: What the Strategy That Won the Cold War Can-and Can't-Do Now", *Foreign Affairs*, Cilt 92, Sayı 2, Mart/Nisan 2013, s. 87.

potansiyel hedefler merkezi bir rol oynayabilmektedir.[124] 2000'li yıllarda güvenlik araştırmacılarının çoğu tarafından caydırıcılık teorisinin sadece askeri alanla özellikle de nükleer silahlar ile sınırlandırılmasının doğru olmadığı kabul edilmektedir. Yine, birçok araştırmacı ve akademisyen tarafından caydırıcılık teorisinin siber uzaya ne ölçüde uygulanabilir olduğu, siber alan üzerine tartışmaların yürütüldüğü kritik konular arasında yer almaktadır.[125]

Soğuk Savaş döneminde caydırıcılık stratejisi, herhangi bir nükleer saldırının saldırganı yok edecek bir nükleer saldırıyla karşılık verileceği durum olan Karşılıklı Kesin Mahvolma (*Mutual Assured Destruction*, MAD) modelinde önem kazanmıştır. Nükleer caydırıcılık, esas olarak misilleme veya cezaya dayanmakla birlikte nükleer cephaneliğe sahip devletlerin kısıtlanmasına ve silahları geliştirmek için gerekli bilgi ve materyallerin yayılması durumuyla bağlantılık göstermektedir.[126] Konuyla ilgili çalışmalar yürüten bilim insanları arasında, aynı teorik çerçevenin siber uzaya uygulanabilirliği konusunda çalışmalar yapanlar bulunmaktadır. Joseph S. Nye'ın da çalışmalar yürüttüğü birçok akademisyen, siber uzay için bir silah kontrol çerçevesi dahi önermişlerdir.[127] Buna rağmen; araştırmacıların çoğu, nükleer caydırıcılığı yarım yüzyıldan fazla bir süredir etkili kılan ilkelerin siber uzayda uygulanabilirliğinin neredeyse imkânsız olduğunu ileri sürmüşlerdir.[128] Siber saldırıları faillerine atfetmenin zorluğu, siber saldırıların asimetrik yapıda olması, siber alanda uluslararası normların oturmamış olması, siber silah edinme ve siber saldırı gerçekleştirmenin kolaylığı gibi unsurlar nedeniyle caydırıcılığın uygulanması yönünde belirli sınırlamalar ortaya çıkmaktadır. [129]

---

[124] Amir Lupovici, "Cyber Warfare and Deterrence: Trends and Challenges in Research", *Military and Strategic Affairs*, Cilt 3, Sayı 3, Aralık 2011, ss. 50-51.
[125] Annegret Bendiek ve Tobias Metzger, "Deterrence Theory in the Cyber-Century," Working Paper RD EU/Europe, *German Institute for International and Security Affairs*, Mayıs 2015, ss. 4-5.
[126] Dorothy E. Denning, "Rethinking the Cyber Domain and Deterrence," *Joint Forces Quarterly 77*, Bahar 2015, s. 11.
[127] Joseph S. Nye, "The World Needs New Norms On Cyber-Warfare," (01.10.2015), *https://www.washingtonpost.com/opinions/the-world-needs-an-arms-control-treaty-for-cybersecurity/2015/10/01/20c3e970-66dd-11e5-9223-70cb36460919_story.html*, (Erişim tarihi: 15.08.2020).
[128] David Elliott, "Deterring Strategic Cyberattack," *IEEE Security & Privacy*, Cilt 9, Sayı 5, Eylül/Ekim 2011, s. 37.
[129] Martin C. Libicki, *Cyberdeterrence and Cyberwar*, RAND Corporation, Kasım 2009, ss. 41-42; Emilio Iasiello, "Is Cyber Deterrence an Illusory Course of Action?" *Journal of Strategic Security*, Cilt *7*, Sayı 1, Bahar 2014, ss. 64-66.

Siber uzaydaki faaliyetlerin hem devletler hem de organize suç örgütleri, siyasi düşmanlar, bilgisayar korsanları ve bireyler gibi çok fazla sayıdaki aktör tarafından gerçekleştirilebiliyor olması ve de siber saldırı yapmanın maliyetsiz ve kolay olması nedeniyle misillemenin bir caydırıcılık durumu oluşturacağı düşünülmemektedir.[130] Bunun yanı sıra, misillemenin gerçekleşebilmesi için saldırganın bir devlet aktörü veya bir devlet adına hareket ediyor olması önemli bir kıstası temsil etmektedir. Aynı zamanda, yanlış bir aktöre karşı yapılan misilleme sonucu siber alanda başlayan bir anlaşmazlık durumunun, muhtemelen ciddi sonuçlarla gerçek dünyaya yayılmasına yol açılabilecektir.[131] Bu nedenle kimliği belirleme, saldırıyı gerçekleştiren aktöre atfedebilmek ve saldırının başlatıldığı doğru kaynağa karşı uygun şekilde yanıt verebilmek amacıyla gereklilik taşımaktadır.

Nükleer caydırıcılık ilkelerinin uygulanmasının oldukça zor olması, siber caydırıcılığın hiçbir zaman başarılı olamayacağı anlamına gelmemektedir. Devletlerin, siber uzay kapsamında belirleyecekleri yeni ilkeler dahilinde caydırıcılık gerçekleştirebilme ihtimalleri bulunmaktadır. Etkili bir siber caydırıcılık, devletin gücünü kullanma isteğiyle birlikte, potansiyel bir saldırganın da hem bu gücün farkındalığına hem de bu gücün kullanılacağına yönelik inancına bağlı olabilmektedir.[132] Yüksek bir siber saldırı gücüne sahip olunmasının yanı sıra teknolojik yenilikler ile donatılmış siber savunma sistemi de saldırganların caydırılabilmesi amacıyla kullanılabilmektedir.[133] Buradan hareketle saldırgana, gerçekleştireceği eylem boşa çaba olarak hissettirilip amaçlarından vazgeçirilerek caydırıcılık eyleminde başarı sağlanabileceği düşünülebilir.

Saldırı ve savunma yeteneklerinin yanı sıra siber saldırganlığa karşı yöntemleri ele alan güçlü bir uluslararası yasal çerçeve, caydırıcılığa yönelik kapsamlı bir yaklaşımın en kritik bileşenleri arasında görülmektedir. Siber alandaki uluslararası hukuk ve normlar, uluslararası işlemlerin yürütülmesi için ortak standartların benimsenmesiyle birlikte devletleri belirli davranış türlerine teşvik etme veya

[130] Şirin Duygulu, *a.g.e.*, ss. 84-85.
[131] Martin C. Libicki, *a.g.e.*, s. 44.
[132] Fred Schreier, *a.g.m.*, s. 78.
[133] Christopher Haley, "A Theory of Cyber Deterrence" *Georgetown Journal of International Affairs*. (06.02.2013), https://www.georgetownjournalofinternationalaffairs.org/online-edition/a-theory-of-cyber-deterrence-christopher-haley, (Erişim tarihi: 16.08.2020).

yasaklama konusunda ortak çıkarların paylaşılmasını sağlaması sebebiyle caydırıcılığın sağlanmasındaki anahtar unsurlardan biri olarak kabul edilmektedir.[134] Çok taraflı antlaşmalar ve iş birliği, bu ortak çıkarları gerçekleştirmenin en etkili yolunu oluşturmakta ve böylelikle siber alanda kuralları ihlal edenlerin belirli davranış normlarını dikkate alması için uyarı veya ceza yöntemleriyle caydırıcılık yürütülebilmektedir.[135]

[134] Charles W. Freeman, *Arts of Power: Statecraft and Diplomacy*, United States Institute of Peace, Ocak 2016, s. 84.
[135] Charles W. Freeman, *a.g.e.*, s. 85.

İKİNCİ BÖLÜM

2. DEĞİŞEN GÜVENLİK ANLAYIŞI PERSPEKTİFİNDE NATO'NUN GÜVENLİK ANLAYIŞI

Güvenlik, Uluslararası İlişkiler ve Siyaset Bilimi disiplini içerisindeki temel kavramlardan biri olarak yer alan çok yönlü, çok boyutlu ve türetilmiş bir kavram olarak kabul edilmektedir. Tarihsel olarak güvenlik, insanoğlunun ilk ortaya çıktığı zamandan günümüze kadar söz konusu olan en hayati ihtiyaçlardan biri olarak kabul edilmektedir. Bir başka deyişle, ilk çağlardan beri insan doğasının rasyonel seçim arayışları içerisinde merkezi bir konumda yer almıştır. Soğuk Savaş dönemi geleneksel güvenlik anlayışında devlet, yani bir bakıma referans nesnesi, güvence altına alınması gereken en önemli unsur olarak görülmüş ve güvenlik arayışının askeri güç yoluyla sağlanabileceği vurgulanmıştır. Soğuk Savaş dönemi boyunca geleneksel anlayışın temelini oluşturduğu güvenlik gündemi, Soğuk Savaş'ın etkisini yitirmeye başlamasıyla birlikte dönüşüme uğramış ve güvenliğin tanımı ve öznesi gibi yaklaşımların etkisi de konu çeşitliliği içeresinde hissedilmeye başlanmıştır.[136] 11 Eylül Saldırıları sonrası derinleşen ve genişleyen güvenlik gündeminde ön plana çıkan küresel terörizm, teknolojik güvenlik, iklim değişikliği ve uluslararası göç gibi yeni tehdit tanımlamalarına karşı devletler, bir yandan ulusal güvenliklerini koruyabilmenin yollarını ararlarken diğer yandan bireysel hak ve özgürlüklerin çiğnenmesine neden oldukları görülmüştür. Bu bağlamda, kişilerin doğduğu ülkeye, dini inancına, toplumsal ve ekonomik altyapılarına, ten rengine ve dış görünüşüne göre tehdit olarak nitelendirilmesiyle karşı karşıya kalınmıştır.[137]

4 Nisan 1949 tarihinde resmi olarak kuruluşu ilan edilen NATO, Soğuk Savaş dönemi güvenlik gündeminde SSCB yayılmacılığının caydırılması; kıtada güçlü bir ABD varlığı yoluyla Avrupa'da milliyetçi militarizmin canlanmasının önlenmesi ve

---

[136] Muzaffer Ercan Yılmaz, "Westphalia'dan Günümüze Savaş", *Uluslararası İlişkilerde Çatışmadan Güvenliğe*, Derleyen: Mustafa Aydın, Hans Günter Brauch, Mitat Çelikpala, Ursula Oswald Spring ve Necati Polat, İstanbul Bilgi Üniversitesi Yayınları, İstanbul 2012, ss. 83-84.

[137] Richard Falk, "Terör ve Devlet Terörizmi", *Uluslararası İlişkilerde Çatışmadan Güvenliğe*, Derleyen: Mustafa Aydın, Hans Günter Brauch, Mitat Çelikpala, Ursula Oswald Spring ve Necati Polat, İstanbul Bilgi Üniversitesi Yayınları, İstanbul 2012, ss. 91-92.

Avrupa'nın siyasi ve askeri entegrasyonunun teşvik edilmesi üzerine üç hedefi yerine getirmek için daha geniş bir çabada önemli rol üstlenmiştir.[138] SSCB'nin dağılması beraberinde Soğuk Savaş'ın sona ermesi sonucunda, NATO'nun varlığı örgüt içerisinde belirli bir kesim tarafından sorgulanmış olmasına rağmen sona ermemiş, sürekli gelişen asimetrik tehditlerin etkisini artırmasıyla birlikte İttifak'ın güvenlik anlayışında dönüşüme gidilerek yeni jeopolitik koşullara adapte olunmaya çalışılmıştır.[139]

2.1. Güvenliğin Tanımı ve Dönüşümü

İnsanoğlu, tarih boyunca öncelikli olarak diğer insanlar olmak üzere canlılar ve doğa olayları gibi hem kendisine hem de yakınlarına karşı risk ve tehdit oluşturabilecek her türlü tehlikelere karşı önlem alma gereksinimi duymuştur. Nitekim, Abraham Harold Maslow'un ihtiyaçlar hiyerarşisi teorisinde insanoğlunun yeme, içme ve barınma gibi başlıca ihtiyaçlarından sonra güvenlik ihtiyacı gelmektedir.[140] Tehdit algısına karşı güvenlik arayışı, tarihsel süreç içerisinde devletlerin inşa edilmesinde temel öncelik olmuş ve güvenliğe bağlı olarak devletler, sınırlarını diğer devletlerin saldırı ve tehditlerinden korumaya çalışarak varlıklarını sürdürmeye çalışmışlardır. Aynı zamanda bu süreç içerisinde güvenlik anlayışı; siyasi, ekonomik, toplumsal ve teknolojik değişimler yaşayarak farklı güvenlik anlayışlarının da ortaya çıkmasına sebep olmuştur.[141]

Günümüzde, güvenliğin kesin tanımı üzerine araştırmacılar arasında hararetli tartışmalar devam etmektedir. Tartışmaların arka planında, referans nesnesinin ana odağının bireysel, ulusal veya uluslararası güvenlik üzerinde olup olmadığı konusunda

---

[138] Tarık Oğuzlu, "NATO's Transformation into a Global Actor in the Age of Great Power Politics", *Perceptions: Journal of International Affairs*, Cilt 26, Sayı 1, Bahar-Yaz 2021, s. 5.

[139] NATO, *The Alliance's New Strategic Concept*, (26.08.2010), https://www.nato.int/cps/en/natohq/official_texts_23847.htm?&utm_source=twitter&utm_medium=smcweb&utm_campaign=23847, (Erişim tarihi: 29.08.2020).

[140] Abraham Maslow, "A Theory of Human Motivation", *Psychological Review*, Cilt 50, Sayı 4, 1943, s. 380.

[141] Barry Buzan ve Lene Hansen, *The Evolution of International Security Studies*. Cambridge University Press, New York 2009, ss. 188-189.

büyük bir anlaşmazlık bulunması yatmaktadır.[142] Türk Dil Kurumu'na (TDK) göre kelime anlamı olarak güvenlik; "*toplum yaşamında yasal düzenin aksamadan yürütülmesi, kişilerin korkusuzca yaşayabilmesi durumu, emniyet*"[143] olarak ifade edilmektedir. Güvenlik kavramı, Uluslararası İlişkiler disiplini içerisinde ilk kez Arnold Wolfers tarafından 1952 yılında yayımlanan "*National Security as an Ambigious Symbol*" adlı çalışma ile ele alınmıştır. Bu çalışma içerisinde Wolfers, güvenliği hem nesnel açıdan hem de öznel açıdan tanımlama gereksinimi duymuştur. Wolfers'e göre güvenlik; sahip olunan değerlere yönelik herhangi tehdit durumunun ve bu değerlerin bir saldırı altında olacağı endişesinin bulunmayışı hali olarak nitelendirilmektedir.[144]

Richard Ullman ise güvenliği, tehditler ile bağdaştırarak tanımlamaya çalışmıştır. Bir devletin ulusal güvenliğine yönelik tehditlerin, o devletin içerisinde yaşayan insanların yaşam düzeylerini düşüreceğini ve hükümet ile hükümet dışı kuruluşların karar alma süreçleri üzerinde olumsuz etki oluşturacağını belirtmektedir. Aynı zamanda, güvenliğin değerinin kaybedilince veya tehdit edilince anlaşılacağına vurgu yapmaktadır.[145] Uluslararası İlişkiler disiplininde Realizm akımının öncü temsilcilerinden olan Edward H. Carr, devletlerin en önemli amacının güç toplayarak güvenliklerini sağlamak olması gerektiğini ifade etmektedir.[146] Ken Booth, devlet güvenliğinin yerine birey güvenliğinin sağlanarak güvenlik durumunun sürdürülebileceğini ve bireylerin güvenliklerinin özgürlükle bağlantılı olduğu çıkarımını yapmıştır.[147]

Kolodziej ise güvenlik kavramının, duygularla ve derin değerlerle yüklü oldukça karmaşık ve tartışmalı olduğunu belirtmiştir. Bu bağlamda; bir kişi, çete, grup ya da devlet bir başkasının hayatına, geçmişine ya da geçim kaynağına tehdit

---

[142] John Baylis, "International and Global Security in the Post-Cold War Era,", *The Globalization of World Politics: An Introduction to IR*, Derleyen: John Baylis ve Steve Smith, Oxford University Press, Oxford 2001, s. 262.
[143] Türk Dil Kurumu, *Türkçe sözlük,* 11.Baskı, Türk Dil Kurumu Yayınları, Ankara 2011, s. 1013.
[144] Arnold Wolfers, "National Security: As An Ambiguous Symbol", *Political Science Quarterly*, Cilt 67, Sayı 4, Aralık 1952, ss. 484-485.
[145] Richard H. Ullman, "Redefining Security", *International Security*, Cilt 8, Sayı 1, Yaz 1983, s. 133.
[146] Edward Hallet Carr, *The Twenty Years' Crisis 1919-1939: An Introduction to the Study of International Relations*, Macmillan & Co. Ltd, Londra 1946, s. 105.
[147] Ken Booth, *Theory of World Security*, Cambridge University Press, Cambridge 2007, ss. 2-3.

oluşturduğu vakit güvenlik sorunlarının ortaya çıkmaya başlayacağını ifade etmiştir.[148] Barry Buzan'a göre güvenlik, devletlerin ve toplumların egemen kimliklerini ve işlevsel bütünlüklerini yerine getirme kabiliyeti olarak tanımlanmaktadır.[149] Buzan, güvenlik kavramının sevgi, özgürlük ve güç kavramları gibi münakaşaya açık ve muğlak bir anlamının bulunması sebebiyle kesin bir tanım üzerinde fikir birliğine varabilmenin oldukça zor olduğu üzerinde durmuştur.[150] Buzan'ın aksine David Allen Baldwin ise güvenliğe yönelik; kim için, hangi değerler için, hangi tehditlere karşı, ne pahasına ve hangi zaman dilimi içerisinde soruları sorularak anlam çerçevesinin netleştirilebileceğini belirtmiştir.[151]

Yukarıda ifade edilen tanımlamalardan hareketle güvenlik kavramının; tarih boyunca herkes için, her yerde ve her zaman aynı durumu ifade etmemiş olduğu değerlendirilebilir. Bu nedenden dolayıdır ki kapsamlı ve sabit bir güvenlik anlayışından söz etmek mümkün görünmemektedir.[152] Ancak, güvenlik kavramı için genel bir tanım yapıldığında, güvenliği; birey, toplum veya devlet gibi herhangi bir referans nesnesinin yapısına, bekasına ve değerlerine yönelik tehdit, korku ve tehlikelerden uzak olma ve onlardan korunuyor olma durumu olarak ifade etmek mümkündür.[153]

Devletlerin geleneksel olarak anarşik uluslararası sistemdeki değerlerine ve bağımsızlıklarına yönelik karşı karşıya kaldığı birçok tehdit ve risk unsuru nedeniyle, güvenlik kavramı uzun zamandır Uluslararası İlişkiler disiplininde önemli bir kavram olarak yer almaktadır. Bu bağlamda güvenliğin, özellikle 1648 Vestfalya Antlaşması ile uluslararası sistemin temel aktörlerinden biri olarak kabul edilen devletlerin en önemli gündem maddeleri arasına girmeye başladığı görülmektedir.[154] İkinci Dünya

---

[148] Edward A. Kolodziej, *Security and International Relations*, Cambridge University Press, Cambridge 2005, s. 1.
[149] John Baylis, *a.g.m.*, p. 194.
[150] Barry Buzan, *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, ECPR Press, Londra 2009, s. 7.
[151] David Allen Baldwin, "The Concept of Security", *Review of International Studies*, Cilt 23 Sayı 1, Ocak 1997, ss. 13-17.
[152] Emre Çıtak, *a.g.e.*, s. 55.
[153] Emre Çıtak, *a.g.e.*, s. 19.
[154] Murat Yorulmaz, "Değişen Uluslararası Güvenlik Algılamaları Bağlamında Türkiye-Yunanistan İlişkilerinde 'Değişmeyen' Güvenlik Paradoksu", *Balkan Araştırma Enstitüsü Dergisi*, Cilt 3, Sayı 1, Edirne 2014, s. 108.

Savaşı'nın sona ermesi ile güvenlik kavramının kullanımının yaygın hale geldiği ve ülkelerin siyasi rejimleri içinde kurumsallaşmaya başladığı dikkat çekmiş, Soğuk Savaş olarak adlandırılan bu dönemdeki güvenlik politikaları, geleneksel güvenlik anlayışı temelinde ele alınmıştır.[155] Bu anlayış çerçevesinde devlet, mutlak bir bütün olarak düşünülmüş ve tehditlerin kaynağının statükodan memnun olmayan revizyonist devletler başta olmak üzere diğer devletler tarafından ortaya konduğu vurgulanmıştır.[156] Dönemin en temel özelliği güvenlik anlayışının devlet ile sınırlandırılması ve bunu sağlamak için askeri gücün ve caydırıcılığın ön plana çıkarılmasıdır.[157] Genel hatlarıyla Soğuk Savaş döneminin iki kutuplu yapısı incelendiği zaman temel güvenlik endişesi olarak devletlerin bekasının görüldüğü, uluslararası sistemin anarşik olarak değerlendirilmesi sonucu devletler arasında silahlanma ve caydırıcılık stratejilerinin ön planda yer aldığı dikkat çekmektedir.[158] Dönemin iki süper gücü olan ABD ve SSCB arasındaki rekabet durumu ve karşılıklı tehdit algılamaları askeri-siyasi bağlamda şekillenmiş, her iki taraf da askeri gücünü sürekli artırarak karşı tarafa caydırıcılık oluşturmaya ve güvenliklerini sağlamaya çalışmışlardır.

ABD ve SSCB arasındaki Soğuk Savaş rekabetinin yumuşamasına dayanarak askeri tehditlerin eski önemini kaybetmesi ile ekonomik, toplumsal ve çevresel güvenlik tehditleri de 1980'li yıllarda daha çok gün yüzüne çıkmaya başlamıştır.[159] 1990'lı yıllarda hem Soğuk Savaş'ın sona ermesi hem de küreselleşme olgusunun etkisini oldukça hissettirmeye başlaması sonucu insanların refahına, mutluluğuna ve onuruna verilen değer artışı, aynı zamanda güvenlik disiplininin genişleme ve derinleşme boyutlarında mihenk taşı oluşturmuştur. Bunun sonucunda insan hak ve özgürlüklerini temel alan, aynı zamanda ekonomik, sosyal, kültürel, siyasi ve çevresel yapıyı da içeren çok boyutlu bir güvenlik anlayışı doğmuştur.[160] Küreselleşmeyle

---

[155] Pınar Bilgin, "Güvenlik Çalışmalarında Yeni Açılımlar: Yeni Güvenlik Çalışmaları", *SAREM Stratejik Araştırmalar Dergisi*, Cilt 8, Sayı 14, Ocak 2010, ss. 76-78.
[156] Jeffrey W. Taliaferro, "Security seeking under anarchy: Defensive realism revisited", *International Security*, Cilt 25, Sayı 3, Kış 2001, ss. 128-129.
[157] Arnold Wolfers, *a.g.m.*, s. 484.
[158] Bradley S. Klein, *Strategic Studies and World Order: The Global Politics of Deterrence*, Cambridge University Press, Mayıs 1994, ss. 33-34.
[159] Keith Krause ve Michael C. Williams, "Broadening the Agenda of Security Studies: Politics and Methods", *Mershon International Studies Review*, Cilt 40, Sayı 2, Ekim 1996, s. 233.
[160] Barry Buzan ve Lene Hansen, *a.g.e.*, ss. 188-190.

beraber sivil toplum kuruluşları, çok uluslu şirketler, organize suç örgütleri gibi devlet dışı aktörler uluslararası sistemde ön plana çıkmaya başlamış, tehdit kaynakları ve bunlara karşı alınabilecek önlemler de çeşitlenmiştir.[161]

ABD'yi hedef alan 11 Eylül 2001 tarihindeki terör saldırıları sonucu uluslararası sistem üzerinde, birey temelli güvenlik anlayışının önem düzeyinde nispeten azalma olmuş, askeri gücün ön plana çıktığı bir anlayış tekrardan hakimiyet kazanmaya başlamıştır. Bu bağlamda, küresel terörizm, istihbarat, teknolojik güvenlik, iklim değişikliği, uluslararası göç ve mülteci gibi kavramların uluslararası sisteme entegre olduğu görülmüştür. Buna ek olarak, güvenliği sağlamak için insanların hak ve özgürlüklerinde sınırlandırılmaya gidilmesi gerektiğini savunan bir anlayışın da tekrardan tartışıldığı dikkat çekmektedir. Bu dönemde, güvenliğe yönelik tehditler zaman ve mekandan bağımsız bir biçimde devlet dışı aktörlerden gelmeye başlamıştır.[162] Bir başka ifade ile, 11 Eylül Saldırılarıyla paralel olarak asimetrik tehdit kavramının uluslararası sistem içerisinde yer almaya başladığı baskın bir şekilde görülebilmektedir.

Yukarıdaki bölümlerde kısaca bahsedildiği üzere güvenlik kavramının Uluslararası İlişkiler disiplininin gündemine girmesi itibarıyla dönüşüm yaşamasında Soğuk Savaş dönemi, Soğuk Savaş sonrası dönem ve 11 Eylül Saldırıları sonrası dönem etkili olmuştur. Çalışmanın devam eden bölümünde bu dönemlerde etkili olan güvenlik anlayışları daha detaylı olarak incelenecektir.

2.1.1. Soğuk Savaş Dönemi Geleneksel Güvenlik Anlayışı

İkinci Dünya Savaşı'nın son bulmasının ardından başlayan Soğuk Savaş dönemiyle, geleneksel güvenlik anlayışı olarak nitelendirilen bir güvenlik anlayışı ortaya çıkmaya başlamıştır. Soğuk Savaş dönemi boyunca ABD ve SSCB liderliğindeki Doğu ve Batı blokları arasındaki güç mücadeleleri ve kısmi çatışma durumları geleneksel güvenlik anlayışı temelinde değerlendirilmiş, çift kutuplu

[161] Ersel Aydınlı, "Küreselleşme ve Güvenlik: Teorik Yaklaşımlar", *Avrasya Dosyası*, Güvenlik Bilimleri Özel, Cilt 9, Sayı 2, 2003, s. 43.
[162] Nihal Ergül, "Yeni Güvenlik Anlayışı Kapsamında Birleşmiş Milletlerin Rolü ve Uygulamaları" *Teoriler Işığında Güvenlik, Savaş, Barış ve Çatışma Çözümleri*, Derleyen: Atilla Sandıklı, Bilgesam Yayınları, İstanbul 2012, s. 181.

uluslararası sistemde geleneksel güvenlik anlayışı temelinde realizm ve neo-realizm teorileri ön plana çıkmıştır.[163] Realizm, Uluslararası İlişkiler disiplininin başlangıcından bu yana en önemli teorilerden biri olarak kabul edilmektedir. Realistlere göre ulus devletler, uluslararası politikanın ana aktörü olarak kabul görmesinin yanı sıra güvenliğin tek referans nesnesi olarak değerlendirilmekte ve mutlak egemenlik kavramı özellikle vurgulanmaktadır. Aynı zamanda, devlet güvenliğinin sağlanmasında askeri güvenlik ve politik güvenlik kavramları ön plana çıkmıştır. Bu anlayış, devletin güvende olması halinde içinde yaşayan bireylerin de güvende olacağı varsayımına dayanmaktadır.[164] Thomas Hobbes, Niccolo Machiavelli ve Jean-Jacques Rousseau gibi realist anlayışın önemli düşünürlerine göre uluslararası sistem, devletlerin çeşitli tehditler pahasına kendi güvenliğini sağlamaya çalışacakları acımasız bir alan olarak tanımlanmaktadır.[165]

İkinci Dünya Savaşı'ndan sonra, Hans Morgenthau ve Edward H. Carr gibi realist anlayışın düşünürleri ile Kenneth Waltz ve John Mearsheirmer gibi neo-realist anlayışının önemli bilim insanlarının, uluslararası sistem hakkında oldukça kötümser değerlendirmeler paylaştıkları görülmektedir.[166] Bu bağlamda, uluslararası sistemin anarşik bir yapıya sahip olduğu ve bu nedenle merkezi hükümet ve devlet davranışlarını yönetebilecek, anlaşmazlıkları çözebilecek veya yaptırım uygulayabilecek hiçbir üst düzey otorite bulunmadığı düşüncesi, Teori kapsamında vurgulanan temel noktalar olarak ön plana çıkarılmıştır. Dönemin hâkim olan realist anlayışı çerçevesinde devletler arasında sürekli bir savaş ve çatışma halinin yaşanması sebebiyle her devletin, ulusunu korumak ve varlığını devam ettirebilmek için kendi başının çaresine bakma ilkesi öncelikli olarak vurgulanmıştır.[167] Buna ilaveten realist yaklaşımda, uluslararası sistemin anarşik yapısından kaynaklı olarak devletlerin, karşılıklı yanlış anlaşılmalar nedeniyle güven eksikliğine ve birbirlerinden korkmaya

---

[163] John Baylis, "The Concept of Security in International Relations", *Globalization and environmental challenges*, Derleyen: Hans Günter Brauch vd., Springer, New York 2008, ss. 497-498.
[164] Ali Balcı ve Tuncay Kardaş, "Realizm", *Uluslararası İlişkilere Giriş,* Derleyen: Şaban Kardaş ve Ali Balcı, Küre Yayınları, İstanbul 2014, s. 122.
[165] John Baylis, *a.g.m.,* s. 266.
[166] Güngör Şahin, *Küresel Güvenlik ve NATO- Teori.Aktör,Tehdit.Risk*, Detay Yayıncılık, Ankara 2016, ss. 48-53.
[167] Sibel Turan, Nergiz Özkural Köroğlu ve İlker Aral Güngör, "Kuramsal Çerçeve: Uluslararası İlişkilerde Güvenlik", *Uluslararası İlişkilerde Güvenlik Kuramları ve Sorunlarına Temel Yaklaşımlar,* Derleyen: Sibel Turan ve Nergiz Özkural Köroğlu, Transnational Press London, Londra 2017, s. 11.

eğilimli olmaları sebebiyle devlet güvenliğinin en önemli öncelik halini almış olduğu ifade edilmiştir.[168] Burada, anarşi kavramı ile herkese karşı bir savaş veya tam bir düzensizlik ve iş birliği eksikliği ya da uluslararası sistemde norm ve kuralların olmaması durumu ifade edilmemektedir. Anarşi kavramı ile; uluslararası sistem içerisinde devletlerin niyet ve hedeflerini kontrol edebilecek devletler üstü bir otoritenin olmaması durumu nitelendirilmektedir.[169]

Geleneksel güvenlik anlayışı temelinde devletin bekasına yönelik en büyük tehlike oluşturacak unsur olarak askeri tehditler görülmüş, bu nedenle askeri olmayan tehditler güvenlik sorunu kapsamı dışında değerlendirilmiştir.[170] Uluslararası sistem içerisindeki tüm egemen devletlerin, güç dengesini sürdürebilmek amacıyla askeri harcamalarını artırarak güvenliğin sağlanması, askeri üstünlüğün elde edilmesi, kendi güvenlik durumlarının iyileştirilmesi ve caydırıcılığın sağlanması gerekliliği çerçevesinde hareket etmeleri özellikle vurgulanmıştır.[171] Geleneksel güvenlik anlayışına göre, uluslararası sistem içerisindeki devletlerin birbirine karşı güven bağı bulunmadığı için herhangi bir risk durumunda dahi iş birliğine gitmeleri oldukça zor görülebilmekte, güç artırımına gidildiği durumlarda ise güvenlik ikilemi ile karşı karşıya kalınabilmektedir. Dolayısıyla, herhangi bir askeri saldırı durumunda iş birliği yapılan devletin yardıma gelmesine kesin gözüyle bakılmamaktadır.[172] Devletler için öncelikli olan hedef maksimum güvenliğe erişmek olduğundan, kendilerine yönelik tehditleri bertaraf edebilecek stratejiler geliştirmeye çalışmaktadırlar.[173] Hobbes, ülke sınırları içerisindeki vatandaşların yaşamlarını ancak devletin bekasının sağlanması ile

---

[168] Kenneth N. Waltz, *Theory of International Politics,* Addison-Wesley Publishing Company, New York 1979, s. 125; John J. Mearsheimer, "A Realist Reply", *International Security*, Cilt 20, Sayı 1, Temmuz 1995, s. 84.

[169] Haluk Özdemir, "11 Eylül: Post-Modern Savaşın Miladı Ya Da Dış Politika Mücadelelerinin Görünmeyen Boyutu", *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,* Cilt 7, Sayı 1, Isparta 2002, s. 155.

[170] Ömer Urhal ve Ünal Acar, *Devlet-Güvenlik-İstihbarat-Terörizm*, 1. Baskı, Adalet Yayınları, Ankara 2007, s. 70.

[171] Oktay F. Tanrısever, "Güvenlik", *Devlet ve Ötesi*, Derleyen: Atila Eralp, 8. Baskı, İletişim Yayınları, İstanbul 2014, s. 109.

[172] Kenneth N. Waltz, "Anarchic Orders and Balances of Power", *Neorealism and Its Critics,* Derleyen: Robert O. Keohane, Columbia University Press, New York 1986, ss. 100-101.

[173] Tarık Oğuzlu, "Dünya Düzenleri ve Güvenlik:Ulus-Devlet Güvenlik Anlayışı Aşılıyor mu?", *Güvenlik Stratejileri Dergisi*, Cilt 3, Sayı 6, Ocak 2007, s. 6.

sürdürebileceklerini, aksi taktirde vatandaşların yaşamının kısa ve sefalet içinde olacağını ifade etmiştir.[174]

Soğuk Savaş dönemi boyunca ABD ve SSCB arasındaki güç mücadelesi çerçevesinde, dönemin güvenlik anlayışı devlet eksenli ele alınmış ve askeri tehdit temelli bir yaklaşım izlenmiştir.[175] Bu çerçevede, ülke sınırlarının dış tehditlere karşı korunması yalnız sert güvenlik önlemleri ile sağlanabilmiş ve ulusun ekonomik refahı da önemli bir unsur olarak kabul edilmiştir.[176] Dönemin iki başat aktörü olan ABD ve SSCB, sürekli konvansiyonel ve nükleer güç maksimizasyonuna giderek caydırıcılık sağlamaya ve ulusal güvenliğini korumaya çalışmaları sonucunda bir bakıma güvenlik ikileminin oluştuğu görülebilmektedir. Dış askeri tehditlere karşı devlet bekasının savunulması, ABD ve SSCB güvenlik politikalarının ana odağı haline gelmiştir.[177] ABD ve SSCB arasındaki mücadele dönemi boyunca askeri ve siyasi dengenin korunması amacıyla birçok güvenlik politikaları geliştirilmiştir.[178] İki süper güç, birbirlerine karşı askeri saldırıda bulunmasa dahi yerel çatışmalar, bölgesel karışıklıklar ve çeşitli propagandalar yürüterek gerginliklere sebep olmuşlardır. Her iki blok da kendi ideolojik yapısını dayatmak amacıyla diğer devletlerin içişlerine müdahale etme eğiliminde dış politikalar yürütmüştür. Sonuç olarak, ABD'nin ve SSCB'nin temel güvenlik politikası dahilinde askeri güvenliği sağlamak ve caydırıcılık oluşturabilmek amacıyla NATO ve Varşova Paktı (*The Warsaw Pact*, WP) gibi uluslararası örgütlerin kuruluşunda başat rol oynadıkları görülmektedir.[179] Uluslararası sistem içerisinde çoğu devletin, bu iki kolektif savunma örgütünden birine üye olması ve askeri kapasite artırımına gitmesi, geleneksel güvenlik anlayışının bir sonucunu oluşturmuştur.

---

[174] Thomas Hobbes, *Leviathan*, Çeviren: Semih Lim, Yapı Kredi Yayınları, Ocak 2019, s. 82.
[175] David A. Baldwin, "Security Studies and the End of the Cold War", *World Politics*, Cilt 48, Sayı 1, Ekim 1995, s. 119.
[176] Ömer Urhal, *Küreselleşen Dünyada Güvenlik: Milli Güvenlik, Kamu Güvenliği, Örgütlü Suçlar ve Suç İstihbaratı*, Adalet Yayınevi, Ankara 2009, s. 99.
[177] David A. Baldwin, *a.g.m.*, ss. 119-121.
[178] Emil Kirchner ve James Sperling, *EU Security Governance*, Manchester University Press, Temmuz 2008, s. 1.
[179] Kadir Sancak, "Güvenlik Kavramı Etrafındaki Tartışmalar ve Uluslararası Güvenliğin Dönüşümü", *KTÜ Sosyal Bilimler Dergisi*, Sayı 6, 2013, ss. 128-129.

1991 yılında SSCB'nin dağılarak Soğuk Savaş'ın sona ermesi, geleneksel güvenlik anlayışının etkinliğini yitirmesinde ve uluslararası sistemin çift kutuplu düzenden tek kutuplu düzene dönüşüm gerçekleştirme sürecine girmesindeki en büyük etkenlerden biri olarak kabul edilmektedir. Geleneksel güvenlik anlayışının temel dayanağını oluşturan realist anlayış çerçevesinde pek çok düşünür tarafından, Soğuk Savaş'ın sona ermesi sonucu çok kutuplu dünya düzenine geçileceği iddia edilmiştir.[180] Bununla birlikte, SSCB'nin çöküşünün arkasında yatan dinamikler içerisinde askeri sebeplerden daha yoğun olarak iç siyasi ve ekonomik faktörlerin yer alması nedeniyle, bir devletin varlığını sürdürmesinde dış faktörlerin yanı sıra iç faktörlerin de oldukça hayati öneme sahip olduğu gün yüzüne çıkmıştır. Realist anlayış, bu tahminleri gerçekleştiremediği ve Soğuk Savaş sonrası güvenliğin genişleme, derinleşme ve devlet dışı sektörleşmesi üzerine bir açıklama getirememesi sebebiyle büyük eleştirilere maruz kalarak önem derecesinde nispeten azalmalar görülmüştür.[181]

Geleneksel güvenlik anlayışının etkinliğini yitirmesindeki en önemli bir diğer unsur küreselleşme olmuştur. Geleneksel anlayış düşünürlerinin çoğu tarafından küreselleşmenin, ulusal güvenliğin sağlanması açısından yeni zorluklar getirdiği kabul edilmesine rağmen; uluslararası örgütler, devletlerin ulusal çıkarlarını gerçekleştirmek için kullandıkları birer araç olarak görülmeye devam edilmiştir. Kenneth Waltz tarafından, küreselleşmeyle birlikte devletin güç kaybetmediği; tam tersine yurt içinde ve yurt dışında toplumlar ve ekonomiler üzerindeki işlevlerini ve kontrolünü genişlettiği belirtilmiştir.[182]

Soğuk Savaş'ın son bulmasıyla birlikte geleneksel güvenlik anlayışının etkisini tamamen yitirdiğini ve yerini diğer güvenlik anlayışlarına bıraktığını söylemek kısmen hatalı bir değerlendirme olacaktır. Zira, Soğuk Savaş'ın resmi olarak sona erdiği dönem itibarıyla devletler arasındaki silahlı çatışmalar ve askeri tehditler azalmış olsa dahi son bulmamıştır. Bu konuda Waltz, 2000 yılında yayımladığı bir çalışmasında Soğuk Savaş sonrasında uluslararası politikanın bütününde köklü

[180] Patrick Morgan, "Security in International Politics: Traditional Approaches", *Contemporary Security Studies,* Derleyen: Alan Collins, Oxford University Press, New York 2007, s. 18.
[181] Emre Çıtak, *a.g.e,* ss. 131-132.
[182] Kenneth N. Waltz, "Globalization and American Power", *The National Interest*, Sayı 59, Bahar 2000, s. 48.

değişimlerin yaşanmadığını ve sistem üzerindeki anarşik yapının etkisinin halen devam ettiğini ifade etmiştir. Buna ek olarak, devletlerin kendi başının çaresine bakma ilkesinin ön planda olduğunu ve güç dengesinin temel aktörlerini devletlerin oluşturduğunu vurgulamıştır.[183]

2.1.2. Soğuk Savaş Sonrası Yeni Güvenlik Anlayışı

Soğuk Savaş sonrası dönemde askeri temelli konularda, sınır problemlerinde ve iç karışıklık gibi klasik güvenlik yaklaşımı konularına ek olarak küresel ölçekte toplumsal, çevresel, ekonomik ve teknolojik tehditleri de içeren yeni güvenlik yaklaşımlarının gündeme geldiği görülmüştür.[184] Yeni güvenlik yaklaşımı genel olarak, güvenliğin kapsam alanının askeri konular dışında bireyden başlayarak üzerinde yaşadığımız dünyanın güvenliğini de kapsar şekilde genişlemesi olarak ifade edilebilir. Yeni güvenlik yaklaşımının temelleri, Soğuk Savaş'ın en gergin dönemlerinde bile yoğun bir ilgi ile kabul görmüş; fakat iki kutup arası rekabetin yüksek seviyede devam etmesinden ve askeri yatırımların öncelikli konumda bulunmasından dolayı ön plana çıkamamıştır.[185] 1980'lere gelindiğinde iki süper güç arasındaki ilişkilerde yumuşamanın işaretleri görülmeye başlanmıştır. Beraberinde, geleneksel güvenlik anlayışının eleştirilerin ana odağı haline geldiği, uluslararası politikada yaşanan gelişmelerin de etkisiyle güvenlik kavramının giderek çeşitliliğini artırdığı dikkat çekmiştir.[186]

Güvenliğin kapsamının, devlet temelli askeri alan ile sınırlı kalmaması gerektiğini ve başka sektörleri de içerecek şekilde genişlemesi gerektiğini ilk ifade edenlerden biri Barry Buzan olmuştur. Buzan; ulusal güvenliğin yanına birey güvenliğinin ve uluslararası güvenliğin eklenerek üç düzey güvenlik anlayışı olması gerektiğini belirtmiştir. Buna ek olarak devlet güvenliği için, askeri güvenliğin yanı

---

[183] Kenneth N. Waltz, "Structural Realism After Cold War", *International Security*, Cilt 25, Sayı 1, Yaz 2000, ss. 5-6.
[184] Sinem Akgül Açıkmeşe, "Algı mı Söylem mi? Kopenhag Okulu ve Yeni-Klasik Gerçekçilikte Güvenlik Tehditleri", *Uluslararası İlişkiler*, Cilt 8, Sayı 30, Yaz 2011, s. 60.
[185] Pınar Bilgin, *Regional Security in the Middle East: A Critical Perspective*, Routledge, Londra 2019, s. 7.
[186] Güngör Şahin, *a.g.e.*, ss. 81-82.

sıra; siyasi, ekonomik, toplumsal ve çevresel gibi sektörlerin de önemli bir husus olduğunu vurgulamıştır.[187]

Geleneksel güvenlik kavramının bir bakıma yıpranmasına sebep olan en önemli unsurlardan biri SSCB'nin çökmesi ise bir diğer unsur da küreselleşme olmuştur. Küreselleşmeyle birlikte güvenlik kavramına yöneltilmiş olan "*Güvenlik nedir?*", "*Kimin ve neyin güvenliği?*", "*Güvenlik nasıl sağlanır?",* "*Güvenlik kim için inşa edilmelidir?*" gibi sorular güvenlik kavramının yeniden irdelenip çeşitlilik kazanmasında etkili olmuştur.[188] Soğuk Savaş sonrası küreselleşme, Soğuk Savaş dönemine göre daha etkili bir şekilde yayılmış ve ülkeleri birbirine daha bağımlı hale getirmiştir. İletişim, ulaşım ve teknoloji alanında yaşanan küreselleşme ve devrim, sadece gelişmiş sanayiye sahip ülkelerde değil, aynı zamanda gelişmekte olan ve gelişmiş sanayiye geçiş yapan ülkelerde sosyal, ekonomik ve politik çevreyi çarpıcı bir şekilde değiştirmiştir.[189] Küreselleşme; malların akışkanlığını, hizmeti ve dünya çapındaki insanların hareketliliğini artırmasına karşın, ulus devletlerin ve toplumlarının dış olaylara ve tehditlere karşı savunmasızlığını tetiklemesiyle birlikte toplumsal bozulma potansiyeli üzerindeki kırılganlığın artmasına neden olmuştur. Rakip devletlerin konvansiyonel ve nükleer silahlanmaya gitmesi, yayılmacı politikalar izlemesinin yanı sıra ekonomik ve finansal bozulmalar, pandemik hastalıklar, çevresel felaketler, etnik çatışmalar, başarısız devlet yönetimleri ve ulus ötesi organize suçlar gibi ulusal, uluslararası ve küresel etkiye sahip yeni güvenlik tehditleri görülmeye başlanmıştır.[190] Bu tehditler; bireyleri, toplumları hatta zamanla küresel anlamda bütün nesneleri hedef almış, bir bakıma yaşadığımız evrenin her bir köşesinin, yeni mücadele alanlarına dönüştüğü görülmüştür. Sonuçta, bu mücadele alanları içerisinde ortaya çıkabilecek tehdit ve riskler, dünya üzerinde çok ciddi fiziki yok oluşlara yol açabilecek kapasitede olmuştur. Kısacası, askeri yönelimli olarak

---

[187] Barry Buzan, *a.g.e.*, s. 363.
[188] Pınar Bilgin, "Dünya Literatürü ve Uygulamasında Güvenlik Sektörü: 'Devlet Merkezli' Güvenlikten 'Yurttaş Merkezli' Güvenliğe Doğru Mu? Yeni Güvenlik", *Güvenlik Sektörü Yönetişimi: Türkiye ve Avrupa,* Derleyen: İbrahim Cerrah ve Ümit Cizre, Tesev Yayınları, İstanbul 2008, s. 49.
[189] Fuat Keyman, "Küreselleşme", *Uluslararası İlişkilere Giriş*, Derleyen: Şaban Kardaş ve Ali Balcı, Küre Yayınları, İstanbul 2014, ss. 499-500.
[190] Murat Yorulmaz, "Bölgeselleşen Güvenlik Anlayışında Yeni Açılımlar ve Türkiye'nin Güvenlik Algısında Yaşanan Değişimler" *Trakya Üniversitesi Sosyal Bilimler Enstitüsü Sosyal ve Beşerî Bilimler Dergisi*, Cilt 5, Sayı 2, Edirne 2013, s. 292.

devletten devlete görülen tek boyutlu tehdit kaynakları etkinliğini, çok boyutlu ve asimetrik tehditlere bırakmıştır.[191] Bunun sonucunda, Soğuk Savaş döneminde olduğu gibi risk ve tehlikelerin kaynağının, şeklinin ve derecesinin önceden tahmin edilmesinin artık neredeyse imkânsız hal aldığı bir döneme geçiş yapılmıştır.

Soğuk Savaş sonrası dönemde devlet merkezli tehditlerin etkisini azaltmasıyla birlikte yeni tehdit alanları etkisini göstermiş, bu durum sonucunda güvenlik alanında derinleşme ve genişleme yaşanmıştır. Güvenlik gündeminde görülen derinleşme ve genişlemeler sonucu tehditler, ulus devletlerin tek başlarına mücadele edemeyeceği küresel bir boyut kazanarak ortak çaba ve iş birliğine yönelmenin önemini artırmıştır.[192] Örneğin; etnik çatışmalar veya yasa dışı göç gibi küresel tehdit oluşturacak potansiyeldeki sorunlar karşısında aralarında anlaşmazlıkların bulunduğu devletlerin bile iş birliği içerisinde mücadele etmesi kaçınılmaz bir zorunluluk haline gelmiştir.[193] Güvenliğin referans özneleri sadece devletler ile sınırlı olmaktan çıkıp; bireyler, toplumlar, özel sektör şirketleri, sivil toplum kuruluşları ve hükümet dışı aktörleri de içine alacak şekilde derinleşme eğilimi göstermiştir.[194]

Soğuk Savaş dönemi geleneksel güvenlik anlayışı düşünürlerine göre küreselleşmenin, ulus devletlerin egemenliklerine bir tehdit oluşturmayacağı ifade edilmesine rağmen, 1990'lar itibarıyla devlet-altı ve devlet-üstü örgütlerin otoritelerini ve güçlerini artırmaya başladığı görülmüştür. Bu durum aynı zamanda, ulus devlet egemenliğinin sorgulanır hale gelmesine de yol açmıştır.[195] Bununla birlikte, küreselleşmenin bir diğer sonucu olarak da devletlerin iç ve dış güvenlik sorunları arasındaki ayrım giderek belirginliğini yitirmiştir.[196] Bireylerin, geleneksel anlayışın en büyük tehdit olarak gördüğü nükleer saldırılara doğrudan maruz kalmasalar bile

---

[191] Bilal Karabulut, *Güvenlik, Küreselleşme Sürecinde Güvenliği Yeniden Düşünmek*, Barış Kitap, Ankara 2011, s. 6.
[192] Gencer Özcan, "Doksanlı Yıllarda Türkiye'nin Değişen Güvenlik Ortamı", *Türkiye'nin Ulusal Güvenlik ve Dış Politika Gündeminde Doksanlı Yıllar: En Uzun On yıl*, Derleyen: Gencer Özcan ve Şule Kut, Büke Yayınları, İstanbul 2000, s. 13.
[193] Emre Çıtak, *a.g.e.*, s. 156.
[194] Zerrin Ayşe Öztürk, "Soğuk Savaş Sonrasında Yeni Güvenlik Teorileri ve Türkiye'nin Güvenlik Algılamaları", *21. Yüzyıl*, Cilt 1, Ekim 2007, s. 42.
[195] Bülent S. Ağır, "Güvenlik Kavramını Yeniden Düşünmek: Küreselleşme, Kimlik ve Değişen Güvenlik Anlayışı", *Güvenlik Stratejileri Dergisi*, Cilt 11, Sayı 22, Ekim 2015, s. 100.
[196] Bülent S. Ağır, *a.g.m.*, s. 110.

vekalet savaşları, çevresel felaketler, iklim değişiklikleri, yoksulluk, salgın hastalıklar, gıdaların yapısında meydana gelen bozulmalar, açlık, şiddet ve insan hakları ihlallerinin yaşanması sonucu yaşamlarını yitirdikleri görülmüştür.[197] Tüm bu tehditler neticesinde yeni güvenlik anlayışı, düşünce ve uygulamada merkezine bireyi koyan bir yaklaşım benimsemiştir. Devlet, geleneksel güvenlik anlayışının aksine yeni güvenlik anlayışı kapsamında vatandaşlarının güvenliğini sağlamakla sorumlu birer araç olarak görülmektedir.[198]

Soğuk Savaş sonrası dönemde, devletler arası sıcak çatışma olasılığının büyük ölçüde azalması, devlet temelli güvenlik anlayışı içerisinde görülen askeri nitelikli çatışmalar, sınırların güvenliği ve mutlak egemenlik gibi kavramlara daha az önem verilmesi sonucunu doğurmuştur. Bu kavramların yerine, yeni güvenlik anlayışı çerçevesinde demokratikleşme, karşılıklı bağımlılık, kolektif güvenlik, sivil toplumun korunması, insani güvenlik ve ekonomik kalkınma gibi kavramlar ön planda yer almıştır.[199] Küreselleşme, sınırlar arası organize suçun yükselişinde de kilit bir rol oynamıştır. Bu bağlamda küreselleşme bir yönden; malların, insanların ve paranın sınırlar arasında serbestçe dolaşımını mümkün kılarken, bir diğer yönden de kara paranın, uyuşturucun, taklit ürünlerin, silahların, yasa dışı göçmenlerin ve nükleer malzemelerin dolaşımını kolaylaştırmıştır.[200]

2.1.3. 11 Eylül Sonrası Güvenlik Anlayışı

11 Eylül 2001 tarihinde ABD'nin ekonomi merkezi olan New York'taki ikiz kuleler ile savunma merkezi olan Washington'daki Pentagon binasına teröristler tarafından kaçırılan yolcu uçakları ile saldırılar gerçekleştirilmiş ve bu saldırılar sonucu 3.000'e yakın kişi yaşamını yitirmiştir.[201] ABD'yi hedef alan bu terör

---

[197] Taylor Owen, "Challenges and Opportunities for defining and Measuring Human Security", *Disarmament Forum*, Sayı 3, 2004, s. 17.
[198] Pınar Bilgin, "Dünya Literatürü ve Uygulamasında…", s. 60.
[199] Ken Booth, "Security and Self: Reflections of a Fallen Realist", *In Critical Security Studies: Concepts and Cases*, Derleyen: Keith Krause ve Michael C. Williams, University of Minnesota Press, Mart 1997, ss. 85-86.
[200] Roy Godson ve Phil Williams, "Strengthening Cooperation Against Transnational Crime", *Survival*, Cilt 40, Sayı 3, 1998, s. 68.
[201] Şükrü Türköz, "Küresel Terörizm Sorununa Güvenlik Perspektifli Bir Yaklaşım", *Niğde Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, Cilt 9, Sayı 2, Niğde 2016, s. 157.

saldırıları, birçok açıdan 21. yüzyıl küresel güvenlik anlayışının dönüm noktasını inşa ederek, güvenlik algısının oluşturmuş olduğu risk, tehdit ve tehlike durumlarının ulusal düzeyden küresel düzeye taşınmasına yol açmıştır.[202] Demokratik hak ve özgürlüklere dair güvenlik kapsamı altında çeşitli kısıtlayıcı yasal düzenlemeler ve baskıcı politikalar getirilerek birey temelli güvenlik anlayışı yerini tekrardan devlet temelli güvenlik anlayışına bırakmaya başlamıştır.[203] Bir diğer ifadeyle devletin güvenliği, içerisinde yaşadığı vatandaşlarının güvenliğinin önüne geçmiş ve devletin güvenliğini garanti altına almak için attığı adımlar toplumun güvenliğine zarar vermeye başlamıştır. Bunun sonucunda, Soğuk Savaş döneminde görülen geleneksel anlayışın devlet merkezli ve güç odaklı ilkelerinden bazılarının, tekrardan ulus devletlerin güvenlik politikalarında öncü konuma gelmeye başladığı dikkat çekmiştir.[204]

11 Eylül saldırıları, uluslararası politikada 'küresel terörizm' olarak ifade edilen yeni bir kavramın uluslararası alanda yaygın kullanımını getirmiştir. Gerçekleştirilen saldırılar sonrasında uluslararası alandaki ciddi tehditlerden birini oluşturan küresel terörizm tehdidi, güvenlik dönüşümünün bu denli kolektif ve keskin bir karakter kazanmasının da ana unsurunu oluşturmuştur.[205] Her ne kadar 1990'lı yıllarda da terör saldırıları, güvenlik tehdidi olarak görülmüşse de 11 Eylül'de gerçekleştirilen saldırılar bu tehdidin yıkıcı etkilerini bütün boyutlarıyla göstermiştir. Bununla birlikte, dünya düzeni içerisindeki her bir bireyin, devletin veya uluslararası kuruluşun terörist saldırıların hedefi olabileceğini ve askeri anlamda dünyanın en büyük gücü olarak görülen ABD'nin bile bu saldırılar karşısında şaşkın ve bir o kadar da çaresiz kalabileceğini hissettirmiştir.[206]

---

[202] Mehmet Özel ve Demet Dönmez, "Toplum Sözleşmecilerinden 11 Eylül'e Güvenlik Anlayışındaki Değişim", *Türk İdare Dergisi*, Sayı 482, 2016, s. 265.
[203] Mark Neocleous, *Critique of Security*, Edinburgh University Press, Edinburgh 2008, s. 108.
[204] Tamar Meisels, *The Trouble With Terror: Liberty, Security, And The Response To Terrorism*, Cambridge University Press, Cambridge 2008, s. 58.
[205] Sibel Kavuncu ve Hasan Dilan, "21. Yüzyıl Eşiğinde Yeni Çelişkiler/Yeni Krizler Ortamında Uluslararası Siyasal Sistemin Çok Kutupluluğa Doğru Evrilmesi", *38. (ICANAS) Uluslararası Asya ve Kuzey Afrika Çalışmaları Kongresi*, Cilt 2, Atatürk Kültür, Dil ve Tarih Yüksek Kurumu Yayınları, Ankara 2011, s. 949.
[206] Emre Çıtak, *a.g.e.*, ss. 168-169.

Küreselleşmenin etkisiyle birlikte dünya üzerindeki sınırların yapay bir hal alması, terör örgütlerinin organize olabilmelerini ve serbest hareket alanı sağlayarak hedeflerine ulaşabilmelerini daha da kolaylaştırmıştır.[207] Terör örgütlerinin ikamet konumlarının, üye sayılarının, finansal kaynaklarının, planlarının ve stratejilerinin tahmin edilebilirliğinin neredeyse imkânsız olması sebebiyle, bu saldırıları düzenleyen terör örgütlerine karşı hem caydırıcılık politikaları hem de silah kontrolü veya askeri alandaki yüksek teknolojiler ile yeterli düzeyde başarı sağlamada etkisiz kalınabildiği görülmüştür.[208] Sonuç olarak, basit yollarla üretilen bir patlayıcıyla bile yüzlerce insanın ölümüne yol açılabildiği ve stratejik hedeflerin vurulabildiği görülmüştür. Terörizm saldırılarına karşı artık tek başına mücadele vermenin neredeyse imkânsız hale gelmesi, devletlerin iş birliğine gidip ortak hareket etmesini zorunlu kılmıştır.

Soğuk Savaş sonrası dönemde kendini hissettirmeye başlayan yeni güvenlik tehditleri, 11 Eylül 2001 itibarıyla sivil toplum kuruluşları, akademik çevreler, kamuoyu, medya, hükümetlerin politikaları ve araştırma gündemleri gibi toplumun hemen hemen tüm dinamiklerinde etkisini giderek artırmıştır.[209] 11 Eylül Saldırılarından itibaren giderek dünya gündeminde kendisini çok çeşitli alanlarda göstermeye başlayan küresel terörizm tehdidinin yanı sıra finansal kargaşa, internet korsanlığı, ekolojik dejenerasyon, uyuşturucu kaçakçılığı, silah ve insan ticareti, yasa dışı göç hatta günümüzde etkisini hala devam ettiren Koronavirüs (*Covid-19*) pandemisi gibi hem ulusal hem de uluslararası güvenlik sorunlarına sebep olacak tehditler ile karşılaşılmaktadır. Bu tehditlerin birçoğunun nasıl, ne zaman ve nereden gelebileceğini kestirebilmenin neredeyse imkansız olduğu ve daha önce insanlık tarihinde herhangi bir ülke veya uluslararası topluluk üzerinde bu denli ciddi, uzun süreli ve de kapsamlı etkilere sahip olmadıkları belirtilmektedir.[210] Bir bakıma 11 Eylül sonrası dönemde güvenliğin kapsamı genişlerken tehdit kaynaklarının da

[207] Hasret Çomak, "Küreselleşme ve Güvenlik", *Küreselleşme ve Küreselleşmenin Türkiye'ye Etkileri*, Derleyen: Caner Sancaktar, Tasam Yayınları, İstanbul 2008, s. 10.
[208] Fuat Keyman, *a.g.e.*, s. 504.
[209] Gökhan Koçer, "Soğuk savaş Sonrasında Uluslararası Güvenlik Ortamı ve Türkiye'nin Ulusal Güvenliği", *Stratejik Araştırmalar Dergisi*, Cilt 3, Sayı 5, 2005, s. 289.
[210] Şükrü Türköz, *a.g.m.*, s. 160.

muğlaklığı ve soyutluğu giderek artış göstermiş, ulusal güvenlik ile uluslararası güvenlik giderek bir bütün halini almıştır.[211]

2.2. Geçmişten Günümüze NATO'nun Güvenlik Anlayışının Dönüşümü

NATO'nun 4 Nisan 1949 tarihindeki kuruluşu, iki süper güç olan ABD ve SSCB arasındaki tehdit ve risk ortamının yarattığı iki kutuplu sistemik yapının bir sonucu niteliğindedir. Böylece, NATO'nun kuruluşunun ilan edilmesiyle beraber iki süper gücün liderleri oldukları Doğu ve Batı Blokları arasındaki çatışmanın süreklilik taşır hale gelmesinin de bir bakıma ilk adımı atılmıştır. Soğuk Savaş dönemi boyunca NATO'nun, askeri ve güvenlik eksenli politikalar izlemesindeki en önemli unsur, caydırıcı bir karşı gücün ve denge sisteminin olmasından kaynaklanmıştır. Bir diğer ifadeyle İttifak, tüm tehdit algısını ve askeri yapılanmasını SSCB'nin izlemiş olduğu strateji ve politika faaliyetlerini göz önünde bulundurarak yürütmüştür.[212]

Berlin Duvarı'nın yıkılması, SSCB'nin dağılması ve uluslararası güvenlik konsepti içerisinde görülen derinleşme ve genişleme adımları, NATO'nun ana varoluş sebebinin, amacının, misyonunun ve hedeflerinin sorgulanmasını getirmiştir. Bu çerçevede, NATO'nun devamlılığını sürdürebilmesi için dış ve güvenlik politikalarında askeri gücün tek başına başat konumda bulunamayacağı, buna ek olarak siyasi, ekonomik, sosyo-kültürel, çevresel ve hukuksal sektörlerin ön planda yer alması gerektiği anlayışı oluşmuştur.[213] Bunun yanı sıra geniş çaplı tehdit ortamı yaratan Bosna-Hersek ve Kosova krizleri, NATO'nun Soğuk Savaş sonrası güvenlik kimliğinin boyutlarını inşa eden önemli gelişmeler arasında yerini almıştır.[214] Bu krizler sonucu İttifak, '*alan dışı müdahale*' ve '*istikrarlaştırma*' ilkelerini devreye sokarak sınırları dışında gerçekleşen güvenlik sorunlarının çözümünde temel

---

[211]Hale Aydoğmuş, "ABD'nin kapıları mültecilere kapalı", (03.10.2019), *https://www.trthaber.com/haber/dunya/abdnin-kapilari-multecilere-kapali-433696.html*, (Erişim tarihi: 18.05.2020).

[212] Tarık Oğuzlu, *a.g.m.*, ss. 5-6.

[213] Ali Karaosmanoğlu, *NATO'nun Dönüşümü*, İstanbul Bilgi Üniversitesi Yayınları, İstanbul 2012, ss. 4-5.

[214] Nurşin Ateşoğlu Güney, *Batı'nın Yeni Güvenlik Stratejileri AB-NATO-ABD,* Bağlam Yayıncılık, İstanbul 2006, ss. 36-37.

mekanizmanın NATO aracılığıyla oluşturulabileceğini de ortaya koymuştur.[215] Başka bir deyişle NATO, üyelerini hedef alan tehdit unsurlarına yönelik koruma sağlayan bir savunma örgütünden, ortak önlem almak üzere yapılanan küresel düzeyde bir kolektif güvenlik örgütüne doğru yapısal değişim süreci içerisine girmiştir.[216]

21. yüzyıl itibarıyla öncelikle 11 Eylül Saldırıları olmak üzere uluslararası sistemin güvenlik algılamalarında kırılmaya neden olan yeni risk alanlarının ortaya çıkması, NATO'nun yeniden güvenlik anlayışını güncellemesini gerekli kılan başlıca unsurlar arasındadır. Bu kapsamda, NATO'nun 2010 yılındaki Stratejik Konsept'i incelendiğinde önleyici diplomasi, kriz yönetimi, eski ve yeni ortaklarla iş birliği ilkelerinin İttifak'ın güvenlik anlayışı içerisinde temel sacayaklarını oluşturduğu görülmektedir.[217] Bunun yanı sıra İttifak'ın gündemine; uluslararası terörizm, sınır problemleri, mülteci krizi, iklim değişikliği, enerji kaynaklarının tüketimi, uyuşturucu ticareti, insan kaçakçılığı, su kıtlığı ve siber sorunlar gibi yeni asimetrik tehdit tanımlamaları girmiştir.[218] Sadece askeri ve siyasi araçlarla üstesinden gelinemeyecek yeni güvenlik risklerinin ortaya çıkması, NATO'nun gerçekleştirdiği bu dönüşümün itici gücünü oluşturmuştur. Buna rağmen, yakın dönem içerisinde İttifak'ın üyeleri arasında başta yük paylaşımı olmak üzere çeşitli kriz durumları sonucunda fikir ayrılıklarının gerçekleşmesi, NATO'nun güvenilirliğinin ve kolektif güvenlik ilkesinin tartışılmasına sebebiyet verebilmektedir.

2.2.1. NATO'nun Kuruluşu ve Soğuk Savaş Dönemi Güvenlik Anlayışı

İkinci Dünya Savaşı'ndan askeri ve ekonomik olarak ciddi yıpranmalar ile çıkan Batı Avrupa devletleri, savaşın son bulmasıyla bir taraftan ekonomik ve sosyal kalkınma çalışmalarına hız verirlerken, diğer taraftan da savunma ve güvenlik

[215]NATO, *Partnership for Peace Programme*, (23.03.2020), https://www.nato.int/cps/en/natohq/topics_50349.htm, (Erişim tarihi: 03.02.2021).
[216] Erdem Özlük ve Duygu Özlük, "NATO'yu Anlamak: Dönüşümü, Yeni Kimlikleri ve Uyum Süreçleri." *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* Sayı 31, Konya 2014, ss. 211-212.
[217] NATO, "Aktif Katılım, Modern Savunma: Kuzey Atlantik Antlaşması Örgütü Üyelerinin Savunması ve Güvenliği için Stratejik Kavram", *NATO Public Diplomacy Division*, Brüksel 2010, *https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120207_strategic-concept-2010-tur.pdf*, (Erişim tarihi: 20.08.2020), ss. 20-24.
[218] NATO, "Aktif Katılım, Modern Savunma: Kuzey Atlantik Antlaşması Örgütü…", ss. 12-14.

alanlarında tedbirler alabilmek için bir araya gelmişlerdir. İkinci Dünya Savaşı'nın etkisini yitirmeye başladığı dönemlerde, Batı Avrupa devletlerinin askeri saldırı ve savunma kuvvetlerini azaltmaya başlamasına rağmen SSCB'nin ordu gücünde artırıma gitmesi, bununla birlikte 1944-1945 yılları arasında Müttefik devletlerin toplam asker sayısı 3 milyon iken SSCB'nin 4 milyona yakın silahlı kuvveti hazır durumda elinde bulunduruyor olması, endişe ve panik ortamının oluşmasına neden olmuştur.[219]

SSCB'nin yayılmacı politikalar izlemeye başlamasının yanı sıra komünizm ideolojisini baskı ve kuvvet kullanarak yayabilmek için elinde bulundurduğu askeri gücünü harekete geçirmesi beraberinde Baltık ülkelerinin tamamıyla birlikte Finlandiya, Romanya ve Polonya'nın bir bölümünü de topraklarına katma girişimlerinde bulunması, Batı Avrupa ülkelerinde endişeyle karşılanmıştır. Ayrıca, Joseph Stalin'in 1945-1946 yıllarında Türkiye'deki boğazların yönetimi gibi taleplerde bulunması ve başta Yunanistan olmak üzere Balkan Yarımadası'nın tamamı üzerinde baskı politikaları yürütmeye başlaması, Batı Avrupa ülkelerinin endişelerini pekiştirirken bölgede de güvenlik riski doğurmuştur.[220] Bu gelişmeler, İkinci Dünya Savaşı sırasında Batı ile SSCB arasındaki olumlu havanın ve tüm iş birliği adımlarının sekteye uğramasına neden olan en önemli meseleleri oluşturmaktadır. SSCB'nin izlemiş olduğu "*Sovyetleştirme*" politikasına karşılık ABD'nin Truman Doktrini ve Marshall Planı'nı faaliyete geçirmesiyle resmen çift kutuplu düzenin yapı taşları inşa edilmiştir. SSCB, 5 Ekim 1947 yılında himayesi altındaki komünist ülkelerle birlikte Komin Formu kurarak çift kutuplu uluslararası sistemin ilk adımlarını atma girişimini gerçekleştirmiştir.[221]

Çekoslovakya Komünist Partisi'nin (*Communist Party of Czechoslovakia*), 1948 yılında askeri darbe gerçekleştirerek ülke yönetimini Sovyet hakimiyeti altına sokması, Batı Avrupa devletlerinin savunma temelli örgütlenme faaliyetlerine

[219] Selim Soley, *NATO- Kuzey Atlantik Anlaşması Teşkilatı*, EU Basımevi, Ankara 1955, s. 30.
[220] Ali Karaosmanoğlu, *a.g.m.*, s. 5.
[221] Nataliia I. Egorova, "Stalin's Foreign Policy and the Cominform, 1947-53", *The Soviet Union and Europe In The Cold War, 1943-53*, Derleyen: Francesca Gori ve Silvio Pons, Macmillan Press Ltd, Londra 1996, s. 198.

gitmelerindeki başat itici gücü oluşturmuştur.[222] Bu gelişme sonucunda, 17 Mart 1948 tarihinde Birleşik Krallık, Fransa, Belçika, Hollanda ve Lüksemburg tarafından Brüksel Antlaşması imzalanmış; 28 Eylül tarihinde ise Batı Birliği Savunma Örgütü (*Western Union Defence Organisation*, WUDO) adı altında askeri bir ittifak resmi olarak faaliyete geçirilmiştir.[223] ABD'nin, savaş sonrası diğer devletler ile krize, çatışmaya veya savaşa yol açabilecek durumların önüne geçmek amacıyla "*yalnızcılık*" olarak nitelendirilen devlet politikasını sürdürmesi nedeniyle İttifak'a dahil olamaması, Batı Birliği Savunma Örgütü'nün SSCB tehdidine karşı caydırıcılık dengesinin sağlanmasındaki nihai eksikliği oluşturmuştur.[224] Buna ek olarak, aynı yıl içerisinde Joseph Stalin'in emriyle Batı Berlin abluka altına alınarak Batı Almanya ile bağlantısı kesilmeye çalışılmıştır. SSCB, Berlin Ablukası ile Batılı güçleri kısa sürede yıldırarak emellerinden vazgeçirmeyi amaçlamış; ancak sıcak savaş çıkma endişesiyle kısa sürede geri adım atmak durumunda kalmıştır.[225]

SSCB'nin, Doğu Avrupa ve Balkanlar üzerinde gerçekleştirdiği tehdit ve saldırı ortamı sonucunda, dış politikasını değiştirmesine yönelik olarak ABD, Batılı devletler tarafından ciddi baskılar ile karşılaşmıştır. Bu yoğun istekler karşısında, 1948 yılında Senatör Vandenberg'in hazırladığı karar tasarısını ABD Senatosuna sunmuş, tasarının onaylanması sonucu ABD'nin, Batı Avrupa ittifak sistemine dahil olmasının önü açılmıştır.[226] Birçok görüşme sonucunda, 4 Nisan 1949'da ABD, Kanada, İtalya, Danimarka, Portekiz, Norveç, İzlanda başta olmak üzere Brüksel Paktı'na üye olan devletler, Washington'da bir araya gelerek Kuzey Atlantik Antlaşması'nı imzaladıklarını ilan etmişlerdir.[227] Böylece, iki bloklu sistemin Batı Bloğu'nun temelleri ABD önderliğinde resmen atılmıştır.

---

[222] Ivo Duchacek, "The Strategy of Communist Infiltration: Czechoslovakia, 1944–48", *World Politics*, Cilt 2, Sayı 3, Nisan 1950, s. 345.
[223] Mehmet Hasgüler ve Mehmet B. Uludağ, *Devletlerarası ve Hükümetler Dışı Uluslararası Örgütler*, Alfa Yayınları, İstanbul 2012, s. 327.
[224] Yusuf Sarınay, *Türkiye'nin Batı İttifakına Yönelişi ve NATO'ya Girişi*, Kültür ve Turizm Bakanlığı Yayınları, Ankara 1988, ss. 72-74.
[225] Oral Sander, *Siyasi Tarih 1918-1994*, 23. Baskı, İmge Yayınevi, Ankara 2013, ss. 224-225.
[226] Fahir Armaoğlu, *20. Yüzyıl Siyasi Tarihi 1914-1980*, Türkiye İş Bankası Yayınları, Ankara 1988, ss. 445-449.
[227] Nejat Doğan, "NATO'nun Örgütsel Değişimi, 1949-1999: Kuzey-Atlantik İttifakından Avrupa-Atlantik Güvenlik Örgütüne" *Ankara Üniversitesi SBF Dergisi*, Cilt 60, Sayı 3, Ankara 2005, s. 73.

NATO'nun kurulması, ABD'nin 1823'ten beri izlediği yalnızcılık politikasını terk ederek kendi kabuğunun dışına çıktığının ve komünist ideoloji ile güçlü bir mücadeleye başladığının göstergesi olmuştur. Dolayısıyla bu dönemde ABD'nin güvenliğinin sağlanmasında deniz aşırı bölgelerde yaşanan gelişmelerin etkili olmaya başladığı dikkat çekmiştir.[228] NATO'nun kurulmasındaki temel amaç; Sovyet yayılmacılığını durdurabilmenin yanı sıra İttifak üyesi olan herhangi bir ülkenin topraklarında silahlı saldırıya karşı müştereken nefsi müdafaa yaparak topluluğun özgürlüğünü ve güvenliğini sağlayabilmek olmuştur.[229] NATO'nun kurulmasının amaçlarından bir diğerini ise; kıtada güçlü bir ABD varlığıyla Avrupa'da ulusal militarizmin yeniden canlanmasını engelleyebilmek ve Avrupa siyasi entegrasyonunu teşvik etmek oluşturmuştur.[230] Neticede NATO, Kuzey Amerika ile Batı Avrupa güvenliğini birbirine eşit olarak kabul eden bir düşünceyle kurulmuş ve kolektif güvenlik ilkesi esas alınarak oluşturulmuş bir örgüt olarak uluslararası alanda yer almıştır.[231] Bu konuyla alakalı olarak NATO'nun ilk Genel Sekreteri Lord H. Ismay tarafından NATO'nun kuruluşundaki esasın; Rusları dışarıda, ABD'yi içeride ve Almanları baskı altında tutabilmek olduğu ifade edilmiştir.[232]

Kuzey Atlantik Antlaşması'nın giriş bölümünde devletler, Birleşmiş Milletler Şartı uyarınca demokrasi, insan hakları ve hukukun üstünlüğü ilkeleri temelinde ortak miraslarını, kültürlerini ve medeniyetlerini koruyacaklarını; istikrar ve refahı geliştireceklerini bildirmişlerdir.[233] Antlaşma'nın en dikkat çekici niteliğinde olan 5. Maddesine göre ise; üyelerden birine veya birkaçına karşı girişilen silahlı saldırının tüm üyelere yöneltilmiş olarak değerlendirileceği taahhüt edilmektedir. Bunun sonucunda tüm üyeler tarafından, bireysel veya toplu olarak, Birleşmiş Milletler

---

[228] Burcu Bostanoğlu, *Türkiye-ABD İlişkilerinin Politikası*, İmge Kitabevi, Ankara 1999, s. 260.
[229]NATO, *A New NATO For A New Century*, (05.11.2008), https://www.nato.int/cps/en/natolive/opinions_25558.htm, (Erişim tarihi: 25.08.2020).
[230] Alptekin Molla, NATO Savunma Politikaları Çerçevesinde Türk-Amerikan İlişkilerinin Analizi, (İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü Uluslararası İlişkiler Anabilim Dalı, Doktora Tezi), İstanbul 2008, ss. 7-8.
[231] Sinem Akgül Açıkmeşe ve Cihan Dizdaroğlu, "NATO-AB İlişkilerinde İşbirliği ve Çatışma Dinamikleri", *Uluslararası İlişkiler*, Cilt 10, Sayı 40, Kış 2014, s. 136.
[232] Geoffrey Wheatcroft, "Who Needs NATO?", *https://www.nytimes.com/2011/06/16/opinion/16iht-edwheatcroft16.html*, (Erişim tarihi: 24.08.2020).
[233]NATO, *Kuzey Atlantik Antlaşması*, (09.12.2008), https://www.nato.int/cps/fr/natohq/official_texts_17120.htm?selectedLocale=tr, (Erişim tarihi: 25.08.2020).

Antlaşması'nın "*meşru müdafaa ilkesi*" bağlamında saldırıya uğrayan ülkeye askeri gücün kullanılması dahil her türlü yardımın gerçekleştirileceği bildirilmektedir.[234] 25 Haziran 1950 tarihinde Kuzey Kore'nin Güney Kore'ye saldırması, saldırının arkasında SSCB desteğinin bulunduğu düşüncesi sonucunda NATO içerisinde askeri kanadın kuvvetlendirilmesinin gerekliliği yönünde tartışmalar çıkmıştır.[235] Bunun sonucunda 1951 yılında NATO, bünyesinde Avrupa Müttefik Kuvvetleri Yüksek Karargâhı (*Supreme Headquarters Allied Powers Europe,* SHAPE) kurulmasıyla İttifak'ın askeri kanadını güçlendirmeye yönelik politika uygulamıştır. Böylece ilk defa uluslararası bir örgütün kendi ordusu, karargâhı ve personeline sahip olduğu görülmüştür.[236]

NATO'nun Avrupalı müttefiklerinin Kore Savaşı sonrasında ekonomik refah ve kalkınmaya ağırlık vermesi, İttifak'ın savunma giderlerinin büyük bir kısmının ABD tarafından karşılanmasına sebep olmuştur. Bunun sonucunda, Einsenhower yönetimi 1953 yılında Kitlesel Karşılık Stratejisinin (*Massive Retaliation*) benimsenmesine yönelik çalışmalar gerçekleştirmiş ve 1954 yılında "*Kitlesel Karşılık Stratejisi*", NATO Konseyi tarafından resmen onaylanmıştır.[237] Bu Stratejinin uygulamaya geçirilmesi sonucunda nükleer silahların konvansiyonel silahlara göre daha ucuz maliyete sahip olması nedeniyle hem Avrupalı müttefiklerin ekonomik kalkınmaya daha fazla bütçe ayırmaları hedeflenmiş hem de NATO'nun savunma giderlerinin karşılanması hususunda olumsuz etkilenen ABD ekonomisini rahatlatmak istenmiştir.[238] Bir diğer öne çıkan sebep ise; Stratejinin kabul edildiği yıllarda ABD'nin nükleer güç yönünden SSCB'ye oranla daha üstün olması sebebiyle caydırıcılığın etkili bir şekilde sağlanacağının düşünülmesidir.[239]

---

[234]NATO, *NATO Handbook*, Public Diplomacy Division, Brüksel 2006, https://www.nato.int/docu/handbook/2006/hb-en-2006.pdf, (Erişim tarihi: 25.08.2020), s. 372.
[235] Robert S. Jordan, "NATO's Structural Changes for the 1990s", *NATO In The Post-Cold War Era: Does It Have a Future*, Derleyen: S. Victor Papacosma ve Mary Ann Heiss, Macmillan Press, 1995, s. 48.
[236] Nejat Doğan, *a.g.m.*, s. 73.
[237] Levent Yiğittepe, *NATO Güvenlik Politikaları ve Terörle Mücadele Stratejileri*, Cinius Yayınları, Şubat 2017, s. 38.
[238] Nejat Doğan, *a.g.m.*, s. 75.
[239] Suat Dönmez, *Güvenlik Anlayışının Dönüşümü İttifak Kavramı ve NATO*, (Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Anabilim Dalı, Doktora Tezi), Ankara 2010, s. 101.

Kitlesel Karşılık Stratejisi kapsamında Kuzey Atlantik bölgesine gerçekleştirilecek her türlü saldırıya nükleer silahlar ile karşılık verileceği ilan edilmiş, askeri hedeflerin yanı sıra aktif sanayi bölgeleri, limanlar ve şehir merkezleri gibi topluma açık alanlar da saldırıyı tetikleyebilecek bölgeler içerisinde yer almıştır.[240] Ancak, SSCB'nin 4 Ekim 1957'de Sputnik füzesini uzaya göndermesi, Kitlesel Karşılık Stratejisi'nin seyrinde kritik değişime yol açmıştır. SSCB'nin bir termonükleer savaş başlığını yirmi dakikaya yakın bir sürede beş millik mesafeye kadar gönderebilmesi sonucu ABD topraklarının tamamı Sovyet füze menzili içerisine girmiş ve ABD tarihinde ilk kez bu kadar ciddi tehdit ve saldırı ile karşı karşıya kalınarak NATO'nun caydırıcılık gücünde nispeten düşüşe ve Kitlesel Karşılık Stratejisi'nin etkinliğini yitirmeye başlamasına sebep oluşturmuştur.[241] Bu bağlamda Kitlesel Karşılık Stratejisi, 1960'lı yıllarda her iki kutup arasında yumuşama dönemine girilmesi ve "*Esnek Karşılık Stratejisi'nin*" (*Flexible Response*) ön plana çıkmaya başlamasıyla önemini gitgide kaybetmiş ve 1967 yılında resmi olarak sona ermiştir.[242]

1962 yılındaki Küba Krizi boyunca iki blok arasında korku ve dehşete yol açacak adımların atılması sonucu sadece Avrupa kıtasının güvenliği tehlikeye atılmamış, bunun yanı sıra tüm dünya yok olma tehlikesinin eşiğinden dönmüştür. Her iki bloğun cephanelerinde bulundurduğu nükleer silah gücü üzerinden sürekli artırıma gitmesi beraberinde dehşet dengesinin oluşmasına sebep olmuş, bunun sonucunda Kitlesel Karşılık Stratejisi'nin oluşturduğu tehdit ortamı sorgulanır hale gelmiştir. Küba Krizi'nin aşılması sonrasında ise Batı Bloğu'nun "*yumuşama*", Doğu Bloğu'nun "*birlikte yaşama*" olarak ifade ettiği yeni bir politika ortamına geçiş yapılmıştır.[243] 13-14 Aralık 1967 tarihlerinde gerçekleştirilen NATO Konseyi toplantısı sonrasında "*Esnek Karşılık*" olarak adlandırılan yeni bir stratejiye geçildiği ilan edilerek, nihai

---

[240]Gregory W. Pedlow, "NATO STRATEGY DOCUMENTS 1949-1969", *https://www.nato.int/docu/stratdoc/eng/intro.pdf*, (Erişim tarihi: 11.12.2021), s. 21; Orhan Arıman, *Zafersiz Barış ya da NATO*, Ajans Türk Matbaacılık Yayınları, Ankara 1977, s. 40.

[241] Çağrı Erhan "ABD ve NATO'yla İlişkiler", *Türk Dış Politikası: Kurtuluş Savaşı'ndan Bugüne Olgular, Belgeler, Yorumlar*, Derleyen: Baskın Oran, Cilt 1, 15. Baskı, İletişim Yayınları, İstanbul 2009, s. 572; Muharrem Gürkaynak, *Avrupa Savuma ve Güvenlik Politikası*, Asil Yayınları, Ankara 2004, s. 82.

[242] John Baylis, "NATO strategy: the case for a new strategic concept", *International Affairs*, Cilt 64, Sayı 1, Kış 1987-1988, ss. 43-44.

[243] Haydar Çakmak, *Avrupa Güvenliği: NATO-AGİT-AGSP*, Akçağ Yayınları, Ankara 2003, ss. 200-202.

kararla aynı gün yumuşama politikasının, NATO'nun güncel hedefi olduğu "*Harmel Raporu*" aracılığıyla bildirilmiştir.[244]

Esnek Karşılık Stratejisi ile temel olarak Batı Bloğu ülkelerine gelebilecek herhangi bir saldırı durumunda hemen nükleer silaha başvurulmasının yerine aşamalı olarak karşılık verilmesi amaçlanmıştır. Bir diğer ifadeyle, rakip hangi silah aracılığıyla saldırı gerçekleştiriyorsa aynı türde silah ile karşılık verileceği belirtilmiştir.[245] Bu sebeple NATO içerisindeki ülkelerin konvansiyonel güçlerinde artırıma gitmeleri istenmiştir. Esnek Karşılık Stratejisi'nin aşamaları içerisinde ilk olarak konvansiyonel silahlara başvurularak rakibin durdurulmaya çalışılması yer almaktadır. Konvansiyonel silahlar ile caydırıcı bir savunma gerçekleştirilemediği takdirde taktiksel nükleer silahlara geçilmesi ve nükleer silaha başvurmak zorunda kalmanın sorumluluğunu karşı tarafa atfedebilmek hedeflenmiştir. Son aşamada ise, uygulanan bütün savunma yöntemlerinin yeterli olmaması durumunda nükleer silah kullanılması planlanmıştır.[246]

İki blok arasında 1960'ların ilk yarısında başlayan yumuşama çabaları, neredeyse 1970'lerin sonuna kadar uluslararası politikanın belirleyici unsuru olmuştur. Bu dönem içerisinde, ABD ile SSCB arasında nükleer ve stratejik silahların kullanımına ilişkin önemli antlaşmaların[247] imzalandığı dikkat çekmektedir. Bloklar arası barış ve iş birliği faaliyetlerinin geliştirilmesi yönünde açıklamalar yapılırken diplomasinin önemi de sık sık vurgulanmıştır. Buna rağmen 1970'lerin ortalarına

---

[244] William C. Cromwell, *The United States and the European Pillar: The Strained Alliance*, St. Martin's Press, New York 1992, s. 183.

[245] John S. Duffield, "The Evolution of NATO's Strategy of Flexible Response: A Reinterpretation", *Security Studies*, Cilt 1, Sayı 1, 1991, ss. 132-133.

[246] Beril Dedeoğlu, *Uluslararası Güvenlik ve Strateji*, Derin Yayınları, İstanbul 2003, ss. 234-235.

[247] Bu bağlamda, ABD-SSCB arasında ilk olarak 1972 yılında Stratejik Saldırı Silahlarının Sınırlandırılmasına İlişkin Tedbirler Antlaşması (SALT-1) imzalanmıştır. Bu antlaşmayı takiben nükleer silahlı balistik füze sistemlerinin sınırlandırılması amacını taşıyan Anti Balistik Füze (ABM) Anlaşması'nı imzalamışlardır. Son olarak ise ABD Başkanı Jimmy Carter ile SSCB Devlet Başkanı Leonid Brejnev tarafından 1979 yılında SALT-2 Antlaşması imzalanmıştır. Detaylı bilgi için bkz. Joseph S. Nye ve David A. Welch, *Understanding Global Conflict & Cooperation: Intro to Theory & History*, 9. Baskı, Pearson Education Limited, 2014, ss. 195-196; Sibel Kavuncu, "Nükleer Silahsızlanma Yolunda Start Süreci", *Bilge Strateji*, Cilt 5, Sayı 8, Bahar 2013, ss. 125-128.

doğru etkisini hissettiren siyasi ve ekonomik krizler, yumuşama dönemine damga vuran dinamiklerin bir süre sonra zarar görmesine neden olmuştur.[248]

1979 yılında ABD, Carter Doktrini temelinde Doğu Bloğu'na karşı yeniden caydırma faaliyetlerine girişmiş; bu kapsamda NATO aracılığıyla Avrupa'ya "*Cruise*", "*Pershing II*", "*Jupiter*" ve "*Thor*" füzelerini yerleştirme kararı almıştır. Batı Bloku tarafından izlenen nükleer silah artırımı politikasına karşılık, SSCB ise 175 adet SS-20 füze bataryasını Doğu Avrupa'ya konuşlandırmış ve bunun sonucunda bölgede tekrardan güvenlik krizi etkisini hissettirmiştir.[249] Tüm bu gelişmelerin yanı sıra İran-Irak Savaşı'nın çıkması, SSCB'nin Afganistan'ı işgalinin yanı sıra Polonya'daki ayrılık yanlısı protestoları sert bir şekilde bastırması sonucu NATO, Esnek Karşılık Stratejisi'nin yanına İleri Savunma Stratejisi ekleyerek politikasını genişletme yoluna gitmiştir. Bu Stratejiyle NATO; uluslararası sistemde ortaya çıkabilecek anlaşmazlık ve gerilimleri, üyesi olan ülke veya stratejik öneme sahip coğrafyaların sınırlarına gelmeden sonlandırabilmeyi hedeflemiştir.[250]

Sonuç olarak SSCB; 1980'lerin ikinci yarısından itibaren tarihinin en büyük ekonomik krizleri ile karşı karşıya kalmış, bunun sonucunda toplumsal barışın ve ülke içi siyasi düzenin etkisini yitirdiği görülmüştür. Bunun yanı sıra Doğu Avrupa'daki bağımsızlık yanlısı ayaklanmaların önünün kesilememesinin de SSCB'nin adım adım çöküşe gitmesinde büyük etkisinin bulunduğu söylenebilir. Netice itibarıyla, 25 Aralık 1991'de SSCB'nin kendini feshettiğini ilan etmesiyle birlikte uluslararası alanda SSCB varlığı da sona ermiştir.[251] Bu kapsamda NATO'nun, kuruluşundan itibaren Doğu Bloğu'nun çözülmesine kadar geçen kırk yılı aşkın bir süre boyunca Avrupa'daki barışı koruma ve SSCB'yi caydırma görevini başarılı bir şekilde sürdürmüş olduğunu ifade etmek mümkündür.

---

[248] Eric Hobsbawm, *Kısa 20. Yüzyıl 1914-1991: Aşırılıklar Çağı*, Çeviren: Yavuz Alogan, Sarmal Yayınevi, İstanbul 1996, ss. 285-288.
[249] Beril Dedeoğlu ve Mesut H. Caşın, "Yeni Avrupa Güvenlik Kimliğinde Stratejik Arayışlar: NATO-BAB-AB-AGİT İlişkilerin Dünü Bugünü ve Geleceği", *Avrasya Dosyası*, Avrupa Birliği Özel, Cilt 5, Sayı 4, Kış 1999, ss. 165-166.
[250] Çağrı Erhan, *a.g.e.,* s. 571.
[251] Ronald G. Suny, *The Revenge Of The Past: Nationalism, Revolution, And The Collapse Of The Soviet Union,* Stanford University Press, California 1993, s. 154.

2.2.2. NATO'nun Soğuk Savaş Sonrası Güvenlik Anlayışı

1989'da Berlin Duvarı'nın yıkılması, 1990'da Almanya'nın yeniden birleşmesi ve 1991'de SSCB'nin dağılması sonucunda Avrupa-Atlantik bölgesinin birincil tehdit kaynağı ortadan kalkarken bu durum, kuruluşundan itibaren tüm strateji ve politikalarını SSCB tehdidi karşısında İttifak'ın güvenliğinin sağlanması üzerine oluşturan NATO'nun asıl varoluş sebebinin de sorgulanmasına yol açmıştır.[252] Bu açıdan örgütün içerisinde iki farklı görüşün hâkim olduğu görülmektedir. Görüşlerden birisi; İttifak'ın temel tehdit unsurunun varlığını yitirmesi ile NATO'nun da meşruiyet kaynağını kaybettiği üzerineyken, diğeri ise İttifak'ın savunmanın yanı sıra siyasi bir işlevinin de olduğunun ve bölgesel krizlerin giderilmesinde NATO'nun şemsiyesine ihtiyaç duyulduğunun savunulması olmuştur.[253] Tüm bu tartışmalar içerisinde 1991 yılında gerçekleştirilen Roma Zirvesi'nde, NATO'nun Yeni Stratejik Konsept'i ilan edilmiştir.[254] Stratejik Konsept kapsamında Atlantik-Avrupa bölgesi içerisindeki istikrar ve güvenliğin sağlanmasına yönelik önemli yaklaşımlar ele alınmış ve yapısal dönüşümler belirlenmiştir.[255]

1991 Stratejik Konsept'i, içeriğinde etnik çekişmeler ve bölgesel anlaşmazlıklar dahil olmak üzere ciddi ekonomik, sosyal ve politik zorluklar nedeniyle esas olarak Orta ve Doğu Avrupa'daki ülkelerden kaynaklanabilecek güvenlik sorunları ve riskleri tanımlanmıştır.[256] Bunun sonucunda, Yeni Stratejik Konsept'in 15. Maddesinde NATO üyesi ülkelere diğer ülkelerden gelebilecek konvansiyonel veya nükleer tehditlerin yanı sıra terörizm faaliyetleri, aşırı milliyetçilik hareketleri, insan hakları ihlalleri, etnik ve dini çatışmalar gibi risk unsurlarına karşı da ortak savunma ve caydırıcılık yoluyla karşılık verileceği ifade edilmiştir.[257]

---

[252] Sibel Kavuncu, "US-Russia Relations In The Context of NATO Enlargement", *Management and Education*, Cilt 6, Sayı 4, 2010, s. 73.
[253] Hasan D. Pekşen, "NATO'nun Dönüşümünün Sınırları: Bir Uygulama Vakası Olarak Enerji Güvenliği", *Güvenlik Stratejileri Dergisi*, Cilt 12, Sayı 23, Nisan 2016, ss. 41-42.
[254]Trevor Taylor, "NATO and Central Europe", (10.04.2002), *https://www.nato.int/docu/review/1991/9105-4.htm*, (Erişim tarihi: 28.08.2020).
[255] Alptekin Molla, *a.g.e.*, s. 28.
[256]NATO, *The Alliance's New Strategic Concept*, (26.08.2010), https://www.nato.int/cps/en/natohq/official_texts_23847.htm?&utm_source=twitter&utm_medium=smcweb&utm_campaign=23847, (Erişim tarihi: 29.08.2020).
[257] Levent Yiğittepe, *a.g.e.*, s. 80.

Roma Zirvesi'nde, İttifak üyelerinin masaya yatırdığı konulardan bir diğeri ise, SSCB'nin dağılmasıyla bağımsızlığını kazanan devletlerin durumu olmuştur. Sözü edilen devletlerin bölgede yaratacağı istikrarsızlık ve kriz ortamının geçmiş yıllarda olduğu gibi Avrupa kıtasının tamamına yayılma ihtimalinin bulunması sebebiyle bu coğrafyalar, NATO'nun yeni tehdit alanları olarak tanımlanmıştır.[258] Ayrıca, başta Rusya olmak üzere tüm Doğu Avrupa, Orta Avrupa, Baltık ve Güney Akdeniz ülkeleriyle iş birliği diyaloğunun geliştirilmesinin yanı sıra Avrupa'nın güvenliğine tehdit oluşturacak anlaşmazlıkların diplomatik yollarla çözülmesine yardımcı olunacağı belirtilmiştir.[259] Bunun sonucunda NATO aracılığıyla 1991 yılında Orta ve Doğu Avrupa devletlerinin taşıdığı kaygıları giderebilmek ve bu ülkelerdeki demokratik adımları desteklemek için Kuzey Atlantik İşbirliği Konseyi (*North Atlantic Cooperation Council,* KAİK) kurulmuştur.[260] Böylece NATO'nun sadece Batı Avrupa'yı değil, Avrupa kıtasının tamamını güvenlik çemberi içerisine aldığını ve bölgede çıkacak krizlere askeri olarak müdahil olma yolunda politikalar izlemeye yöneldiği sonucuna varılabilmektedir. Bir bakıma NATO'nun, Soğuk Savaş sonrası varlığını sürdürebilmek için başlattığı dönüşüm sürecinin ilk adımının Roma Zirvesi ile atıldığı ifade edilebilir.

KAİK, süreç içinde eski Varşova Paktı üyeleri ile eski Sovyet Cumhuriyetleri arasında çıkan anlaşmazlıklar sebebiyle üyeler için sadece danışma görevi yürütür hale gelmiştir. Bunun üzerine, 10-11 Ocak 1994 tarihlerinde Brüksel'de gerçekleştirilen NATO Zirvesi sırasında Doğu ve Orta Avrupa devletlerinin güvenlik kaygılarını gidermek ve uyum sürecini hızlandırabilmek için Barış İçin Ortaklık (*Partnership for Peace,* BİO) projesinin uygulamaya geçirildiği deklare edilmiştir.[261] NATO, BİO girişimi kapsamında askeri konuların yanı sıra siyasi, ekonomik ve çevresel meseleler üzerine müşterek bir iş birliği, danışma ve görüşme faaliyetleri oluşturabilmek amacıyla harekete geçmiştir.[262] BİO projesi dahilinde NATO kuvvetleri ile ortaklığa

---

[258]NATO, *Rome Declaration on Peace and Cooperation*, (27.10,2000), https://www.nato.int/docu/comm/49-95/c911108a.htm, (Erişim tarihi: 30.08.2020).
[259] Güngör Şahin, *a.g.e.*, ss. 186-187.
[260]NATO, *North Atlantic Cooperation Council (NACC)*, (30.01.2017), https://www.nato.int/cps/en/natolive/topics_69344.htm, (Erişim tarihi:30.08.2020).
[261] Esra Çayhan ve Nurşin Ateşoğlu Güney, *Avrupa'da Yeni Güvenlik Arayışları: NATO- AB Türkiye*, AFA Yayınları, İstanbul 1996, s. 52.
[262] Beril Dedeoğlu, *a.g.e.*, s. 322.

üye ülkelerin askeri kuvvetleri arasında müşterek eğitim ve tatbikatlar yürütülerek herhangi bir kriz durumunda kolektif müdahale edebilecek seviyeye ulaşılmak hedeflenmiştir.[263]

Soğuk Savaş sonrası güvenlik ortamında ilk ciddi etnik kriz, 1992 yılında Bosna-Hersek'in Yugoslavya Sosyalist Federal Cumhuriyeti'nden bağımsızlığını ilan etmesinin ardından ülkede yaşayan Sırplar tarafından çoğu Müslüman olan Boşnaklara yönelik saldırılar gerçekleştirilmesiyle Doğu Avrupa'da yer alan Bosna-Hersek topraklarında yaşanmıştır.[264] Bunun sonucunda, Birleşmiş Milletler (*United Nations*, BM) ve NATO tarafından saldırıların son bulmasına yönelik çağrılar yapılmasına rağmen Bosnalı Sırpların saldırılarını devam ettirmesi üzerine NATO, 1995 yılında bölgenin güvenliğini sağlayabilmek adına hava operasyonları başlatmıştır.[265] Bosna Hersek Operasyonu ile NATO'nun, tarihinde ilk kez Kuzey Atlantik Antlaşması'nın 5. Maddesinin dışına çıkarak İttifak sınırlarının ötesinde bir bölgeye askeri harekat gerçekleştirdiği görülmektedir.[266] Böylece NATO'nun, Roma Zirvesi ile vermiş olduğu güvenlik temelindeki dönüşüm sinyallerinin ilk somut adımını Bosna Hersek müdahalesiyle atmış olduğu ifade edilebilir.

NATO'nun, doğuya doğru genişleme politikası karşısında Avrupa'da oluşabilecek kutuplaşmanın önüne geçebilmek amacıyla 1997 yılında NATO ile Rusya arasında karşılıklı ilişkileri ve iş birliğini geliştirme çabaları olmuştur. Bu çabaların arka planında ise, NATO'nun bazı siyasi liderlerinin Avrupa-Atlantik bölgesinin bütününde daimi bir barış ve güvenlik ortamının NATO-Rusya iş birliğiyle sağlanabileceği düşüncesini dile getirmelerinin yer aldığı değerlendirilebilir.[267]

NATO'nun dönüşüm ve genişleme hedefleri temelinde en önemli dönüm noktalarından biri 8-9 Temmuz 1997 tarihlerinde gerçekleştirilen Madrid Zirvesi ile

---

[263] Rob de Wijk, *NATO On The Brink Of The New Millennium: The Battle For Consensus*, Brassey's Atlantic Commentaries, Londra 1997, s. 79.
[264] Mustafa Selver, *Balkanlara Stratejik Yaklaşım ve Bosna*, IQ Kültür Sanat Yayıncılık, İstanbul 2003, s. 143.
[265] Joseph Lepgold, "NATO's Post-Cold War Collective Action Problem", *International Security*, Cilt 23, Sayı 1, Yaz 1998, s. 82.
[266] Ryan C. Hendrickson, "Crossing the Rubicon", (01.09.2005), *https://www.nato.int/cps/en/natohq/opinions_21881.htm?selectedLocale=en*, (Erişim tarihi: 31.08.2020).
[267] Muharrem Gürkaynak, *a.g.e.*, s. 137.

atılmış ve Zirve Sonuç Bildirisi kapsamında Polonya, Macaristan ve Çek Cumhuriyeti ile üyelik müzakerelerine bir an önce başlanacağı ve diğer adaylara da gerekli kriterleri karşılaması durumunda NATO'nun kapısının daima açık olacağı deklare edilmiştir.[268] Madrid'de gerçekleştirilen toplantı sırasında İttifak üyeleri tarafından masaya yatırılan önemli konulardan biri de Avrupa Güvenlik ve Savunma Kimliği'nin (*The European Security and Defence Identity*, AGSK) sorumluluğunun artırılması ve BİO projesi kapsamında yürütülen siyasi yapılanma sürecinin hızlandırılmasına karar verilmesi olmuştur.[269] Ayrıca, Avrupa'nın güvenlik ve savunmasını sağlayabilmek amacını taşıyan Batı Avrupa Birliği'ne (*Western European Union,* BAB), NATO tarafından verilecek desteğin kapsamı da belirlenmiştir. Bunun sonucunda, NATO'nun katılmadığı kriz durumlarına BAB'ın, kendi komuta kontrol yapısıyla müdahale edebilmesinin ve gerektiği durumda NATO'nun yeteneklerini kullanabilmesinin önü açılmıştır.[270]

1999 yılı, NATO'nun 50. Kuruluş yıl dönümü olması, Sırp güçlerinin Kosova'ya müdahale gerçekleştirmesi ve Yeni Stratejik Konsept'in belirlenmesi sebebiyle İttifak açısından oldukça kritik bir tarihi temsil etmiştir. 23-24 Nisan 1999 tarihlerinde gerçekleştirilen Washington Zirvesi'ne, İttifak'ın yeni üyeleri olan Polonya, Macaristan ve Çek Cumhuriyeti ilk kez katılmışlardır.[271] Bu zirvenin bir diğer önemli gelişmesi ise Yeni Stratejik Konsept'in ilan edilmesi olmuş, konsept kapsamında öncelikli olarak; NATO'nun artık Avrupa-Atlantik bölgesinin güvenliğinin korunmasında ve geliştirilmesinde en önemli örgüt halini aldığı vurgulanmıştır. Stratejik Konsept içerisinde dikkat çeken noktalardan biri de küreselleşmenin etkisiyle genişleyen güvenlik gündeminin, NATO'nun tehdit unsurlarının tanımlanması açısından önemli bir yere sahip olduğu anlaşılmıştır.[272] Bu kapsamda İttifak, askeri meselelerin yanı sıra etnik çatışma, siyasi baskı, ekonomik

---

[268] Gülnur Aybet, "NATO's New Missions", *Journal Of International Affairs*, Cilt 4, Sayı 1, Mart-Mayıs 1999, *http://www.sam.gov.tr/pdf/perceptions/Volume-IV/march-may-1999/GulnurAybet3.pdf*, (Erişim tarihi: 31.08.2020). s. 5.

[269]NATO, *NATO's Enlargement*, (04.07.1997), https://www.nato.int/docu/comm/1997/970708/infopres/e-enl.htm, (Erişim tarihi: 01.09.2020).

[270] NATO, *NATO Handbook*…, ss. 245-246.

[271]The North Atlantic Council, *Washington Summit Communiqu*, (24.04.1999), https://www.nato.int/docu/pr/1999/p99-064e.htm, (Erişim tarihi: 01.09.2020).

[272]NATO, *The Alliance's Strategic Concept*, (25.06.2009), https://www.nato.int/cps/en/natolive/official_texts_27433.htm, (Erişim tarihi 11.12.2021).

istikrarsızlık, terörizm, uluslararası göç, ırkçılık, insan kaçakçılığı ve hayati kaynaklara erişimin engellenmesi gibi unsurları yeni risk tanımlamaları olarak gündemine almıştır.[273] Ayrıca, NATO'nun temel görevlerinin arasına kriz yönetimlerini aktif olarak sürdürmek ve ortaklık yoluyla karşılıklı güvenin tesis edilmesi de eklenmiştir.[274]

11 Eylül 2001 tarihinde New York'taki ikiz kuleler ile Washington'daki Pentagon binasına düzenlenen terör saldırıları hem ABD'nin ulusal güvenliğinin ağır darbe almasına hem de NATO'nun saldırı, tehdit ve terör tanımlamalarında dönüşüme yol açmıştır.[275] Bu saldırılar sonucunda ortaya çıkan yeni tehditlerin hakim olduğu kaygı ortamı, tüm devletler tarafından ciddi derecede hissedilmiştir. Bir diğer ifadeyle uluslararası politika içerisinde post modern terörizm kavramı ortaya çıkmış ve her ülkenin terör tehdidiyle karşı karşıya kalabileceği anlaşılmıştır. 11 Eylül terör saldırıları sonrası 21-22 Kasım 2002 tarihlerinde düzenlenen Prag Zirvesi, NATO'nun küresel terörizm ile mücadele edebilmek adına yeni görev ve sorumluluk kararlarının alındığı ilk zirve olmasıyla dikkat çekmektedir.[276] Toplantı sonrasında terörizm tehdidiyle kolektif olarak mücadele edebilmek adına NATO'nun müttefiklerinin dahil olduğu terörizme karşı ortak eylem planı, İttifak misyonunun bir parçası olarak kabul edilmiştir. [277] Bu plan içerisine, üyeler arası istihbarat paylaşımı, sınır güvenliği, kitle imha silahları, hafif silahlar ve çevresel kirlilik gibi konular dahil edilerek İttifak'ın varlığına tehdit oluşturabilecek tüm unsurlara yönelik gerekli adımların atılacağı bildirilmiştir.[278] Böylece NATO'nun, yeni güvenlik tehditlerine karşı ihtiyaç duyulan her an müdahalede bulunabilecek çok yönlü bir örgüt olma yolunda ilerlediği

---

[273] Richard Rupp, "NATO 1949 and NATO 2000: From Collective Defense Toward Collective Security", *Journal of Strategic Studies*, Cilt 23, Sayı 3, Ocak 2008, s. 163.
[274]NATO, *Washington Summit*, (06.11.2008), https://www.nato.int/cps/en/natohq/news_27286.htm?selectedLocale=en, (Erişim tarihi: 01.09.2020).
[275] Victoria Macchi ve Jessie Kratz, "9/11 Archives: In our New York office: A day like no other", *https://www.archives.gov/news/articles/national-archives-nyc-september-11*, (Erişim tarihi: 13.12.2021); The Guardian, *Ground Zero stops burning, after 100 days*, (20.12.2001), https://www.theguardian.com/world/2001/dec/20/september11.usa, (Erişim tarihi: 13.12.2021); BBC News, "In pictures: Atrocities' aftermath", (12.09.2001), http://news.bbc.co.uk/2/hi/americas/1538664.stm, (Erişim tarihi: 13.12.2021).
[276] Didem Yaman, "NATO'nun Yeni Görevi: Terörizmle Mücadele ve Bu Eksende Atılan Adımlar", *Uluslararası Hukuk ve Politika Dergisi*, Cilt 2, Sayı 7, 2006, s. 47.
[277] Levent Yiğittepe, *a.g.e.*, s. 86.
[278] Derya Gonca Peksarı, *NATO'nun Değişen Konsepti*, Asil Yayın Dağıtım, Ankara 2007, s. 245.

görülebilmektedir. Yine 2002 yılında, her sektörden gelebilecek güvenlik tehdidine yönelik yapılanma ihtiyacı olduğu vurgulanmış, bu bağlamda NATO Müttefik Dönüşüm Komutanlığı (*Allied Command Transformation*, ACT) ile esnek, sürdürülebilir ve konuşlandırılabilir bir NATO Mukabele Gücü'nün kurulmasına karar verilmiştir.[279]

2006 yılında Riga'da gerçekleştirilen NATO Zirvesi dahilinde başarısız devletlerin durumu, bölgesel ve küresel problemlerin tespiti, kitle imha silahlarına yönelik önlemler ve terörizmle mücadelenin tüm kararlılıkla sürdürülmesi konuları ele alınmıştır.[280] Buna ek olarak Zirve Sonuç Bildirisi'nde, NATO önderliğindeki müdahalelerin daha etkili olabilmesi için bütün üyelerin kara kuvvetlerinin %40'ını herhangi bir bölgeye gerçekleştirilecek operasyon için hazır halde bulundurması gerektiği ve kısa sürede dünyanın her yerine müdahale edebilecek 25.000 kişilik Acil Mukabele Gücü'nün (*NATO Response Force*, NRF) tamamıyla aktif hale geldiği belirtilmiştir.[281] Buradan, NATO'nun terörizmin yanı sıra uluslararası sisteme tehdit oluşturabilecek diğer sorunlar üzerine sorumluluk alan çalışmaları yürütme kararları aldığı bir küresel güvenlik örgütü gibi hareket etmeye başladığı değerlendirmesi yapılabilir. NATO'nun, küresel iş birliğini sürdürmeye yönelik politikalarıyla birlikte asker sayısını artırmaya yönelik çalışmalarıyla, örgütün gelecekte yumuşak gücünün yanında sert gücüyle de varlık göstereceğinin işaretlerini sunmuştur.

2008 yılında Romanya'nın Bükreş şehrinde gerçekleştirilen NATO Zirvesi'ne; 24 devlet başkanı, 26 hükümet başkanı ve 87 bakanın katılmasıyla İttifak tarihinin o güne kadar ki en kapsamlı liderler zirvesi toplanmıştır.[282] Zirvede en ağırlıklı konulardan biri, ABD'nin Doğu Avrupa'da devreye sokmayı planladığı füze kalkanı sistemi projesi; diğeri, Hırvatistan, Arnavutluk, Ukrayna ve Gürcistan'ın

---

[279] Claire Taylor, "NATO: The Prague Summit and Beyond", Araştırma Makalesi 03/05, *House Of Commons Library*, Ocak 2003, *https://researchbriefings.files.parliament.uk/documents/RP03-05/RP03-05.pdf*, (Erişim tarihi: 06.09.2020), s. 58.

[280] NATO, *Riga Summit Declaration*, (08.05.2014), https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en, (Erişim tarihi: 06.09.2020).

[281] Congressional Research Service, *The NATO Summit at Riga 2006*, https://www.everycrsreport.com/files/20070301_RS22529_f6d0725b6d3fabb66fc2bdaa613dc3554ffc42ec.pdf, (Erişim tarihi: 06.09.2020).

[282] Levent Yiğittepe, *a.g.e.*, s. 91.

İttifak'a üyelikleri konuları olmuştur.[283] Zirve toplantısı sonunda, Hırvatistan ve Arnavutluk ile üyelik müzakerelerine başlanması kararlaştırılırken, Ukrayna ve Gürcistan'ın durumu ise bu ülkelerle Rusya arasında yaşanan gerginlikler nedeniyle askıya alınmak zorunda kalınmıştır.[284] Rusya'nın sert bir tavırla her iki ülkenin NATO üyeliklerini kırmızı çizgisi olarak açıklaması, Ukrayna ve Gürcistan'ın üyeliklerinin askıya alınmasını getirmiştir.[285] Ayrıca, Ukrayna ve Gürcistan'ın NATO ekseninde strateji ve politikalar sürdürmesi, Rusya'nın dış politikasında değişimi de getirerek ilerleyen süreçte her iki ülkeyle arasında büyük krizlerin yaşanmasına neden olmuştur.

Nisan 2009'daki Strasburg/Kiehl Zirvesi'nde NATO liderleri öncülüğünde, 1999 Stratejik Konsepti'nin yerini alacak yeni bir Stratejik Konsept taslağı hazırlanmaya karar verilmiş ve böylelikle yeni belge aracılığıyla İttifak'ın gelecekteki amacı, rolü ve yeteneklerine ilişkin sürdüreceği politikaların ana çerçevesinin oluşturulması hedeflenmiştir.[286] Yeni Stratejik Konsept, 19 Kasım 2010 tarihinde NATO'nun Lizbon Zirvesi'nde Devlet ve Hükümet Başkanları tarafından "*Aktif Katılım, Modern Savunma*" başlığıyla kabul edilmiştir.[287] Stratejinin temelinde; toplu savunma ve caydırıcılık, kriz yönetimi aracılığıyla güvenlik, iş birliği içinde güvenliğe teşvik etmek olmak üzere NATO'nun sürdürmesi gereken üç önemli sütun üzerine inşa edilmiştir.[288] Bunun yanı sıra belgede, NATO'nun amacının tüm üyelerinin özgürlüğünü ve güvenliğini korumak olduğu, ve de örgütün varlığının uluslararası sistemin güvenliği açısından eşsiz bir değere sahip olduğu anlayışı vurgulanmıştır.[289] Strateji kapsamında birinci sütun ile Kuzey Atlantik Antlaşması'nın 5. Maddesi; ikinci sütun ile güvenliği etkileyebilecek krizlerde çatışmayı önlemek, durdurmak veya

---

[283] Spencer P. Boyer ve Caroline Wadhams, "The NATO Summit in Bucharest", (02.04.2008), *https://www.americanprogress.org/issues/security/news/2008/04/02/4215/the-nato-summit-in-bucharest/,* (Erişim tarihi: 07.09.2020).

[284]NATO, *Bucharest Summit Declaration,* (08.05.2014), http://www.nato.int/cps/en/natolive/official_texts_8443.htm, (Erişim tarihi: 01.10.2020).

[285] Paul Gallis, "The NATO Summit at Bucharest 2008", *CRS Report for Congress*, Mart 2008, *https://apps.dtic.mil/sti/pdfs/ADA478830.pdf*, (Erişim tarihi: 07.09.2020), ss. 3-5.

[286] Claire Taylor, "NATO Summit 2010", SN/IA/5788, *House Of Commons Library*, Aralık 2010, *https://researchbriefings.files.parliament.uk/documents/SN05788/SN05788.pdf*, (Erişim tarihi: 08.09.2020), s. 3.

[287] NATO, "Aktif Katılım, Modern Savunma: Kuzey Atlantik Antlaşması Örgütü…", s. 1.

[288] NATO, "Aktif Katılım, Modern Savunma: Kuzey Atlantik Antlaşması Örgütü…", s. 3.

[289]NATO, *Lisbon Summit Declaration,* (20.11.2010), https://www.nato.int/cps/en/natolive/official_texts_68828.htm, (Erişim tarihi: 08.09.2020).

istikrarı sağlamak için siyasi ve askeri müdahalelerin gerçekleştirileceğinin, üçüncü sütun ile de güvenliğin sağlanması için İttifak sınırları dışındaki ülkeler veya uluslararası örgütler ile etkileşim kurulmasının gerekliliği ifade edilmiştir.[290]

Stratejik Konsept içerisinde, öngörülebilir gelecekte NATO'nun karşı karşıya kalacağı en ciddi tehdit unsurlarının İttifak topraklarına yönelik konvansiyonel saldırılardan değil; nükleer ve kitle imha silahlarının yayılması, balistik füzeler, siber saldırılar, uluslararası terörizm, kritik enerji altyapısına yönelik tehditler ve gelişen teknolojinin yol açacağı risklerden oluşacağı belirtilmiştir.[291] Böylece NATO'nun, Yeni Stratejik Konsept öncülüğünde Soğuk Savaş dönemi güvenlik sorunlarının yanı sıra küresel tehdit oluşturabilecek potansiyele sahip tehdit unsurlarını da güvenlik gündemine eklemesi sonucu resmi olarak reform, modernizasyon ve dönüşüm sürecini başlattığı değerlendirilebilir.[292] 2010 Zirve Sonuç Bildirisi'nde; caydırıcılık doktrininin, İttifak'ın güvenlik politikalarının en önemli unsurunu oluşturacağı ve nükleer silahlar etkisini yitirmediği sürece NATO'nun nükleer gücünü koruyacağı beyan edilmiştir. 2010 Stratejik Konsepti'nde, bir diğer vurgu yapılan konu da Rusya ile ortaklık ilişkilerinin güçlendirileceği olmuştur.[293] Ancak, bu vurgu karşısında birçok araştırmacı, Rusya-NATO arasındaki iş birliği yapısının her iki aktörün birbirlerine zıt güvenlik stratejilerine sahip olması nedeniyle fazla uzun sürmeyeceği değerlendirmesinde bulunmuştur.[294]

2012 yılında Chicago'da ve 2014'te Galler'de gerçekleştirilen NATO Zirve toplantıları genel olarak, Lizbon'da ilan edilen Yeni Stratejik Konsept'in güncellenmesi şeklinde sürdürülmüştür. 20-21 Mayıs tarihlerinde Chicago'da

---

[290] NATO, "Aktif Katılım, Modern Savunma: Kuzey Atlantik Antlaşması Örgütü…", ss. 15-33.
[291] Jens Ringsmose ve Sten Rynning, "NATO's New Strategıc Concept:A Comprehensıve Assessment", *Danish Institute for International Studies*, Kopenhag 2011, s. 34.
[292] Alessandro Marrone, "The Equilibrium of the 2010 NATO Strategic Concept", *The International Spectator*, Cilt 46, Sayı 3, Eylül 2011, ss. 108-109.
[293] David Yost, "NATO's Evolving Purposes and the Next Strategic Concept", *International Affairs*, Cilt 86, Sayı 2, Mart 2010, ss. 501-509.
[294]James S. Obe, "NATO and Russia: 'Refresh' but no Transformation", *https://www.chathamhouse.org/media/comment/view/163647*, Erişim tarihi: 08.09.2020); Steven Erlanger ve Jackie Calmes, "NATO Agrees to Build Missile Defense System", (19.11.2010), *https://www.nytimes.com/2010/11/20/world/europe/20prexy.html*, (Erişim tarihi: 09.09.2020); Elizabeth Zolotukhina ve Christian Ostermann, "The Evolution of NATO: the 2010 Strategic Concept and Beyond", (21.05.2010), *https://www.wilsoncenter.org/event/the-evolution-nato-the-2010-strategic-concept-and-beyond*, (Erişim tarihi: 08.09.2020).

düzenlenen 2012 NATO Zirvesi'nde akıllı savunma sisteminden Afganistan'ın gelecekteki statüsüne kadar çeşitli konular ele alınmış ve birçok güvenlik sorunu da çözüm arayışlarıyla beraber değerlendirilmiştir. Afganistan'ın geleceğine yönelik NATO'nun izleyeceği yöntem ve politikaların şekillendirilmesi, akıllı savunma girişimi öncülüğünde NATO'nun savunma ve güvenlik hedeflerinin gerçekleştirebilmesi için atılması gereken adımların ortaya konulması, İttifak dışındaki devlet ve örgütler ile iş birlikleri, füze savunma sisteminin ana yeteneğinin faaliyete geçirilmesi konuları, bu kapsamda ele alınan konuları oluşturmuştur.[295] Zirve Sonuç Bildirisi'nde en dikkat çeken konulardan biri akıllı savunma sisteminin faaliyete geçirilmesi olmuştur. Bunun sonucunda, Avrupalı üye devletlerin ekonomik olarak rahatlamasına yol açılarak daha adil bir yük paylaşımının sağlanabilmesi ve sınırlı kaynakların olabildiğince verimli kullanılmasının amaçlandığı belirtilmiştir.[296]

2014 yılında gerçekleştirilen Galler Zirvesi'nde toplantı boyunca üzerinde en çok tartışılan konular, Ukrayna Krizi ve Rusya'nın tutumu olmuştur. İttifak hükümet başkanları tarafından Zirve Bildirisi'nde, Rusya'nın eylemleri "saldırgan" olarak nitelendirilirken, bu eylemlerin NATO'nun özgür ve barış yanlısı Avrupa vizyonuna yönelik bir meydan okuma olduğu belirtilmiştir.[297] Ayrıca İttifak üyelerinin, NATO'nun sınırları içerisine sıçrayacak herhangi bir kriz durumuna karşı kolektif savunma ilkesine olan bağlılıkları da yinelenmiştir. Galler Zirvesi'nde, toplantının ağırlıklı konusu Rusya'nın tutumu olurken, ele alınan diğer konular; Akdeniz'de geniş çaplı göç sorunu ve İttifak içi mali kriz olmuştur.[298] NATO'nun kolektif savunmasını güçlendirmek ve doğu sınırında yer alan üyelere güvence vermek amacıyla Çok Yüksek Hazırlıklı Müşterek Görev Gücü (*Very High Readiness Joint Task Force,*

---

[295]NATO, *Chicago Summit Declaration,* (01.08.2012), https://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en, (Erişim tarihi: 09.09.2020).

[296] Stéfanie von Hlatky, "NATO's Chicago Summit: Alliance Cohesion above All Else?", *Center for Security Studies*, Sayı 116, Zürih 2012, s. 3; Arif Bağbaşlıoğlu, "Güncelliğini Yitirmeyen Bir Sorun Olan Yük Paylaşımına Yeni Bir Çözüm Arayışı: Akıllı Savunma ve NATO", *Akademik Bakış*, Cilt 10, Sayı 19, Kış 2016, ss. 214-215.

[297]NATO, *Joint Statement of the NATO-Ukraine Commission,* (04.09.2014), https://www.nato.int/cps/en/natohq/news_112695.htm?mode=pressrelease, (Erişim tarihi: 09.09.2020).

[298]NATO, *Wales Summit Declaration,* (30.08.2018), https://www.nato.int/cps/en/natohq/official_texts_112964.htm, (Erişim tarihi: 09.09.2020).

VJTF) gibi girişimler de dahil edilerek NATO Hazırlık Eylem Planı kabul edilmiştir.[299]

8-9 Temmuz 2016 tarihli Varşova Zirvesi'nde, NATO'nun doğu ve güney sınırlarına yönelik tehdit ele alınarak iki politika üzerinde odaklanılmıştır. Bunlardan biri; İttifak'ın savunmasını ve caydırıcılığını artırmak, diğeri de NATO'nun sınırları dışındaki istikrarı sağlamak olarak belirtilmiştir.[300] Bunun yanı sıra Zirve'nin ana başlıkları arasında Irak'ta eğitim ve kapasiteyi geliştirmeye yönelik çalışmalar, Deniz Güvenliği Operasyonu, siber uzay, balistik füze savunması, Afganistan'a ve Ukrayna'ya daha fazla yardım konuları yer almıştır.[301] Zirve Sonuç Bildirisi'nde Estonya, Letonya, Litvanya ve Polonya'ya dört muharebe taburu yerleştirilerek İttifak'ın doğu kesimindeki askeri varlığın rotasyonel olarak artırılacağı açıklanmıştır. Savunma taburlarının çok uluslu bir yapıya sahip olacağı ve herhangi bir üyeye karşı girişilecek bir saldırıya, İttifak'ın dört bir yanındaki güçler ile karşılık verileceği vurgulanmıştır.[302] Zirve Sonuç Bildirisi belgesinden, NATO; Rusya'dan gelebilecek tehditlere yönelik Galler Zirvesi'yle öncelik verdiği askeri ve siyasi güvenlik politikalarını Varşova'da güncelleyerek sürdürmeye çalışırken bir yandan da Rusya'nın hızlı potansiyele sahip asker konuşlandırmasına yönelik hazırlıklarını da artırmaya gitmekte olduğu anlaşılmaktadır.

Varşova Zirvesi'nde ayrıca, Suriye, Irak ve Libya'da devam eden krizler kapsamında NATO'nun, bu bölgelerdeki güvenlik personellerini kapsayan eğitim faaliyetlerini genişletmesi için Havadan Erken Uyarı ve Kontrol (*Airborne Warning and Control System*, AWACS) uçaklarını bölgeye konuşlandırması kararlaştırılmıştır.[303] Son olarak ise; Ukrayna'nın daha dinamik ve verimli güvenlik

---

[299] NATO, "NATO's Readiness Action Plan", Fact Sheet, *Public Diplomacy Division*, Temmuz 2016, *https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-rap-en.pdf*, (Erişim tarihi: 09.09.2020), ss. 1-2.
[300] Levent Yiğittepe, *a.g.e.*, s. 103.
[301] NATO, "Warsaw Summit Key Decisions", Fact Sheet, *Public Diplomacy Division*, Şubat 2017, *https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170206_1702-factsheet-warsaw-summit-key-en.pdf*, (Erişim tarihi: 09.09.2020), ss. 1-2.
[302]NATO, *Warsaw Summit Communiqué*, (29.03.2017), https://www.nato.int/cps/en/natohq/official_texts_133169.htm, (Erişim tarihi: 10.09.2020).
[303] Paul Belkin, "NATO's Warsaw Summit: In Brief", Teknik Rapor, *Congressional Research Service*, Kasım 2016, *https://apps.dtic.mil/sti/pdfs/AD1021858.pdf*, (Erişim tarihi:10.09.2020), s. 4.

politikaları oluşturmasına destek çıkmak için kapsamlı bir yardım paketi NATO'nun 13. Genel Sekreteri Jens Stoltenberg tarafından onaylanmıştır.[304]

11-12 Temmuz 2018 tarihlerinde gerçekleştirilen NATO'nun Brüksel Zirvesi'nde; Rusya'nın uluslararası hukuku sürekli ihlal ettiği, Doğu Avrupa'nın yanı sıra Baltık bölgesi ülkelerinde yumuşak ve sert güç kullandığı, Avrupa ülkelerinde dezenformasyonun yayılmasına aracılık ederek Batı demokrasilerine zarar verme girişimlerinde bulunduğu tartışılmış, toplantı sonucunda Galler ve Varşova zirvelerinde Rusya'ya yönelik belirtilen politikaların sürdürüleceği vurgulanmıştır.[305] Buna ek olarak, İttifak'ın doğu kanadındaki savunma ve caydırıcılık gücünün geliştirilmesi çalışmalarının devam edeceği ve de Rusya ile tüm iş birliği ilişkilerinin askıya alındığı bildirilmiştir.[306] Ayrıca, NATO Askeri Komuta Yapısına personel ve komuta ilavesi ile daha güçlü bir güvenlik yapısının oluşturulması kararlaştırılmış ve NATO Genel Sekreteri Stoltenberg tarafından, askeri hareketlilik konusunda NATO-AB iş birliğini hızlandırma ve hibrit tehditlere yönelik mücadelede ortak adımlar atılmasına yönelik çalışmaların yürütüldüğü ifade edilmiştir.[307] Dolayısıyla, Brüksel Zirvesi'nin NATO açısından; Rusya ile olan ilişkilerde gerginlik seviyesinin arttığı, AB ile çok yönlü iş birliği adımlarının atıldığı, İttifak'ın caydırıcılığının ve savunmasının geliştirilmesine yönelik kararlılığın sürdürüldüğü bir zirveyi yansıttığı sonucuna varılabilir.

3-4 Aralık 2019 tarihlerindeki Londra Zirvesi'nde, NATO'nun 30 üye ülkesinin devlet ve hükümet başkanları bir araya gelerek,[308] NATO'nun 70. yıldönümü

---

[304] NATO, *Joint statement of the NATO-Ukraine Commission at the level of Heads of State and Government,* (09.07.2016), https://www.nato.int/cps/en/natohq/official_texts_133173.htm?selectedLocale=en, (Erişim tarihi: 10.09.2020).

[305]NATO, *Brussels Summit Declaration,* (30.08.2018), https://www.nato.int/cps/en/natohq/official_texts_156624.htm, (Erişim tarihi: 11.09.2020).

[306] Nodar Pkhaladze, "A Look Back on the 2018 NATO Brussels Summit", Politika Raporu, *Institute for Politics and Society*, Ağustos 2018, *https://www.politikaspolecnost.cz/wp-content/uploads/2018/08/The-2018-NATO-Brussels-Summit-IPPS.pdf*, (Erişim tarihi: 11.09.2020), ss. 1-2.

[307] NATO, "Brussels Summit Key Decisions 11 – 12 July 2018", Fact Sheet, *Public Diplomacy Division,* Kasım 2018, *https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_11/20181105_1811-factsheet-key-decisions-su.pdf*, (Erişim tarihi: 10.10.2020), s. 2.

[308] 27 Mart 2020 tarihinde NATO'ya resmi olarak üye olan Kuzey Makedonya, Londra Zirvesi'ne gözlemci statüsünde katılmıştır. Detaylı bilgi için bkz. U.S. Department of State, *NATO Summits and Meetings,* https://2017-2021.state.gov/nato-summits/index.html, (Erişim tarihi: 11.10.2020).

kapsamında İttifak'ın geçmişten günümüze başarı ve faaliyetlerinin anılmasının yanı sıra Rusya'dan algılanan tehditler, Orta ve Kuzey Afrika'daki istikrarsızlığın artması, terörizmin yayılması, siber ve hibrit tehditler gibi hem bölgesel hem de küresel güvenliğe tehdit oluşturan sorunlarla mücadele etme çabalarını değerlendirmişlerdir.[309] İttifak içerisinde artan siyasi görüş ayrılıkları ve ABD'nin 45. Devlet Başkanı Donald Trump'ın İttifak'a yönelik eleştirisinin yanı sıra Suriye ve Afganistan ile ilgili politik kararlar alınması konusunda transatlantik koordinasyon eksikliğinin dikkat çekmesi gibi konuların, NATO'nun güvenilirliği üzerinde soru işaretleri oluşturduğu değerlendirilmiştir.[310] Bunun üzerine Genel Sekreter Stoltenberg tarafından; İttifak'ın birliğini sağlamlaştırmak, müttefikler arasındaki siyasi istişare ve koordinasyonu artırmak ve NATO'nun siyasi rolünün güçlendirilmesi üzerine çalışmalar yapmakla görevli 10 uzmandan oluşan bir grubun kurulduğu açıklanmıştır.[311]

NATO'nun 2021 yılındaki Brüksel Zirvesi'nde, İttifak'ın siber savunmayı geliştirmeye yönelik verdiği önem tekrardan teyit edilmiş ve İttifak'ın dayanıklılığını daha da artırmak için caydırıcılık ve savunma yapısını destekleyen yeni bir Kapsamlı Siber Savunma Politikası onaylanmıştır. Ayrıca, NATO'nun siber saldırılarla etkin mücadelesinde üç önemli görev olarak; uluslararası hukuka uygunluk gözetilerek siber tehditleri caydırmak, siber savunma sistemlerinin gelişimini sürdürmek ve siber tehditlere karşı koymak için tüm yeteneklerin kullanılmasında kararlı olunacağı bildirilmiştir.[312]

---

[309] NATO, *London Declaration*, (04.09.2019), https://www.nato.int/cps/en/natohq/official_texts_171584.htm, (Erişim tarihi: 11.10.2020).

[310] Joe Gould, "US, European lawmakers swipe Trump and Turkey in new Syria joint statement", (21.10.2019), *https://www.defensenews.com/congress/2019/10/21/us-european-lawmakers-swipe-trump-and-turkey-in-new-syria-joint-statement/*, (Erişim tarihi: 11.10.2020).

[311] NATO, *Secretary General appoints group as part of NATO reflection process*, (09.06.2020), https://www.nato.int/cps/en/natohq/news_174756.htm, (Erişim tarihi: 11.10.2020).

[312]NATO, *Brussels Summit Communiqué*, (14.06.2021), https://www.nato.int/cps/en/natohq/news_185000.htm, (Erişim tarihi: 20.09.2021).

ÜÇÜNCÜ BÖLÜM

3. NATO'NUN SİBER GÜVENLİK ANLAYIŞININ DEĞERLENDİRİLMESİ: FIRSATLAR VE ZORLUKLAR

2000'li yıllar itibarıyla küresel güvenliğe tehdit oluşturan unsurların bilgi ve iletişim teknolojilerindeki gelişmeleri kullanarak güvenlik algısı, kapsam ve boyutu üzerindeki etkisini giderek artırdığı bir gerçektir. Teknolojik gelişmelerin, askeri sistemler ile entegre hale gelmesi sonucu çatışmaların doğasının tamamıyla değişime uğradığı gözlemlenebilmektedir.[313] İçinde bulunduğumuz dijital çağda, teknolojik yeniliklere ayak uydurabilmek, bilgiye ulaşmak ve onu tehditlerden koruyabilmek öncelikli konulardan biri halini almıştır.[314] Küresel sistem içerisinde karşılıklı bağımlılığın artışı beraberinde, siber tehditlerin devlet ve toplum üzerindeki etkisinin hızla artışını getirmiştir.[315]

Bilgi teknolojilerinin aktif olarak yaygınlaşması, uygulanması ve kullanılması, bu teknolojilerin yalnızca bilgi alışverişi ve işleme aracı olarak değil, aynı zamanda tehdit oluşturmanın bir yolu olarak kullanılmaya başlanmasına da neden olmuştur. Sanal dünyanın gittikçe gerçek dünya ile iç içe geçmesiyle beraber NATO'nun siber güvenlik tehditleriyle mücadelede ortak durumsal farkındalık, kesintisiz bilgi paylaşımı, kolektif karar alma ve erken müdahale konuları siber güvenlik politikasının önceliklerinde yer almıştır.[316] Bu bağlamda, 2002'deki Prag Zirvesi'nde NATO, İttifak bütününde siber güvenliği güçlendirme gereğini tespit etmiş[317] ve 2008'de ilk siber savunma politikasını benimsemiştir.[318] Artan uluslararası

---

[313] Andrew F. Krepinevich, "Cavalry to Computer: The Pattern of Military Revolutions", *Strategic Studies A Reader*, Derleyen: Thomas Mahnken ve Joseph Maiolo, Routledge, Nisan 2008, s. 375.
[314] Joseph S. Nye, "Cyber Power", *Harvard Kennedy School- Belfer Center for Science and International Affairs,* Mayıs 2010, *https://apps.dtic.mil/sti/pdfs/ADA522626.pdf*, (Erişim tarihi: 02.10.2020), ss. 1-2.
[315] Mustafa Şenol, "Siber Güçle Caydırıcılık Ama Nasıl?", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, Cilt 2, Sayı 2, 2016, ss. 10-11.
[316] Doğan Şafak Polat, "NATO'nun Yeni Operasyon Alanı: Siber Uzay", *Güvenlik Bilimleri Dergisi*, UGK Özel Sayısı, Şubat 2020, s. 151.
[317] NATO, *The Prague Summit and NATO's Transformation*, A Reader's Guide, NATO Public Diplomacy Division, 2003, s. 12.
[318]NATO, *Bucharest Summit Declaration*, (08.05.2014), http://www.nato.int/cps/en/natolive/official_texts_8443.htm, (Erişim tarihi: 01.10.2020).

gerilimler ve siber tehditlerin yol açtığı hasarlara karşı, Galler Zirvesi'nde Gelişmiş NATO Siber Savunma Politikası benimsenmiş ve bir sonraki adım olarak NATO üye devletlerine yönelik bir siber saldırının silahlı saldırıyla ilişkilendirilebileceği ve kolektif müdahale ilkesini harekete geçirebileceği belirtilerek NATO'nun siber saldırılarla mücadelede tutumu net bir şekilde ortaya konulmuştur.[319] 2016 yılındaki Varşova Zirvesinde siber alanın beşinci bir operasyon alanı olarak tanınması ve 2018 yılında Siber Uzay Operasyon Merkezi'nin kurulması kararları, İttifak'ın siber saldırı ve tehditlerle mücadelede geldiği son durumu göstermektedir.[320]

3.1. NATO'nun Siber Güvenlik Anlayışı

Bilgi ve iletişim ağlarındaki güvenlik açıklarından faydalanarak tehdit oluşturan siber saldırılar, günümüz uluslararası sistemi içerisinde giderek daha önemli bir güvenlik sorunu haline gelmiştir. Yeni tehdit unsurları içerisinde en dikkat çekenlerden birisi de siber tehditler olmuştur. Siber tehditlerin asimetrik yapısı, öngörülemez olmaları, coğrafi mesafenin engel teşkil etmemesi ve oldukça düşük sermaye ile saldırılar gerçekleştirebilmesi gibi nedenlerden dolayı siber alandaki olayların belirlenmesi ve tehdit karşısında önlem alınmasının önüne geçilebilmesi zorluklar oluşturmaktadır.

NATO'nun Soğuk Savaş dönemi boyunca temel amacı; Doğu Bloğu'na karşı caydırıcı bir güç olarak hareket etmek ve Kuzey Atlantik bölgesinin istikrarını ve güvenliğini askeri gücü öncülüğünde sağlayarak uluslararası sistemde bir güçler dengesi oluşturmak üzerine kuruluyken, Soğuk Savaş sonrası dönemde yeni tehdit unsurlarının çok yönlü bir hal alması, NATO'nun güvenlik anlayışında değişim ve dönüşüme gidilmesi gereğini ortaya çıkarmıştır.[321]

21. yüzyılda siber tehditler, NATO için en önemli güvenlik sorunlarından birini oluşturur hale gelmiştir. Bunun en öncelikli sebebi ise, internetin ve siber uzayın

---

[319] NATO, *Cyber Defence*, (25.09.2020), https://www.nato.int/cps/en/natohq/topics_78170.htm, (Erişim tarihi: 05.10.2020).
[320]NATO, *Warsaw Summit Communiqué*, (29.03.2017), https://www.nato.int/cps/en/natohq/official_texts_133169.htm, (Erişim tarihi: 09.10.2020); NATO, *Brussels Summit Declaration*, (30.08.2018), https://www.nato.int/cps/en/natohq/official_texts_156624.htm, (Erişim tarihi: 12.10.2020).
[321] David Yost, *a.g.m.*, s. 490.

NATO için potansiyel olarak tehdit oluşturan devlet ve devlet dışı aktörler tarafından kullanılabilir olmasından kaynaklanmaktadır. Geçtiğimiz yirmi yıla yakın bir süre boyunca NATO, toplu savunma ve iş birliğine dayalı güvenlik misyonunun hava, kara, deniz ve uzay alanlarında olduğu kadar siber uzayda da etkili olmasına yönelik çalışmalar yürütmektedir. Bu kapsamda, İttifak'ın süreç içerisinde gelişen ve derinleşen bir siber güvenlik anlayışından bahsedilebilir.

3.1.1. 2000-2010 Yılları Arası Siber Güvenlik Algısı

Joe Burton, NATO'nun siber güvenlik anlayışının gelişiminde dört önemli dinamiğin etkili olduğunu ifade etmektedir.[322] Burton'a göre bunlar arasında ilk olarak; 1999 yılında Kosova, 2007 yılında Estonya, 2008 yılında Gürcistan ve 2014'te Ukrayna'da yaşananlar dahilindeki operasyonel deneyimler nedeniyle NATO, örgüt bütününde siber güvenliğini geliştirme yolunda adımlar atmıştır. Kosova, Estonya, Gürcistan ve de Ukrayna gelişmeleri, siber boyut kazanmış ve bunun sonucunda NATO, siber güvenliği stratejik planlamaya dahil etmek durumunda kalmıştır. İkinci olarak; 11 Eylül Saldırıları, NATO konjonktüründe siber alanın teröristler aracılığıyla etkin bir şekilde kullanılacağı konusunda ciddi endişeler yaratmış, bu bağlamda İttifak'ın siber güvenliğe odaklanmasında itici gücü oluşturmuştur. Üçüncü önemli dinamik olarak, Rusya ve Çin ile jeostratejik rekabetin giderek daha teknolojik bir boyut kazanması sonucu bu rekabet ortamının NATO'nun siber alanda strateji ve politikalar geliştirmesini gerektirdiği ifade edilmiştir. NATO'ya yönelik siber saldırılardaki artışın yanı sıra saldırıların maddi ve manevi hasarının boyutunun son on beş yıl içerisinde hızla yükselmesi ise dördüncü dinamik olarak belirlenmiştir.[323] Bu bağlamda değişen dinamiklerin, NATO'nun siber güvenlik yeteneklerini geliştirmesi hususunda farkındalık yarattığı ve kurumsal değişim için tetikleyici olduğu savunulmuştur.[324]

---

[322] Joe Burton, "NATO's Cyber Defence: Strategic Challenges And Institutional Adaptation", *Defence Studies*, Cilt 15, Sayı 4, Kasım 2015, ss. 304-305.
[323] Joe Burton, "NATO's Cyber Defence: Strategic Challenges And Institutional Adaptation", *Defence Studies*, Cilt 15, Sayı 4, Kasım 2015, s. 305.
[324] Diána Szőke, "NATO's Evolving Approach to Cybersecurity", *Foreign Policy Review*, Cilt 12, Budapeşte 2019, s. 135.

NATO için yeni ortaya çıkan bir güvenlik endişesi kapsamında siber alanın önemi ilk olarak, 1999 yılında bilgisayar korsanlarının Sırbistan'a yönelik hava harekatını protesto etmek doğrultusunda İttifak'ın web sitelerine ve e-posta sunucularına siber saldırı düzenlemesinin ardından ortaya çıkmıştır.[325] Yapılan ağ tabanlı incelemeler sonucunda protesto saldırılarının başta Sırbistan olmak üzere Rusya ve Çin'deki bilgisayar korsanları tarafından gerçekleştirildiği açıklanmıştır.[326] Saldırılar sonrasında, İttifak'ın 1999 yılında ilan ettiği 'Stratejik Konsept' içerisinde devlet ve devlet dışı aktörler tarafından tasarlanan çeşitli tehdit ve saldırı operasyonları aracılığıyla İttifak'ın bilgi ve teknoloji sistemlerinin istismar edilebileceğine NATO'nun konvansiyonel silahlar aracılığıyla sağlamış olduğu caydırıcılığa karşı koymak için bu tür yeni güvenlik tehditleriyle karşı karşıya kalınabileceğine vurgu yapılmıştır.[327]

Siber güvenlik kavramı, NATO'nun resmi gündemine ilk kez 2002 yılındaki Prag Zirvesi'nde 19 üyenin devlet ve hükümet başkanlarının siber saldırılara karşı savunma kapasitelerini güçlendirebilmek amacıyla önlemler alınması gerektiğini taahhüt etmeleri üzerine girmiştir.[328] Bunun yanı sıra aynı yıl içerisinde NATO, İttifak'ın ve üyelerinin artan endişelerini kontrol altına alabilmek ve siber tehditlerle mücadele edebilmek amacıyla iki önemli karar almıştır. Bunlardan biri; kurumsal bir kalkınma programı olarak NATO Siber Savunma Programı'nın ilan edilmesi iken, diğeri ise kötü niyetli siber eylemleri önlemek, tespit etmek ve bunlara yönelik ilk müdahaleyi gerçekleştirmek için NATO Bilgisayar Olaylarına Müdahale Yeteneği (*The NATO Computer Incident Response Capability,* NCIRC) programının faaliyete

---

[325] Kenneth Geers, "Cyperspace and the Changing Nature…", ss. 4-5; Dan Verton, "Serbs launch cyberattack on NATO", (04.04.1999), *https://fcw.com/1999/04/serbs-launch-cyberattack-on-nato/195288/*, (Erişim tarihi: 15.12.2021); Julian Borger, "Pentagon kept the lid on cyberwar in Kosovo", (09.11.1999), *https://www.theguardian.com/world/1999/nov/09/balkans*, (Erişim tarihi: 15.12.2021); Ellen Messmer, "Kosovo cyber-war intensifies: Chinese hackers targeting U.S. sites, government says", (12.05.1999), *http://edition.cnn.com/TECH/computing/9905/12/cyberwar.idg/*, (Erişim tarihi: 15.12.2021).

[326] Jason Healey ve Leendert van Bochoven, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow", *The Atlantic Council*. Şubat 2012, *https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022712_ACUS_NATOSmarter_IBM.pdf*, (Erişim tarihi:18.10.2020), s. 1.

[327] Ilai Saltzman, "Cyber Posturing and the Offense-Defense Balance", *Contemporary Security Policy*, Cilt 34, Sayı 1, Mart 2013, s. 53.

[328] NATO, *The Prague Summit and NATO's…*, s. 12.

geçirilmesi olmuştur.[329] Ancak, bilgi ve iletişim teknolojileri altyapısını korumakla görevli olan NCIRC, hem uzun vadeli askeri planlama kapasitesinden yoksun olduğu hem de siber saldırılara yönelik müttefik sistemlerin korunmasını her ülkenin kendi sorumluluğuna bıraktığı yönünde eleştirilirken, etkililiği de faaliyete geçişinden itibaren tartışılan bir konu olmuştur.[330] Prag Zirvesi'nde, NATO üyesi ülkelerin devlet ve hükümet başkanlarının siber saldırılara karşı savunma yeteneklerini artıracaklarını deklare etmelerine karşın ilerleyen yıllar içerisinde bu konuda çok az adım atıldığı dikkat çekmektedir. Bu kapsamda siber güvenlik konusunun, 2006'daki Riga Zirvesi'ne kadar Kuzey Atlantik Konseyi'nin resmi toplantılarında gündeme gelmediği görülmektedir.

11 Eylül saldırılarının yarattığı korku, kaygı ve de organize suç örgütlerinin teknolojik sistemleri kullanarak devletlere yönelik büyük saldırılar gerçekleştirme olasılığı, bazı NATO üyesi ülkelerin siber güvenlik alanında strateji ve politikaları faaliyete geçirmesinde önemli itici güç oluşturmuştur. Bu alandaki ilk ve en güçlü adımlardan biri, ABD'nin 11 Eylül 2001 tarihindeki saldırılar sonrasında Siber Uzayı Güvenli Hale Getirme Ulusal Stratejisi'ni ilan etmesiyle atılmıştır.[331] Buna ilaveten Kasım 2003'te, dokuz NATO üyesi ülke olan Kanada, Fransa, Almanya, İtalya, Hollanda, Norveç, İspanya, Birleşik Krallık ve ABD tarafından NATO'nun Ağ Destekli Yetenek (*The NATO Network Enabled Capability*, NNEC) programı ile ilgili fizibilite çalışmasının finansmanına katılmak üzere bir düzenleme imzalanmıştır.[332] Bütün bu gelişmelerin, aynı zamanda NATO'nun siber tehditlere yönelik rolünün artmasına da ortam sağladığı ifade edilebilir.

Siber saldırı ve tehdit unsurlarının, NATO'nun gündem maddeleri içerisine girmesi ilk olarak 2002 Prag Zirve Sonuç Bildirisi aracılığıyla olmasına karşın, 2006 Riga Zirvesi sırasında toplu siber savunmaya yönelik atılan öncü adımların NATO'nun siber güvenlik gündemine önemli katkı sağladığı söylenebilir. 2006

---

[329] Jason Healey ve Leendert van Bochoven, *a.g.m.*, s. 2.
[330] Ilai Saltzman, "Cyber Posturing and the Offense-Defense Balance", *Contemporary Security Policy*, Cilt 34, Sayı 1, 2013, s. 53.
[331] Jangirala Srinivas, Ashok Kumar Das ve Neeraj Kumar, *a.g.m.*, ss. 7-8.
[332] NATO, *Signing Ceremony to Initiate a Study on NATO Network Enabled Capability (NNEC)*, (03.11.2008), https://www.nato.int/cps/us/natohq/news_20084.htm?selectedLocale=en, (Erişim tarihi: 30.09.2020).

yılında Letonya'da gerçekleştirilen Riga Zirvesi'nde, İttifak'ın siber güvenliğinin geliştirilmesi çabalarının sürdürülmesi gereği bir kez daha vurgulanmıştır.[333] Buna ek olarak Riga Zirvesi Deklarasyonu'nun 24. Maddesinde; İttifak'ın çağdaş tehdit ve zorluklarla başa çıkabilmesine yönelik girişimlerin yanı sıra siber tehditlere karşı koymada atılabilecek adımlardan bahsedilmiştir. Bu kapsamda NNEC programının, İttifak'ın gerçekleştirdiği operasyonlarda güvenilir ve zamanında veri, bilgi ve istihbarat sağlanması hususunda hizmet edebilmesi için gerekli çalışmaların yapılacağı belirtilmiştir.[334] Son olarak, üye ülkelerin liderleri tarafından, siber saldırılara karşı NATO'nun kilit bilgi sistemlerinin korunmasına yönelik çalışmaların artırılacağının altı çizilmiştir.[335]

1999 yılında Kosova'da yaşanan çatışma sırasında NATO'nun hedef alındığı siber saldırıların üzerinden sekiz yıl geçmesinin ardından 2007 yılında İttifak üyesi olan Estonya'ya yönelik siber saldırılar ile karşı karşıya kalınmıştır. Saldırıların, Estonya'da tarihsel, etnik ve siyasi gerginliklerin artması üzerine Estonya hükümetinin, ülke içerisindeki Rus kültürünün etkilerini sınırlandırmak amacıyla çeşitli politikaları faaliyete geçirmesi nedeniyle kaynaklandığı düşünülmektedir.[336] Estonya hükümetinin, İkinci Dünya Savaşı'nda Nazi Almanyası'na karşı SSCB zaferinin bir anısı olarak Sovyet döneminde yapılmış olunan Bronz Asker anıtının yerini değiştirmeye yönelik adımlar atması üzerine Estonya'da yaşayan Rus kökenli halk tarafından anıtın dikileceği yeni yerin, eskisine oranla coğrafi olarak önemsiz ve gözden uzak olması sebebiyle ayaklanma ve protesto gösterileri başlamıştır.[337] Bu bağlamda Estonyalılar açısından anıtın, ülkenin SSCB tarafından işgalini temsil ettiği; Estonya'daki Rus azınlığı için ise, İkinci Dünya Savaşı'ndaki kahramanlığın ve mücadelenin bir sembolü olarak görüldüğü ifade edilmiştir.[338]

---

[333] Joe Burton, *a.g.m.,* s. 297.
[334] NATO, *Riga Summit Declaration,* (27.02.2009), https://www.nato.int/docu/pr/2006/p06-150e.htm, (Erişim tarihi: 30.09.2020).
[335] NATO, *Cyber Defence*, (25.09.2020), https://www.nato.int/cps/en/natohq/topics_78170.htm, (Erişim tarihi: 30.09.2020).
[336] Stephen Herzog, "Revisiting Estonian Cyber Attacks: Digital Threats and Multinational Responses" *Journal of Strategic Security*, Cilt 2, Sayı 4, Yaz 2011, ss. 49-50.
[337] Salih Bıçakcı, "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun…", ss. 214-215.
[338] Martin Ehala, "The Bronze Soldier: Identity Threat and Maintenance in Estonia", *Journal of Baltic Studies*, Cilt 40, Sayı 1, Mart 2009, ss. 143-145.

Protesto gösterilerini ve ayaklanmaların ardından Estonya'daki bakanlıkları, kamu bankalarını ve siyasi partilerin web sitelerini hedef alan DDoS saldırılarının etkisi tüm ülkede görülmüştür. Siber saldırıların tüm ülkeye çok kısa sürede ve ciddi bir şekilde yayılmasının nedeni Estonya'nın kritik altyapı sistemlerinin büyük çoğunluğunun internet aracılığıyla işlevlerini yürütmesinden kaynaklanmıştır.[339] Bunun sonucunda, kamu hizmetlerinin yürütülmesinde ve vatandaşlarının günlük yaşamında internet erişiminin yaygın kullanımı nedeniyle siber saldırılar için potansiyel bir hedef halini almıştır. Bu bağımlılık; Estonya hükümetinin, kurumlarının, ülkedeki ekonomik birimlerin ve nüfusun savunmasız kalmasının yanı sıra büyük ölçekli kesintilere de açık hale gelmesine yol açmıştır.[340] Zombi bilgisayarların (Botnet)[341] aracı olarak kullanıldığı DDoS saldırıları sonucu Estonya hükümetinin bütün internet sitelerinin yanı sıra iki büyük banka, bazı siyasi parti ve ülkenin en büyük üç medya kuruluşunun sitelerindeki faaliyetleri tamamen durma noktasına gelmiştir.

Genel algı ve kanaatler çerçevesinde Estonya siber saldırısının arka planında Rusya hükümetinin yer aldığı iddia edilmesine rağmen, kapsamlı incelemeler sonrası saldırının arkasında Rusya'nın yer aldığı kanıtlanamamıştır.[342] Arbor Networks tarafından yapılan araştırma sonucu saldırıların sadece belirli bir coğrafi bölgeden değil, dünya çapından yapıldığı anlaşılmıştır.[343] Bunun yanı sıra, Devlet Bilgisayar Bilimleri Merkezi (*The State Informatics Centre*) tarafından saldırıların kaynağının

---

[339] İnternet, 2007 yılında Estonya'da teknolojik ağların, elektrik şebekelerinin ve banka işlemlerinin %97'sinin ayrılmaz bir parçası durumundaydı. Detaylı bilgi için bkz. Rain Ottis, "Analysis of the 2007 cyber attacks against Estonia from the information warfare perspective", *Proceedings of the 7th European Conference on Information Warfare*, Derleyen: Dan Remenyi, Academic Publishing Limited, Dublin 2008, s. 164; Tom Esplner, "Estonia's CTO speaks out on cyberattacks", (24.10.2007), *https://www.zdnet.com/article/estonias-cto-speaks-out-on-cyberattacks/,* (Erişim tarihi: 29.09.2020).

[340] Eneken Tikk, Kadri Kaska ve Liis Vihul, *a.g.e.*, s. 18.

[341] Botnet: Kişisel bilgisayarlar, sunucular, mobil cihazlar ve Nesnelerin İnterneti (IoT) cihazlarının yaygın kötü amaçlı yazılım türü tarafından ele geçirilmesi sonrası uzaktan kontrol edildiği internete bağlı aygıtlar topluluğu olarak ifade edilmektedir. Detaylı bilgi için bkz. Kaspersky, *What is a Botnet?,* https://usa.kaspersky.com/resource-center/threats/botnet-attacks, (Erişim tarihi: 30.09.2020).

[342] Robert A. Miller ve Daniel T. Kuehl, "Cyberspace and the 'First Battle' in 21st Century War", *Defense Horizons,* Sayı 68, Eylül 2009, *https://apps.dtic.mil/sti/pdfs/ADA508696.pdf*, (Erişim tarihi: 30.09.2020), s. 3; Jason Fritz, "How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness," *Culture Mandala*, Cilt 8, Sayı 1, Ekim 2008, s. 58.

[343] Jose Nazario, "Politically Motivated Denial of Service Attacks", *The Virtual Battlefield: Perspectives on Cyber Warfare*, Derleyen: Christian Czosseck ve Kennth Geers, IOS Press, Ekim 2009, ss. 173-174.

178 ülkede yer alan bilgisayarlardan geldiği açıklanmıştır.[344] Saldırılardan bir süre sonra dönemin Estonya Dışişleri Bakanı Urmas Paet, Rusya'nın siber saldırılara doğrudan aracılık ettiğini ileri sürmüştür.[345] Ancak, konuyla alakalı olarak Jason Healey ve Leendert van Bochoven, saldırıyla ilgili birçok kötü amaçlı yazılım kodunun Rusça yazılması veya koordinasyonun Rus web siteleri aracılığıyla yapıldığı gibi çeşitli göstergelere rağmen, siber saldırıları Rusya'ya atfetmek için hala kesin kanıtın oluşmadığını belirtmektedirler.[346] Üç hafta boyunca süren siber saldırılar, Estonya'nın finansal, ekonomik, sosyal ve politik yönden büyük hasar almasına neden olmuş, bu saldırıların yol açtığı ciddi hasarlar sonucu Estonya, 2008 yılında Siber Güvenlik Stratejisi'ni kabul etmiştir.[347]

Estonya'ya yönelik 2007 yılında gerçekleştirilen siber saldırılar, İttifak içerisinde siber güvenlik sorununu gündeme getirmiş ve internetin çok güçlü bir asimetrik tehdit aracı olarak kullanılabileceği gerçeğini ortaya çıkarmıştır. Estonya hükümetine danışmanlık yapan Linnar Viik'e göre Estonya'yı hedef alan uzun süreli saldırılar, bir ülkeyi Taş Devri'ne geri götürme girişimi olarak ifade edilmiştir.[348] Ayrıca Estonya saldırıları sonrasında, bir siber saldırının Kuzey Atlantik Antlaşması'nın 5. Maddesi uyarınca toplu savunma ilkesinin uygulamaya geçirilip geçirilemeyeceği hususunda İttifak içinde uzun süreli tartışmalar yaşanmıştır.[349] Ancak, NATO içerisindeki tartışmalarda, uluslararası hukuk çerçevesinde herhangi bir mevzuat düzenlemesi bulunmayan "siber saldırı/saldırıların" Kuzey Atlantik Antlaşması'nın 5. Maddesinde tanımlanan "silahlı saldırı" niteliği taşıyıp taşımadığı konusunda kesin karara varılamamıştır. Ayrıca, siber tabanlı saldırıların o dönem itibarıyla henüz yeni bir saldırı türü olarak kabul edilmesi sebebiyle yanlış bir atfetmenin ciddi sorunlara yol açabileceği düşünülmüştür.[350] Yine de Estonya olayı,

---

[344] Eneken Tikk, Kadri Kaska ve Liis Vihul, *a.g.e.*, s. 23.
[345] Arthur Bright, "Estonia accuses Russia of cyber-attack" (17.05.2007), *http://www.csmonitor.com/2007/0517/p99s01-duts.html*, (Erişim tarihi: 30.09.2020).
[346] Jason Healey ve Leendert van Bochoven, *a.g.m.*, s. 2.
[347] Eneken Tikk, Kadri Kaska ve Liis Vihul, *a.g.e.*, s. 29.
[348] Lene Hansen ve Helen Nissenbaum, "Digital Disaster, Cyber Security and the Copenhagen School", *International Studies Quarterly,* Cilt 53, Sayı 4, Aralık 2009, s. 1169.
[349] NATO, *Bucharest Summit Declaration,* (08.05.2014), http://www.nato.int/cps/en/natolive/official_texts_8443.htm, (Erişim tarihi: 01.10.2020).
[350] Miron Lakomy, "Conditions to Invoke the Principle of Article 5 of The North Atlantic Treaty in Case of a Cyberattack or a Cyber Conflict", *NATO Road to Cybersecurity,* Derleyen: Joanna Świątkowska, The Kosciuszko Institute, Krakow 2016, s. 35.

NATO'nun siber güvenliğe yönelik yeteneklerini geliştirmesi ve çeşitli kurumları faaliyete geçirmesi üzerine kritik bir dönüm noktasını temsil etmektedir.[351] 2013'te Macaristan Savunma Politikası'nda görevli Gergely Szentgáli'nin belirttiği gibi Estonya'ya yönelik siber saldırılar, siber savaşın uluslararası sistem içerisindeki potansiyel tehdit gerçekliğinin ilk operasyonel örneği olmasına ilaveten hem devletleri hem de uluslararası örgütleri siber alana yönelik daha ciddi önlemler almaya sevk etmiştir.[352]

2007'de Estonya'nın özel ve kamu kurumlarına yönelik siber saldırılar, NATO açısından bir bakıma tehdidin ciddiyetiyle tanışılmasını getirmiş, bunun üzerine 2008 yılında Bükreş'te gerçekleştirilen NATO Zirvesi'nde, üye ülkelerin savunma bakanları tarafından siber savunma konusunda çalışmaların ivedilikle yürütülmesi gerektiği belirtilmiştir.[353] Bu doğrultuda NATO, Ocak 2008'de Siber Savunma Politikası'nı onaylayarak Estonya siber saldırısı sonrası siber savunma alanındaki ilk resmi adımını atmıştır.[354] Siber Savunma Politikası dahilinde NATO ve üye devletlerin temel bilgi sistemlerinin korunması, NATO ile müttefik ülkelerin siber savunma konusundaki ilişkilerinin ilerletilmesi, üye devletlerin siber konularla ilgili deneyimlerinin paylaşılması ve müttefik ülkelerin talebi üzerine bir siber saldırıya karşı konulması konusunda yardım yeteneğinin altı çizilmiştir.[355] Bükreş Zirve Sonuç Bildirisi'nin 47. paragrafında, siber saldırılara karşı İttifak'ın temel bilgi sistemlerinin savunmasını güçlendirme ve Siber Savunma Politikası'nın uygulanmasından sorumlu yapı ve organları oluşturma kararlılığı yeniden teyit edilmiştir. Bilgi sistemlerinin hem NATO hem de üye ülkeler tarafından korunması gerektiği vurgulanmıştır. Buna ek olarak, siber saldırılarla mücadelede müttefiklere yardım etme ve üye ülkelerin ulusal makamlarıyla yakın iş birliği içinde NATO'nun siber savunma potansiyelini geliştirme

---

[351] Christian Czosseck, Rain Ottis ve Anna-Maria Talihärm, "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security", *International Journal of Cyber Warfare and Terrorism,* Cilt 1, Sayı 1, Tallinn 2011, s. 26.

[352] Gergely Szentgáli, "The NATO Policy on Cyber Defense: The Road so Far", *AARMS 1*, Cilt 12, 2013, s. 88.

[353]NATO, *Bucharest Summit Declaration,* (08.05.2014), http://www.nato.int/cps/en/natolive/official_texts_8443.htm, (Erişim tarihi: 01.10.2020).

[354] Rex B. Hugges, "NATO and Cyber Defence: Mission Accomplished?" *Atlantisch Perspectief 33,* Cilt 1, Sayı 4, 2009, s. 1.

[355] Piret Pernik, "Improving Cyber Security: NATO and the EU", *International Centre for Defence Studies,* Tallinn 2014, s. 4.

taahhüdü verilmiştir.[356] İttifak, Siber Savunma Politikası'nın onaylandığı tarihten itibaren siber savunma konularına giderek daha fazla önem vermeye başlamış ve çeşitli strateji, politika ve kurumlar aracılığıyla çalışmalarını yürütmüştür.

Bükreş Zirve Sonuç Bildirisi'nde ayrıca siber savunma alanında iki kurumun faaliyete geçirildiği bildirilmiştir. Bunlardan biri; operasyonel kapasiteyi artırmak ve siber savunma kapasitesini tek bir otorite altında merkezileştirmek amacıyla kurulan NATO Siber Savunma Yönetim Otoritesi (*The Cyber Defence Management Authority*, CDMA) olmuştur.[357] CDMA, siber savunma girişimlerini hem merkezi düzeyde hem de bireysel üye düzeyinde denetlemenin yanı sıra İttifak'a veya üyelere yönelik saldırılara karşılık vermekle görevli bir kurumu temsil etmektedir.[358] Ayrıca CDMA'nın, her üye devletin kendi operasyonel yeteneklerini geliştirmesi hususunda yardımcı olma misyonuyla hareket ettiği belirtilmiştir.[359] Bir diğer kurum olan NATO CCDCOE ise Estonya'nın başkenti Tallinn'de kurulmuş ve bir araştırma ve eğitim merkezi olarak hareket etmek üzere tasarlanmıştır. Kurumun misyonu; eğitim, araştırma ve geliştirme, öğrenilen dersler ve danışmanlık yoluyla NATO üye ülkeleri ve siber savunma ortakları arasındaki yetenek, iş birliği ve bilgi paylaşımını artırmak olarak ifade edilmiştir.[360] Bu kapsamda kurumun temel sorumlulukları arasında üye ülkelerin kendi siber yeteneklerini geliştirmelerine katkı sağlamak, eğitime yönelik çalışmalar yürütmek ve doktrinlerin, stratejilerin ve yasal çerçevenin oluşturulmasına yardımcı olmak yer almaktadır.[361] Estonya'yı hedef alan siber saldırı, NATO'nun siber eksikliklerini askeri, siyasi ve altyapı düzeyinde ortaya çıkarmış, bu doğrultuda İttifak'ın saldırıya yönelik tepkisi ve Bükreş Zirvesi'nde kurulan kurumların neredeyse tamamı siber saldırılara karşı savunma amaçlı geliştirilen önlemler olarak dikkat çekmiştir.

---

[356] NATO, *Bucharest Summit Declaration*, (08.05.2014), http://www.nato.int/cps/en/natolive/official_texts_8443.htm, (Erişim tarihi: 01.10.2020).
[357] NATO, *Bucharest Summit Declaration*, (08.05.2014), http://www.nato.int/cps/en/natolive/official_texts_8443.htm, (Erişim tarihi: 01.10.2020).
[358] Stephen Herzog, *a.g.m.*, s. 54.
[359] Jason Healey ve Leendert van Bochoven, *a.g.m.*, s. 2.
[360] Marios P. Efthymiopoulos, "A cyber-security framework for development, defense and innovation at NATO", *Journal of Innovation and Entrepreneurship*, Cilt 8, Sayı 12, Haziran 2019, s. 17.
[361] Salih Bıçakcı, "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda…", s. 122.

Estonya'ya yönelik siber saldırıların üzerinden henüz bir yıl bile geçmeden 2008 yılında Rusya ile Gürcistan arasında gerçekleşen Güney Osetya Savaşı, siber saldırıların konvansiyonel savaşın önemli bir bileşeni olabileceğini göstermiş ve hibrit olarak ifade edilen yeni bir çatışma alanının doğmasını sağlamıştır.[362] Güney Osetya, Gürcistan ve Rusya arasında yer alan ve tarihsel olarak çözülmemiş birçok sorunu barındıran bir bölge olmuş ve 1991'deki Gürcistan-Osetya çatışmasından sonra bölge, Gürcistan'dan ayrılarak fiili olarak bağımsız hale gelmiştir.[363] Güney Osetya, uluslararası toplum tarafından Gürcistan ile entegre olarak tanınmasına rağmen, 2003 yılının sonundan itibaren ayrılıkçı hareketlerin etkisini artırması neticesinde ortaya çıkan gerilim gitgide sıcak bir çatışmaya dönüşmüştür.[364] Sürpriz ve radikal bir kararla Gürcistan Silahlı Kuvvetleri'nin, 7 Ağustos 2008 tarihinde ayrılıkçı grupların kışkırtmasına konvansiyonel karşılık vermesi üzerine Gürcistan ile Rusya arasındaki gerilim açığa çıkmıştır. Gürcistan'ın ayrılıkçı gruplara müdahalesinin hemen sonrasında büyük çoğunluğunun Rusya merkezli internet sitelerinden yapıldığı ileri sürülen siber saldırılar başlatılmıştır.[365] Saldırılar kapsamında, kötü amaçlı yazılım ve saldırı yönergeleri dağıtılmış, saldırılar son derece koordineli bir şekilde yürütülmüş ve spam amaçlı hedef olarak Gürcü politikacıların e-posta adreslerinin listesi yayınlanmıştır.[366] 8 Ağustos 2008'de Rus kuvvetlerinin sınır ötesi askeri operasyonlara başlamasıyla aynı anlarda, Gürcistan tarafından siber saldırıların, Gürcistan'ın cumhurbaşkanlığı, savunma ve dışişleri bakanlıkları, parlamento ve ulusal bankasının web sitelerini hedef aldığı açıklanmıştır.[367] Yapılan araştırmalar sonucu hazırlanan raporlarda, aynı Estonya olayında olduğu gibi Gürcistan'ı hedef alan siber saldırıların tamamının, sadece Rusya merkezli sitelerden değil dünyanın

---

[362] NATO, *Cyber Defence,* (25.09.2020), https://www.nato.int/cps/uk/natohq/topics_78170.htm?selectedLocale=en, (Erişim tarihi: 01.10.2020).

[363] Jim Nichol, "Russia-Georgia Conflict in South Ossetia: Context and Implications for U.S. Interests", *Congressional Research Service*, Ağustos 2008, *https://www.everycrsreport.com/files/20080813_RL34618_af7d22e7f33f1eadc090b329791f1bbc6fad71e4.pdf*, (Erişim tarihi: 01.10.2020), s. 1.

[364] Brian Ellison, "Russian grand strategy in the South Ossetia War" *Demokratizatsiya,* Cilt 19, Sayı 4, Eylül 2011, s. 351.

[365] Salih Bıçakcı, "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun …", s. 218.

[366] Stephen W. Korns ve Joshua E. Kastenberg, "Georgia's Cyber Left Hook", *Parameters*, Kış 2008-2009, https://apps.dtic.mil/sti/pdfs/ADA636632.pdf, (Erişim tarihi: 14.03.2021), s. 65.

[367] Ariel Cohen ve Robert E. Hamilton, *The Russian Military and the Georgia War: Lessons and Implications,* CreateSpace Independent Publishing Platform, Haziran 2011, s. 44.

çeşitli bölgelerindeki bilgisayarların ele geçirilen ağ sistemleri üzerinden gerçekleştirildiği ifade edilmiştir.[368]

Çeşitli politikacılar ve araştırma şirketleri tarafından Gürcistan'ı hedef alan siber saldırının Rusya'nın çıkarlarıyla yakın bir şekilde uyumluluk gösterdiği iddia edilmesine karşın Rusya'nın, saldırılara doğrudan müdahil olduğuna dair bir kanıt bulunamamıştır.[369] Bütün bunlara rağmen, Gürcistan'ın bilgi teknolojilerini nispeten düşük oranda benimsemesi ve ülkedeki vatandaşların yalnızca %7'sinin internet erişimine sahip olması nedeniyle siber saldırılar sonucu kritik altyapı sistemleri üzerinde çok ciddi hasarlar oluşmamıştır.[370] Güney Osetya Savaşı, ilk defa bir konvansiyonel saldırının bir siber saldırıyla birleştirilmesini temsil etmektedir.[371] Gürcistan'ın, Rusya ile gerilim yaşamasının arka planında, Batı yanlısı politikalar izlemesi ve NATO'ya üyelik çalışmaları yürüttüğü düşünülmektedir. NATO, Gürcistan'ın İttifak'a üyeliği olmaması sebebiyle savaş boyunca doğrudan yardım sağlayamamış olmasına karşın, artan saldırılar sonucu Estonya hükümetinin inisiyatifiyle Gürcistan'a bir grup siber uzman göndermiştir. Bu uzmanların desteğiyle, kısa bir süre sonra ülkedeki ağ ve bilgi sistemlerinin normale döndürülmesinde başarılı olunmuştur.[372] 2007-2008 yıllarında büyük etkiye sahip iki siber saldırının yaşanması; yerel, bölgesel ve küresel düzeyde çalışmaların yürütülmesi, hukuksal norm boşluğunun giderilmesi ve siber güvenlik tehditlerine cevap verebilmek için çok yönlü mekanizmaların geliştirilmesi ihtiyacını açık bir şekilde ortaya koymuştur.

Nisan 2009'da Strazburg/Kehl Zirvesi'nde, siber savunma yeteneklerinin geliştirilmesine dikkat çekilmiş, bu kapsamda NATO'nun eğitim ve tatbikat yapısı içerisinde siber savunmaya yönelik çalışmalara yer verilmesi ve siber tehditlerle mücadelede NATO ile uluslararası örgütler arasındaki iş birliğinin güçlendirilmesine karar verilmiştir.[373] NATO açısından siber güvenliğe yönelik bir sonraki önemli

---

[368] Scott W. Beidleman, *Defining and Deterring Cyber War*, Strateji Araştırma Raporu, U.S. Army War College, Ocak 2009, *https://apps.dtic.mil/sti/pdfs/ADA500795.pdf*, (Erişim tarihi: 01.10.2020), s. 5.
[369] Joseph S. Nye, "Cyber Power…", s. 6.
[370] Eneken Tikk, Kadri Kaska ve Liis Vihul, *a.g.e.*, s. 89.
[371] Nezir Akyeşilmen, *a.g.e.*, s. 241.
[372] P.W. Singer ve Allan Friedman, *a.g.e.*, ss. 167-168.
[373]NATO, *Strasbourg / Kehl Summit Declaration*, (08.05.2014), https://www.nato.int/cps/en/natolive/news_52837.htm, (Erişim tarihi: 02.10.2020).

kurumsal gelişme, 2010 NATO Stratejik Konsepti'ne siber savunmanın dahil edilmesi olmuştur.[374] Stratejik Konsept içerisinde siber güvenlik konusuyla ilgili olarak siber saldırıların sadece ulusal bir sorun teşkil etmediği, aynı zamanda tüm Avrupa-Atlantik bölgesinin refahı, güvenliği ve istikrarına yönelik kolektif bir tehdit ortamı oluşturduğu vurgulanmıştır. Bu çerçevede, siber saldırıların her geçen gün artan hasar verme potansiyeli ve daha iyi organize hale gelmeleri sonucu kamu kuruluşlarına, işletmelere, ekonomilere, ulaşım ve tedarik ağlarının yanı sıra diğer kritik altyapılara daha sıklıkla ve yüksek maliyetli zararlar verebileceği belirtilmiştir.[375]

Rakip devletlerin orduları ve istihbarat servisleriyle birlikte organize suç örgütleri ve aşırılık yanlısı gruplar, siber saldırıların olası kaynakları olarak sıralanmıştır.[376] Bunun sonucunda, 2010 yılında Lizbon'da gerçekleştirilen zirvede NATO, ulusal siber savunma yeteneklerinin geliştirilmesi ve koordine edilmesi; siber saldırıları önleme ve tespit etme; siber farkındalık, uyarı ve tepki verici donanımlar, üye ülkelerle daha iyi entegrasyonu sağlama ve siber saldırı sonrası toparlanma yetenekleri geliştirme ihtiyacını ortaya koymuştur.[377] Zirvede, siber güvenlik konusuyla alakalı olarak Kuzey Atlantik Konseyi'nin ayrıntılı bir siber savunma politikası geliştirmek ve bu politika için bir eylem planı hazırlamakla görevlendirilmesi kararına ek olarak Haziran 2011'e kadar derinlemesine bir Siber Savunma Politikası geliştirileceğinin taahhüdü verilmiştir.[378] Lizbon Zirvesi'nde gündeme getirilen en önemli konulardan biri, NATO'nun siber savunma konularında AB ile daha yakın çalışma ve iş birliği yapma çağrısı olmuştur. NATO ile AB arasında daha yakın iş birliği faaliyetleri yürütmenin her iki örgüte de sağlayacağı avantajlardan bahsedilmiş, böylelikle iki örgüt arasında günümüze kadar yürütülmekte olan siber savunma alanındaki çalışmaların ilk resmi adımı atılmıştır.[379]

---

[374] NATO, "Aktif Katılım, Modern Savunma: Kuzey Atlantik Antlaşması Örgütü…", s. 17.
[375]NATO, *Strategic Concept 2010,* (03.02.2012), https://www.nato.int/cps/en/natohq/topics_82705.htm, (Erişim tarihi: 02.10.2020).
[376] NATO, "Aktif Katılım, Modern Savunma: Kuzey Atlantik Antlaşması Örgütü…", ss. 12-13.
[377] Sally McNamara, "NATO Summit 2010: Time to Turn Words Into Action", *The Heritage Foundation,* Sayı 2498, Aralık 2010, *https://www.heritage.org/global-politics/report/nato-summit-2010-time-turn-words-action*, (Erişim tarihi: 02.10.2020), s. 7.
[378]NATO, *Cyber Defence,* (25.09.2020), https://www.nato.int/cps/en/natohq/topics_78170.htm, (Erişim tarihi: 02.10.2020).
[379]NATO, *Lisbon Summit Declaration,* (31.07.2012), https://www.nato.int/cps/en/natolive/official_texts_68828.htm, (Erişim tarihi: 03.10.2020).

Sonuç itibarıyla, 2010 Lizbon Zirvesi çerçevesinde NATO'nun siber güvenlik alanında kurumsal ve stratejik yönelimlerini artıracağı izlenimi doğrudan verilmiştir. Stratejik Konsept içerisinde; NATO'nun siber saldırıları önleme, tespit etme, savunma ve bu saldırılardan kurtulmasına yönelik açıklamalar geçmesine rağmen, siber caydırıcılık kavramının hiç ele alınmamış olması önemli bir eksik olarak değerlendirilebilir.[380]

3.1.2. 2010-2020 Yılları Arası Siber Güvenlik Anlayışı

NATO'nun siber saldırı tehdidine yönelik kurumsal modernizasyonu, 2011 yılında revize edilmiş bir Siber Savunma Politikası'nın ve Eylem Planı'nın kabulüyle devam etmiştir.[381] Revize edilmiş politika, siber saldırıları önlemeye ve mevcut ağların dayanıklılığını artırmaya odaklanarak İttifak genelinde siber savunmaya koordine bir yaklaşım sunmuştur.[382] Yeni Stratejik Konsept'in kabul edilmesinden kısa bir süre sonra ilan edilen Siber Savunma Politikası çerçevesinde, Lizbon Zirvesi'nde ele alınmış olan NATO'nun siber saldırıları engelleme, tespit etme, siber saldırılara karşı savunma konularında ortak kapasitenin geliştirilmesi üzerine çalışmalar yürütülmüştür.[383] Bu hususta, NATO'nun merkezi siber koruması için NATO İletişim ve Bilgi Ajansı (*The NATO Communications and Information Agency*, NCIA) görevlendirilirken, NCIRC ise NCIA'nın bir parçası halini almıştır.[384] Bununla birlikte, İttifak üyelerinin kendi ulusal ağlarını korumaya yönelik gelişimlerini sürdürmeleri çerçevesinde, güncellenmiş politika içerisinde NATO'nun birincil olarak

---

[380] NATO, *Strategic Concept 2010*, (03.02.2012), https://www.nato.int/cps/en/natohq/topics_82705.htm, (Erişim tarihi: 02.10.2020).
[381] Wiesław Goździewicz, "From Riga to Wales. NATO's Road to Collective Cyberdefence", *NATO Road to Cybersecurity*, Derleyen: Joanna Świątkowska, Kosciuszko Institute, Krakow 2016, s. 12.
[382] Reyhaneh Noshiravani, "NATO and Cyber Security Building on the Strategic Concept", Rapporteur Report, *Chatham House*, Mayıs 2011, s. 4.
[383]NATO, *Defending the networks: The NATO Policy on Cyber Defence*, https://www.ccdcoe.org/uploads/2018/10/NATO-110608-CyberdefencePolicyExecSummary.pdf, 2011, (Erişim tarihi: 03.10.2020), s. 1.
[384] Piret Pernik, *a.g.m.*, s. 5.

kendi ağ sistemlerini korumaktan sorumlu olduğu vurgulanmıştır.[385] İttifak'ın, Siber Savunma Politikası çerçevesinde belirlemiş olduğu yeni yaklaşımının ana unsurları;[386]

1) NATO'nun temel toplu savunma ve kriz yönetimi görevlerini yerine getirmek için siber konuların, NATO yapılarına ve planlama süreçlerine entegrasyonunun sağlanması;

2) NATO ve üyeleri için kritik öneme sahip siber varlıkların önlenmesine, dayanıklılığına ve savunmasına odaklanılması;

3) Güçlü siber savunma yeteneklerinin uygulanmasına yönelik çalışmalar yürütülmesi ve NATO'nun kendi ağlarının merkezi olarak korunmasının sağlanması;

4) NATO'nun temel görevlerinin yerine getirilmesi hususunda kritik öneme sahip ulusal ağların siber savunması için minimum gereksinimlerinin tanımlanması;

5) Ulusal kritik altyapının güvenlik açıklarını azaltmak ve asgari düzeyde siber savunma elde etmek için müttefiklere yardım edilmesi;

6) Ortaklarla, diğer uluslararası kuruluşlarla, özel sektör şirketleriyle ve akademik kurumlarla etkileşim faaliyetlerinin geliştirilmesi;

7) NATO'ya üye devletlerin, Tallinn'deki Müşterek Siber Savunma Mükemmeliyet Merkezi'nden uzmanlık ve destek almaya teşvik edilmesi olarak belirtilmiştir.[387]

NATO'nun Siber Savunma Politikası kapsamındaki herhangi bir kolektif savunma müdahalesinin Kuzey Atlantik Konseyi kararlarına tabi olduğunun deklare edilmesinin yanı sıra 4 önemli kurumun öncülüğünde hiyerarşik bir NATO Siber Savunma Yönetim Yapılanması kurulmuştur.[388] NATO'nun kurumsal siber savunma

---

385 NATO, *Defending the networks: The NATO Policy on Cyber Defence*, https://www.ccdcoe.org/uploads/2018/10/NATO-110608-CyberdefencePolicyExecSummary.pdf, 2011, (Erişim tarihi: 03.10.2020), s. 1.

386 NATO, *Defending the networks: The NATO Policy on Cyber Defence*, https://www.ccdcoe.org/uploads/2018/10/NATO-110608-CyberdefencePolicyExecSummary.pdf, 2011, (Erişim tarihi: 03.10.2020), ss. 1-2.

387 NATO, *Defending the networks: The NATO Policy on Cyber Defence*, https://www.ccdcoe.org/uploads/2018/10/NATO-110608-CyberdefencePolicyExecSummary.pdf, 2011, (Erişim tarihi: 03.10.2020), ss. 1-2.

388 Joe Burton, a.g.m., ss. 307-308.

modernizasyonunda, Kuzey Atlantik Konseyi'nin nihai itici güç olarak yer aldığı yapının yanı sıra Savunma Politikası ve Planlama Komitesi (*The Defence Policy and Planning Committee*, DPPC), NATO Siber Savunma Yönetim Kurulu (*The NATO Cyber Defence Management Board*, CDMB) ve NCIRC yer almaktadır.[389]

2012 yılında NATO devlet ve hükümet başkanları, yeni bir NATO zirvesi için Chicago'da toplanmışlardır. Chicago Zirve Sonuç Bildirisi'nin 49. Paragrafı kapsamında üye devletlerin liderlerinin, Lizbon Zirvesi'nde yapılan siber savunma taahhütlerini yineledikleri görülmüştür. Bu hususta, öncelikle NCIRC ve Tam Harekat Kabiliyeti (*The Full Operational Capability*, FOC) gibi kurumlara uygulanacak bazı geliştirmelerle birlikte merkezi bir savunma yapısı altında NATO'nun bilgi ve iletişim sistemlerinin siber güvenliğini artırmaya yönelik taahhüt verilmiştir. Aynı zamanda AB, Avrupa Konseyi, BM ve Avrupa Güvenlik ve İşbirliği Teşkilatı (*The Organization for Security and Co-operation in Europe*, AGİT) ile siber tehditlerle mücadele konusunda gerekli iş birliği faaliyetlerinin yapılacağı bildirilmiştir.[390] NATO'nun siber savunma yeteneklerinin geliştirilmesi, birlikte çalışabilirlik ve işbirlikçi amaçlar için daha gelişmiş prosedürlerin ve yapıların uygulanma fikrinin Chicago Zirvesi bütününde öncü konulardan biri olduğu görülebilmektedir.[391]

2012 yılında, gelecekteki siber saldırılar kapsamında ortaya çıkabilecek hasarı azaltmak ve dayanıklılığı artırmak, siber saldırılara gerçek zamanlı olarak müdahale etmek ve de ağ istismarı durumlarında bilgisayar ağlarının işlevselliğini yeniden sağlamakla görevli altı NATO bilgisayar uzmanından oluşan Hızlı Tepki Ekibi'nin (*Rapid Reaction Team*, RRT) kurulma kararı alınması, İttifak'ın işlevlerinde önemli bir adım olmuştur.[392] Chicago Zirvesi'nde ayrıca, üye ülkeler arasında hala önemli bağlantı ve iş birliği sorunları olduğunun altı çizilmiştir.[393] 2013 yılına

---

[389]NATO, *Cyber Defence*, https://www.nato.int/cps/en/natohq/topics_78170.htm, (Erişim tarihi: 04.10.2020).
[390]NATO, *Chicago Summit Declaration*, (01.08.2012), https://www.nato.int/cps/en/natolive/official_texts_87593.htm#cyber, (Erişim tarihi: 06.10.2020).
[391] NATO, "NATO 2012 Chicago Summit Guide- NATO's 25th summit meeting", 20-21 Mayıs 2012, *https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120905_SummitGuideChicago 2012-eng.pdf*, (Erişim tarihi: 06.10.2020), ss. 120-122.
[392]NATO, *NATO Rapid Reaction Team to fight cyber attack*, (13.03.2012), https://www.nato.int/cps/en/natolive/news_85161.htm, (Erişim tarihi: 06.10.2020).
[393]NATO, *Chicago Summit Declaration*, (01.08.2012), https://www.nato.int/cps/en/natolive/official_texts_87593.htm#cyber, (Erişim tarihi: 06.10.2020).

gelindiğinde beş NATO üye ülkesi olan Danimarka, Hollanda, Kanada, Norveç ve Romanya öncülüğünde ortak çalışma ve koordinasyonun sağlanması için Çokuluslu Siber Savunma Yeteneği Geliştirme Projesi (*Multinational Cyber Defence Capability Development*, MN CD2) faaliyete geçirilmiş; ancak sadece adı geçen beş ülke tarafından desteklenmesi sebebiyle proje kapsamında siber savunma yeteneğini geliştirme üzerine ileriye dönük çalışmalar yürütülememiştir.[394]

NATO'nun siber güvenlik sorunlarıyla mücadele edebilmesine yönelik bir başka önemli katkı, Mart 2013'te siber savaş durumunda uyulması gerekli kuralların temel alındığı "*Siber Savaşta Uygulanacak Uluslararası Hukukla ilgili Tallinn El Kitabı'nın*"[395] yayınlanmasıyla olmuştur. Bu belge, NATO CCD COE ile ortak çalışan yasal ve teknik uzmanlardan oluşan bir ekip tarafından yazılmış ve mevcut uluslararası hukuku siber güvenlik alanına uygulayarak siber saldırılarla ilgili hem yasal hem de stratejik çelişkileri açıklığa kavuşturmayı amaçlamıştır.[396] NATO CCD COE tarafından yayınlanan Tallinn El Kitabı, devletlerin bir siber saldırı eylemiyle karşı karşıya kalmaları durumunda uluslararası hukuk bağlamında angajman kurallarını, karşı önlemleri, misilleme operasyonlarını ve diğer müdahale biçimlerini nasıl tanımlayabileceklerine dair bir dizi kılavuza yer vermiştir. NATO'nun resmi görüşünden ziyade uluslararası uzmanlar grubunun kişisel görüşleri dahilinde ortaya çıkmasına rağmen, NATO'nun siber saldırılara yönelik atıf sorunu da dahil olmak üzere önemli siber güvenlik konularındaki hukuki ve stratejik düşüncelerini geliştirmesinde yol gösterici nitelikte olduğu ifade edilebilir.[397]

Uluslararası hukuk üzerine akademik çalışmalar yürüten Khatuna Burkadze'ye göre Tallinn El Kitabı, devletler üzerinde bağlayıcı nitelikte olabilecek bir belge özelliği taşımamaktadır. Bunun arkasındaki sebebin ise; Tallinn El Kitabının, hukukun ikincil kaynaklar statüsünde yer almasından kaynaklandığını

[394] A. Burak Darıcılı, *a.g.e.*, s. 415.
[395] Tallinn El Kitabı: NATO Siber Savunma Mükemmeliyet Merkezi tarafından Uluslararası Bağımsız Uzmanlar Grubu'na mevcut uluslararası hukuk normlarının, siber savaş haline göre uygulanacağı düzeye ilişkin hazırlanmış bir dokümandır. Detaylı bilgi için bkz: Micheal Schmitt, *The Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, New York 2013.
[396] Alexander Klimburg, *a.g.e.*, s. 168.
[397] Gös. yer.

belirtmektedir.[398] Bir diğer ifadeyle belgenin ikincil kaynak olması sebebiyle ilk defa gerçekleşen bir duruma yönelik herhangi bir hukuksal yorum gerçekleştiremeyeceğini, buna karşın sadece var olan kuralları açıklayabilecek niteliğe sahip olduğu görüşünü savunmaktadır.[399]

2014 yılında Galler'de gerçekleştirilen NATO Zirvesi'nde, hızla gelişen tehdit ortamına ayak uydurabilmek ve güçlü bir siber savunma ağı oluşturabilmek için müttefikler tarafından yeni bir Siber Savunma Politikası ve Eylem Planı onaylanmıştır. Politika kapsamında siber savunmanın İttifak'ın temel toplu savunma misyonunun bir parçası olduğu ortaya konmuştur.[400] Galler Zirvesi'nde NATO, herhangi bir üye devletin siber saldırılara maruz kalması sonucunda Kuzey Atlantik Antlaşması'nın 5. Maddesi uyarınca toplu bir yanıt verebileceğini ilk kez deklare ederek siber güvenlik alanında caydırıcılığı yüksek bir adım atmıştır.[401] Bu durum aynı zamanda NATO'nun, siber uzayı yeni bir savaş alanı olarak kabul ettiği ve ciddi bir siber saldırı durumunda konvansiyonel silahlarla karşılık verebileceği değerlendirmelerinin yapılmasını getirmiştir.[402] Siber uzayın bir savaş alanı olarak resmi olarak tanınması, Kuzey Atlantik Antlaşması'nın 3. Maddesinden hareketle, üye devletlerin ulusal siber güvenlik altyapısını savunma ve geliştirme sorumluluğunu da ortaya koymuştur.[403] Bunun sonucunda üye devletler, ulusal siber savunma yeteneklerini daha fazla geliştirmeyi ve İttifak'ın ağ altyapısının siber güvenliğini artırmaya yönelik adımların atılacağını taahhüt etmişlerdir.[404]

---

[398] Khatuna Burkadze, "A Shift in NATO's Article 5 in the Cyber Era?", *The Fletcher Forum of World Affairs*, Cilt 42, Sayı 2, Yaz 2018, s. 223.
[399] Khatuna Burkadze, *a.g.m.*, ss. 223-224.
[400]NATO, *Cyber Defence*, (25.09.2020), https://www.nato.int/cps/en/natohq/topics_78170.htm, (Erişim tarihi: 05.10.2020).
[401] Anders F. Rasmussen, "Press Conference following the meeting of the North Atlantic Council at the level of Heads of State and Government during the NATO Wales Summit", (05,09.2014), *https://www.nato.int/cps/en/natohq/opinions_112871.htm*, (Erişim tarihi: 05.10.2020).
[402]NATO, *Cyber Defence Pledge*, (08.07.2016), https://www.nato.int/cps/en/natohq/official_texts_133177.htm?selectedLocale=en, (Erişim tarihi: 06.10.2020).
[403] Mateusz Krupczynski, "NATO's Reaffirmed Commitment to Cyber Security", (15.08.2016), *http://futurenato.org/articles/natos-reaffirmed-commitment-to-cyber-security/*, (Erişim tarihi: 06.10.2020).
[404]NATO, *Wales Summit Declaration*, (30.08.2018), https://www.nato.int/cps/en/natohq/official_texts_112964.htm, (Erişim tarihi: 06.10.2020).

Galler Zirvesi'nin bir diğer önemli gelişmesi, NATO ile özel sektör arasında 'artan siber tehdit algısı' konusunda çok daha yakın bir iş birliğine ihtiyaç duyan sektör liderlerinin ve politika belirleyicilerinin katıldığı iki günlük bir konferans sonucunda NATO Sanayi Siber Ortaklığı'nın (*The NATO Industry Cyber Partnership,* NICP) kurulması olmuştur.[405] Böylece NATO'nun siber güvenlik gündemine, başarılı bir siber savunma sistemi oluşturabilmek için özel sektör ile güçlü iletişim ve iş birliği eylemlerinin yürütülmesi fikrinin girdiği görülmektedir. NATO ve sanayi sektöründeki kuruluşların siber alanda ortak risklerle karşı karşıya olduğu fikrine dayalı kurulmuş olan bu ortaklık sonucunda sanayi ile iş birliği resmileştirilmiş ve siber tehditlerle mücadele çerçevesinde yeni eylem planlarının faaliyete geçirilmesi üzerinde anlaşılmıştır.[406]

Galler Zirvesi'nde, sanayi kuruluşları ile yakın ilişkilerin önemi vurgulanırken; aynı zamanda AB ve BM gibi uluslararası örgütlerle, ortak ülkelerle ve akademi ile iş birliği girişimleri yürütmenin 2014 yılında açıklanan Siber Savunma Politikası'nın en önemli sütunlarından biri olduğu dile getirilmiştir. Bu bağlamda, İttifakın siber savunması için eğitim ve bilgi paylaşımı, tatbikatlara katılım ve üye devletler ile bu alanda yürütülecek olan gelişim çabalarının, NATO'nun siber güvenlik gündemindeki öncelikli konular olarak yer alacağı belirtilmiştir.[407] Ayrıca, siber saldırıları önlemek ve saldırılara gerekli tüm müdahaleleri gerçekleştirebilmek amacıyla AB ve NATO arasında siber güvenlik konusunda teknik bir düzenlemeye gidilmiştir. Bu düzenleme ile, iki örgüt arasında siberle ilgili konular hakkında bilgi, deneyim ve uygulama paylaşımlarının gerçekleştirilebilmesi hedeflenmiştir.[408]

---

[405]NATO, *Cyber Defence*, (25.09.2020), https://www.nato.int/cps/en/natohq/topics_78170.htm, (Erişim tarihi: 07.10.2020).

[406]NATO, *NATO launches Industry Cyber Partnership*, (18.09.2014), https://www.nato.int/cps/en/natohq/news_113121.htm, (Erişim tarihi: 07.10.2020).

[407]NATO, *Wales Summit Declaration*, (05.09.2014), https://www.nato.int/cps/en/natohq/official_texts_112964.htm, (Erişim tarihi: 07.10.2020).

[408] European Parliament, "Cybersecurity in the EU Common Security and Defence Policy (CSDP)-Challenges and risks for the EU", *European Parliamentary Research Service*, Brüksel 2017, *http://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf,* (Erişim tarihi: 08.10.2020), s. 13; CCDCOE, *EU Cyber Defence Policy Framework Presents More Than 40 Action Measures,* https://ccdcoe.org/incyder-articles/eu-cyber-defence-policy-framework-presents-more-than-40-action-measures/, (Erişim tarihi: 08.10.2020).

Sonuç itibarıyla, 2014 yılında onaylanan gelişmiş Siber Savunma Politikası kapsamında, 2011 güncellemelerine ek olarak İttifak'ın temel önceliği olan kendi ağlarını korumanın yanı sıra müttefiklerin ulusal ağlarını geliştirmelerine yardımcı olma sorumluluğu benimsenmiştir. Ayrıca NATO, Kuzey Atlantik Antlaşması'nın 5. Maddesi uyarınca kolektif savunma ilkesi içerisine siber savunma kavramının girdiğini resmi yollarla ilan etmiştir.[409] NATO'nun Siber Savunma Politikası hem savunma politikası hem de bir güvenlik stratejisi olarak hizmet verme misyonuyla oluşturulmuştur, çünkü NATO'nun faaliyete geçirdiği kavramlar ve ilkeler sadece ortaya çıkan tehditlere karşı bir önlem olarak değil, aynı zamanda onları caydırabilmek ve üye ülkelerinin nüfusunu ulusal güvenliğe yönelik gelecekteki her türlü tehditten korumak için de uygulanmaktadır.[410]

2014 yılında Rusya'nın, Kırım'ı ilhak etme girişimleri sonucu Doğu Avrupa'da yeni bir sorun ortaya çıkmış, Rusya-Ukrayna arasındaki kriz kısa süre içerisinde siber alana taşınmış ve Rusya merkezli internet sitelerinden başlatıldığı ileri sürülen siber saldırılar, çatışmanın başlarından itibaren Ukrayna iletişim ve medya ağlarını kesintiye uğratmayı başarmıştır.[411] Şubat ayında bilgisayar korsanları, DDoS saldırıları başlatarak NATO ve Ukrayna medya ajanslarına karşı propaganda faaliyetleri yürütmüşlerdir. Buna ek olarak Ekim 2014'te yapılan Ukrayna seçimleri sırasında kamuoyunda karışıklık ve güvensizlik yaratmak için, seçim komitesinin web sitelerine de DDoS saldırıları gerçekleştirilmiştir.[412] Bilgisayar korsanlarının, Ukrayna'nın siyasi, askeri, telekomünikasyon ve özel bilgi teknolojisi altyapısına sürekli saldırılar düzenlemek için fişleme, kötü amaçlı yazılım, DDoS saldırıları ve cep telefonu ağı kesintilerinden diğer siber suç ve casusluk faaliyetlerine kadar Ukrayna'daki bilgi ve teknoloji ağını kontrol etmek için etkileyici siber saldırı yöntemleri kullandığı belirlenmiştir.[413] Bağlantıyı kesmek, hükümet belgelerini ve

---

[409] NATO CCD COE, *NATO Summit Updates Cyber Defence Policy*, https://ccdcoe.org/incyder-articles/nato-summit-updates-cyber-defence-policy/, (Erişim tarihi: 11.10.2020).
[410] Dean C. ALEXANDER, "Cyber threats against the North Atlantic Treaty Organization (NATO) and selected responses", *İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi*, Cilt 1, Sayı 2, 2014, s. 22.
[411] Sorin D. Ducaru, "The Cyber Dimension Of Modern Hybrid Warfar and Its Relevance For NATO", *Europolity-Continuity and Change in European Governance*, Cilt 10, Sayı 1, Ekim 2016, ss. 17-18.
[412] Marie Baezner ve Patrice Robin, "Hotspot Analysis: Cyber and Information warfare in the Ukrainian conflict", *Center for Security Studies (CSS)*, Zürih 2018, ss. 7-8.
[413] Kenneth Geers, *Cyber War ın Perspective: Russian Aggression Against Ukraine*, NATO CCD COE Publications, Tallinn 2015, ss. 10-11.

planlarını ele geçirmek, sızdırmak ve ülke içerisindeki çeşitli web sitelerini ve bilgisayar sistemlerini yok etmek hedefli gerçekleştirildiği görülen siber saldırılar, aynı zamanda Ukrayna hükümeti ve ordusunun iletişim ve hareket yeteneğini de büyük ölçüde sabote etmiştir.[414]

Estonya ve Gürcistan'a yönelik siber saldırılarda olduğu gibi, Ukrayna hedeflerine yönelik siber saldırıların da Moskova'nın stratejik hedeflerine hizmet ettiği ve saldırılara Kremlin'in kaynak sağladığı konusunda çeşitli iddialar ortaya atılmıştır.[415] Bu çerçevede, Ukrayna'nın Karşı İstihbarat Başkanı Vitaly Naida; dünyada bu saldırılardan yararlanacak tek bir ülke bulunduğunu ve bu ülkenin de Rusya olduğunu düşündüklerini belirten bir açıklama yapmıştır.[416] Açıklama karşısında Kremlin'in sözcüsü Dmitry Peskov, tüm suçlamaları reddederek, birçok hacker grubunun Ukrayna'ya olduğu gibi düzenli olarak Rusya bilgisayar sistemlerine de saldırı düzenlediğini ifade etmiştir.[417]

Gürcistan'ın ardından Ukrayna'ya gerçekleştirilen hibrit saldırılar hem NATO düzeyinde hem de üye ülkelerde tedirginliğe yol açmış ve bu olay sonrası NATO'nun, siber alanda kendini savunmak için daha ciddi önlemler alması gerektiği anlayışı hakim olmuştur.

2016 yılındaki Varşova Zirvesi'nde, öncelikli olarak siber alanın hava, deniz, kara ve uzaya ek olarak beşinci bir operasyon alanı olarak tanınması üzerine siber güvenlik konusunda önemli ve uzun vadeli kararlar alınmıştır.[418] Siber uzayın beşinci operasyon alanı olarak tanınması, aynı zamanda siber alanın kara, deniz, hava ve uzay ile aynı stratejik öneme sahip olduğu sonucunu doğurmaktadır. Bu kararla beraber,

---

[414] Michael Connell ve Sarah Vogler, "Russia's Approach to Cyber Warfare", Teknik Rapor, *Center for Naval Analyses Arlington*, Washington 2017, *https://apps.dtic.mil/sti/pdfs/AD1032208.pdf*, (Erişim tarihi: 18.10.2020), s. 19.

[415] Sergei A. Medvedev, *Offense-Defense Theory Analysis Of Russian Cyber*, Naval Postgraduate School, Monterey 2015, s. 13.

[416] Joseph Marks, "Ukraine's intel chief: We weren't ready", (23.06.2015), *https://www.politico.eu/article/ukraines-intel-chief-we-werent-ready/,* (Erişim tarihi: 08.10.2020).

[417] Margaret Coker ve Paul Sonne, "Ukraine: Cyberwar's Hottest Front", (09.09.2015), *https://www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671,* (Erişim tarihi: 08.10.2020).

[418] NATO, *Warsaw Summit Communiqué*, (29.03.2017), https://www.nato.int/cps/en/natohq/official_texts_133169.htm, (Erişim tarihi: 09.10.2020).

örgütün savunma misyonu ve uluslararası hukuka olan bağlılığının aynı doğrultuda sürdürüleceği, NATO'nun kendisini başka herhangi bir alanda olduğu gibi etkili bir şekilde savunurken, hala tırmanıştan kaçınacağını ve uluslararası hukuka saygı duyacağını, böylece gelecekte olası aktif savunma ve saldırı amaçlı siber operasyonların kapısının aralanmasına yönelik adım atılmaya devam edileceği belirtilmiştir.[419]

Varşova'daki toplantılar esnasında, üye ülkelerin tamamının siber uzayı beşinci operasyon alanı olarak kabul etmesinin yanı sıra her üye ülkenin siber dayanıklılığını güçlendirme konusundaki bireysel sorumluluğunu vurgulayan Siber Savunma Taahhüdü imzalanmıştır.[420] Taahhüdün faaliyete geçirilmesinde, 2014 yılında Kırım'ın ilhakı, Ukrayna'daki iç savaşın ardından yürütülmüş olunan dezenformasyon kampanyaları ve hibrit savaşların yarattığı tehlikelerin giderek artan farkındalığının etkili olduğu düşünülmektedir.[421] Varşova Zirvesi'nde NATO müttefikleri, Siber Savunma Taahhüdü aracılığıyla ulusal altyapıların ve ağların siber savunmasını güçlendirme ve siber savunma alanında eğitim, öğretim ve farkındalık sürecini geliştirme niyetlerini vurgulamışlardır.[422] Ayrıca Zirvede, AB ile ortaklığın yanı sıra NICP üzerinden özel sektör ile iş birliği de yeniden vurgulanmıştır.[423]

NATO ve AB, NATO'nun Bilgisayar Olaylarına Müdahale Yeteneği ile AB'nin Bilgisayarla Acil Müdahale Ekibi arasındaki iş birliğini, iletişimi ve bilgi paylaşımını güçlendirmek için Şubat 2016'da Siber Savunma Teknik Düzenlemesi (*Technical Arrangement on Cyber Defence*) imzalamışlardır.[424]

---

[419]NATO, *Cyber Defence*, (25.09.2020), https://www.nato.int/cps/en/natohq/topics_78170.htm, (Erişim tarihi: 09.10.2020).
[420]NATO, *Warsaw Summit Communiqué*, (29.03.2017), https://www.nato.int/cps/en/natohq/official_texts_133169.htm, (Erişim tarihi: 09.10.2020).
[421] NATO CCD COE, *NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit*, https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/, (Erişim tarihi: 08.10.2020).
[422]NATO, *Cyber Defence Pledge*, (08.07.2016), https://www.nato.int/cps/en/natohq/official_texts_133177.htm?selectedLocale=en, (Erişim tarihi: 06.10.2020).
[423] NATO, "Warsaw Summit Key Decisions", Fact Sheet, *Public Diplomacy Division*, Şubat 2017, s. 2.
[424] NATO, *NATO and the European Union Enhance Cyber Defence Cooperation*, (10.02.2016), https://www.nato.int/cps/en/natohq/news_127836.htm, (Erişim tarihi: 09.10.2020).

Varşova Zirve Sonuç Bildirisi'nin 71. paragrafında; NATO Genel Sekreteri, Avrupa Konseyi Başkanı ve Avrupa Komisyonu Başkanı tarafından hibrit tehditlerle mücadele, esnekliği artırma, savunma kapasitesi geliştirme ve siber savunma konuları üzerine ortak bir deklarasyona imza atıldığı bildirilmiştir.[425] Bu kapsamda her iki örgütün de siber tehditlerle mücadelede ortak çıkarlar paylaşması nedeniyle siber savunma konusundaki iş birliğini derinleştirme yönündeki çalışmaları artırma kararı üzerinde durulmuştur.

16 Şubat 2017'de Brüksel'de gerçekleştirilen NATO Savunma Bakanları Konsey toplantısında, siber güvenliğe dair konular kapsamlı olarak ele alınmıştır.[426] Bu çerçevede, Siber Savunma Eylem Planı güncellenmiş ve siber uzayın operasyonel bir alan içerisine girdiğine dair beyanın uygulamaya geçirilebilmesi için yol haritası oluşturulmuştur.[427] Böylece, NATO'nun siber duruşunda son yılların en belirleyici politika değişim yolunun açıldığı gözlenmiştir. Güncellenen Siber Savunma Eylem Planı kapsamında müttefiklerin birlikte çalışma, yeteneklerini geliştirme ve bilgi paylaşma becerilerinin artırılmasının amaçlandığı belirtilmiştir.[428] Toplantıda ayrıca, müttefiklerin ulusal siber yeteneklerini NATO misyonları ve operasyonlarına entegre edilebilmesi hususunda fikir birliğine varıldığı üzerinde durulmuştur.[429] Savunma bakanları toplantısının ardından düzenlenen basın konferansında, NATO Genel Sekreteri Jens Stoltenberg tarafından, uyarlanmış NATO Komuta Yapısının bir parçası olarak yeni bir Siber Operasyon Merkezi'nin kurulması üzerine anlaşmaya varıldığı açıklanmıştır, General Wolfgang Renner de, NATO Siber Operasyon Merkezi aracılığıyla bir yandan İttifak'ın siber savunma gücünün artırılacağını diğer yandan da her seviyedeki NATO planlama ve operasyonlarına siber çalışmalarının entegre

---

[425]NATO, *Warsaw Summit Communiqué*, (29.03.2017), https://www.nato.int/cps/en/natohq/official_texts_133169.htm, (Erişim tarihi: 09.10.2020).

[426] Michael Birnbaum, "Facing Russian threat, NATO boosts operations for the first time since the Cold War", (08.11.2017), *https://www.washingtonpost.com/world/facing-russian-threat-nato-boosts-operations-for-the-first-time-since-the-cold-war/2017/11/08/9b47f542-c49b-11e7-9922-4151f5ca6168_story.html*, (Erişim tarihi: 10.10.2020).

[427] NATO, "NATO Summit Guide Brussels 11-12 July 2018", *Public Diplomacy Division*, Brüksel 2018, s. 39.

[428] NATO, *Cyber Defence*, (25.09.2020), https://www.nato.int/cps/en/natohq/topics_78170.htm, (Erişim tarihi: 05.10.2020).

[429] NATO, *Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers*, (08.11.2017), https://www.nato.int/cps/en/natohq/opinions_148417.htm, (Erişim tarihi: 11.10.2020).

edilmesine yardımcı olunacağını ifade etmiştir.[430] Aynı yıl içerisinde, CCDCOE ABD Donanması Komutanı Michael Widmann tarafından; NATO zihniyetinde, tıpkı uçaklar ve gemiler gibi bilgisayarların da saldırı kabiliyetine sahip olduğunun kabul edilmesi konusunda bazı değişikliklerin olduğu yönünde açıklamalar yapılmıştır.[431]

2018 yılında Brüksel'de gerçekleştirilen NATO Zirvesi'nde müttefik liderler, NATO'nun güçlendirilmiş Komuta Yapısı kapsamında Belçika'nın Mons şehrinde yeni bir Siber Uzay Operasyon Merkezi (*Cyberspace Operations Centre*) kurulmasını onaylamışlardır. Operasyon Merkezi'nin, 2023'e kadar faaliyete geçirilmesinin planlandığını ve en temel görevinin de siber saldırılarla mücadele olacağını ifade etmişlerdir.[432] Müttefiklerin 2016 yılında siber uzayı operasyonel alan olarak tanımalarından bu yana NATO açısından konu kapsamındaki en önemli gelişmelerden birinin Siber Uzay Operasyon Merkezi'ni faaliyete geçirme kararı olduğu değerlendirilmektedir.[433] Merkez aracılığıyla, NATO'nun siber uzayda yürütmüş olduğu operasyonel faaliyetlerinin durumsal farkındalığının ve koordinasyonunun sağlanması amaçlanmıştır.[434] Brüksel Zirvesi'nde üye devletlerin siyasi liderleri, Siber Uzay Operasyon Merkezi'nin yanı sıra üye bir devlet tarafından talep gelmesi üzerine siber savunma, dezenformasyon veya enerji güvenliği gibi çeşitli alanlardaki ulusal çabaları desteklemek üzere konuşlandırılabilecek Hibrit Karşıtı Destek Ekipleri (*Counter Hybrid Support Team*) kurma konusunda anlaşmışlardır.[435] Brüksel'deki 2018 NATO Zirvesi'nde müttefik liderler aracılığıyla, ilk kez Galler Zirvesi'nde deklare edilen herhangi bir üyeye yönelik siber saldırı durumunda toplu olarak karşılık verilebileceği ilkesinin bir kez daha vurgulandığı görülmektedir. Bu çerçevede; siber tehditlerle mücadele etmek, siber saldırıları caydırmak, İttifak'ı ve tüm üyeleri siber

---

[430] Robin Emmott, "NATO cyber command to be fully operational in 2023", 16.10.2018, *https://www.reuters.com/article/us-nato-cyber-idUSKCN1MQ1Z9*, (Erişim tarihi: 10.10.2020).
[431] Robin Emmott, "NATO mulls 'offensive defense' with cyber warfare rules", (30.11.2017), *https://www.reuters.com/subjects/aerospace-and-defense/article/us-nato-cyber/nato-mulls-offensive-defense-with-cyber-warfare-rules-idUSKBN1DU1G4*, (Erişim tarihi: 11.10.2020).
[432]NATO, *Brussels Summit Declaration*, (30.08.2018), https://www.nato.int/cps/en/natohq/official_texts_156624.htm, (Erişim tarihi: 12.10.2020).
[433]Laura Brent, "NATO's Role in Cyberspace", (12.02.2019), *https://www.nato.int/docu/review/articles/2019/02/12/natos-role-in-cyberspace/index.html*, (Erişim tarihi: 12.10.2020).
[434] NATO, "NATO Summit Guide Brussels…", s. 300.
[435] NATO, "Brussels Summit Key Decisions…", s. 2.

ve hibrit saldırılara karşı korumak için konvansiyonel güç dahil olmak üzere tüm yetenekleri kullanmada tereddüt edilmeyeceği ifade edilmiştir.[436]

2019 yılında gerçekleştirilen Londra Zirvesi'nde, siber güvenlik konusu, İttifak'ın gündemindeki öncelikli konulardan biri olmuş, bu bağlamda NATO'nun propaganda, aldatma sabotaj ve diğer konvansiyonel olmayan unsurlar dahil olmak üzere artan hibrit tehditlere karşı koyma yeteneklerinin güçlendirilmesi üzerine kararlar ele alınmıştır. Bu hususta atılması gereken temel adımlar olarak; stratejik iletişimin güçlendirilmesi, uygun tatbikat senaryolarının geliştirilmesi ve hibrit tehditlerle etkin mücadeleyi sürdürebilmek için AB ile koordinasyon çalışmalarının artırılmasına karar verilmiştir.[437] 2020 yılında İsviçre'de gerçekleştirilen Dünya Ekonomik Forumu'nda (*The World Economic Forum*, WEF), NATO Genel Sekreteri Stoltenberg tarafından NATO'nun siber tehditlere karşı caydırıcılık oluşturmak için üst düzey teknolojik gelişmeler üzerine yatırımlara devam edildiği belirtilmiş, Kuzey Atlantik Antlaşması'nın 5. Maddesinin siber saldırılara yanıt olarak faaliyete geçirilebileceği de bir kez daha vurgulanmıştır.[438] 3 Haziran 2020 tarihinde Kuzey Atlantik Konseyi, Koronavirüs pandemisi bağlamında meydana gelen istikrarı bozucu ve kötü niyetli siber faaliyetleri kınayan bir bildiri yayınlamıştır. Bildiri kapsamında sağlık hizmetleri, hastaneler ve araştırma enstitüleri dahil olmak üzere kötü amaçlı siber saldırılar sonucunda zarar gören kurumlara yönelik dayanışma ve iş birliği çerçevesinde gerekli desteğin verileceği ifade edilmiştir.[439]

Sonuç olarak, siber güvenlik kavramının İttifak'ın güvenlik gündemine ilk kez 2002 yılındaki Prag Zirvesi'nde girmesinden bu yana 18 yılı aşkın süredir en

---

[436] Susan Davis**, "**NATO in the Cyber Age: Strengthening Security & Defence, Stabilising Deterrence", Genel Rapor, *NATO Parliamentary Assembly*, Nisan 2019, *https://www.nato-pa.int/document/2019-nato-cyber-age-strenghtening-security-and-defence-stabilising-deterrence*, (Erişim tarihi: 13.10.2020), s. 1.

[437] Paul Belkin, "NATO: Key Issues Following the 2019 Leaders' Meeting", CRS Report R46066, *Congressional Research Service*, Nisan 2020, *https://www.everycrsreport.com/files/20200401_R46066_a0abb404b866107cd315ba156d0d673c81ae4898.pdf*, (Erişim tarihi:11.10.2020), s. 3.

[438] Şerife Çetin, "NATO Genel Sekreteri Stoltenberg: Türkiye'nin NATO üyeliğinin önemini anlamak zorundayız", (23.01.2020), *https://www.aa.com.tr/tr/dunya/nato-genel-sekreteri-stoltenberg-turkiyenin-nato-uyeliginin-onemini-anlamak-zorundayiz/1711411*, (Erişim tarihi: 13.10.2020).

[439] NATO, *Statement by the North Atlantic Council concerning malicious cyber activities,* (03.06.2020), https://www.nato.int/cps/en/natohq/official_texts_176136.htm?selectedLocale=en, (Erişim tarihi: 14.10.2020).

öncelikli alanlardan birini oluşturduğu belirtilebilir. İttifak'ın, siber savunmaya yönelik yeni strateji ve politikalar geliştirmesinin kilit faktörleri arasında 2007 yılında Estonya'ya yönelik siber saldırılar, 2008 yılında Gürcistan ve 2014'te Ukrayna'yı hedef alan hibrit saldırılar yer almıştır. Bu çerçevede NATO, kendini ve müttefiklerini siber saldırılardan koruyabilmek ve siber tehditlerle aktif mücadele edebilmek amacıyla 2008, 2011, 2014 ve 2021 yıllarında siber savunma politikaları ilan etmiştir.[440] Bunun yanı sıra NATO, son 15 yıl içerisinde eğitimler, tatbikatlar, kötü amaçlı yazılım istihbarat paylaşımı, erken uyarı ve olay müdahalesi dahil olmak üzere müttefiklere yardım şeklinde yapılabilecek bir dizi eylem planını kabul etmiştir.[441] Buna rağmen siber saldırılar, her geçen gün İttifak ve üyeler açısından daha ciddi tehdit oluşturur bir duruma gelmişlerdir. Dolayısıyla NATO'nun, öngörülebilir gelecekte devletlerden, organize suç örgütlerinden, terör örgütlerinden ve de aşırılık yanlısı gruplardan gelebilecek siber saldırı ve tehditlerle ilgili çok daha karmaşık çıkmazlara karşı kendini hazırlaması gerekliliği oluşmuştur. Bu bağlamda, asimetrik siber tehditlerle toplu olarak mücadele edilmesi ve NATO'nun siber saldırılara karşı direncinin iş birliği içinde güçlendirilmesinin siber saldırı ve tehditlerle mücadelede fayda sağlayacağı düşünülmektedir. NATO'nun siber savunma alanında çalışmalar yürütürken; uluslararası örgütler, müttefikler, ortak ülkeler, özel sektör kuruluşları gibi diğer aktörler ile sürekli bir etkileşim içerisine girmesi ve faaliyetlerine bu aktörleri dahil etmesinin yerel, bölgesel ve de küresel alanda siber güvenliğin iyileştirilmesi konusunda gerçekleştirilecek gelişmelerde büyük önem taşıdığı değerlendirilmektedir.[442]

3.2. NATO'nun Siber Tehditlerle Mücadelede Karşılaştığı Zorluklar, Kurumsallaşma ve İş birliği Çabaları

[440]NATO, *Bucharest Summit Declaration*, (08.05.2014), http://www.nato.int/cps/en/natolive/official_texts_8443.htm, (Erişim tarihi: 01.10.2020); NATO, *Defending the networks: The NATO Policy on Cyber Defence*, https://www.ccdcoe.org/uploads/2018/10/NATO-110608-CyberdefencePolicyExecSummary.pdf, 2011, (Erişim tarihi: 03.10.2020), s. 1; NATO, *Wales Summit Declaration*, (30.08.2018), https://www.nato.int/cps/en/natohq/official_texts_112964.htm, (Erişim tarihi: 06.10.2020).

[441] NATO, "NATO Summit Guide Brussels…", s. 39.

[442] Marios Panagiotis Efthymiopoulos, "Cyber-Challenges and NATO", *Handbook of Cyber Development*, Cyber-Democracy, and Cyber-Defense, Derleyen: E. G. Carayannis vd, Springer International Publishing, 2018, s. 957.

2000'li yılların ortalarından itibaren NATO, siber alanın gün geçtikçe artan tehdit yapısıyla mücadele edebilmek için aktif bir rol üstlenmekte ve çeşitli kurumsal reformları faaliyete geçirmektedir.[443] Bu kapsamda uygulamaya geçirilen kurumların yanı sıra eğitim, öğretim ve tatbikatlar da hem ulusal hem de örgütsel düzeyde siber tehdit ve saldırıların caydırılması hususunda rol oynamaktadırlar. Uluslararası alanda, siber saldırıların sayısındaki öngörülemez artış ve siber uzayın yeni bir savaş alanı olarak ortaya çıkması, NATO'yu bu konuda iş birliği arayışlarına yöneltmiş, NATO ve AB, esnek siber yetenekler geliştirme, siber alanda karşılıklı istişareler ve koordinasyonu artırma çerçevesinde ortaklık girişimleri başlatmışlardır. Sanayi, akademi ve özel sektör ile iş birliği de; İttifak'ın siber savunma yeteneklerinin geliştirilmesine çok yönlü yöntemlerin ve fikirlerin entegre edilmesi hususunda kritik rol oynamıştır.[444]

3.2.1. Kurumlar ve Tatbikatlar

NATO, 2008 yılından itibaren siber alandaki savunma yeteneklerinin ve politikalarının işleyişini ortaya koyacak ve İttifak'ın siber güvenliğini sağlama hususunda kilit rol oynayabilecek NCIA, NCIRC, NATO CCD COE, NATO Siber Menzili, NATO Savunma Koleji ve Oberammergau NATO Okulu gibi bir dizi askeri, politik ve teknik organın faaliyete geçirilmesi üzerine çalışmalar yürütmektedir.[445]

NATO'nun ana danışma komuta ve kontrol birimi olan NCIA, 2012 yılında NATO Karargâh Bilgi ve İletişim Teknolojileri Servisi, NATO İletişim ve Bilgi Sistemleri Hizmet Ajansı, NATO İstişare, Komuta ve Kontrol Örgütü, NATO Hava Komuta ve Kontrol Sistemi Yönetim Ajansı ve NATO Danışma Kurumu'nun birleştirilmesi sonucunda kurulmuştur.[446] NCIA, NATO komuta yapılarına, karargahlarına ve ajanslarına teknik destek temin etmenin yanı sıra İttifak içerisindeki bilgi ve enformasyon sistemlerinin sağlayıcısı olarak da hizmet vermektedir.[447]

---

[443] NATO, "NATO Cyber Defence", Fact Sheet, *Public Diplomacy Division*, Temmuz 2016, s. 1.
[444] Andrew Nicholson, Tim Watson, Peter Norris, Alistair Duffy ve Roy Isbell, "A taxonomy of technical attribution techniques for cyber attacks", *11th European Conference on Information Warfare and Security*, Academic Conferences International Limited, Ocak 2012, s. 192.
[445] NATO, "NATO Cyber Defence", Fact Sheet, *Public Diplomacy Division*, Temmuz 2016, ss. 1-2.
[446] Marios Panagiotis Efthymiopoulos, *a.g.m.*, ss. 951-952.
[447]NATO, *NATO Communications and Information Agency (NCI Agency)*, https://www.nato.int/cps/en/natohq/topics_69332.htm, (Erişim tarihi: 01.12.2020); NATO, "NCI

NCIA'nın günlük faaliyetleri içerisinde yüzlerce siber saldırı sensörünü, e-posta sunucularını ve NATO web sitelerini izlemekten penetrasyon testlerine ve siber güvenlik eğitimine kadar çok sayıda departmana yönelik çalışmalar yürütülmektedir.[448]

NATO, sahip olduğu siber kurumlarla milyonlarca siber saldırının İttifak içerisinde dolaşımda olan bilgilerin gizliliğine, bütünlüğüne ve erişilebilirliğine ciddi tehdit oluşturmadan önce etkisizleştirilmesinin amaçlandığını belirtmektedir.[449] Çeşitli NATO zirvelerinde ve siber savunma politikaları içerisinde müttefik ülkelerin talep etmeleri halinde ağ güvenliğini sağlamalarına ve sibernetik yeteneklerini güçlendirmelerine destek verileceği de NATO tarafından sıklıkla vurgulanmaktadır.[450]

2012 yılında kapsamlı olarak faaliyete geçirilen NCIRC, Belçika'nın Mons kentindeki SHAPE içerisinde NATO'ya ait altmış beşten fazla noktaya 7/24 bilgi teknolojisi yönetimi ve siber savunma desteği sağlayarak, İttifak'ın siber güvenlik alanındaki teknik ve operasyonel yeteneklerinin ana kaynağı olarak çalışmalarını sürdürmektedir.[451] NATO'nun siber güvenlik ve bilgi güvenliği çatısı altındaki temel organlardan biri olarak, siber güvenlik konularında AB, BM, ITU ve AGİT gibi uluslararası partnerleriyle iş birliği halinde faaliyetlerini gerçekleştirmektedir. Buna ek olarak, özel sektör kuruluşları ve akademi ile siber güvenlik çemberi içerisinde kalan konular üzerine kapsamlı ve yoğun bilgi paylaşımının sağlanmasında da rol almaktadır.[452] Ayrıca NCIRC kapsamında operasyonel yeteneklerin güçlü olmasının

---

Academy C4ISR & Cyber Training Catalogue- 2021", Version 5.0, *NATO Communications and Information Academy*, Ekim 2020, s. 6.

[448] NATO, "Introducing the NCI Academy", *NATO Communications and Information Agency,* Temmuz 2020, s. 8.

[449] NCI Agency, *NATO's Cyber Security Centre*, https://www.ncia.nato.int/what-we-do/cyber-security.html, (Erişim tarihi: 05.12.2020).

[450] NATO, *Brussels Summit Declaration*, (30.08.2018), https://www.nato.int/cps/en/natohq/official_texts_156624.htm, (Erişim tarihi: 12.10.2020); NATO, *Warsaw Summit Communiqué*, (29.03.2017), https://www.nato.int/cps/en/natohq/official_texts_133169.htm, (Erişim tarihi: 09.10.2020); NATO, *Wales Summit Declaration*, (05.09.2014), https://www.nato.int/cps/en/natohq/official_texts_112964.htm, (Erişim tarihi: 07.10.2020).

[451] Salih Bıçakcı, "Yeni Savaş ve Siber Güvenlik Arasında…", s. 214; Jens Stoltenberg, "Secretary General's Annual Report 2015", *NATO Public Diplomacy Division*, Brüksel 2016, s. 23.

[452] David P. Fidler, Richard Peregent ve Alex Vandurme, "NATO, Cyber Defense and International Law", *St. John's Journal Of International & Comparative Law*, Cilt 4, Sayı 1, Güz 2013, s. 11.

gerekliliğinin yanı sıra, NATO siber savunması için iş birliğinin son derece önemli hale geldiği de sıklıkla vurgulanmaktadır.[453]

NCIRC, NCIA'nın İttifak bütünündeki bilgi ve iletişim teknolojisi ağlarını savunma görevini başarıyla yürütebilmesinde kritik rol oynayan kurumlardan biri olarak kabul edilmektedir.[454] Bu kapsamda NCIA, bir yandan NATO genelinde teknik siber güvenlik hizmetleri sunarken, diğer yandan İttifak'a karşı herhangi bir siber saldırı gerçekleşmesi durumunda gerekli yanıt sisteminin harekete geçirilmesini NCIRC aracılığıyla yerine getirmektedir.[455] Bunun yanı sıra NATO Askeri Komitesi (*The North Atlantic Treaty Organisation Military Committee*, NATO MC) ile birlikte, NATO'nun siber savunma yeteneklerinin operasyonel gereksinimlerinin belirlenmesi, edinilmesi, uygulanması ve işletilmesi görevini yürütmektedir.[456]

NATO, çoğu zaman truva atları ve fidye yazılımları gibi küresel etki kapasitesine sahip ve genellikle siber suçlular tarafından tasarlanmış kötü amaçlı genel ve özel tehditleri içeren bir siber saldırı ortamıyla karşı karşıya kalabilmektedir. Kasıtlı olarak NATO'ya veya personeline yönelik olmasa bile bu tür kötü amaçlı yazılımlar aracılığıyla gizli bilgiler ele geçirilebilmekte ve ağır finansal kayıplar yaşanabilmektedir.[457] Dolayısıyla NATO, bünyesinde görev alan personellerinin bilinçli veya bilinçsiz davranışları sonucunda NATO bilgi ve teknoloji sistemlerine yönelik tehditler ve riskler oluşturan siber güvenlik sorunlarıyla da mücadele etmek zorunda kalabilmektedir. NATO'nun gizli bilgileri depolama ve paylaşma sistemleri herhangi bir ağ sistemine bağlı olmasa dahi; NCIRC, internete bağlı başka bir cihazın e-posta adresi yoluyla veya depolama cihazları aracılığıyla gizli bilgileri iletmeye çalışan NATO personellerini birçok kez tespit edip belgelendirmiştir.[458] NCIRC'ın metodolojisine bakıldığında; önleme, tespit etme, yanıt verme, kurtarma ve geri

[453] David P. Fidler, Richard Peregent ve Alex Vandurme, *a.g.m.*, s. 12.
[454] Alexander Klimburg, *a.g.e.*, s. 181.
[455] Jason Healey ve Klara T. Jordan," NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow", *Atlantic Council*, Eylül 2014, *https://www.atlanticcouncil.org/wp-content/uploads/2014/08/NATOs_Cyber_Capabilities.pdf*, (Erişim tarihi: 01.12.2020), s. 4.
[456] Myriam D. Cavalty, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, Routledge, New York 2007, ss. 13-14.
[457] David P. Fidler, Richard Peregent ve Alex Vandurme, *a.g.m.*, s. 9.
[458] David P. Fidler, Richard Peregent ve Alex Vandurme, *a.g.m.*, s. 8.

bildirim olmak üzere siber saldırılarla mücadelede beş önemli işleyiş sürecinin olduğu görülmektedir.[459]

Bu işleyiş çerçevesinde NCIRC, İttifak ağlarına yönelik proaktif siber çözümler için merkezi bir koordinasyon birimi olarak hizmet vermektedir. Bu bağlamda ise; tehditlerin önlenmesi, izinsiz girişlerin tespit edilmesi, olaylara yanıt verilmesi, sızıntılardan kurtarılması ve geri bildirim süreçleri sonucunda NATO'nun karşı karşıya olduğu siber tehditleri ele almaktadır.[460] NCIRC, bu yaklaşımın her alanında NATO'nun siber savunmasını geliştirmek için yetenekler ve hizmetler geliştirmeye devam etmektedir.[461]

NCIRC, tehditleri önleme görevi kapsamında potansiyel güvenlik açıklarını azaltmak amacıyla hedefi güçlendirmek için bilgi sistemlerinin güvenli bir şekilde oluşturulmasına odaklanmanın yanı sıra İttifak'ı hedef alan siber saldırılara karşı sürekli destek sağlamaktadır. NCIRC, risk değerlendirmesi ve yönetiminin bir parçası olarak penetrasyon testleri de dahil olmak üzere NATO sistemlerinin savunma açıklarının giderilmesi kapsamında çalışmalar yürütmekte ve eğitim, tatbikat, eğitim materyalleri ve bildirimler yoluyla NATO personelinin farkındalığını artırarak siber saldırıların önlenebilmesi için güçlü bir kalkan oluşturmaktadır. Aynı zamanda NCIRC, siber saldırıların olumsuz etkilerini en aza indirmek için çevrim içi ve yerinde kurtarma destek hizmetleri ve olay sonrası inceleme de sağlamaktadır.[462] NCIRC Merkezi'nin, gündelik olarak NATO'nun ağlarında meydana gelen ortalama 200 milyondan fazla siber olayı analiz ettiği ve bunlara yönelik gerekli önlem ve müdahaleleri gerçekleştirdiği belirtilmektedir.[463]

NCIRC'ın bir diğer önemli misyonu ise, büyük bir siber saldırı durumunda sistemin kurtarılması ve onarımı için NATO tesislerine, operasyonel alanlarına veya

---

[459] David P. Fidler, Richard Pregent ve Alex Vandurme, *a.g.m.*, ss. 8-9.
[460] Vincent Joubert, "Five Years After Estonia's Cyber Attack: Lessons Learned for NATO?", Araştırma Makalesi, *Research Division- NATO Defense College*, Sayı 76, Mayıs 2012, *https://www.files.ethz.ch/isn/143191/rp_76.pdf*, (Erişim tarihi: 02.12.2020), s. 2.
[461] Vincent Joubert, *a.g.m.*, s. 7.
[462] Alessandro Marrone ve Ester Sabatino, "Cyber Defence in NATO Countries: Comparing Models", *Istituto Affari Internazionali*, Şubat 2021, *https://www.iai.it/sites/default/files/iaip2105.pdf*, (Erişim tarihi: 12.04.2021), s. 26; Vincent Joubert, *a.g.m.*, ss. 2-6.
[463]NATO, *Men in black – NATO's cybermen*, (24.04.2015), https://www.nato.int/cps/en/natolive/news_118855.htm, (Erişim tarihi: 04.12.2020).

Kuzey Atlantik Konseyi'nin onayı ile müttefik ülkelere destek olmak üzere konuşlandırılabilen Hızlı Tepki Ekibi'ne (*Rapid Reaction Team,* RRT) sahip olmasıdır.[464] Hızlı Tepki Ekibi, 6 uzmandan oluşmakta ve olay gerçekleştirildikten sonraki 24 saat içinde faaliyete geçebilmektedir.[465] Hızlı Tepki Ekibi'nin öncelikli görevleri arasında; müttefiklerin siber zorluklarla başa çıkmalarına yardımcı olmak için gönderilebilecek hızlı tepki veren siber savunma ekiplerinin sağlanması, müttefiklerin siber savunma güçleriyle ortak çalışmaların yürütülmesi, NATO üyeleri ve iş birliği halindeki uluslararası örgütlerle eğitim ve tatbikatların yürütülmesine yönelik çalışmalar yapılması, siber tehditler hakkında gerçek zamanlı bilgilerin elde edilmesinin sağlanması ve siber tehditler ile başa çıkmak için en iyi yöntemlerin paylaşılması bulunmaktadır.[466] 2012 yılında Belçika'nın Mons kentinde faaliyete geçirilen NATO İletişim ve Bilgi Sistemleri Grubu (*The NATO Communications and Information Systems Group,* NCISG) ise; üye ülkelerin ihtiyaç duyması halinde operasyonel destek, teknik yardım ve tatbikatlar için konuşlandırılabilir bilgi ve teknoloji uzmanlarıyla destek sağlamaktadır.[467]

NATO'nun siber savunma alanındaki önemli kurumsal dönüşümü ve temel iş birliği motivasyonu olarak, 2008 yılında altı NATO ülkesi tarafından Estonya'nın Tallinn şehrinde NATO CCD COE'nin kurulması gösterilir.[468] Merkez, diğer kurumlardan farklı olarak NATO'nun komuta yapısının bir parçası olarak görev almamakta ve İttifak tarafından finanse edilmemektedir. NATO CCD COE, 2020 yılı itibarıyla NATO üyesi olmayan devletlerin de yer aldığı toplam 25 ülke tarafından yönetilmekte ve finanse edilmektedir.[469] Bünyesine yeni üye devletleri katabilmek için

---

[464]NATO, *Men in black – NATO's cybermen,* (24.04.2015), https://www.nato.int/cps/en/natolive/news_118855.htm, (Erişim tarihi: 02.12.2020).

[465] Susan Davis, *a.g.m.*, s. 10.

[466]NATO, *NATO Rapid Reaction Team to fight cyber-attack,* (13.03.2012), https://www.nato.int/cps/en/natolive/news_85161.htm, (Erişim tarihi: 03.12.2020).

[467]NATO, *Allied Command Operations (ACO),* (23.10.2020), http://www.nato.int/cps/en/natolive/topics_52091.htm, (Erişim tarihi: 06.12.2020); NATO, *About Us,* https://ncisg.nato.int/about-us, (Erişim tarihi: 08.12.2020).

[468] Vincent Joubert, *a.g.m.*, ss. 4-5.

[469] 2020 yılı itibarıyla NATO CCD COE'ye üye devletler arasında; Belçika, Bulgaristan, Çek Cumhuriyeti, Danimarka, Estonya, Fransa, Almanya, Yunanistan, Macaristan, İtalya, Letonya, Litvanya, Hollanda, Norveç, Polonya, Portekiz, Romanya, Slovakya, İspanya, Türkiye, Birleşik Krallık, ABD, Avusturya, Finlandiya ve İsveç yer almaktadır. Detaylı bilgi için bkz: https://ccdcoe.org/about-us/.

genişleme çalışmalarının sürdürülmesi çerçevesinde Japonya, Hırvatistan, Karadağ, Slovenya ve İsviçre ile müzakerelerin devam ettiği ve Kanada, Lüksemburg ve Avustralya'nın da yakın bir tarih içerisinde Mükemmeliyet Merkezi'ne katılım niyetinde oldukları açıklanmıştır.[470]

NATO CCD COE'nin temel misyonu; araştırma, eğitim, öğretim ve danışma faaliyetleri aracılığıyla siber savunma alanında NATO'nun kurumsal yapısı, üye devletleri ve ortak ülkeler arasındaki yetenek, bilgi paylaşımı ve iş birliğini geliştirmektir.[471] NATO CCDCOE, yalnızca siber savunma alanında küresel düzeyde çalışmalar yürüten kurum ve kuruluşlar arasında değil, aynı zamanda her geçen gün siber güvenlik sorunlarıyla karşı karşıya kalan bakanlar, diğer hükümet yetkilileri ve ülkelerin üst komuta birimleri gibi önemli yetkililer arasında da giderek daha fazla tanınmakta ve de siber tehditlere yönelik faaliyetlerini yürütme hususunda NATO merkezli ve disiplinler arası bir yaklaşım benimseyerek teknoloji, strateji, operasyonel ve uluslararası hukuk olmak üzere dört temel alana odaklanmaktadır.[472] Bunun yanı sıra Merkez'in, üye devletler için teknik, stratejik, politik ve hukuki konular üzerine üstlendiği 6 önemli program; 1) İttifak için siber alanla ilgili konularda doktrinler ve kavramlar üretmek; 2) Üye devletler için akademik araştırma, eğitim ve öğretim kursları, atölye çalışmaları ve siber savunma tatbikatları düzenlemek; 3) Araştırmalar yapmak ve gelişmeler üzerine konferanslar ve toplantılar düzenlemek; 4) Geçmişteki ve mevcut durumdaki siber saldırılar üzerine araştırmalar yaparak gerekli çıkarımları sağlamak; 5) Devam eden saldırılara yönelik talep karşılığında danışmanlık hizmeti sunmak; 6) 2018 yılından bu yana, İttifak'taki tüm NATO organları için siber savunma alanında eğitim ve öğretim çözümlerinin belirlenmesi ve koordinasyonun sağlanması görevini yürütmek olarak sıralanabilir.[473]

---

[470] Jaak Tarien, "National Cyber Defence Policies and the Role of International Cooperation", *Partnership for Peace Consortium of Defense Academies and Security Studies Institutes*, Cilt 19, Sayı 1, Kış 2020, s. 5.

[471] NATO CCD COE, *About Us*, https://ccdcoe.org/about-us/, (Erişim tarihi: 04.12.2020).

[472] Ann Väljataga, "Tracing Opinio Juris in National Cyber Security Strategy Documents" *NATO Cooperative Cyber Defence Centre of Excellence,* Tallinn 2018, *https://ccdcoe.org/uploads/2019/01/Tracing-opinio-juris-in-NCSS-2.docx.pdf*, (Erişim tarihi:04.12.2020), s. 2.

[473] Salih Bıçakcı, "Yeni Savaş ve Siber Güvenlik Arasında …", s. 218; Diána Szőke, *a.g.m.,* s. 102.

Kuruluşundan bu yana siber güvenlik alanında önemli katkılara imza atan NATO CCD COE, 3 önemli, hatta konu kapsamında "yapı taşı" olarak değerlendirilebilecek gelişme ile hem NATO hem de uluslararası sistem içerisindeki etki kapasitesini oldukça yükseltmiştir.[474] Bunlardan ilki, mevcut uluslararası hukukun siber alana uygulanabilirliğini analiz eden en kapsamlı kılavuz niteliğindeki Tallinn El Kitabı'dır. İlk versiyonu 2013 yılında NATO CCD COE inisiyatifiyle Michael N. Schmitt editörlüğünde kaleme alınmasının üzerinden kısa bir süre geçtikten sonra 2017 yılında 19 uluslararası hukuk uzmanı tarafından 'Tallinn El Kitabı 2.0' adıyla güncellenmiş ve önemli ölçüde genişletilmiş olan ikinci baskısı da yayınlanmıştır.[475]

İkinci olarak, NATO CCD COE'nin ev sahipliğinde 2009 yılından itibaren her yıl düzenlenen Uluslararası Siber Çatışma Konferansı (*International Conference on Cyber Conflict,* CyCon), siber savunma toplumuyla ilgili güncel konuları ele almaktadır.[476] 2019 yılında Tallinn'de gerçekleştirilen konferanslarla birlikte ikinci on yıllık dönemine giren CyCon, dünyanın dört bir yanından siber güvenlik profesyonelleri için en yüksek akademik araştırma standartlarına bağlı kalan önemli bir multidisipliner konferans ve topluluk oluşturma etkinliği olarak ön plana çıkmaktadır.[477] CyCon, yıllar boyunca siber savunma ve güvenliğin teknik, hukuki, politika, strateji ve askeri perspektiflerine odaklanan açılış ve paneller gerçekleştirme görevini sürdürmektedir.[478] Uluslararası Siber Çatışma Konferansı'nda, siber çatışmanın tüm odak alanlarının tek bir etkinlik kapsamında ele alınmasının yanı sıra teknoloji, eğitim ve öğretim sorunları, kötü amaçlı yazılım geliştirme, siber çatışmanın yasal boyutu gibi belirli konular hakkında derinlemesine fikir alışverişi ortaya konmaktadır. Her yıl, yaklaşık 50 ülkenin hükümet, ordu, akademi ve endüstrisinden yaklaşık 600 hukuk ve teknoloji uzmanının, karar vericinin ve fikir önderinin mevcut

---

[474] Federico Plantera, "NATO CCDCOE – Expertise and cooperation make our cyber space safer", Ekim 2018, *https://e-estonia.com/nato-ccdcoe-expertise-cyber-space-safer/,* (Erişim tarihi: 05.12.2020).
[475] Michael N. Schmitt, *Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations*, Cambridge University Press, Şubat 2017, s. 2.
[476] NATO CCD COE, *The Virtual Battlefield: Perspectives on Cyber Warfare (Proceedings 2009)*, https://ccdcoe.org/library/publications/the-virtual-battlefield-perspectives-on-cyber-warfare-proceedings-2009/, (Erişim tarihi: 07.12.2020).
[477] T. Minárik, S. Alatalu, S. Biondi, M. Signoretti, I. Tolga ve G. Visky, *11th International Conference on Cyber Conflict: Silent Battle*, NATO CCD COE Publications, Tallinn 2019, s. 1.
[478] Jean-François Morel ve Merle Maigre, *a.g.m.*, s. 71.

siber güvenlik sorunlarını disiplinler arası bir şekilde ele almak için Uluslararası Siber Çatışma Konferansı'nda bir araya geldiği belirtilmektedir.[479]

Üçüncü olarak, NATO CCD COE öncülüğünde müttefik ülkelere sağlanan başlıca katkılarından bir diğeri ise; ulusal siber savunma ekiplerinin yeteneklerinin geliştirilmesine yönelik eğitimler ve tatbikatlar düzenlenmesidir. Bu kapsamda NATO CCDCOE; teknik, operasyonel ve stratejik düzeyde gerçekleştirmiş olduğu siber eğitim, öğretim ve tatbikatlar aracılığıyla NATO'ya destek veren temel kurum görevi görmektedir. Uluslararası ölçekte yürütülen en büyük siber tatbikatlar olaraktan Kilitli Kalkanlar (*Locked Shield*) ve Siber Koalisyon (*Cyber Coalition*) tatbikatları ön plana çıkmaktadır.[480]

2010'dan beri, dünyanın en büyük ve en karmaşık uluslararası canlı ateş (*live-fire*) siber savunma tatbikatı olarak nitelendirilen Kilitli Kalkanlar tatbikatında, bilgi teknolojisi ve kritik altyapı sistemlerine senaryo tabanlı ve gerçek zamanlı siber saldırılar düzenlenerek NATO üyesi ülkelerden, ortak ülkelerden ve özel sektörden katılan siber güvenlik uzmanlarının savunma becerilerinin geliştirilmesi hedeflenmektedir.[481] Tatbikatlar boyunca rekabetçi senaryolar, en son teknolojik sistemler, stratejik karar verme ve yasal konular dikkate alınarak gerçek dünyada karşılaşılabilecek büyük bir siber saldırının tüm karmaşıklığı simüle edilmeye çalışılmakta ve bu simülasyon çalışmasında Estonya'nın NATO'ya tahsis ettiği siber savunma menzilinden yararlanılmaktadır.[482] Kilitli Kalkanlar; teknolojinin ulus ötesi bir yapıya sahip olduğu günümüzde, NATO müttefiklerinin müşterek olarak hareket ettiklerinde elde edebilecekleri kazanımları gösteren ve ulusların ortaya çıkan siber zorluklarla dinamizm çerçevesinde başa çıkma yeteneklerini artırmalarına yardımcı

---

[479] NATO CCD COE, *CyCon*, https://ccdcoe.org/cycon/, (Erişim tarihi: 09.12.2020).

[480]NATO CCD COE, *NATO Team Wins the Locked Shields Cyber Defence Exercise*, https://ccdcoe.org/news/2013/nato-team-wins-the-locked-shields-cyber-defence-exercise/, (Erişim tarihi: 09.12.2020); NCI Agency, *NATO's Cyber Defenders win Exercise Locked Shields 2015*, (28.04.2015), https://www.ncia.nato.int/about-us/newsroom/natoe28099s-cyber-defenders-win-exercise-locked-shields-2015.html, (Erişim tarihi: 09.12.2020).

[481] NATO CCD COE, *Locked Shield*, https://ccdcoe.org/exercises/locked-shields/, (Erişim tarihi: 10.12.2020).

[482] Ensar Şeker ve Hasan Hüseyin Özbenli, "The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation", Conference Paper, *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, IEEE, Tallinn 2018, s. 3.

olan benzersiz bir tatbikat olarak nitelendirilmektedir.[483] 2019 yılının Nisan ayında Tallinn'de gerçekleştirilen Kilitli Kalkanlar tatbikatında, 30 ülkeden 1000'den fazla siber uzmanın yer aldığı ve tatbikat boyunca yaklaşık 4000 sanallaştırılmış sistem içerisine 2500'den fazla siber saldırı gerçekleştirildiği açıklanmıştır.[484]

2007 yılından itibaren her sene düzenli olarak NATO üyelerinin, ortaklarının, sanayi ve akademi sektöründen katılımcıların dahil olduğu Siber Koalisyon Tatbikatı, NATO ve müttefikler arasındaki koordinasyonu ve iş birliğini geliştirmeyi, İttifak'ın siber alanının savunma yeteneğini güçlendirmeyi ve siber alanda askeri operasyonlar yürütmeyi amaçlamaktadır.[485] Tatbikat, son olarak 2020'nin Kasım ayında Koronavirüs pandemisi tedbirleri kapsamında ilk kez sanal bir ortamda NATO üye devletleri, Finlandiya, İrlanda, İsveç, İsviçre ile AB'den yaklaşık 1000 siber savunucunun Estonya'daki Siber Güvenlik Eğitim Merkezi aracılığıyla birbirine bağlandıkları bir çevrim içi ağ sistemi üzerinden gerçekleştirilmiştir.[486] Siber Koalisyon 2020'de, NATO'nun kendi bilgi ve teknoloji ağlarını siber saldırılara karşı günde 24 saat koruma ve siber tehditlerle ilgili bilgileri AB de dahil olmak üzere müttefikler ve ortaklarla gerçek zamanlı olarak paylaşma yetenekleri test edilmiştir.[487] Bu kapsamda Tatbikat Direktörü Robert Buckles, 2020 yılında gerçekleştirilen Siber Koalisyon dahilinde NATO'nun Koronavirüs gibi bir salgınla mücadele sırasında bile her türlü siber tehdide uyum sağlama ve bunlara karşı koyma yeteneğini kanıtladığını ifade etmiştir.[488]

---

[483] Naz Göçek, "A Glimpse into Locked Shields 2019", (06.06.2019), *https://natoassociation.ca/a-glimpse-into-locked-shields-2019/*, (Erişim tarihi: 10.12.2020).

[484]NATO CCD COE, *France Wins Cyber Defence Exercise Locked Shields 2019*, https://ccdcoe.org/news/2019/france-wins-cyber-defence-exercise-locked-shields-2019/, (Erişim tarihi: 10.12.2020).

[485] Jeffrey L. Caton, *NATO Cyberspace Capability: A Strategic and Operational Evolution*, Strategic Studies Institute, Haziran 2016, s. 23.

[486] SHAPE Public Affairs Office, *Exercise Cyber Coalition 2020 Underway*, (16.11.2020), https://shape.nato.int/news-archive/2020/exercise-cyber-coalition-2020-underway, (Erişim tarihi: 11.12.2020).

[487] SHAPE Public Affairs Office, *Exercise Cyber Coalition 2020 Underway*, (16.11.2020), https://shape.nato.int/news-archive/2020/exercise-cyber-coalition-2020-underway, (Erişim tarihi: 11.12.2020).

[488] Himanshu Sharma, "NATO Conducts Cyber Coalition Exercise Virtually", (07.11.2020), *https://www.newdelhitimes.com/nato-conducts-cyber-coalition-exercise-virtually/*, (Erişim tarihi: 16.12.2020).

Sonuç itibarıyla NATO'nun; NCIRC, NCIA, CCD COE ve RRT gibi zorlu siber müdahale kurumlarına sahip olmasının yanında bilgi ve teknoloji kaynaklarını oluşturması, organize etmesi ve kullanması, İttifak'ın siber savunma politikasını kurumsal düzeyde geliştirdiğini göstermiştir.

3.2.2. Avrupa Birliği ile İş birliği Girişimleri

Dijital çağın hızlanan değişimi, siber tehditlere coğrafi mesafelerin engel teşkil etmemesi ve gelecek yıllardaki konvansiyonel operasyonların büyük ölçüde siber saldırılar ile destekleneceğini ortaya koyan yeni bir çatışma normu, siber alandaki uluslararası iş birliği girişimlerine daha fazla odaklanmayı gerekli hale getirmiştir.[489] Siber uzay üzerindeki küresel tehdit ortamı ve siber saldırıların yol açtığı artan güvenlik riski, uluslararası iş birliği içerisinde kolektif hareket etme durumunu doğurmuştur.[490] Bu konuda NATO'nun, AGİT ve BM ile siber alanda yürüttüğü iş birliği faaliyetlerinin yanı sıra en derin uluslararası ortaklıklardan birinin AB ile kurulduğu belirtilmektedir.[491] Son on yıllık dönemde siber güvenlik alanında atılmış olan öncü ve caydırıcı adımlar içerisinde NATO'nun ve AB'nin iş birliğine yönelik faaliyete geçirmiş olduğu strateji ve politikalar ön plana çıkmaktadır. Bu durumun ortaya çıkmasında, 2021 yılı itibarıyla NATO'nun 22 üyesinin aynı zamanda AB'nin bir parçası olmasının önemli etkisinin bulunduğu ifade edilmiştir.[492]

21. yüzyılın siber tehdit ortamında NATO'nun ve AB'nin özellikle terör örgütleri, organize suç örgütleri, bilgisayar korsanları ve devlet destekli siber suç grupları gibi çeşitli aktörler tarafından hedef alındığı görülmektedir.[493] Askeri, siyasi, ekonomik ve toplumsal güvenliğe yönelik ciddi tehdit unsuru oluşturan siber saldırılar, AB ve NATO arasındaki iş birliği mekanizmaları arasına siber güvenlik ve savunma

---

[489] Bruno Lété ve Piret Pernik, "EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions", *German Marshall Fund of the United States,* Sayı 38, Aralık 2017, *https://www.gmfus.org/news/eu-nato-cybersecurity-and-defense-cooperation-common-threats-common-solutions*, (Erişim tarihi: 14.12.2020), s. 8.

[490] Jason Healey ve Klara T. Jordan, *a.g.m.,* s. 3.

[491]NATO, *Cyber defence,* (25.09.2020), https://www.nato.int/cps/en/natohq/topics_78170.htm, (Erişim tarihi: 14.12.2020).

[492]Alexandros Papaioannou, "Strengthening EU-NATO Relations", (16.07.2019), *https://www.nato.int/docu/review/articles/2019/07/16/strengthening-eu-nato-relations/index.html*, (Erişim tarihi: 12.12.2020).

[493] Bruno Lété ve Piret Pernik, *a.g.m.,* s. 1.

konusunu ekleme gereğini doğurmuştur. NATO'nun somut siber iş birliği, öncelikli olarak İttifak'a ait ağlardaki veri akışının kesintisiz bir şekilde sürdürülmesi ve korunması anlayışına dayanırken; ikincil olarak eğitim, öğretim, tatbikatlar ve karşılıklı yardımlaşma yoluyla İttifak ve müttefikler arasındaki siber güvenlik ve savunmanın geliştirilmesine odaklanmıştır.[494] NATO'nun da politikaları içerisinde vurguladığı gibi AB, siber tehditleri karşı karşıya kaldığı en önemli güvenlik sorunlarından biri olarak tanımlamaktadır.[495] AB'nin siber güvenlik stratejisi çerçevesinde ağ ve bilgi güvenliği sistemlerinin korunmasının ve dayanıklılığının sağlanması, siber tehditlerle mücadelenin sürdürülerek gelebilecek tüm tehdit unsurlarının önlenmesi ve Avrupa coğrafyasının bütününde daha güçlü bir siber güvenlik politikasının oluşturulması olmak üzere üç temel amacı bulunduğu belirtilmektedir.[496]

AB ve NATO, 2001 yılının başlarında birbirlerini güvenlik alanı içerisinde stratejik ortak olarak ilan etmelerine karşın, 2010 yılına kadar siber güvenlik ve savunma kavramı her iki örgütün iş birliği ve ortaklık kapsamında öncelik verdiği alanlar arasında yerini almamıştır. Siber güvenliğin ulusal güvenlik ve savunma yönleri konusunda NATO ile kıyaslandığında AB'nin, daha geç kalan bir örgüt konumunda olduğu gerçekleştirilmiş çalışmalardan anlaşılabilmektedir. Öyle ki, siber tehditler, Estonya hükümetini hedef alan saldırılar sonrasında AB'ye üye devletlerin bir kısmı tarafından proaktif olarak ele alınmaya başlanmıştır.[497] Bu kapsamda siber tehditler; ekonomik, siyasi ve toplumsal olmanın yanı sıra askeri bir boyutu olan temel bir sorun olarak tanımlanmıştır.[498] 2010 yılına kadar AB içinde siber güvenlikle alakalı

---

[494] Susan Davis, *a.g.m*., s. 7.

[495]European Commission, *Cybersecurity*, (16.12.2020), https://ec.europa.eu/digital-single-market/en/cybersecurity#Other, (Erişim tarihi: 28.12.2020).

[496] László Kovács, "Cyber Security Polcy and Strategy In The European Union and NATO", *Land Forces Academy Review*, Cilt 23, Sayı 1, Mayıs 2018, ss. 17-18.

[497] Matthew Crandall, "Soft Security Threats and Small States: the Case of Estonia", *Defence Studies*, Cilt 14, Sayı 1, Mart 2014, s. 37.

[498]Council of the European Union, "European Security Strategy A Secure Europe In A Better World", *European Communities*, Brüksel 2009, *https://www.consilium.europa.eu/media/30823/qc7809568enc.pdf*, (Erişim tarihi: 19.12.2020), s. 13.

olarak daha çok ağ ve bilgi güvenliği, siber suç ve siber terörizm konularının gündeme alındığı görülmektedir.[499]

2010 yılında Lizbon'da gerçekleştirilen NATO Zirvesi'nde, stratejik ortak olarak AB'nin ön plana çıkarılması ve kapsamlı bir kriz yönetimi için her iki örgütün iş birliğine ihtiyaç duyulduğunun vurgulanması dikkat çekmiştir.[500] Bunun yanı sıra 2010 yılı, NATO-AB arasında siber savunma alanında üst düzey personeller arası istişarelerin ve yıllık olarak yapılan gayri resmi toplantıların başlaması nedeniyle önemli bir yıl olmuştur.[501]

Avrupa Komisyonu ve AB Dış İlişkiler Servisi (*The European External Action Service*, EEAS), 2013 yılında AB'nin ilk Siber Güvenlik Strateji Belgesi'ni deklare etmişlerdir. Belgede, siber suçlular tarafından giderek daha karmaşık saldırı yöntemlerinin faaliyete geçirildiğine dikkat çekilmiş ve temel hizmetler ile kritik altyapılara hasar oluşturabilecek olası saldırıların altı çizilmiştir.[502] Bunun sonucunda siber suçlarla mücadele, Avrupa güvenlik gündeminde mücadele edilmesi gereken üç önemli güvenlik alanından biri olarak belirlenmiştir.[503] Buna ek olarak belgede, AB'nin siber güvenlik alanında öncelikli hedefleri arasında; AB siber savunma politikası ve yeteneklerinin geliştirilmesi, siber dayanıklılığın artırılması, kamu-özel sektör ortaklığının güçlendirilmesi, ulusal ve uluslararası iş birliğinin ve bilgi paylaşımının teşvik edilmesi, siber güvenlik için endüstriyel ve teknolojik kaynakların iyileştirilmesi ve AB için tutarlı bir uluslararası siber uzay politikası oluşturulması ilkelerinin yer aldığına dikkat çekilmiştir.[504] O dönem içerisinde NATO'nun Siber

---

[499] Alexander Klimburg ve Tiirmaa H. Klaar, "Cybersecurity and Cyberpower: Concepts, Conditions, and Capabilities for Cooperation for Action within the EU ", *European Parliament*, Nisan 2011, s. 29.
[500] NATO, *Lisbon Summit Declaration*, https://www.nato.int/cps/en/natolive/official_texts_68828.htm, (31.07.2012), (Erişim tarihi: 19.12.2020).
[501] European Union External Action Service, *EU and NATO Increase Information Sharing on Cyber Incidents*, (10.02.2016), https://eeas.europa.eu/generic-warning-system-taxonomy/404_en/5254/EU (Erişim tarihi: 15.12.2020).
[502] European Commission, *EU Cybersecurity Initiatives- Working Towards A More Secure Online Environment*, Factsheet, Ocak 2017 https://ec.europa.eu/newsroom/dae/document.cfm?doc_id= 16540, (Erişim tarihi: 16.12.2020), s. 2.
[503] European Commission, "The European Agenda on Security", Communicatıon From The Commission to the European Parliament, The Council, The European Economic And Social Committee and the Committee of the Regions, COM (2015) 185 final, Strazburg 2015, ss. 19-20.
[504] European Commission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace." Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and the Committee of Regions. JOIN(2013) 1 final, Brüksel 2013,

Savunma Politikası geliştirmiş olmasına ek olarak AB'nin de Siber Güvenlik Strateji Belgesi'ni ilan etmesi, NATO ve AB üye devletlerinin büyük çoğunluğunun ulusal siber yeteneklerini geliştirmeleri hususunda farkındalık oluşturulmasını sağlamış ve bu gelişmelerin siber savunma alanında kurumsal gelişim için itici güç olduğu değerlendirilmiştir.[505]

2016 yılında Avrupa ve Kuzey Atlantik bölgesinin sınırları içerisinde; radikal düşünce ve eylemlerin yol açtığı terörist saldırı girişimleri, kimyasal saldırılar, siber saldırılar ve dezenformasyon girişimleri gibi ani gelişen yeni tehditler temelli risk ve tehdit ortamıyla ciddi derecede karşı karşıya kalındığı birçok kez vurgulanmıştır.[506]

8 Temmuz 2016 tarihinde Varşova'da, 13. Dönem NATO Genel Sekreteri Jens Stoltenberg, Avrupa Konseyi Başkanı Donald Tusk ve Avrupa Komisyonu Başkanı Claude Juncker tarafından daha somut bir ortaklık ve iş birliği girişimine rehberlik edecek AB-NATO İşbirliği Ortak Deklarasyonu'na imza atılmıştır.[507] Bu kapsamda, iki örgüt arasındaki ortaklığın derinleşebilmesine yönelik yedi önemli iş birliği alanından biri olarak siber güvenliğin yer aldığı belirtilmiştir.[508]

NATO ve AB arasında bilgi ve teknoloji ortamının getirmiş olduğu tehditlerin doğası dikkate alındığında, siber güvenlik ve savunmanın gelişimine yönelik dinamik adımlardan bir diğerinin ise; NATO-AB Siber Savunma Teknik Düzenlemesi üzerinde anlaşmaya varılmasıyla atılmış olduğu söylenebilir.[509] Teknik Düzenleme, 2016'nın Şubat ayındaki NATO savunma bakanlarının yıllık toplantısı öncesinde Avrupa Birliği Bilgisayar Acil Müdahale Ekibi (CERT-EU) Başkanı Freddy Dezeure ve NCIRC

---

https://www.eumonitor.eu/9353000/1/j4nvke1fm2yd1u0_j9vvik7m1c3gyxp/vkcwedvmmjzx/v=s7z/f=/join(2013)1_en.pdf, (Erişim tarihi: 16.12.2020), ss. 4-5.

[505] European Parliament, "Cybersecurity in the EU Common Security…", ss. 53.54.

[506] European Union External Action Service, *A Europe that Protects: Countering Hybrid Threats*, Haziran 2018, https://eeas.europa.eu/sites/eeas/files/hybrid_threats_en_final.pdf, (Erişim tarihi: 16.12.2020), ss. 1-2.

[507] Jolyon Howorth, "EU–NATO Cooperation: The Key to Europe's Security Future", *European Security*, Cilt 26, Sayı 3, Temmuz 2017, s. 455.

[508] NATO, *Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization*, (05.12.2017), https://www.nato.int/cps/en/natohq/official_texts_133163.htm, (Erişim tarihi: 16.12.2020).

[509] Luukas K. Ilves, Timothy J. Evans, Frank J. Cilluffo ve Alec A. Nadeau, "European Union and NATO Global Cybersecurity Challenges", *Institute for National Strategic Security*, Cilt 6, Sayı 2, Temmuz 2016, s. 136.

Başkanı Ian West tarafından imzalanmıştır.[510] Bunun sonucunda hem NATO'ya hem de AB'ye tehdit oluşturan siber eylemler hakkında NCIRC ve CERT-EU arasında bilgi paylaşımı, siber eğitim programları ile tatbikatlarının ortak yürütülmesi ve siber güvenlik hakkında diğer önemli gelişmeler hakkında bilgi ve ileri deneyimlerin paylaşılması üzerine taahhüt verilmiştir.[511]

AB siber güvenlik personeli, 2017 ve 2018 yıllarında NATO'nun yürütmüş olduğu Siber Koalisyon ve Kilitli Kalkanlar tatbikatlarına katılım sağlamıştır.[512] Buna ek olarak Kasım 2018'de AB, Trident Juncture 18 kapsamındaki NATO personel komuta sonrası tatbikatına paralel olarak bir sivil-askeri kriz yönetimi tatbikatı gerçekleştirmiştir.[513] Bu tatbikatlar, personeller arası etkileşimin daha da geliştirilmesi için bir ortam sunarken, uzun süredir taahhüt edilen ortak saha tatbikatlarının teoriden pratiğe dönüştürülmesini getirmiş ve siber alandaki sorunların çözümüne yönelik gelecekte atılacak NATO-AB iş birliği adımları için de kapı açmıştır denilebilir.

2018 yılında ise AB ve NATO, siber tehditlerle mücadelenin temel hedefler arasında yer aldığı ortak bir deklarasyona imza atmışlardır. 2018 Ortak Deklarasyonu, siber saldırılara birlikte yanıt verme konusundaki iş birliği taahhüdünü yinelemiş ve AB-NATO iş birliğinin sürdürülebilirliğinin her iki örgüt açısından önemini vurgulamıştır.[514] Ancak, AB ve NATO'nun siber tehditlerle mücadeledeki farklı yaklaşımları göz önüne alındığında ortak deklarasyonun başarılı bir çizgide sürdürülüp sürdürülemeyeceği soru işareti oluşturmuştur. Nitekim, son yıllarda AB ile NATO

---

[510] NATO, *NATO and The European Union Enhance Cyber Defence Cooperation*, (10.02.2016), https://www.nato.int/cps/en/natohq/news_127836.htm, (Erişim tarihi: 17.12.2020).
[511] NATO, *NATO and EU Press Ahead With Cooperation On Cyber Defence*, (25.11.2016), https://www.nato.int/cps/en/natohq/news_138122.htm, (Erişim tarihi: 17.12.2020).
[512] EU-NATO, *Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017*, https://www.consilium.europa.eu/media/39782/fourth-report-ue-nato-cooperation-en.pdf, (Erişim tarihi: 16.12.2020), s. 5; European Defence Agency, *EDA Supports NATO CCD COE 'Locked Shields' Cyber Defence Exercise*, (05.04.2019), https://www.eda.europa.eu/info-hub/press-centre/latest-news/2019/04/05/eda-supports-nato-ccd-coe-locked-shields-cyber-defence-exercise, (Erişim tarihi: 18.12.2020).
[513] European Union External Action Service, *Crisis Preparedness: EU Launches Civil-Military Crisis Management Exercise*, (16.11.2018), https://eeas.europa.eu/delegations/fiji/53926/crisis-preparedness-eu-launches-civil-military-crisis-management-exercise_en, (Erişim tarihi: 18.12.2020).
[514] NATO, *Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organizatio*n, (10.07.2018), http://www.nato.int/cps/en/natohq/official_texts_156626.htm, (Erişim tarihi: 19.12.2020).

arasında siber güvenlik üzerine ortak tatbikatlar ve eğitim programları gerçekleştirilse dahi iş birliği faaliyetlerinin genel olarak pratik ve çalışma düzeyinde ilerlemesi sebebiyle hedeflenen seviyeden oldukça uzak olduğu görülmüştür. Bu duruma, Brexit Krizi ve ABD-AB arasındaki değişen politik tavır gibi transatlantik ilişkilerde dalgalanmanın oldukça yüksek olduğu bir döneme girilmesinin yanı sıra AB'nin stratejik özerklik ilkesi çerçevesinde yeni siyasi hedefler belirlemesinin de kısmen etkisinin bulunduğu ifade edilmektedir.[515]

Bruno Lete ve Piret Pernik'e göre, NATO ile AB'nin siber alandaki saldırı ve tehdit unsurlarına yönelik güçlü iş birliği faaliyetleri yürütmesini engelleyen üç temel sorun bulunmaktadır.[516] Bu bağlamda sorunlardan ilki, iki örgüt arasında ortak durumsal farkındalık ve bilgi paylaşımı eksikliğinin bulunması olarak belirtilmiştir. Bu kapsamda, NATO ve AB arasında stratejik, operasyonel ve taktiksel düzeydeki istihbarat verilerinin, siber olaylarla ilgili güvenlik açıklarının ve siber hazırlık durum bilgilerinin paylaşımı konusunda isteksiz olunmasının, siber tehditlerin erken tespit edilip ortak bir durumsal farkındalık oluşturulmasını engellediği savunulmaktadır.[517]

NATO ve AB'nin siber güvenlik alanında ortaklık faaliyeti yürütmesinde zorluk yaratan ikinci sorunun, iki örgütün siber hazırlık ve esneklik seviyelerindeki gelişmişliğin farklı olmasından kaynaklandığı ifade edilmektedir.[518] AB, NATO'nun aksine siber saldırı altındaki üye ülkelerine çeşitli kurum ve ekipler aracılığıyla doğrudan teknik destek sağlamamaktadır.[519] Bunun yerine, ENISA ve Avrupa Savunma Ajansı (*The European Defence Agency*, EDA) gibi kurumların girişimleri üzerinden bilgi alışverişine katkıda bulunmakta ve üyelerinin en güncel siber güvenlik uygulamalarını benimsemesinde bir forum görevi görmektedir.[520] Ayrıca, AB'nin siber alanda gelişmiş komuta ve yönetim bilgi sistemlerine ve de NATO'nun siber savunma yeteneğinin geliştirilmesinde denetim ve kontrolü elinde bulunduran Kuzey Atlantik Konseyi gibi en üst düzey siyasi karar verme organına sahip olmaması, iki örgütün ortaklık çerçevesinde atılacak adımların benimsenmesi hususunda

[515] Jolyon Howorth, *a.g.m.*, ss. 454-459.
[516] Bruno Lété ve Piret Pernik, *a.g.m.*, ss. 2-4.
[517] Bruno Lété ve Piret Pernik, *a.g.m.*, s. 3.
[518] Bruno Lété ve Piret Pernik, *a.g.m.*, s. 4.
[519] Jeffrey L. Caton, *a.g.e.*, s. 31.
[520] Piret Pernik, *a.g.m.*, s. 8.

problemlerin oluşmasına ve saldırılara karşı fiilen harekete geçen ortak yanıt olanaklarının verilememesine neden olduğu söylenebilir.

Üçüncü olarak ise, siber güvenlik üzerine iki örgütün dinamik iş birliği faaliyetleri yürütememesinde, ortak siber eğitim, öğretim ve tatbikatların beklenilen başarıyı henüz gösterememiş olmasının da büyük etkisinin bulunduğu belirtilmiştir.[521] AB ve NATO, kuruluşlarından günümüze sadece 2003 yılında siber yetenekleri içermeyen askeri bir ortak tatbikat gerçekleştirmişlerdir.[522] 2007, 2010 ve 2014 yıllarında planlanan ortak tatbikatlardan ise somut bir sonuç alınamamıştır.[523] Yakın dönemde AB'nin, NATO'nun çatısı altında organize edilen tatbikatlara katılım göstermesi konusunda yukarı yönlü bir ivme yakalanmasına rağmen, siber güvenlik ve savunma alanındaki tatbikatların büyük oranda ayrı ayrı yürütüldüğü görülmektedir.[524]

NATO temelinde öncelikle güçlü ve caydırıcı bir siber savunma yeteneği inşa edebilmek, ardından bölgeselden küresele askeri, siyasi, ekonomik, toplumsal ve hukuki boyutları kapsayan siber güvenlik alanı oluşturabilmek için AB'nin ve NATO'nun, siber güvenlik tehditlerine nasıl yaklaşılacağı ve yanıt verileceği konusunda fikir birliğine varmasının faydalı olacağına yönelik değerlendirmeler NATO toplantılarında gündeme gelmekte; bu hususta, siber saldırıların daha kısa süre içerisinde ve etkili yollarla önlenmesi, tespit edilmesi, caydırılması ve uluslararası hukuki boyutların harekete geçirilmesi için transatlantik iş birliğinin anahtar görevi görebileceği belirtilmektedir.[525] Gaiser ve Hagelstam gibi araştırmacılar tarafından ise,

---

[521] Bruno Lété ve Piret Pernik, *a.g.m.,* s. 5.

[522] Paul Cornish, "EU and NATO: Co-operation or Competition?", Briefing Paper, *Security and Defence*, European Parliament- Policy Department External Policies, Ekim 2006, https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/eunatorelations_/eunatorelations_en.pdf, (Erişim tarihi: 08.07.2021), ss. 10-12; European Parliament, "Cybersecurity in the EU Common Security…", s. 52.

[523] Bruno Lété ve Piret Pernik, *a.g.m.,* s. 3.

[524] European Parliament, "Cybersecurity in the EU Common Security…", s. 55.

[525]NATO, *Brussels Summit Declaration*, (30.08.2018), https://www.nato.int/cps/en/natohq/official_texts_156624.htm, (Erişim tarihi: 12.10.2020); NATO, "Brussels Summit Key Decisions…", s. 2; NATO, *Warsaw Summit Communiqué*, (29.03.2017), https://www.nato.int/cps/en/natohq/official_texts_133169.htm, (Erişim tarihi: 09.10.2020); Axel Hagelstam, "Cooperating to counter hybrid threats", (23.11.2018), *https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html*, (Erişim tarihi: 23.01.2021); Peter Pindják, "Deterring hybrid warfare: a chance for NATO and the EU to work together?", (18.11.2014),

her iki örgütün ortak siber savunma ve saldırı tatbikatlarını faaliyete geçirmesine, ortak siber güvenlik fonu oluşturulmasına ve siber alanda küresel norm ve davranış kurallarının geliştirilmesinde öncü olma çalışmaları yürütülmesine ihtiyaç duyulduğuna vurgu yapılmaktadır.[526]

3.2.3. Sanayi, Özel Sektör ve Akademiyle İş birliği Faaliyetleri

NATO'nun siber güvenlik yapısını korumak ve müttefiklerin kritik ağ altyapılarını güçlendirmeye teşvik etmek için attığı somut adımların bir diğeri ise; sanayi, akademi ve özel sektör temsilcileriyle iş birliğini derinleştirmek olmuştur.[527] Sanayi ve özel sektör alanındaki işletmelerin siber ortamda yer alan tehditlerle caydırıcı bir şekilde mücadele edebilmek için yeni teknolojileri benimseme ve teknolojik gelişimlere hızlı ayak uydurma dinamizmi oldukça yüksektir. Bu durum, aynı zamanda devletler, uluslararası örgütler ve özel sektör arasındaki siber alanı kapsayan iş birliğinin önem derecesinin artışını da tetiklemektedir.[528] Günümüzde, eğitim ve öğretim, bilgi paylaşım faaliyetleri, tatbikatlar ve çok uluslu akıllı savunma projeleri dahil olmak üzere NATO ile sanayi, akademi ve özel sektörün çalıştığı birçok iş birliği alanı bulunmaktadır.[529]

Son on yıl içerisindeki NATO politikalarında ve zirve sonuç bildirilerinde, siber güvenlik ve savunmanın önemli bir bileşeni olarak sanayi ile ortaklığın vurgulandığı görülmektedir. Sanayi, teknik çözümler ve yenilikler sağlamada merkezi

---

https://www.nato.int/docu/review/articles/2014/11/18/deterring-hybrid-warfare-a-chance-for-nato-and-the-eu-to-work-together/index.html, (Erişim tarihi: 22.01.2021).

[526] Laris Gaiser, "NATO-EU Collaboration on Hybrid Threats: Cooperation Out of Necessity with Potential Consequences on International Legal Framework", *National Security and The Future*, Cilt 20, Sayı 1-2, Aralık 2019, ss. 19-20; Axel Hagelstam, "Cooperating to counter hybrid threats", (23.11.2018), https://www.nato.int/docu/review/articles/2018/11/23/cooperating-to-counter-hybrid-threats/index.html, (Erişim tarihi: 23.01.2021); Bruno Lété, "Cooperation in Cyberspace", *The EU and NATO- The Essential Partners*, Derleyen: Gustav Lindstrom ve Thierry Tardy, European Union Institute for Security Studies, Paris 2019, ss. 35-36.

[527] Jens Stoltenberg, "The Secretary General's Annual Report 2019", *https://www.nato.int/nato_static_fl2014/assets/pdf/2020/3/pdf_publications/sgar19-en.pdf*, (Erişim tarihi: 26.12.2020), s. 27.

[528] Kyoung Min, Chai, Seung Chai, ve Mijeong Han, "An International Comparative Study on Cyber Security Strategy" *International Journal on Security and Its Applications*, Cilt 9, Sayı 2, Şubat 2015, s. 14.

[529] NATO, *Cyber defence*, (25.09.2020), https://www.nato.int/cps/en/natohq/topics_78170.htm, (Erişim tarihi: 23.12.2020).

bir rol oynamanın yanı sıra müttefik bilgi sistemlerinin önemli bir kısmının işletilmesini de sağlamaktadır.[530] Bu alandaki ilk iş birliği faaliyeti, 2014 yılındaki NATO Galler Zirvesi'nde, NICP'ın kurulması ile kurumsallaşmıştır.[531] İttifak, NICP projesi çerçevesinde NATO'nun siber güvenlik alanında çalışmalar yürüten personellerin ve uzmanların, üye devletlerden sanayi, özel sektör ve akademik alandan katılan temsilciler ile iletişim kurmaları için bir forum sağlamaktadır. Ortaklığın hedefleri arasında; özel şirketlerin uygulamış olduğu güncel teknolojik bilgi, inovasyon ve mesleki uzmanlığı İttifak'ın günlük eylemleri içerisine monte etmek, İttifak ile sanayi sektörü arasında bilgi paylaşım kanalı oluşturarak siber tehditler ve riskler hakkında ortak anlayış ve farkındalık yaratmak, İttifak'ın siber savunma eğitimi, öğretimi ve tatbikatlarındaki çabalarına katkıda bulunmak ve NATO'nun savunma tedarik zincirinde siber güvenliğin gelişimini sağlamak gibi unsurlar yer almaktadır.[532] NATO ve özel sektör arasında iş birliğinin gelişmesine yönelik bir diğer önemli gelişme, 2015 yılında Hollanda'nın Lahey kentinde düzenlenen Küresel Siber Uzay Konferansı olmuştur. Konferans boyunca NATO ile özel şirketler arasındaki iş birliğini artırmanın önemi vurgulanmış ve siber tehditlere karşı savunmasızlığın önüne geçilmesi konuları ele alınmıştır.[533]

NATO, siber güvenlik yeteneklerini artırabilmek için faaliyete geçirmiş olduğu İşbirliğine Dayalı Etkileşim Çerçevesi (*The Framework For Collaborative Interaction*, FFCI) programı kapsamında akademi, sanayi ve özel sektörle iş birliği çalışmalarının bel kemiğinin oluşturulmasında dinamik adımlar atmıştır.[534] NATO Müttefik Dönüşüm Komutanlığı (*The Allied Command Transformation*, ACT)

---

[530]NATO, *Brussels Summit Declaration*, (30.08.2018), https://www.nato.int/cps/en/natohq/official_texts_156624.htm, (Erişim tarihi: 12.10.2020); NATO, *Warsaw Summit Communiqué*, (29.03.2017), https://www.nato.int/cps/en/natohq/official_texts_133169.htm, (Erişim tarihi: 09.10.2020); NATO, *Wales Summit Declaration*, (05.09.2014), https://www.nato.int/cps/en/natohq/official_texts_112964.htm, (Erişim tarihi: 07.10.2020).

[531] Sorin D. Ducaru, *a.g.m.*, s. 19.

[532] Susan Davis, *a.g.m.*, s. 8; NCI Agency, *NATO launches Industry Cyber Partnership*, (18.09.2014), https://www.ncia.nato.int/about-us/newsroom/nato-launches-industry-cyber-partnership.html, (Erişim tarihi: 22.12.2020).

[533] NCI Agency, *Business Leaders Discuss NATO Industry Cyber Partnership*, (28.04.2015), https://www.ncia.nato.int/about-us/newsroom/business-leaders-discuss-nato-industry-cyber-partnership.html, (Erişim tarihi: 23.12.2020).

[534]NATO, *FRAMEWORK FOR COLLABORATIVE INTERACTION (FFCI)*, https://www.act.nato.int/ffci, (Erişim tarihi: 25.12.2020).

tarafından geliştirilen program; akademi ve sanayi temsilcileri ile ortaklıkları teşvik etmeyi amaçlamaktadır. FFCI kapsamında NATO, İttifak'ın genel etkinliğini artırmak, güncel tehditleri incelemek ve bu tehditlerle mücadele etmek için potansiyel ortakları iş birliği yapmaya davet etmiştir.[535] Bunun sonucunda İttifak, güncel bilgi ve teknolojilere erişim elde ederken aynı zamanda şirketlere de dünyanın en büyük askeri örgütüyle ortaklık çerçevesinde siber güvenliğin gelişimi üzerine çalışma fırsatına sahip olma imkanı tanınmıştır. NATO, yakın dönem içerisinde Oracle, Everis ve Havelsan gibi savunma ve bilişim sektöründe önemli şirketler ile iş birliği anlaşmaları imzalayarak bu alana verdiği önemi göstermiştir.[536] Bunun yanı sıra 2019 yılında NATO'nun 13. Genel Sekreteri Jens Stoltenberg, NATO'nun siber savunma yeteneklerini geliştirmek için özel sektör ile olan ilişkilerini ilerletmesi gerektiğini vurgulamıştır.[537]

Sonuç olarak günümüzün teknoloji şirketlerinin, siber güvenlik alanında devletler ve uluslararası örgütler karşısında tarihteki tüm sektörlerden daha fazla güce sahip olduğu belirtilmektedir.[538] Örneğin, dünyada sadece 14 ülkenin gayri safi yurt içi hasılasının, Apple'ın 2019 yılındaki piyasa değeri olan 1,4 trilyon dolardan daha yüksek seviyede olduğu açıklanmıştır.[539] NATO'nun siber uzayda özel sektörle iş birliği yapmasının öneminin anlaşılması, siber savunmasını geliştirmeye yönelik önemli bir adım olarak değerlendirilebilir. Bu kapsamda NATO, özel sektörle iş birliğini her fırsatta vurgulayarak teknolojik inovasyonun ve özel sektördeki uzmanlığın kritik öneme sahip olduğunu belirtmektedir.[540]

---

[535] NATO, *Framework For Collaborative Interaction (FFCI),* https://www.act.nato.int/ffci, (Erişim tarihi: 24.12.2020).

[536] NCI Agency, *Three NATO Industry Cyber Partnership agreements signed at NIAS'19*, (17.10.2019), https://www.ncia.nato.int/about-us/newsroom/three-nato-industry-cyber-partnership-agreements-signed-at-nias19-.html, (Erişim tarihi:24.12.2020); CyberMag, *HAVELSAN ile NATO Muhabere ve Bilgi Ajansı (NCIA) Arasında Siber Güvenlik İş Birliği Anlaşması*, (22.10.2019), https://www.cybermagonline.com/havelsan-ile-nato-muhabere-ve-bilgi-ajansi-ncia-arasinda-siber-guvenlik-is-birligi-anlasmasi, (Erişim tarihi:25.12.2020).

[537]Jens Stoltenberg, "NATO Will Defend Itself", (29.08.2019), *https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en*, (Erişim tarihi:25.12.2020).

[538] Susan Davis, *a.g.m.*, s. 10.

[539] Mark Kolakowski, "At $1.3 Trillion, Apple Is Bigger Than These Things." (06.01.2020), *https://www.investopedia.com/news/apple-now-bigger-these-5-things/*, (Erişim tarihi:27.12.2020).

[540] James Black ve Alice Lynch, "Cyber Threats to NATO from a Multi-Domain Perspective", *Cyber Threats and NATO 2030: Horizon Scanning and Analysis*, Derleyen: Amy Ertan, Kathryn H. Floyd, Piret Pernik ve Tim Stevens, NATO CCDCOE Publications, Tallinn 2020, s. 140.

3.2.4. Kuzey Atlantik Antlaşması'nın 5. Maddesi Kapsamında Yetki Sınırı ve Atıf Sorunu

Siber uzayda, askeri tabanlı sistemlere sızılarak verileri manipüle etmekten, kritik altyapılarda kasti olarak tahrip edici arızalara neden olmaya ve tüm ülkeyi felç edecek DDoS saldırılarıyla siyasi, ekonomik, toplumsal ve çevresel sektörlerde yıkıcı girişimler doğurmaya kadar çeşitli siber saldırı yöntemleri bulunmaktadır. Bu nedenle siber uzayda, tüm saldırılarla mücadele etmek teoride ve pratikte imkânsız bir hal almıştır.[541] Bununla birlikte; siber saldırıların yol açtığı hasarın, benzer bir konvansiyonel saldırı sonucu oluşan tahribatla karşılaştırılmasına yönelik küresel siber norm ve davranış kuralları eksikliği, uluslararası sistemdeki çeşitli aktörlerin bu alanda sağlam temellere dayanan adımlar atmasına engel teşkil edebilmektedir.[542]

Günümüzün değişken, karmaşık ve belirsiz dünyasında modern saldırı ve tehdit yöntemlerinin siber alanda geniş ölçüde yer bulmaya başlamasıyla beraber NATO'nun, güvenlik ortamını korumaya yönelik geniş kapsamlı reformlar uygulamaya geçirdiği görülmektedir. Bu alanda yapılmış en önemli girişim olarak, 2014 yılındaki Galler Zirvesi'nde İttifak'ın devlet ve hükümet başkanları tarafından siber savunmanın, Kuzey Atlantik Anlaşması'nın 5. Maddesine dayanan kolektif savunma ilkesinin bir parçası halini aldığının ilan edilmesi olmuştur.[543] Bir diğer ifadeyle, 11 Eylül 2001 tarihindeki terörist saldırılara yanıt olarak uygulamaya geçirildiği gibi İttifak'a veya üye ülkelere yönelik siber saldırılar karşısında toplu müdahalenin potansiyel olarak mümkün olduğu deklare edilmiştir.[544] Galler Zirvesi Sonuç Bildirisi aracılığıyla, Kuzey Atlantik bölgesinin güvenliğini sağlamak ve korumak için silahlı kuvvet kullanımı dahil olmak üzere siber saldırgana karşı harekete geçmek için hukuksal bir çerçeve oluşturulmaya çalışılmıştır.[545] Galler Zirvesi Sonuç

---

[541] Jonathan Solomon, "Cyber Deterrence Between Nation-States: Plausible Strategy or a Pipe Dream?", *Strategic Studies Quarterly*, Cilt 5, Sayı 1, Bahar 2011, ss. 5-6.
[542] Michael Horowitz, "A Common Future? NATO and the Protection of the Commons" *The Chicago Council On Global Affairs*, Transatlantic Paper Series Sayı 3, Ekim 2010, s. 6.
[543] NATO, *The Atlantic Charter*, (02.07.2018), https://www.nato.int/cps/bu/natohq/official_texts_16912.htm, (Erişim tarihi: 01.01.2021).
[544] Joe Burton, *a.g.m.*, s. 308.
[545]NATO, *Wales Summit Declaration*, (05.09.2014), https://www.nato.int/cps/en/natohq/official_texts_112964.htm, (Erişim tarihi: 06.10.2020).

Bildirisi'nde; bir yandan siber tehditlerle etkin bir mücadele belirlenmesi hususunda oldukça önemli kararlar bulunmaktayken, diğer yandan toplu savunma ilkesinin uygulamaya geçirileceği somut koşulların tanımlanması konusunda ortak bir karar alınmaması, İttifak'ın siber güvenlik politikası içerisinde yeni anlaşmazlıkların doğmasına neden olmuştur.[546]

Esas olarak, siber uzaydan gelebilecek tehditlere yanıt vermek için Kuzey Atlantik Antlaşması'nın 5. Maddesinin devreye sokulabileceği belirli bir eşiğin tanımlanmaması, bazı ikilemleri de beraberinde getirmiştir.[547] Bu ikilemler bağlamında NATO'nun, siber güvenlik politikası çerçevesinde Kuzey Atlantik Antlaşması'nın 5. Maddesini uygulamaya geçirebilmesi için iki temel şartı dikkate alması gerektiği değerlendirilmektedir.[548] Dikkate alınmasının fayda sağlayabileceği şartlardan ilki, NATO'yu veya üye devletleri hedef alan tehlikeli siber saldırılar durumunda, İttifak'ın siber güvenlik alanındaki uzmanları ve karar vericileri tarafından saldırıların doğrudan ve dolaylı etkilerinin yanı sıra hedefleri açısından da incelenmesi gerektiği üzerinedir.[549] Bu kapsamda Lakomy, siber saldırıların; askeri yeteneklerin, kritik altyapının ve daha az olumsuz etkiye yol açabilecek unsurların hedef alınması olarak üç farklı kategori içerisinde ele alınması gerektiğini belirtmektedir.[550] Birinci kategori temelinde, askeri tesisler ve silah sistemlerine saldırı gerçekleştirmenin BM Antlaşması'nın 51. Maddesi kapsamında değerlendirilebileceği için Kuzey Atlantik Antlaşması'nın 5. Maddesinin harekete geçirilmesine yönelik herhangi bir tartışma yaratmayacağı ifade edilmektedir.[551]

İkinci kategori içerisinde yer alan kritik altyapı sistemleri, hava kontrol sistemleri ve sağlık sistemleri gibi hayati hizmetleri hedef alan dijital saldırılar; önemli derecede can kaybına, fiziksel hasara ve devletlerin işleyişinin yeterince uzun bir süre bozulmasına neden olabilmektedir.[552] Beraberinde, NATO'nun komuta ve kontrol

[546]Warwick Ashford, "NATO to adopt new cyber defence policy", (03.09.2014), *https://www.computerweekly.com/news/2240228071/Nato-to-adopt-new-cyber-defence-policy*, (Erişim tarihi: 02.01.2021).
[547] Miron Lakomy, *a.g.m.*, s. 36.
[548] Piret Pernik, *a.g.m*., ss. 12-13.
[549] Miron Lakomy, *a.g.m.*, s. 37.
[550] Miron Lakomy, *a.g.m.*, ss. 37-38.
[551] Miron Lakomy, *a.g.m.*, s. 38.
[552] Miron Lakomy, *a.g.m.*, s. 39.

sistemleri, enerji şebekeleri veya üye bir devletin güvenliği, ekonomisi, halk sağlığı ve anayasal düzeni üzerinde geri döndürülemez hasara yol açabilecek olan bu siber saldırılar, aynı zamanda silahlı saldırı eşiğini aşabileceğinden NATO'nun 5. Madde kapsamında harekete geçebilmesinin siyasi ve hukuki yolları üzerine çalışmalara başlaması için de öncü olabileceği belirtilmiştir.[553]

Üçüncü kategori kapsamında ise; bilgisayar, bilgisayar sistemleri, web siteleri, e-posta sunucularını hedef alan siber saldırılar sonucu sistemin veya verilerin silinmesi, bozulması, değiştirilmesi gibi saldırılar ile karşı karşıya kalınabilmektedir. Bu kategori içerisinde değerlendirilen referans nesnelerinin siber saldırılara hedef olması halinde ortaya çıkacak hasar, ikinci kategoriye göre oldukça düşük kalabilmektedir.[554] Sözü geçen bileşenlerin saldırıya uğraması halinde can kaybına yol açma ihtimalinin düşük olması ve zarar gören ağların geri dönüştürülmesinin nispeten daha kolay olması nedeniyle 5. Madde yerine örgüt düzeyinde siber diplomasinin faaliyete geçirilmesinin veya caydırıcı yaptırımların devreye sokulmasının daha doğru bir adım oluşturacağı düşünülmektedir.[555] Yukarıdaki üç farklı kategoriden yola çıkarak Kuzey Atlantik Antlaşması'nın 5. Maddesini faaliyete geçirebilmek için yalnızca askeri yeteneklerin hedef alınmasının tek koşul olarak belirlenmemesi, bunun yanı sıra kritik altyapı sistemlerinin işleyişi üzerinde hayati sonuçlar doğurabilecek siber saldırıların da kapsam içerisine dahil edilmesi üzerine çalışmalar yürütülmesi gerektiği değerlendirilmektedir.[556] Bu bağlamda NATO CCD COE'de avukat olarak görev yapan Eneken Tikk, siber saldırının silahlı bir saldırıyla karşılaştırılabilir bir hasar yaratma durumuna göre 5. Maddenin tetiklenmesine yönelik kritik eşik değerlendirmesinin yapılması gerektiğini belirtmektedir.[557]

---

[553] Murat Doğrul, Adil Aslan ve Eyyüp Çelik, "Developing an international cooperation on cyber defense and deterrence against cyber terrorism", 3rd International Conference on Cyber Conflict, *CCD COE Publications*, Tallinn 2011, s. 40.

[554] Marco Roscini, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Nisan 2014, ss. 52-53.

[555] Oliver Fitton, "Cyber operations and gray zones: Challenges for NATO", *The Quarterly Journal*, Cilt 15, Sayı 2, Bahar 2016, s. 111.

[556] Oliver Fitton, *a.g.m.*, s. 117.

[557] Michael Smith and Peter Warren, "Nato Warns of Strike Against Cyber Attackers", (06.06.2010), *https://www.thetimes.co.uk/article/nato-warns-of-strike-against-cyber-attackers-97qkr5lbtwp*, (Erişim tarihi: 08.01.2021).

NATO'nun, siber alanda kolektif müdahaleyi devreye sokabilmesinin ikinci bir şartı, saldırıyı gerçekleştiren aktöre yönelik atıf sorununu kesin olarak çözmesiyle ilgili olarak değerlendirilmektedir. Buna göre, siber saldırıların ardındaki faillerin kimliğinin kesin olarak tespiti ve kanıtlanması hem uzun bir süreci kapsayabilmekte hem de zordan imkansıza kadar değişebilmektedir.[558] Siber saldırıları gerçekleştirebilmek için gerekli donanımın ucuz olması ve kolayca erişilebilmesi, siber suçları gerçekleştiren aktör/aktörlerin kapsamını da genişletmiş, bireylerden ulus devletlere kadar hemen her aktör, bu kapsamda değerlendirilir hale gelmiştir. Buna ek olarak, saldırının hemen her konumdan başlatılabilmesi ve gizli olarak erişimin sağlandığı herhangi bir ağa yönlendirmenin gerçekleştirilmesi, saldırının veya tehdit oluşturan yazılımın kaynağını takip etme hususunda engeller oluşturabilmektedir.[559] Thomas Rid ve Ben Buchanan'ın; mükemmel siber saldırının failini tespit etmenin, hatasız olarak işlenmiş bir suç kadar zor olduğu ifadeleri, bu bağlamda bir değerlendirme olarak ele alınabilir.[560]

Son yıllarda siber saldırıların kaynağının takibi üzerine önemli teknolojik atılımlar gerçekleştirilmesine rağmen, siber güvenlik uzmanları tarafından faillerin kesin olarak tespitinin somut kanıtlar yerine öncüllere dayanmaya devam ettiği kabul edilmektedir.[561] Bazı siber güvenlik birimleri tarafından, bilgisayar korsanlarının IP adreslerinin takibi ve kullanılan saldırı yöntemlerinin ayırt edici özelliklerinin analiz edilerek suçlularla bağdaştırılabilmenin teknik olarak mümkün olduğu açıklanmış olmasına karşın, failin kesin olarak bilinmesinin ve yeterli kanıtın toplanmasının oldukça zor olması nedeniyle yasal olarak harekete geçme durumu oluşmamaktadır.[562] Üst düzey siber korsanlar; farklı bir IP adresi üzerinden saldırı gerçekleştirerek, belirli bir programlama dilini kullanarak veya kodlama hatası gibi görünen verileri ustaca sisteme yerleştirerek siber operasyonlardaki rollerini belli bir dereceye kadar

---

[558] Rex Hughes, "A Treaty For Cyberspace", *International Affairs*, Cilt 86, Sayı 2, Mart 2010, ss. 528-529.
[559] P.W. Singer ve Allan Friedman, *a.g.e.*, ss. 108-109.
[560] Thomas Rid ve Ben Buchanan, "Attributing Cyber Attacks," *Journal of Strategic Studies*, Cilt 38, Sayı 1-2, Haziran 2015, s. 32.
[561] Warwick Ashford, "Cyber attack retaliation a bad idea, says international panel", (27.09.2013), *https://www.computerweekly.com/news/2240206279/Cyber-attack-retaliation-a-bad-idea-says-international-panel*, (Erişim tarihi: 05.01.2021).
[562] Miron Lakomy, *a.g.m.*, s. 39.

saklayabilme potansiyeliyle hareket edebilmektedir.[563] Bu da çoğu zaman siber saldırıların faillerinin tespitini, siber güvenlik alanındaki en yetkili firmalar tarafından siber saldırı analizleri yapılıyor olsa dahi zorlaştırmakta ve hatta mümkün kılmamaktadır.[564]

Sonuç olarak, yetki sınırı ve atıf sorunlarına yönelik tüm bu değerlendirmeler ışığında, kolektif savunma prensibi temelinde izin verilen eylem biçimlerinin net biçimde kararlaştırılmadan Kuzey Atlantik Antlaşması'nın 5. Maddesinin faaliyete geçirilmesinin oldukça düşük bir ihtimal olduğu değerlendirilebilir. Bununla birlikte NATO'nun gelecek yıllarda 5. Maddeyi devreye sokma girişimine karar vermesi halinde, etkili ve güvenilir bir yaklaşım ortaya koyulması için bazı adımların atılmasının gerekliliği ortaya çıkmaktadır. Bu adımlardan biri olarak, sadece askeri yetenekler ve ülkelerin olağan işleyişleri üzerine hayati etki yaratan siber saldırı durumlarında toplu siber savunma mekanizmasının tetiklenmesinin yeterli bir koşul olarak belirlenmesi üzerine hukuki çalışmaların yürütülmesinin gerekliliğidir.[565] Bir başka gereklilik ise, NATO'nun ve müttefiklerinin siber saldırılara hedef olması halinde gerekli tedbirlerin alınmasını ve müdahalenin yapılmasını sağlayacak bir erken uyarı sisteminin kurulması olarak ortaya çıkmaktadır.[566] Saldırının asıl sorumlusunun kesin olarak belirlenmesi hem savunma sistemleri üzerinde gerekli önlemlerin alınabilmesi hem de mücadele yeteneklerinin harekete geçirilerek saldırıya cevap verilebilmesi açısından önemli görülmektedir.

---

[563] Nikolay Koval, "Revolution Hacking", *Cyber War in Perspective: Russian Aggression against Ukraine,* Derleyen: Kenneth Geers, NATO CCD COE Publications, Tallinn 2015, s. 55.

[564]Tim Worstall, "Stuxnet Was a Joint US/ Israeli Project", (01.01.2012), *https://www.forbes.com/sites/timworstall/2012/06/01/stuxnet-was-a-joint-us-israeli-project/?sh=7bef79ab7a8a*, (Erişim tarihi: 07.01.2021); Jim Finkle ve Joseph Menn, "Some Flame code found in Stuxnet virus-experts", (11.06.2012), *https://www.reuters.com/article/us-media-tech-summit-flame/some-flame-code-found-in-stuxnet-virus-experts-idUSBRE85A0TN20120611*, (Erişim tarihi: 08.01.2021).

[565] Miron Lakomy, *a.g.m.,* ss. 40-41.

[566] Jason Healey ve Leendert van Bochoven, "Strategic Cyber Early Warning: A Phased Adaptive Approach for NATO", Issue Brief, *Atlantic Council,* Kasım 2012, *https://www.atlanticcouncil.org/wp-content/uploads/2012/11/NATO-Cyber-Warning-2012.pdf*, (Erişim tarihi: 14.01.2021), s. 7.

SONUÇ

21. yüzyıl itibarıyla bilgi ve teknoloji alanında öngörülemeyen hızdaki gelişmeler sonucu, ‘siber’ kavramının ön plana çıktığı görülmektedir. Dijital ağlara erişimin zamanla askeri alandan sivil hayata kadar genişlemesi, sonsuz bir sanal dünyanın oluşumunu sağlamıştır. Bilgi teknolojilerinin aktif gelişimini sürdürmesi, uygulama alanını genişletmesi ve kullanım alanını artırması, bu teknolojilerin sadece bilgi alışverişi ve bilgiyi işleme aracı olarak değil, aynı zamanda uluslararası güvenlik tehdidi oluşturmanın bir yolu olarak da kullanılmasına yol açmıştır. Böylece, devletlerin ulusal güvenlik politikalarına bilginin elde edilmesi ve korunması dahil edilmeye başlanmış ve devletler açısından sınır güvenliğini korumak ne kadar önemliyse bilgi güvenliğini sağlamak da o derece önemli hale gelmiştir. Ulusal ve uluslararası güvenliğin kapsam alanına bilgi ve iletişim teknolojilerinin dahil edilmesiyle, siber tehditlerin yıkıcı etkilerine karşı daha etkili ve güncel önlemler alınmasında teknolojik gelişmeler itici güç oluşturmuşlardır. Günümüzde, ülkelerin sahip olduğu klasik orduların yanı sıra teknolojinin hızla gelişiminden yararlanılarak geliştirilen tanklar, denizaltılar, balistik füzeler, insansız hava araçları, savaş uçakları ve savaş gemileri aracılığıyla güvenlik tehditleriyle mücadelede etkili savunma ve caydırıcılık sağlanabilmektedir.

Son yirmi yıl içerisinde “siber” ön ekli terimler; politikacılar, bilgi ve iletişim teknolojileri yöneticileri, hükümet temsilcileri ve ulusal güvenlik uzmanları gibi farklı aktörlerin söylemlerinde yaygın olarak yer almaya başlamış ve böylelikle, NATO da dahil olmak üzere bazı devletlerin ve uluslararası örgütlerin siber alanın güvenliğini sağlama faaliyetleri önem kazanmıştır. Birbirine bağlı ve bağımlı bilgi ve iletişim teknolojileri ağından oluşan küresel alan, siber uzay olarak nitelendirilmekte; siber güvenlik ise, fiziksel ve sanal dünyanın sürekli olarak birbirleri ile etkileşim halinde bulunması sonucu bu ağların içerisinde yer alan verilerin ve hizmetlerin saldırganlar tarafından yasa dışı yollarla erişilip zarar verilmesinden korunması olarak ifade edilmektedir.

NATO'nun 4 Nisan 1949'daki kuruluşu, dönemin süper güçleri olan ABD ve SSCB arasındaki Soğuk Savaş mücadelesinin iki kutupluluğundan

kaynaklanmaktadır. NATO'nun kuruluşuna bir yanıt olarak 1955 yılında SSCB öncülüğünde Varşova Paktı kurulmuştur. NATO ve Varşova Paktı, ABD ve SSCB arasındaki askeri ve siyasi mücadelenin bir aracı olmalarının yanı sıra iki blok arasındaki karşılıklı tehdit ve askeri eylem algılarını paylaşan kolektif savunma örgütü görevi görmüşlerdir. 1991 yılında SSCB'nin dağılması, Soğuk Savaş dönemi boyunca strateji ve politikalarını SSCB tehdidini gözeterek faaliyete geçiren NATO'nun varoluş nedeninin, misyonunun ve amacının da sorgulanmasına yol açmıştır. 1991 ve 1999 yıllarında açıklanan NATO'nun stratejik konseptlerinin, İttifak'ın siyasi misyonunun yeniden oluşturulmasında, derinleşen ve genişleyen uluslararası güvenlik ortamında yeni rolünün tanımlanmasında ve transatlantik ortaklığın kurumsallaşmasında önemli dönüşüm noktalarını temsil ettiği söylenebilir. Böylece 2000'li yıllarda NATO, yeni bir uluslararası rol arayışı içinde savunma örgütünden, ortak durumsal farkındalık, bilgi paylaşımı, kriz yönetimi, iş birliği ve erken müdahale konularına da öncelik veren küresel düzeyde bir kolektif güvenlik örgütüne yönelik yapısal bir dönüşüm sürecine girmiştir. Bu yapısal dönüşüm süreci içerisinde NATO'nun genişleyen güvenlik anlayışında siber alanla bağlantılı konular daha geniş yer kaplamış ve siber güvenliğin önem düzeyi gittikçe artış göstermiştir.

Siber alandan yayılan tehditlerin önemli güvenlik krizlerine yol açabileceği, NATO'nun siyasi gündeminde ilk kez 2002 yılındaki Prag Zirvesi'nde yer almıştır. Ayrıca, İttifak'ın siber güvenlik algısının gelişiminde kritik dönüm noktalarını, 2007'de Estonya'yı hedef alan etkisi büyük siber saldırılar, 2008'de Gürcistan'a düzenlenen hibrit saldırılar ve 2014 yılında Ukrayna'ya gerçekleştirilen DDoS ağırlıklı siber saldırılar oluşturmuştur. NATO'nun saldırı amacıyla kendi siber yeteneklerine sahip olmadığı göz önünde bulundurulduğunda, İttifak'ın siber güvenlik politikası içerisinde üye devletlerin bireysel sorumluluğunun kritik önemi ön plana çıkmıştır. Bu nedenle NATO, siber uzaydaki tehlikelerle başa çıkma konusunda üye devletlerin sahip olduğu ulusal sorumluluğun önemine daima vurgu yapmaktadır. Bu kapsamda 2016 yılında açıklanan Siber Savunma Taahhüdü ile üye devletler, ulusal saldırı önleme sistemlerini güçlendirmeyi ve siber dayanıklılığını artırma çalışmalarını hızlandırmayı kabul etmişlerdir. 2021 yılındaki NATO Brüksel Zirvesi Sonuç Bildirisi'nde, uluslararası sistem içerisinde hem devlet hem de devlet dışı aktörlerden

gelecek siber tehdit ve saldırı ortamına uyum sağlanması hususunda gerekli olan değişim ve dönüşüm çalışmalarına devam edileceğinin ve üye devletlerin siber alandaki yeteneklerinin İttifak'ın operasyonlarına etkin entegrasyonunun artırılacağı belirtilmiştir. 2018 yılında ise, NATO Brüksel Zirvesi'nde üye devletler tarafından 2023 yılında kapsamlı faaliyete geçecek ortaklaşa bir Siber Uzay Operasyon Merkezi kurulması onaylanmıştır. Bu bağlamda NATO'nun, son yirmi yıl boyunca siber alandan gelebilecek çok yönlü ve çok boyutlu tehditlere yönelik kritik güvenlik sistemlerinin savunmasının artırılması, üye ülkelerin barış ve istikrarını tehlikeye atabilecek siber saldırılarla mücadele etmeye İttifak'ın güvenlik öncelikleri arasında yer verdiği anlaşılmaktadır.

NATO, CCD COE öncülüğünde gerçekleştirilen Kilitli Kalkanlar ve Siber Koalisyon gibi özel siber tatbikatların yanı sıra kriz yönetiminin hem siyasi hem de askeri yönlerini ele alan ve büyük ölçekli tatbikatlara entegre edilmiş dinamik eğitim, öğretim ve konferans programları faaliyete geçirilmiştir. Bu sebeple NATO'nun, her türlü tehdide yönelik daha güçlü bir siber savunma geliştirmek için kurumsal yapılanmasında esnekliği artırmanın yanı sıra eğitim, öğretim ve tatbikat programlarına dikkate değer bir zaman, çaba ve kaynak yatırımı sağladığı görülebilmektedir. Buna rağmen eleştirel bağlamda, bir zincirin en zayıf halkası kadar güçlü olduğu prensibinin dışına çıkılarak öncelikle kendi siber savunmasının gelişimine odaklanıldığı ve üye devletlerin siber güvenlik alanındaki gelişim ve dönüşümlerini bireysel inisiyatiflerine bırakıldığı birçok kez NATO zirvelerinde ifade edilmiştir. Ayrıca, siber güvenlik alanında NATO ile üyeler arasındaki ve üyelerin kendi aralarındaki bilgi paylaşımını ve iletişim kanallarını açık tutma hususundaki eksiklik nedeniyle gelecek yıllarda İttifak'ı ve üyelerini hedef alacak siber saldırılarda oldukça büyük fiziksel, toplumsal ve finansal kayıplar ile karşı karşıya kalınabilme ihtimali bulunmaktadır. Bu doğrultuda NATO'nun, kolektif ve bireysel siber savunma yeteneklerini güçlendirmek için siber güvenlik alanındaki kurumlarının desteğiyle her üye devletin siber alanda iş birliği yapmasına ve bilgi paylaşımı gerçekleştirmesine teşvik edecek çalışmaları ve politikaları bir an önce somutlaştırmasının önemine ilişkin değerlendirmeler de NATO bünyesinde ele alınan konular arasındadır.

2010 yılındaki NATO Lizbon Zirvesi'nden itibaren AB'nin ve NATO'nun, siber alan odaklı kurumsal bir ortaklık ve iş birliği çabalarına ağırlık vermelerine rağmen, iki örgüt arasındaki siber güvenlik alanındaki sorunların ve olası çözüm yollarının net bir çerçevede ele alınmasındaki eksiklikler nedeniyle siber sorunlarla mücadelede karşılıklı anlaşmazlıkların yaşanabildiği görülmektedir. Buna ek olarak AB'nin ve NATO'nun farklı yönetişim seviyelerine ve ortak olmayan bazı üyelere sahip olması, bu sorunun giderek daha karmaşık bir duruma gelmesine de neden olabilmektedir. Dijitalleşme ve teknolojik gelişimin uluslararası yapının her bir noktasına etki etmeye başladığı günümüzde, AB ve NATO arasında siber güvenlik konusunda anlaşmazlıklara neden olan konuların detaylıca analiz edilmesinin ve çözüm yollarının olabildiğince hızlı uygulamaya geçirilmesinin, siber güvenliğe yönelik uluslararası iş birliği mekanizmalarının niteliğinin geliştirilmesinin ve sıklığının artırılmasının gerekli olduğu ortaya çıkmaktadır. Bu bağlamda, NATO'nun; siber güvenliğin stratejik, operasyonel ve taktiksel düzeylerinde AB ile daha uyumlu çalışmasının hem siber savunma sistemlerin gelişiminde hem de mevcut savunma ve caydırıcılık yeteneklerinin ileri seviyelere taşınmasında katkı sağlayacağı çeşitli NATO platformlarında değerlendirilmektedir.

2014 yılındaki NATO Galler Zirvesi'nde, İttifak'ı veya üye devletleri hedef alan bir saldırının Kuzey Atlantik Antlaşması'nın 5. Maddesinin devreye sokulmasını tetikleyebileceğini belirten bir politika onaylanmıştır. 2014 yılından günümüze kadar geçen süreçte, NATO zirvelerinde ve İttifak'ın temsilcileri tarafından siber uzay yoluyla saldırıya uğranması durumunda 5. Maddenin uygulanmasına karar verme durumunun öncelikle tartışılacağına, uluslararası hukuka ters düşecek ani kararların alınmasından kaçınılacağına ve bu nedenle karar verilen eylem biçiminin esnekliğini koruyacağına yönelik açıklamalar yapılmıştır. 2021 yılındaki NATO'nun Brüksel Zirvesi'nde ise, Kuzey Atlantik Antlaşması kapsamında 5. Maddenin devreye sokulmasını gerektiren kararların, olay bazında incelemeler sonrası alınacağı belirtilmiştir. Siber saldırılara yönelik olay bazında incelemelerin gerçekleştirileceği ifade edilmesine rağmen, siber uzayda devlet davranışlarını ele alan uluslararası norm ve ilkelerin eksikliği, aynı zamanda NATO'nun kümülatif yapıdaki siber tehditlerle mücadele çabalarını zorlaştırmaktadır. Böylece, uluslararası alanda hangi siber

olaylara nasıl yanıt verileceği konusunda fikir birliğine varılamamış olması sebebiyle, NATO'nun siber saldırılara yanıt konusundaki belirsizlik durumunun henüz çözülemediği anlaşılmaktadır. Ayrıca, gizli olarak erişimin sağlandığı IP adresi veya adresleri üzerinden siber saldırı gerçekleştirilebilmesi, somut kanıtlar elde edilmesinin ve saldırıyı gerçekleştiren aktöre kesin olarak atfetmenin önüne geçebilmektedir. Bunun sonucunda, NATO'yu veya üyelerini hedef alan siber saldırılara yanıt olarak Kuzey Atlantik Antlaşması'nın 5. Maddesi kapsamındaki kolektif müdahale ilkesinin uygulamaya geçirilmesini oldukça güçleştirmektedir.

KAYNAKÇA

Kitaplar / Raporlar:

AKAD, Mehmet T., *Modern Savaşın Temel Kavramları*, Kitap Yayınevi, Ankara 2011.

AKYEŞİLMEN, Nezir, *Disiplinlerarası Bir Yaklaşım ile Siber Politika ve Siber Güvenlik,* Orion Kitabevi, Ekim 2018.

ANDRESS, Jason ve Steve WINTERFELD, *Cyber Warfare: Techniques, Tactics And Tools For Security Practitioners*, 2. Baskı, Syngress, Ekim 2013.

ARIMAN, Orhan, *Zafersiz Barış ya da NATO*, Ajans Türk Matbaacılık Yayınları, Ankara 1977.

ARMAOĞLU, Fahir, *20. Yüzyıl Siyasi Tarihi 1914-1980*, Türkiye İş Bankası Yayınları, Ankara 1988.

BAEZNER, Marie ve Patrice ROBIN, *Hotspot Analysis: Cyber-Conflict Between The United States Of America And Russia*, Center for Security Studies (CSS), Zürih 2017.

BAEZNER, Marie ve Patrice, ROBIN, *Hotspot Analysis: Cyber and Information warfare in the Ukrainian conflict*, Center for Security Studies (CSS), Zürih 2018.

BAYRAKTAR, Gökhan, *Siber Savaş ve Ulusal Güvenlik Stratejisi*, Yeniyüzyıl Yayınları, İstanbul 2015.

BENDIEK, Annegret ve Tobias METZGER, "Deterrence Theory in the Cyber-Century," Working Paper RD EU/Europe, *German Institute for International and Security Affairs*, Mayıs 2015.

BİLGİN, Pınar, *Regional Security in the Middle East: A Critical Perspective*, Routledge, Londra 2019.

BOOTH, Ken, *Theory of World Security*, Cambridge University Press, Cambridge 2007.

BOSTANOĞLU, Burcu, *Türkiye-ABD İlişkilerinin Politikası*, İmge Kitabevi, Ankara 1999.

BULL, Hedley, *The Anarchical Society: A Study Of Order in World Politics*, 3. Baskı, Columbia University Press, Ekim 2002.

BUZAN, Barry, *People, States and Fear: An Agenda for International Security Studies in the Post-Cold War Era*, ECPR Press, Londra 2009.

BUZAN, Barry ve Lene HANSEN, *The Evolution of International Security Studies*. Cambridge University Press, New York 2009.

CARR, Edward Hallet, *The Twenty Years' Crisis 1919-1939: An Introduction to the Study of International Relations*, Macmillan & Co. Ltd, Londra 1946.

CATON, Jeffrey L., *NATO Cyberspace Capability: A Strategic and Operational Evolution*, Strategic Studies Institute, Haziran 2016.

CHOUCRI, Nazli, *Cyberpolitics in International Relations*, The MIT Press, Londra 2012.

CLARK, David, Thomas BERSON ve Herbert, S. LIN, *At the Nexus of Cybersecurity and Public Policy: Some Basic Concepts and Issues*, Washington DC: The National Academies Press, Temmuz 2014.

CLARKE, Richard A. ve Robert K. KNAKE, *Cyber War – The Next Threat to National Security and What to Do About It*, HarperCollins, Nisan 2010.

COHEN, Ariel ve Robert, E. HAMILTON, *The Russian Military and the Georgia War: Lessons and Implications*, CreateSpace Independent Publishing Platform, Haziran 2011.

CROMWELL, William C., *The United States and the European Pillar: The Strained Alliance*, St. Martin's Press, New York 1992.

ÇAKMAK, Haydar, *Avrupa Güvenliği: NATO-AGİT-AGSP*, Akçağ Yayınları, Ankara 2003.

ÇAYHAN, Esra ve Nurşin ATEŞOĞLU GÜNEY, *Avrupa'da Yeni Güvenlik Arayışları: NATO- AB Türkiye*, AFA Yayınları, İstanbul 1996.

ÇITAK, Emre, *Güvenlik ve İstihbarat: Yeni Güvenlik Politikaları Bağlamında Türkiye'de İstihbaratın Dönüşümü*, Yeniyüzyıl Yayınları, İstanbul 2017.

ÇİFCİ, Hasan, *Her Yönüyle Siber Savaş*, 2. Baskı, TÜBİTAK Bilim Kitapları, Temmuz 2017.

DEDEOĞLU, Beril, *Uluslararası Güvenlik ve Strateji*, Derin Yayınları, İstanbul 2003.

DÖNMEZ, Suat, *Güvenlik Anlayışının Dönüşümü İttifak Kavramı ve NATO*, (Ankara Üniversitesi, Sosyal Bilimler Enstitüsü, Uluslararası İlişkiler Anabilim Dalı, Doktora Tezi), Ankara 2010.

DUNN CAVELTY, Myriam, *Cyber-Security and Threat Politics: US Efforts to Secure the Information Age*, Routledge, New York 2007.

DUYGULU, Şirin, *Dönüşen Savaşların Değişen Araçları*, SETA Yayınları, Temmuz 2019.

EREN, Mehmet, *Avrupa Birliği'nin Siber Güvenlik Politikası*, Beta Yayınları, İstanbul 2017.

ERGÜL, Nihal, "Yeni Güvenlik Anlayışı Kapsamında Birleşmiş Milletlerin Rolü ve Uygulamaları" *Teoriler Işığında Güvenlik, Savaş, Barış ve Çatışma Çözümleri*, Derleyen: Atilla Sandıklı, Bilgesam Yayınları, İstanbul 2012.

ERHAN, Çağrı, "ABD ve NATO'yla İlişkiler", *Türk Dış Politikası: Kurtuluş Savaşı'ndan Bugüne Olgular, Belgeler, Yorumlar*, Derleyen: Baskın Oran, Cilt 1, 15. Baskı, İletişim Yayınları, İstanbul 2009.

European Commission, "The European Agenda on Security", Communicatıon From The Commission to the European Parliament, The Council, The

European Economic and Social Committee and the Committee of the Regions, COM (2015) 185 final, Strazburg 2015.

FREEMAN, Charles W., *Arts of Power: Statecraft and Diplomacy*, United States Institute of Peace, Ocak 2016.

GEERS, Kenneth, *Cyber War ın Perspective: Russian Aggression Against Ukraine*, NATO CCD COE Publications, Tallinn 2015.

GIBSON, William, *Neuromancer*, ACE Book, New York 2004.

GÜNEY, Nurşin Ateşoğlu, *Batı'nın Yeni Güvenlik Stratejileri AB-NATO-ABD*, Bağlam Yayıncılık, İstanbul 2006.

GÜNGÖR, Murat, "Ulusal Bilgi Güvenliği: Strateji ve Kurumsal Yapılanma", *T.C. Kalkınma Bakanlığı Bilgi Toplumu Dairesi Başkanlığı*, Yayın No: 2919, Uzmanlık Tezi, Mart 2015.

GÜRKAYNAK, Muharrem, *Avrupa Savuma ve Güvenlik Politikası*, Asil Yayınları, Ankara 2004.

HASGÜLER, Mehmet ve Mehmet B. ULUDAĞ, *Devletlerarası ve Hükümetler Dışı Uluslararası Örgütler*, Alfa Yayınları, İstanbul 2012.

HOBBES, Thomas, *Leviathan*, Çeviren: Semih Lim, Yapı Kredi Yayınları, Ocak 2019.

HOBSBAWM, Eric, *Kısa 20. Yüzyıl 1914-1991: Aşırılıklar Çağı*, Çeviren: Yavuz Alogan, Sarmal Yayınevi, İstanbul 1996.

HOCKING, Brian ve Jan MELISSEN, *Diplomacy in the Digital Age*, Clingendael Institute, Temmuz 2015.

HUGGES, Rex B, "NATO and Cyber Defence: Mission Accomplished?" *Atlantisch Perspectief 33*, Cilt 1, Sayı 4, 2009.

ITU, "ITU-T X.1205 – Supplement on framework of security information sharing negotiation", SERIES X: DATA NETWORKS, OPEN SYSTEM

COMMUNICATIONS AND SECURITY, *International Telecommunication Union,* Nisan 2013.

ITU-T X.1208, "Series X: Data Networks, Open System Communıcations and Security: Telecommunations Security – Overview of Cybersecurity", *International Telecommunication Union,* Nisan 2008.

KARA, Mahruze, *Siber Saldırılar- Siber Savaşlar ve Etkileri*, (İstanbul Bilgi Üniversitesi, Sosyal Bilimler Enstitüsü, Bilişim ve Teknoloji Hukuku Yüksek Lisans Programı, Yayımlanmış Yüksek Lisans Tezi), İstanbul 2013.

KARABULUT, Bilal, *Güvenlik, Küreselleşme Sürecinde Güvenliği Yeniden Düşünmek*, Barış Kitap, Ankara 2011.

KARAOSMANOĞLU, Ali, *NATO'nun Dönüşümü*, İstanbul Bilgi Üniversitesi Yayınları, İstanbul 2012.

KELEŞTEMUR, Atalay, *Siber İstihbarat*, Yazın Basın Yayınevi Matbaacılık Trz.Tic.Ltd.Şti, İstanbul 2015.

KIRCHNER, Emil ve James SPERLING, *EU Security Governance*, Manchester University Press, Temmuz 2008.

KLEIN, Bradley S., *Strategic Studies and World Order: The Global Politics of Deterrence*, Cambridge University Press, Mayıs 1994.

KLIMBURG, Alexander, *National Cyber Security Framework Manual*, NATO CCD COE Publication, Tallinn 2012.

KLIMBURG, Alexander ve Tiirmaa, H. KLAAR, *Cybersecurity and Cyberpower: Concepts, Conditions, and Capabilities for Cooperation for Action within the EU*, European Parliament, Brüksel 2011.

KOLODZIEJ, Edward A., *Security and International Relations*, Cambridge University Press, Cambridge 2005.

KORFF, Douwe, "Cyber Security Definitions", *Associate of the Oxford Martin School of the University of Oxford's Global Cybersecurity Capacity Centre*, Oxford 2011.

KREMLING, Janine ve Amanda M. Sharp PARKER, *Cyberspace, Cybersecurity, and Cybercrime*, SAGE Publications, 2017.

LIBICKI, Martin C., *Cyberdeterrence and Cyberwar*, RAND Corporation, Kasım 2009.

MEDVEDEV, Sergei A., *Offense-Defense Theory Analysis Of Russian Cyber*, Naval Postgraduate School, Monterey 2015.

MEISELS, Tamar, *The Trouble With Terror: Liberty, Security, And The Response To Terrorism*, Cambridge University Press, Cambridge 2008.

MERAL, Mustafa, *Siber Güvenlik Kapsamında Kritik Altyapıların Korunmasının Önemi*, Harp Akademileri Stratejik Araştırmalar Enstitüsü, Savunma Kaynakları Yönetimi Ana Bilim Dalı, Yüksek Lisans Tezi, İstanbul 2015.

MINÁRIK, T.- S. ALATALU- S. BIONDI, M. SIGNORETTI, I. TOLGA ve G. VISKY, *11th International Conference on Cyber Conflict: Silent Battle*, NATO CCD COE Publications, Tallinn 2019.

MOLLA, Alptekin, *NATO Savunma Politikaları Çerçevesinde Türk-Amerikan İlişkilerinin Analizi*, (İstanbul Üniversitesi, Sosyal Bilimler Enstitüsü Uluslararası İlişkiler Anabilim Dalı, Doktora Tezi), İstanbul 2008.

NATO, *The Prague Summit and NATO's Transformation*, A Reader's Guide, NATO Public Diplomacy Division, 2003.

NATO, *NATO Summit Guide Brussels 11-12 July 2018*, NATO Public Diplomacy Division, Brüksel 2018.

NATO, *NCI Academy C4ISR & Cyber Training Catalogue- 2021*, Version 5.0, NATO Communications and Information Academy, Ekim 2020.

NATO, *Introducing the NCI Academy*, NATO Communications and Information Agency, Temmuz 2020.

NEOCLEOUS, Mark, *Critique of Security*, Edinburgh University Press, Edinburgh 2008.

NICHOLSON, Andrew, Tim WATSON, Peter NORRIS, Alistair DUFFY ve Roy ISBELL "A taxonomy of technical attribution techniques for cyber attacks", *11th European Conference on Information Warfare and Security*, Academic Conferences International Limited, Ocak 2012.

NOSHIRAVANI, Reyhaneh, "NATO and Cyber Security Building on the Strategic Concept", Rapporteur Report, *Chatham House*, May 2011.

NYE, Joseph S. ve David A. WELCH, *Understanding Global Conflict & Cooperation: Intro to Theory & History*, 9. Baskı, Pearson Education Limited, 2014.

PEKSARI, Derya Gonca, *NATO'nun Değişen Konsepti*, Asil Yayın Dağıtım, Ankara 2007.

PERNIK, Piret, "Improving Cyber Security: NATO and the EU", *International Centre for Defence Studies*, Tallinn 2014.

REARDON, Robert ve Nazli CHOUCRI, *The Role of Cyberspace in International Relations: A View of the Literature*, ISA Annual Convention, Cilt 1, Nisan 2012.

ROSCINI, Marco, *Cyber Operations and the Use of Force in International Law*, Oxford University Press, Nisan 2014.

SANDER, Oral, *Siyasi Tarih 1918-1994*, 23. Baskı, İmge Yayınevi, Ankara 2013.

SARINAY, Yusuf, *Türkiye'nin Batı İttifakına Yönelişi ve NATO'ya Girişi*, Kültür ve Turizm Bakanlığı Yayınları, Ankara 1988.

SCHMITT, Michael N., *Tallinn Manual on the International Law Applicable to Cyber Warfare*, Cambridge University Press, New York 2013.

SCHMITT, Michael N., *Tallinn Manual 2.0 On The International Law Applicable To Cyber Operations,* Cambridge University Press, Şubat 2017.

SELVER, Mustafa, *Balkanlara Stratejik Yaklaşım ve Bosna*, IQ Kültür Sanat Yayıncılık, İstanbul 2003.

SINGER, P.W. ve Allan FRIEDMAN, *Siber Güvenlik ve Siber Savaş*, Çev. Ali Atav, 2. Baskı, Buzdağı Yayınevi, Şubat 2008.

SOLEY, Selim, *NATO- Kuzey Atlantik Anlaşması Teşkilatı*, EU Basımevi, Ankara 1955.

STOLTENBERG, Jens, "Secretary General's Annual Report 2015", *NATO Public Diplomacy Division,* Brüksel 2016.

SUNY, Ronald G., *The Revenge Of The Past: Nationalism, Revolution, And The Collapse Of The Soviet Union,* Stanford University Press, Kaliforniya 1993.

ŞAHİN, Güngör, *Küresel Güvenlik ve NATO- Teori,Aktör,Tehdit-Risk,* Detay Yayıncılık, Ankara 2016.

TIKK, Eneken, Kadri KASKA ve Liis VIHUL, *International Cyber Incidents: Legal Considerations,* NATO CCDCOE Publication, Tallinn 2010.

TURGUT, Arzu, *Wikileaks Belgelerinde Türkiye ve Yakın Çevresi- Türkiye, Rusya, Güney Kafkasya ve Ortadoğu ile İlgili Belgeler*, Uluslararası Stratejik Araştırmalar Kurumu Yayınları, Rapor No: 11-03, Nisan 2011.

Türk Dil Kurumu, *Türkçe sözlük,* 11.Baskı, Türk Dil Kurumu Yayınları, Ankara 2011.

URHAL, Ömer, *Küreselleşen Dünyada Güvenlik: Milli Güvenlik, Kamu Güvenliği, Örgütlü Suçlar ve Suç İstihbaratı*, Adalet Yayınevi, Ankara 2009.

URHAL, Ömer ve Ünal ACAR, *Devlet-Güvenlik-İstihbarat-Terörizm*, 1. Baskı, Adalet Yayınları, Ankara 2007.

U.S. Department of Defence, *Cyberspace Operations*, Joint Publication 3-12, Haziran 2018.

ÜNAL, Ahmet Naci, *Siber Güvenlik ve Elektronik Bileşenleri*, Nobel Akademik Yayıncılık Eğitim Danışmanlık Tic.Ltd.Şti, Eylül 2015.

ÜNVER, Mustafa, Cafer CANBAY ve Ayşe Gül MİRZAOĞLU, *Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler,* Bilgi Teknolojileri ve İletişim Kurumu, Nisan 2011.

WALTZ, Kenneth N., *Theory of International Politics*, Addison-Wesley Publishing Company, New York 1979.

WEIMANN, Gabriel, *Terror On The Internet: The New Arena The New Challenges*, United States Institute of Peace Press, Mart 2006.

WHITTAKER, Jason, *The Cyberspace Handbook*, Routledge, Şubat 2004.

WIGHT, Martin, *Systems Of States*, Leicester University Press, Leicester 1979.

WIJK, Rob de, *NATO On The Brink Of The New Millennium: The Battle For Consensus*, Brassey's Atlantic Commentaries, Londra 1997.

YILMAZ, Sait, *21. Yüzyılda Güvenlik ve İstihbarat*, Milenyum Yayınları, İstanbul 2007.

YILMAZ, Sait ve Olcay SALCAN, *Siber Uzay'da Güvenlik ve Türkiye*, Milenyum Yayınları, İstanbul 2008.

YİĞİTTEPE, Levent, *NATO Güvenlik Politikaları ve Terörle Mücadele Stratejileri*, Cinius Yayınları, Şubat 2017.

Makaleler / Kitap Bölümleri:

AKGÜL- AÇIKMEŞE, Sinem, "Algı mı Söylem mi? Kopenhag Okulu ve Yeni-Klasik Gerçekçilikte Güvenlik Tehditleri", *Uluslararası İlişkiler*, Cilt 8, Sayı 30, Yaz 2011, ss. 43-73.

AKGÜL- AÇIKMEŞE, Sinem ve Cihan DİZDAROĞLU, "NATO-AB İlişkilerinde İşbirliği ve Çatışma Dinamikleri", *Uluslararası İlişkiler*, Cilt 10, Sayı 40, Kış 2014, ss. 131-163.

ADESINA, Olubukola S., "Foreign Policy In An Era Of Digital Diplomacy", *Cogent Social Sciences,* Cilt 3, Sayı 1, Mart 2017, ss. 1-13.

AĞIR, Bülent S., "Güvenlik Kavramını Yeniden Düşünmek: Küreselleşme, Kimlik ve Değişen Güvenlik Anlayışı", *Güvenlik Stratejileri Dergisi*, Cilt 11, Sayı 22, Ekim 2015, ss. 97-130.

ALEXANDER, Dean C., "Cyber threats against the North Atlantic Treaty Organization (NATO) and selected responses", *İstanbul Gelişim Üniversitesi Sosyal Bilimler Dergisi*, Cilt 1, Sayı 2, 2014, ss. 1-36.

ASLAY, Fulya, "Siber Saldırı Yöntemleri ve Türkiye'nin Siber Güvenlik Mevcut Durum Analizi", *International Journal of Multidisciplinary Studies and Innovative Technologies,* Cilt 1, Sayı 1, Kasım 2017, ss. 24-28.

AYDINLI, Ersel, "Küreselleşme ve Güvenlik: Teorik Yaklaşımlar", *Avrasya Dosyası*, Güvenlik Bilimleri Özel, Cilt 9, Sayı 2, 2003, ss. 36-50.

BAĞBAŞLIOĞLU, Arif, "Güncelliğini Yitirmeyen Bir Sorun Olan Yük Paylaşımına Yeni Bir Çözüm Arayışı: Akıllı Savunma ve NATO", *Akademik Bakış*, Cilt 10, Sayı 19, Kış 2016, ss. 209-225.

BALCI, Ali ve Tuncay KARDAŞ, "Realizm", *Uluslararası İlişkilere Giriş,* Derleyen: Şaban Kardaş ve Ali Balcı, Küre Yayınları, İstanbul 2014, ss. 119-135.

BALDWIN, David A., "Security Studies and the End of the Cold War", *World Politics*, Cilt 48, Sayı 1, Ekim 1995, ss. 117-141.

BALDWIN, David A., "The Concept of Security", *Review of International Studies,* Cilt 23 Sayı 1, Ocak 1997, ss. 5-26.

BARRINHA, Andre ve Thomas RENARD, "Cyber-Diplomacy: The Making of an International Society In The Digital Age", *Global Affairs*, Cilt 3, Sayı 4-5, Aralık 2017, ss. 353-364.

BARRINHA, Andre ve Thomas RENARD, "Power and diplomacy in the post-liberal cyberspace", *International Affairs*, Cilt 96, Sayı 3, 2020, ss. 749-766.

BAYLIS, John, "International and Global Security in the Post-Cold War Era,", *The Globalization of World Politics: An Introduction to IR*, Derleyen: John Baylis ve Steve Smith, Oxford University Press, Oxford 2001, ss. 253-276.

BAYLIS, John, "The Concept of Security in International Relations", *Globalization and Environmental Challenges*, Derleyen: Hans Günter Brauch vd., Springer, New York 2008, ss. 495-502.

BAYLIS, John, "NATO strategy: the case for a new strategic concept", *International Affairs*, Cilt 64, Sayı 1, Kış 1987-1988, ss. 43-59.

BERNER, Sam, "Cyber-Terrorism: Reality or Paranoia?", *South African Journal of Information Management,* Cilt 5, Sayı 1, Mart 2003, ss. 1-4.

BETTS, Richard K., "The Lost Logic of Deterrence: What the Strategy That Won the Cold War Can-and Can't-Do Now", *Foreign Affairs,* Cilt 92, Sayı 2, Mart/Nisan 2013, ss. 87-99.

BIÇAKCI, Salih, "Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu" *Uluslararası İlişkiler*, Cilt 9, Sayı 34, Yaz 2012, ss. 205-226.

BIÇAKCI, Salih, "NATO'nun Gelişen Tehdit Algısı: 21. Yüzyılda Siber Güvenlik", *Uluslararası İlişkiler*, Cilt 10, Sayı 40, Kış 2014, ss. 100-130.

BİLGİN, Pınar, "Dünya Literatürü ve Uygulamasında Güvenlik Sektörü: 'Devlet Merkezli' Güvenlikten 'Yurttaş Merkezli' Güvenliğe Doğru Mu? Yeni Güvenlik", *Güvenlik Sektörü Yönetişimi: Türkiye ve Avrupa,* Derleyen: İbrahim Cerrah ve Ümit Cizre, Tesev Yayınları, İstanbul 2008, ss. 43-61.

BİLGİN, Pınar, "Güvenlik Çalışmalarında Yeni Açılımlar: Yeni Güvenlik Çalışmaları", *SAREM Stratejik Araştırmalar Dergisi*, Cilt 8, Sayı 14, Ocak 2010, ss. 69-96.

BLACK, James ve Alice LYNCH, "Cyber Threats to NATO from a Multi-Domain Perspective", *Cyber Threats and NATO 2030: Horizon Scanning and*

Analysis, Derleyen: Amy Ertan, Kathryn H. Floyd, Piret Pernik ve Tim Stevens, NATO CCDCOE Publications, Tallinn 2020, ss. 126-150.

BOOTH, Ken, "Security and Self: Reflections of a Fallen Realist", *In Critical Security Studies: Concepts and Cases*, Derleyen: Keith Krause ve Michael C. Williams, University of Minnesota Press, Mart 1997, ss. 83-120.

BRIANT, Emma L. ve Alicia WANLESS, "A Digital Ménage à Trois- Strategic Leaks, Propaganda and Journalism", *Countering Online Propaganda and Extremism- The Dark Side of Digital Diplomacy*, Derleyen: Corneliu Bjola ve James Pamment, New York 2019, ss. 44-65.

BURKADZE, Khatuna, "A Shift in NATO's Article 5 in the Cyber Era?", *The Fletcher Forum of World Affairs*, Cilt 42, Sayı 2, Yaz 2018, ss. 215-226.

BURTON, Joe, "NATO's Cyber Defence: Strategic Challenges And Institutional Adaptation", *Defence Studies*, Cilt 15, Sayı 4, Kasım 2015, ss. 297-319.

CANBEK, Gürol ve Şeref SAĞIROĞLU, "Bilgi, Bilgi Güvenliği ve Süreçleri Üzerine Bir İnceleme", *Politeknik Dergisi*, Cilt 9, Sayı 3, 2006, ss. 165-174.

CHOUCRI, Nazli, "Introduction: CyberPolitics in International Relations", *International Political Science Review*, Cilt 21, Sayı 3, 2000, ss. 243-263.

CLARK, David ve Nazli CHOUCRI, "Who Controls the Cyberspace?" *Bulltein of the Atomic Scientists*, Cilt 69, Sayı 5, Eylül 2013, ss. 21-31.

COLLINS, Alan, "Introduction: What is Security Studies", *Contemporary Security Studies*, Derleyen: Alan Collins, Oxford University Press, New York 2007, ss. 1-11.

CORNISH, Paul, "Governing Cyberspace Through Constructive Ambiguity", *Survival*, Cilt 57, Sayı 3, Haziran-Temmuz 2015, ss. 153-176.

CRAIGEN, Dan, Nadia DIAKUN-THIBAULT ve Randy PURSE, "Defining Cybersecurity", *Technology Innovation Management Review*, Cilt 4, Sayı 10, Ekim 2014, ss. 13-21.

CRANDALL, Matthew, "Soft Security Threats and Small States: the Case of Estonia", *Defence Studies*, Cilt 14, Sayı 1, Mart 2014, ss. 30-55.

CZOSSECK, Christian, Rain OTTIS ve Anna-Maria TALIHÄRM, "Estonia After the 2007 Cyber Attacks: Legal, Strategic and Organisational Changes in Cyber Security", *International Journal of Cyber Warfare and Terrorism*, Cilt 1, Sayı 1, Tallinn 2011, ss. 24-34.

ÇATAL, Betül, "Diplomaside Değişim ve Dönüşüm: Siber Diplomasi", *Medeniyet Araştırmaları Dergisi,* Cilt 2, Sayı 3, İstanbul 2015, ss. 43-54.

ÇOMAK, Hasret, "Küreselleşme ve Güvenlik", *Küreselleşme ve Küreselleşmenin Türkiye'ye Etkileri*, Derleyen: Caner Sancaktar, Tasam Yayınları, İstanbul 2008, ss. 8-18.

DABAN, Cihan, "Siber Güvenlik ve Uluslararası Güvenlik İlişkisi" *Siber Politikalar Dergisi*, Cilt 1, Sayı 1, Kış 2016, ss. 78-94.

DARICILI, A. Burak ve Barış ÖZDAL, "Rusya Federasyonu'nun Siber Güvenlik Kapasitesini Oluşturan Enstrümanların Analizi", *Ahmet Yesevi Üniversitesi Türk Dünyası Sosyal Bilimler Dergisi (BİLİG)*, Avrasya'nın Siyasal İktisadı Özel Sayısı, Sayı 83, Güz 2017, ss. 121-146.

DARICILI, A. Burak, "NATO'nun Siber Güvenlik Stratejisi'nin Analizi", *Uluslararası Sistemde Yeni Düzen Arayışları*, Derleyen: Tayyar Arı ve Barış Özdal, Dora Basım, Bursa 2015, ss. 407-417.

DEDEOĞLU, Beril ve Mesut, H. CAŞIN, "Yeni Avrupa Güvenlik Kimliğinde Stratejik Arayışlar: NATO-BAB-AB-AGİT İlişkilerin Dünü Bugünü ve Geleceği", *Avrasya Dosyası*, Avrupa Birliği Özel, Cilt 5, Sayı 4, Kış 1999, ss. 155-196.

DENNING, Dorothy E., "Framework and principles for active cyber defense", *Computers & Security*, Cilt 40, Şubat 2014, ss. 108-113.

DENNING, Dorothy E., "Rethinking the Cyber Domain and Deterrence" *Joint Forces Quarterly 77*, Bahar 2015, ss. 8-15.

DOĞAN, Nejat, “NATO'nun Örgütsel Değişimi, 1949-1999: Kuzey-Atlantik İttifakından Avrupa-Atlantik Güvenlik Örgütüne” *Ankara Üniversitesi SBF Dergisi*, Cilt 60, Sayı 3, Ankara 2005, ss. 69-108.

DOĞRUL, Murat, Adil ASLAN ve Eyyüp ÇELİK, "Developing an international cooperation on cyber defense and deterrence against cyber terrorism", 3rd International Conference on Cyber Conflict, *CCD COE Publications*, Tallinn 2011, ss. 1-15.

DOHERTY, Neil F., Leonidas ANASTASAKIS ve Heather FULFORD, “The Information Security Policy Unpacked: A Critical Study of the Content of University Policies”, *International Journal of Information Management*, Cilt 29, Sayı 6, Aralık 2009, ss. 449-457.

DUCARU, Sorin D., “The Cyber Dimension Of Modern Hybrid Warfar and Its Relevance For NATO”, *Europolity-Continuity and Change in European Governance*, Cilt 10, Sayı 1, Ekim 2016, ss. 7-23.

DUCHACEK, Ivo, "The Strategy of Communist Infiltration: Czechoslovakia, 1944–48”, *World Politics*, Cilt 2, Sayı 3, Nisan 1950, ss. 345-372.

DUFFIELD, John S., “The Evolution of NATO's Strategy of Flexible Response: A Reinterpretation”, *Security Studies*, Cilt 1, Sayı 1, 1991, ss. 132-156.

DUNN CAVELTY, Myriam, “Cyber-Security”, *Contemporary Security Studies*, Derleyen: Alan Collins, Oxford University Press, Mayıs 2012, ss. 362-378.

EFTHYMIOPOULOS, Marios P., “A cyber-security framework for development, defense and innovation at NATO”, *Journal of Innovation and Entrepreneurship*, Cilt 8, Sayı 12, Haziran 2019, ss. 1-26.

EFTHYMIOPOULOS, Marios P., “Cyber-Challenges and NATO”, *Handbook of Cyber Development*, Cyber-Democracy, and Cyber-Defense, Derleyen: E. G. Carayannis vd, Springer International Publishing, 2018, ss. 937-959.

EGOROVA, Nataliia I., “Stalin's Foreign Policy and the Cominform, 1947-53”, *The Soviet Union and Europe In The Cold War, 1943-53*, Derleyen: Francesca Gori ve Silvio Pons, Macmillan Press Ltd, Londra 1996, ss. 197-208.

EHALA, Martin, “The Bronze Soldier: Identity Threat and Maintenance in Estonia”, *Journal of Baltic Studies*, Cilt 40, Sayı 1, Mart 2009, ss. 139-158.

ELLIOTT, David, “Deterring Strategic Cyberattack,” *IEEE Security & Privacy,* Cilt 9, Sayı 5, Eylül-Ekim 2011, ss. 36-40.

ELLISON, Brian, "Russian grand strategy in the South Ossetia War" *Demokratizatsiya,* Cilt 19, Sayı 4, Eylül 2011, ss. 343-366.

EOM, Jung ho, “Roles and Responsibilities of Cyber Intelligence for Cyber Operations in Cyberspace”, *International Journal of Software Engineering and Its Applications,* Cilt 8, Sayı 9, Ocak 2014, ss. 137-146.

FALK, Richard, “Terör ve Devlet Terörizmi”, *Uluslararası İlişkilerde Çatışmadan Güvenliğe*, Derleyen: Mustafa Aydın, Hans Günter Brauch, Mitat Çelikpala, Ursula Oswald Spring ve Necati Polat, İstanbul Bilgi Üniversitesi Yayınları, İstanbul 2012, ss. 89-116.

FIDLER, David P., Richard PEREGENT ve Alex VANDURME, “NATO, Cyber Defense and International Law”, *St. John’s Journal Of International & Comparative Law,* Cilt 4, Sayı 1, Güz 2013, ss. 1-25.

FITTON, Oliver, “Cyber operations and gray zones: Challenges for NATO”, *The Quarterly Journal*, Cilt 15, Sayı 2, Bahar 2016, ss. 109-119.

FRITZ, Jason, “How China Will Use Cyber Warfare to Leapfrog in Military Competitiveness,” *Culture Mandala*, Cilt 8, Sayı 1, Ekim 2008, ss. 28-80.

GAISER, Laris, "NATO-EU Collaboration on Hybrid Threats: Cooperation Out of Necessity with Potential Consequences on International Legal Framework", *National Security and The Future,* Cilt 20, Sayı 1-2, Aralık 2019, ss. 13-24.

GODSON, Roy ve Phil WILLIAMS, “Strengthening Cooperation Against Transnational Crime”, *Survival,* Cilt 40, Sayı 3, 1998, ss. 66-88.

GOODMAN, Seymour E., "Critical Information Infrastructure Protection", *Responses To Cyber Terrorism NATO Science For Piece and Security,* Derleyen: Centre Of Excellence Defence Against Terrorism, IOS Press, Cilt 34, Ankara 2008, ss. 24-33.

GOŹDZIEWICZ, Wiesław, "From Riga to Wales. NATO's Road to Collective Cyberdefence", *NATO Road to Cybersecurity,* Derleyen: Joanna Świątkowska, Kosciuszko Institute, Krakow 2016, ss. 11-17.

GÜNTAY, Vahit, "Siber Güvenliğin Uluslararası Politikada Etki Aracına Dönüşmesi ve Uluslararası Aktörler", *Güvenlik Stratejileri Dergisi*, Cilt 14, Sayı 27, 2018, ss. 79-111.

GÜNTAY, Vahit, "Uluslararası Sistem ve Güvenlik Açısından Değişen Savaş Kurgusu; Siber Savaş Örneği", *Güvenlik Bilimleri Dergisi*, Cilt 6, Sayı 2, Kasım 2017, ss. 81-108.

HANSEN, Lene ve Helen NISSENBAUM, "Digital Disaster, Cyber Security and the Copenhagen School", *International Studies Quarterly,* Cilt 53, Sayı 4, Aralık 2009, ss. 1155-1175.

HERZOG, Stephen, "Revisiting Estonian Cyber Attacks: Digital Threats and Multinational Responses" *Journal of Strategic Security*, Cilt 2, Sayı 4, Yazı 2011, ss. 49-60.

HLATKY, Stéfanie von, "NATO's Chicago Summit: Alliance Cohesion above All Else?", *Center for Security Studies*, Sayı 116, Zürih 2012, ss. 1-3.

HOROWITZ, Michael, "A Common Future? NATO and the Protection of the Commons" *The Chicago Council On Global Affairs*, Transatlantic Paper Series Sayı 3, Ekim 2010, ss. 1-18.

HOWORTH, Jolyon, "EU–NATO Cooperation: The Key to Europe's Security Future", *European Security*, Cilt 26, Sayı 3, Temmuz 2017, ss. 454-459.

HUGHES, Rex B., "A Treaty For Cyberspace", *International Affairs*, Cilt 86, Sayı 2, Mart 2010, ss. 523-541.

HURLEY, Matthew M., "For and from Cyberspace: Conceptualizing Cyber Intelligence, Surveillance, and Reconnaissance", *Air & Space Power Journal*, Kasım-Aralık 2012, ss. 12-33.

IASIELLO, Emilio, "Is Cyber Deterrence an Illusory Course of Action?" *Journal of Strategic Security,* Cilt *7,* Sayı 1, Bahar 2014, ss. 54-67.

JENSEN, Eric T., "Cyber Deterrence", *Emory Internatıonal Law Revıew*, Cilt 26, Sayı 2, Mayıs 2012, ss. 773-824.

JORDAN, Robert S., "NATO's Structural Changes for the 1990s", *NATO In The Post-Cold War Era: Does It Have a Future,* Derleyen: S. Victor Papacosma ve Mary Ann Heiss, Macmillan Press, 1995, ss. 41-69.

KAVUNCU, Sibel, "US-Russia Relations In The Context of NATO Enlargement", *Management and Education*, Cilt 6, Sayı 4, 2010, ss. 72-77.

KAVUNCU, Sibel ve Hasan DİLAN, "21. Yüzyıl Eşiğinde Yeni Çelişkiler/Yeni Krizler Ortamında Uluslararası Siyasal Sistemin Çok Kutupluluğa Doğru Evrilmesi", *38. (ICANAS) Uluslararası Asya ve Kuzey Afrika Çalışmaları Kongresi*, Cilt 2, Atatürk Kültür, Dil ve Tarih Yüksek Kurumu Yayınları, Ankara 2011, ss. 945-953.

KAVUNCU, Sibel, "Nükleer Silahsızlanma Yolunda Start Süreci", *Bilge Strateji*, Cilt 5, Sayı 8, Bahar 2013, ss. 119-148.

KELLO, Lucas, "The Meaning of the Cyber Revolution: Perils to Theory and Statecraft", *International Security,* Cilt 38, Sayı 2, Güz 2013, ss. 7-40.

KEYMAN, Fuat, "Küreselleşme", *Uluslararası İlişkilere Giriş*, Derleyen: Şaban Kardaş ve Ali Balcı, Küre Yayınları, İstanbul 2014, ss. 497-511.

KOÇER, Gökhan, "Soğuk savaş Sonrasında Uluslararası Güvenlik Ortamı ve Türkiye'nin Ulusal Güvenliği", *Stratejik Araştırmalar Dergisi,* Cilt 3, Sayı 5, 2005, ss. 287-304.

KOVACS, Amos, "Using Intelligence", *Intelligence and National Security,* Cilt 12, Sayı 4, 1997, ss. 145-164.

KOVACS, László, "Cyber Security Polcy and Strategy In The European Union and NATO", *Land Forces Academy Review*, Cilt 23, Sayı 1, Mayıs 2018, ss. 16-24.

KOVAL, Nikolay, "Revolution Hacking", *Cyber War in Perspective: Russian Aggression against Ukraine*, Derleyen: Kenneth Geers, NATO CCD COE Publications, Tallinn 2015, ss. 55-58.

KRAUSE, Keith ve Michael C. WILLIAMS, "Broadening the Agenda of Security Studies: Politics and Methods", *Mershon International Studies Review*, Cilt 40, Sayı 2, Ekim 1996, ss. 229-254.

KREPINEVICH, Andrew F., "Cavalry to Computer: The Pattern of Military Revolutions", *Strategic Studies A Reader*, Derleyen: Thomas Mahnken ve Joseph Maiolo, Routledge, Nisan 2008, ss. 374-386.

LAKOMY, Miron, "Conditions to Invoke the Principle of Article 5 of The North Atlantic Treaty in Case of a Cyberattack or a Cyber Conflict", *NATO Road to Cybersecurity*, Editor: Joanna Świątkowska, The Kosciuszko Institute, Krakow 2016, ss. 35-43.

LEPGOLD, Joseph, "NATO's Post-Cold War Collective Action Problem", *International Security*, Cilt 23, Sayı 1, Yaz 1998, ss. 78-106.

LÉTÉ, Bruno, "Cooperation in Cyberspace", *The EU and NATO- The Essential Partners*, Editors: Gustav Lindstrom ve Thierry Tardy, European Union Institute for Security Studies, Paris 2019, ss. 28-36.

LIN, Herbert S., "Offensive Cyber Operations and the Use of Force" *Journal Of Natıonal Securıty Law & Polıcy*, Cilt 4, Sayı 63, Ağustos 2010, ss. 63-86.

LUPOVICI, Amir, "Cyber Warfare and Deterrence: Trends and Challenges in Research", *Military and Strategic Affairs*, Cilt 3, Sayı 3, Aralık 2011, ss. 49-62.

LUUKAS, K. Ilves, Timothy J. EVANS, Frank J. CILLUFFO ve Alec A., NADEAU, "European Union and NATO Global Cybersecurity Challenges", *Institute for National Strategic Security*, Cilt 6, Sayı 2, Temmuz 2016, ss. 126-141.

LYNN, William J., "Defending a New Domain: The Pentagon's Cyberstrategy", *Foreign Affairs*, Cilt 89, Sayı 5, Eylül/Ekim 2010, ss. 97-108.

MANOR, Ilan ve Elad SEGEV, "America's Selfie: How The US Portrays Itself On Its Social Media Accounts", *Digital Diplomacy Theory and Practice*, Derleyen: Corneliu Bjola ve Marcus Holmes, Routledge, New York 2015, ss. 103-122.

MARRONE, Alessandro, "The Equilibrium of the 2010 NATO Strategic Concept", *The International Spectator*, Cilt 46, Sayı 3, Eylül 2011, ss. 93-111.

MASLOW, Abraham, "A Theory of Human Motivation", *Psychological Review*, Cilt 50, Sayı 4, 1943, ss. 370-396.

MEARSHEIMER, John J., "A Realist Reply", *International Security*, Cilt 20, Sayı 1, Temmuz 1995, ss. 82-93.

MEER, Sico van der, "Defence, Deterrence, and Diplomacy: Foreign Policy Instruments to Increase Future Cybersecurity," *Securing Cyberspace: International and Asian Perspectives*, Derleyen: Cherian Samuel ve Munish Sharma, Pentagon Press, Hindistan 2016, ss. 95-106.

MELNITZKY, Alexander, "Defending America Against Chinese Cyber Espionage Through The Use Of Active Defenses" *Cardozo Journal of International & Comparative Law*, Cilt 20, Sayı 2, Kış 2012, ss. 537-570.

MIN, Kyoung, SEUNG-Woan CHAI ve Mijeong, HAN, "An International Comparative Study on Cyber Security Strategy" *International Journal on Security and Its Applications*, Cilt 9, Sayı 2, Şubat 2015, ss. 13-20.

MORGAN, Patrick, "Security in International Politics: Traditional Approaches", *Contemporary Security Studies*, Derleyen: Alan Collins, Oxford University Press, New York 2007, ss. 11-34.

NAZARIO, Jose, "Politically Motivated Denial of Service Attacks", *The Virtual Battlefield: Perspectives on Cyber Warfare*, Derleyen: Christian Czosseck ve Kennth Geers, IOS Press, Ekim 2009, ss. 163-181.

NYE, Joseph S., "Nuclear Lessons for Cyber Security?", *Strategic Studies Quarterly,* Cilt 5, Sayı 4, Kış 2011, ss. 18-38.

OĞUZLU, Tarık, "Dünya Düzenleri ve Güvenlik: Ulus-Devlet Güvenlik Anlayışı Aşılıyor mu?", *Güvenlik Stratejileri Dergisi*, Cilt 3, Sayı 6, Ocak 2007, ss. 1-35.

OĞUZLU, Tarık, "NATO's Transformation into a Global Actor in the Age of Great Power Politics", *Perceptions: Journal of International Affairs,* Cilt 26, Sayı 1, Bahar-Yaz 2021, ss. 2-28.

OTTIS, Rain, "Analysis of the 2007 cyber attacks against estonia from the information warfare perspective", *Proceedings of the 7th European Conference on Information Warfare,* Derleyen: Dan Remenyi, Academic Publishing Limited, Dublin 2008, ss. 163-168.

OWEN, Taylor, "Challenges and Opportunities for defining and Measuring Human Security", *Disarmament Forum,* Cilt 3, 2004, ss. 15-24.

ÖĞÜN, Mehmet N. ve Adem KAYA, "Siber Güvenliğin Milli Güvenlik Açısından Önemi ve Alınabilecek Tedbirler", *Güvenlik Stratejileri Dergisi,* Cilt 9, Sayı 18, Temmuz 2013, ss. 145-181.

ÖZCAN, Gencer, "Doksanlı Yıllarda Türkiye'nin Değişen Güvenlik Ortamı", *Türkiye'nin Ulusal Güvenlik ve Dış Politika Gündeminde Doksanlı Yıllar: En Uzun On yıl*, Derleyen: Gencer Özcan ve Şule Kut, Büke Yayınları, İstanbul 2000, ss. 13-44.

ÖZDEMIR, Haluk, "11 Eylül: Post-Modern Savaşın Miladı Ya Da Dış Politika Mücadelelerinin Görünmeyen Boyutu", *Süleyman Demirel Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi*, Cilt 7, Sayı 1, Isparta 2002, ss. 153-173.

ÖZEL, Mehmet ve Demet DÖNMEZ, "Toplum Sözleşmecilerinden 11 Eylül'e Güvenlik Anlayışındaki Değişim", *Türk İdare Dergisi,* Sayı 482, 2016, ss. 239-282.

ÖZLÜK, Erdem ve Duygu ÖZLÜK, "NATO'yu Anlamak: Dönüşümü, Yeni Kimlikleri ve Uyum Süreçleri." *Selçuk Üniversitesi Sosyal Bilimler Enstitüsü Dergisi,* Sayı 31, Konya 2014, ss. 209-225.

ÖZTÜRK, Zerrin Ayşe, "Soğuk Savaş Sonrasında Yeni Güvenlik Teorileri ve Türkiye'nin Güvenlik Algılamaları", *21. Yüzyıl,* Cilt 1, Ekim 2007, ss. 33-50.

PEKŞEN, Hasan D., "NATO'nun Dönüşümünün Sınırları: Bir Uygulama Vakası Olarak Enerji Güvenliği", *Güvenlik Stratejileri Dergisi*, Cilt 12, Sayı 23, Nisan 2016, ss. 35-69.

POLAT, Doğan Şafak, "NATO'nun Yeni Operasyon Alanı: Siber Uzay", Güvenlik Bilimleri Dergisi, UGK Özel Sayısı, Şubat 2020, ss. 135-158.

RID, Thomas ve Ben BUCHANAN, "Attributing Cyber Attacks," *Journal of Strategic Studies,* Cilt 38, Sayı 1-2, Haziran 2015, ss. 4-37.

RINGSMOSE, Jens ve Sten RYNNING, "NATO's New Strategıc Concept:A Comprehensıve Assessment", *Danish Institute for International Studies,* Kopenhag 2011, ss. 7-23.

RUPP, Richard, "NATO 1949 and NATO 2000: From Collective Defense Toward Collective Security", *Journal of Strategic Studies,* Cilt 23, Sayı 3, Ocak 2008, ss. 154-176.

SALTZMAN, Ilai, "Cyber Posturing and the Offense-Defense Balance", *Contemporary Security Policy,* Cilt 34, Sayı 1, Mart 2013, ss. 40-63.

SAĞIROĞLU, Şeref, "Siber Güvenlik ve Savunma: Önem, Tanımlar, Unsurlar ve Önlemler", *Siber Güvenlik ve Savunma- Farkındalık ve Caydırıcılık,* Derleyen: Şeref Sağıroğlu ve Mustafa Alkan, Grafiker Yayınları, Ankara 2018, ss. 21-48.

SALTZMAN, Ilai, "Cyber Posturing and the Offense-Defense Balance", *Contemporary Security Policy*, Cilt 34, Sayı 1, 2013, ss. 40-63.

SANCAK, Kadir, "Güvenlik Kavramı Etrafındaki Tartışmalar ve Uluslararası Güvenliğin Dönüşümü", *KTÜ Sosyal Bilimler Dergisi*, Sayı 6, 2013, ss. 123-134.

SCHREIER, Fred, "On Cyberwarfare", DCAF Horizon 2015, Araştırma Makalesi, *The Geneva Centre for the Democratic Control of Armed Forces* (DCAF), No. 7, Cenevre 2013, ss. 7-10.

SOLOMON, Jonathan, "Cyber Deterrence Between Nation-States: Plausible Strategy or a Pipe Dream?", *Strategic Studies Quarterly*, Cilt 5, Sayı 1, Bahar 2011, ss. 1-25.

SRINIVAS, Jangirala, Ashok Kumar DAS ve Neeraj KUMAR, "Government Regulations In Cyber Security: Framework, Standards And Recommendations", *Future Generation Computer Systems*, Cilt 92, Mart 2019, ss. 178-188.

SZENTGÁLI, Gergely, "The NATO Policy on Cyber Defense: The Road so Far", *AARMS 1*, Cilt 12, Sayı 1, 2013, ss. 83-91.

SZŐKE, Diána, "NATO's Evolving Approach to Cybersecurity", *Foreign Policy Review*, Cilt 12, Budapeşte 2019, ss. 128-142.

ŞEKER, Ensar ve Hasan Hüseyin ÖZBENLİ, "The Concept of Cyber Defence Exercises (CDX): Planning, Execution, Evaluation", *2018 International Conference on Cyber Security and Protection of Digital Services (Cyber Security)*, IEEE, Tallinn 2018, ss. 1-9.

ŞENOL, Mustafa, "Siber Güçle Caydırıcılık Ama Nasıl?", *Uluslararası Bilgi Güvenliği Mühendisliği Dergisi*, Cilt 2, Sayı 2, 2016, ss. 10-17.

ŞENTÜRK, Hakan, Celal Z. ÇİL ve Şeref SAĞIROĞLU, "Cyber Security Analysis of Turkey", *International Journal Of Information Security Science*, Cilt 1, Sayı 4, Ankara 2012, ss. 112-125.

TALIAFERRO, Jeffrey W., "Security seeking under anarchy: Defensive realism revisited", *International Security*, Cilt 25, Sayı 3, Kış 2001, ss. 128-161.

TANRISEVER, Oktay F., "Güvenlik", *Devlet ve Ötesi,* Derleyen: Atila Eralp, 8. Baskı, İletişim Yayınları, İstanbul 2014, ss. 107-125.

TARIEN, Jaak, "National Cyber Defence Policies and the Role of International Cooperation", *Partnership for Peace Consortium of Defense Academies and Security Studies Institutes,* Cilt 19, Sayı 1, Kış 2020, ss. 5-7.

TURAN, Sibel, Nergiz ÖZKURAL KÖROĞLU ve İlker Aral GÜNGÖR, "Kuramsal Çerçeve: Uluslararası İlişkilerde Güvenlik", *Uluslararası İlişkilerde Güvenlik Kuramları ve Sorunlarına Temel Yaklaşımlar,* Derleyen: Sibel Turan ve Nergiz Özkural Köroğlu, Transnational Press London, Londra 2017, ss. 9-18.

TÜRKÖZ, Şükrü, "Küresel Terörizm Sorununa Güvenlik Perspektifli Bir Yaklaşım", *Niğde Üniversitesi İktisadi ve İdari Bilimler Fakültesi Dergisi,* Cilt 9, Sayı 2, Niğde 2016, ss. 153-162.

ULLMAN, Richard H., "Redefining Security", *International Security,* Cilt 8, Sayı 1, Yaz 1983, ss. 129-153.

ULUTAŞ, Güzin, "Siber Güvenlik", *Siber Güvenlik ve Savunma- Farkındalık ve Caydırıcılık,* Derleyen: Şeref Sağıroğlu ve Mustafa Alkan, Grafiker Yayınları, Ankara 2018, ss. 87-105.

UMA, Murugesan ve Ganapathi PADMAVATHI, "A Survey On Various Cyber-Attacks and Their Classification", *International Journal of Network Security,* Cilt 15, Sayı 5, Eylül 2013, ss. 390-396.

ÜNVER, Mustafa ve Cafer CANBAY, "Ulusal ve Uluslararası Boyutlarıyla Siber Güvenlik", *Elektrik Mühendisliği Dergisi*, Sayı 438, Mart 2010, ss. 94-103.

WALTZ, Kenneth N., "Anarchic Orders and Balances of Power", *Neorealism and Its Critics,* Derleyen: Robert O. Keohane, Columbia University Press, New York 1986, ss. 98-131.

WALTZ, Kenneth N., "Globalization and American Power", *The National Interest,* Sayı 59, Bahar 2000, ss. 46-56.

WALTZ, Kenneth N., "Structural Realism After Cold War", *International Security*, Cilt 25, Sayı 1, Yaz 2000, ss. 5-41.

WEISSBRODT, David, "Cyber-Conflict, Cyber-Crime and Cyber-Espionage", *Mınnesota Journal Of International Law*, Cilt 22, Sayı 2, 2013, ss. 347-387.

WOLFERS, Arnold, "National Security: As An Ambiguous Symbol", *Political Science Quarterly*, Cilt 67, Sayı 4, Aralık 1952, ss. 481-502.

WORTHAM, Anna, "Should Cyber Exploitation Ever Constitute A Demonstration Of Hostile Intent That May Violate UN Charter Provisions Prohibiting The Threat Or Use Of Force?", *Federal Communications Law Journal*, Cilt 64, Sayı 3, Güz 2012, ss. 643-660.

YAMAN, Didem, "NATO'nun Yeni Görevi: Terörizmle Mücadele ve Bu Eksende Atılan Adımlar", *Uluslararası Hukuk ve Politika Dergisi*, Cilt 2, Sayı 7, 2006, ss. 41-53.

YILMAZ, Muzaffer Ercan, "Westphalia'dan Günümüze Savaş", *Uluslararası İlişkilerde Çatışmadan Güvenliğe*, Derleyen: Mustafa Aydın, Hans Günter Brauch, Mitat Çelikpala, Ursula Oswald Spring ve Necati Polat, İstanbul Bilgi Üniversitesi Yayınları, İstanbul 2012, ss. 75-87.

YORULMAZ, Murat, "Bölgeselleşen Güvenlik Anlayışında Yeni Açılımlar ve Türkiye'nin Güvenlik Algısında Yaşanan Değişimler" *Trakya Üniversitesi Sosyal Bilimler Enstitüsü Sosyal ve Beşerî Bilimler Dergisi*, Cilt 5, Sayı 2, Edirne 2013, ss. 288-297.

YORULMAZ, Murat, "Değişen Uluslararası Güvenlik Algılamaları Bağlamında Türkiye-Yunanistan İlişkilerinde 'Değişmeyen' Güvenlik Paradoksu", *Balkan Araştırma Enstitüsü Dergisi*, Cilt 3, Sayı 1, Edirne 2014, ss. 103-135.

YOST, David S., "NATO's Evolving Purposes and the Next Strategic Concept", *International Affairs*, Cilt 86, Sayı 2, Mart 2010, ss. 489-522.

İnternet Kaynakları:

AMACKER, Christopher, "The Functions of Diplomacy,", (20.07.2011), *http://www.e-ir.info/2011/07/20/the-functions-of-diplomacy/*, (Erişim tarihi: 15.08.2020).

AON*, Siber Saldırı Kayıplarının Toplam Maliyeti Yıllık 6 Trilyon Dolara Ulaşacak*, (16.03.2020), https://www.aon.com/turkey/tr/about-aon/newsroom-2020/Siber-Saldırı-Kayıplarının-Toplam-Maliyeti-Yıllık, (Erişim tarihi: 10.08.2020).

ASHFORD, Warwick, "NATO to adopt new cyber defence policy", (03.09.2014), *https://www.computerweekly.com/news/2240228071/Nato-to-adopt-new-cyber-defence-policy*, (Erişim tarihi: 02.01.2021).

AYBET, Gülnur, "NATO's New Missions", *Journal Of International Affairs*, Cilt 4, Sayı 1, Mart-Mayıs 1999, *http://www.sam.gov.tr/pdf/perceptions/Volume-IV/march-may-1999/GulnurAybet3.pdf*, (Erişim tarihi: 31.08.2020).

AYDOĞMUŞ, Hale, "ABD'nin kapıları mültecilere kapalı", (03.10.2019), *https://www.trthaber.com/haber/dunya/abdnin-kapilari-multecilere-kapali-433696.html*, (Erişim tarihi: 18.05.2020).

BARRETT, Mark, Dick BEDFORT, Elizabeth SKINNER ve Eva VERGLES, "Assured Access to the Global Commons", *Supreme Allied Command Transformation, North Atlantic Treaty Organisation*, Virginia 2011, *https://meerverstehen.net/wp-content/uploads/2012/05/global-commons.pdf*, (Erişim tarihi: 11.08.2020).

BBC News, *Edward Snowden: Leaks That Exposed US Spy Programme*, (17.01.2014), https://www.bbc.com/news/world-us-canada-23123964, (Erişim tarihi: 19.07.2020).

BBC News, *In pictures: Atrocities' aftermath, (12.09.2001),* http://news.bbc.co.uk/2/hi/americas/1538664.stm, (Erişim tarihi: 13.12.2021).

BEIDLEMAN, Scott W., *Defining and Deterring Cyber War*, Strateji Araştırma Raporu, U.S. Army War College, Ocak 2009, *https://apps.dtic.mil/sti/pdfs/ADA500795.pdf*, (Erişim tarihi: 01.10.2020).

BELKIN, Paul, "NATO's Warsaw Summit: In Brief", Teknik Rapor, *Congressional Research Service*, Kasım 2016, *https://apps.dtic.mil/sti/pdfs/AD1021858.pdf*, (Erişim tarihi: 10.09.2020).

BELKIN, Paul, "NATO: Key Issues Following the 2019 Leaders' Meeting", CRS Report R46066, *Congressional Research Service*, Nisan 2020, *https://www.everycrsreport.com/files/20200401_R46066_a0abb404b866107cd315ba156d0d673c81ae4898.pdf*, (Erişim tarihi: 11.10.2020).

BIÇAKCI, Salih, "Siber Güvenlik ve Savunma", *Güvenlik Yazıları Serisi*, No 42, Kasım 2019, https://trguvenlikportali.com/wp-content/uploads/2019/11/SiberGuvenlik_SalihBicakci_v.1.pdf, (Erişim tarihi: 22.04.2021).

BIRNBAUM, Michael, "Facing Russian threat, NATO boosts operations for the first time since the Cold War", (08.11.2017), *https://www.washingtonpost.com/world/facing-russian-threat-nato-boosts-operations-for-the-first-time-since-the-cold-war/2017/11/08/9b47f542-c49b-11e7-9922-4151f5ca6168_story.html*, (Erişim tarihi: 10.10.2020).

BORGER, Julian, "Pentagon kept the lid on cyberwar in Kosovo", (09.11.1999), *https://www.theguardian.com/world/1999/nov/09/balkans*, (Erişim tarihi: 15.12.2021).

BOYER, Spencer P. ve Caroline WADHAMS, "The NATO Summit in Bucharest", (02.04.2008), *https://www.americanprogress.org/issues/security/news/2008/04/02/4215/the-nato-summit-in-bucharest/,* (Erişim tarihi: 07.09.2020).

BRENT, Laura, "NATO's Role in Cyberspace", (12.02.2019), *https://www.nato.int/docu/review /articles/2019/02/12/natos-role-in-cyberspace/index.html*, (Erişim tarihi: 11.08.2020).

BRIGHT, Arthur, "Estonia accuses Russia of 'cyber-attack'" (17.05.2007), *http://www.csmonitor.com/2007/0517/p99s01-duts.html*, (Erişim tarihi: 30.09.2020).

COKER, Margaret ve Paul SONNE, "Ukraine: Cyberwar's Hottest Front", (09.09.2015), *https://www.wsj.com/articles/ukraine-cyberwars-hottest-front-1447121671,* (Erişim tarihi: 08.10.2020).

Congressional Research Service, *The NATO Summit at Riga 2006*, https://www.everycrsreport.com/files/20070301_RS22529_f6d0725b6d3fabb66fc2bdaa613dc3554ffc42ec.pdf, (Erişim tarihi: 06.09.2020).

CONNELL, Michael ve Sarah VOGLER, "Russia's Approach to Cyber Warfare", Teknik Rapor, *Center for Naval Analyses Arlington,* Washington 2017, *https://apps.dtic.mil/sti/pdfs/AD1032208.pdf*, (Erişim tarihi: 08.10.2020).

Council of the European Union, "European Security Strategy A Secure Europe In A Better World", *European Communities*, Brüksel 2009, https://www.consilium.europa.eu/media/30823/qc7809568enc.pdf, (Erişim tarihi: 19.12.2020).

CORNISH, Paul, "EU and NATO: Co-operation or Competition?", Briefing Paper, *Security and Defence*, European Parliament- Policy Department External Policies, Ekim 2006, https://www.europarl.europa.eu/meetdocs/2004_2009/documents/dv/eunatorelations_/eunatorelations_en.pdf, (Erişim tarihi: 08.07.2021).

CyberMag, *HAVELSAN ile NATO Muhabere ve Bilgi Ajansı (NCIA) Arasında Siber Güvenlik İş Birliği Anlaşması*, (22.10.2019), https://www.cybermagonline.com/havelsan-ile-nato-muhabere-ve-bilgi-ajansi-ncia-arasinda-siber-guvenlik-is-birligi-anlasmasi, (Erişim tarihi:25.12.2020).

ÇAVUŞ, Mutlu, "Kurumların Siber Güvenlik Için Ayırdığı Bütçe Artacak", (08.11.2018), *https://www.btgunlugu.com/kurumlar-siber-guvenlik-butce*/, (Erişim tarihi: 19.07.2020).

ÇETİN, Şerife, "NATO Genel Sekreteri Stoltenberg: Türkiye'nin NATO üyeliğinin önemini anlamak zorundayız", (23.01.2020),

https://www.aa.com.tr/tr/dunya/nato-genel-sekreteri-stoltenberg-turkiyenin-nato-uyeliginin-onemini-anlamak-zorundayiz/1711411, (Erişim tarihi: 13.10.2020).

DAVIS, Susan**, "**NATO in the Cyber Age: Strengthening Security & Defence, Stabilising Deterrence", Genel Rapor, *NATO Parliamentary Assembly,* Nisan 2019, *https://www.nato-pa.int/document/2019-nato-cyber-age-strenghtening-security-and-defence-stabilising-deterrence*, (Erişim tarihi: 13.10.2020).

DEMİRCİ, Zuhal, "İnsanoğlunun Uzay Macerası 61 Yıl Önce Başladı", (03.10.2018), *https://www.aa.com.tr/tr/bilim-teknoloji/insanoglunun-uzay-macerasi-61-yil-once-basladi/1271438*, (Erişim tarihi: 27.07.2020).

DiploFoundation, *Digital diplomacy, E-diplomacy, Cyber diplomacy*, https://www.diplomacy.edu/e-diplomacy, (Erişim tarihi: 15.08.2020).

EMMOTT, Robin, "NATO mulls 'offensive defense' with cyber warfare rules", (30.11.2017), *https://www.reuters.com/subjects/aerospace-and-defense/article/us-nato-cyber/nato-mulls-offensive-defense-with-cyber-warfare-rules-idUSKBN1DU1G4,* (Erişim tarihi: 11.10.2020).

EMMOTT, Robin, "NATO cyber command to be fully operational in 2023", 16.10.2018, *https://www.reuters.com/article/us-nato-cyber-idUSKCN1MQ1Z9,* (Erişim tarihi: 10.10.2020).

ERLANGER, Steven ve Jackie CALMES, "NATO Agrees to Build Missile Defense System", (19.11.2010), *https://www.nytimes.com/2010/11/20/world/europe/20prexy.html*, (Erişim tarihi: 09.09.2020).

ESPLNER, Tom, "Estonia's CTO speaks out on cyberattacks", (24.10.2007), *https://www.zdnet.com/article/estonias-cto-speaks-out-on-cyberattacks/*, (Erişim tarihi: 29.09.2020).

European Commission, *EU Cybersecurity Initiatives- Working Towards A More Secure Online Environment,* Factsheet, Ocak 2017 https://ec.europa.eu/newsroom/dae/document.cfm?doc_id= 16540, (Erişim tarihi: 16.12.2020).

European Commission, *Cybersecurity*, (16.12.2020), https://ec.europa.eu/digital-single-market/en/cybersecurity#Other, (Erişim tarihi: 28.12.2020).

European Commission, "Cybersecurity Strategy of the European Union: An Open, Safe and Secure Cyberspace." Joint Communication to the European Parliament, The Council, The European Economic and Social Committee and the Committee of Regions. JOIN(2013) 1 final, Brüksel 2013, *https://www.eumonitor.eu/9353000/1/j4nvke1fm2yd1u0_j9vvik7m1c3gyxp/vkcwedvmmjzx/v=s7z/f=/join(2013)1_en.pdf*, (Erişim tarihi: 16.12.2020).

European Defence Agency, *EDA Supports NATO CCD COE 'Locked Shields' Cyber Defence Exercise*, (05.04.2019), https://www.eda.europa.eu/info-hub/press-centre/latest-news/2019/04/05/eda-supports-nato-ccd-coe-locked-shields-cyber-defence-exercise, (Erişim tarihi: 18.12.2020).

European Parliament, "Cybersecurity in the EU Common Security and Defence Policy (CSDP)- challenges and risks for the EU", *European Parliamentary Research Service*, Brüksel 2017, *http://www.europarl.europa.eu/RegData/etudes/STUD/2017/603175/EPRS_STU(2017)603175_EN.pdf*, (Erişim tarihi: 08.10.2020).

European Union External Action Service, *EU and NATO Increase Information Sharing on Cyber Incidents*, (10.02.2016), https://eeas.europa.eu/generic-warning-system-taxonomy/404_en/5254/EU (Erişim tarihi: 15.12.2020).

European Union External Action Service, *A Europe that Protects: Countering Hybrid Threats*, Haziran 2018, https://eeas.europa.eu/sites/eeas/files/hybrid_threats_en_final.pdf, (Erişim tarihi: 16.12.2020).

European Union External Action Service, *Crisis Preparedness: EU Launches Civil-Military Crisis Management Exercise*, (16.11.2018), https://eeas.europa.eu/delegations/fiji/53926/crisis-preparedness-eu-launches-civil-military-crisis-management-exercise_en, (Erişim tarihi: 18.12.2020).

EU-NATO, *Fourth progress report on the implementation of the common set of proposals endorsed by NATO and EU Councils on 6 December 2016 and 5 December 2017*, https://www.consilium.europa.eu/media/39782/fourth-report-ue-nato-cooperation-en.pdf, (Erişim tarihi: 16.12.2020).

FINKLE, Jim ve Joseph MENN, "Some Flame code found in Stuxnet virus-experts", (11.06.2012), *https://www.reuters.com/article/us-media-tech-summit-flame/some-flame-code-found-in-stuxnet-virus-experts-idUSBRE85A0TN20120611*, (Erişim tarihi: 08.01.2021).

GALLIS, Paul, "The NATO Summit at Bucharest 2008", *CRS Report for Congress*, Mart 2008, *https://apps.dtic.mil/sti/pdfs/ADA478830.pdf*, (Erişim tarihi: 07.09.2020).

GEERS, Kenneth, "Cyperspace and the Changing Nature of Cyber Space", *NATO CCD COE Publication*, Tallinn 2008, *https://www.ccdcoe.org/uploads/2018/10/Geers2008_CyberspaceAndTheChangingNatureOfWarfare.pdf*, (Erişim tarihi: 14.07.2020).

GOULD, Joe, "US, European lawmakers swipe Trump and Turkey in new Syria joint statement", (21.10.2019), *https://www.defensenews.com/congress/2019/10/21/us-european-lawmakers-swipe-trump-and-turkey-in-new-syria-joint-statement/,* (Erişim tarihi: 11.10.2020).

GÖÇEK, Naz, "A Glimpse into Locked Shields 2019", (06.06.2019), *https://natoassociation.ca/a-glimpse-into-locked-shields-2019/*, (Erişim tarihi: 10.12.2020).

HALEY, Christopher, "A Theory of Cyber Deterrence" *Georgetown Journal of International Affairs*. (06.02.2013), https://www.georgetownjournalofinternationalaffairs.org/online-edition/a-theory-of-cyber-deterrence-christopher-haley, (Erişim tarihi: 16.08.2020).

HEALEY, Jason ve Leendert van BOCHOVEN, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow", *The Atlantic Council*. Şubat 2012,

https://www.atlanticcouncil.org/wp-content/uploads/2012/02/022712_ACUS_NATO Smarter_IBM.pdf, (Erişim tarihi: 18.10.2020).

HEALEY, Jason ve Leendert van, BOCHOVEN, "Strategic Cyber Early Warning: A Phased Adaptive Approach for NATO", Issue Brief, *Atlantic Council,* Kasım 2012, *https://www.atlanticcouncil.org/wp-content/uploads/2012/11/NATO-Cyber-Warning-2012.pdf*, (Erişim tarihi: 14.01.2021).

HEALEY, Jason ve Klara T., JORDAN, "NATO's Cyber Capabilities: Yesterday, Today, and Tomorrow", *Atlantic Council*, Eylül 2014, *https://www.atlanticcouncil.org/wp-content/uploads/2014/08/NATOs_Cyber_Capabilities.pdf*, (Erişim tarihi: 01.12.2020).

HENDRICKSON, Ryan C., "Crossing the Rubicon", (01.09.2005), *https://www.nato.int/cps/en/natohq/opinions_21881.htm?selectedLocale=en*, (Erişim tarihi: 31.08.2020).

JOUBERT, Vincent, "Five Years After Estonia's Cyber Attack: Lessons Learned for NATO?", *Research Division- NATO Defense College,* Sayı 76, Mayıs 2012, *https://www.files.ethz.ch/isn/143191/rp_76.pdf*, (Erişim tarihi: 02.12.2020).

Kaspersky, *What is a Botnet?*, https://usa.kaspersky.com/resource-center/threats/botnet-attacks, (Erişim tarihi: 30.09.2020).

KAYA, Alper, "World Wide Web (WWW) Nedir?" (28.04.2016), *https://www.tech-worm.com/world-wide-web-www-nedir*/, (Erişim tarihi: 14.07.2020).

KOLAKOWSKI, Mark, "At $1.3 Trillion, Apple Is Bigger Than These Things." (06.01.2020), *https://www.investopedia.com/news/apple-now-bigger-these-5-things/*, (Erişim tarihi:27.12.2020).

KORNS, Stephen W. ve Joshua E. KASTENBERG, "Georgia's Cyber Left Hook", *Parameters,* Kış 2008-2009, https://apps.dtic.mil/sti/pdfs/ADA636632.pdf, (Erişim tarihi: 14.03.2021), ss. 60-76.

KRUPCZYNSKI, Mateusz, "NATO's Reaffirmed Commitment to Cyber Security", (15.08.2016), *http://futurenato.org/articles/natos-reaffirmed-commitment-to-cyber-security/*, (Erişim tarihi: 06.10.2020).

LÉTÉ, Bruno ve Piret PERNIK, "EU–NATO Cybersecurity and Defense Cooperation: From Common Threats to Common Solutions", *German Marshall Fund of the United States,* Sayı 38, Aralık 2017, *https://www.gmfus.org/news/eu-nato-cybersecurity-and-defense-cooperation-common-threats-common-solutions*, (Erişim tarihi: 14.12.2020).

MACCHI, Victoria ve Jessie KRATZ, "9/11 Archives: In our New York office: A day like no other", *https://www.archives.gov/news/articles/national-archives-nyc-september-11*, (Erişim tarihi: 13.12.2021).

MARKS, Joseph, "Ukraine's intel chief: We weren't ready", (23.06.2015), *https://www.politico.eu/article/ukraines-intel-chief-we-werent-ready/,* (Erişim tarihi: 08.10.2020).

MARRONE, Alessandro ve Ester SABATINO, "Cyber Defence in NATO Countries: Comparing Models", *Istituto Affari Internazionali*, Şubat 2021, *https://www.iai.it/sites/default/files/iaip2105.pdf*, (Erişim tarihi: 12.04.2021).

MCNAMARA, Sally, "NATO Summit 2010: Time to Turn Words Into Action", *The Heritage Foundation,* Sayı 2498, Aralık 2010, *https://www.heritage.org/global-politics/report/nato-summit-2010-time-turn-words-action*, (Erişim tarihi: 02.10.2020).

MESSMER, Ellen, "Kosovo cyber-war intensifies: Chinese hackers targeting U.S. sites, government says", (12.05.1999), *http://edition.cnn.com/TECH/computing/9905/12/cyberwar.idg*/, (Erişim tarihi: 15.12.2021).

MILLER, Robert A. ve Daniel T. KUEHL, "Cyberspace and the 'First Battle' in 21st Century War", *Defense Horizons*, Sayı 68, Eylül 2009, *https://apps.dtic.mil/sti/pdfs/ADA508696.pdf*, (Erişim tarihi: 30.09.2020).

MILLER, Susan, “What is WikiLeaks?”, (07.03.2017), *https://www.usatoday.com/story/news/2017 /03/07/what-wikileaks/98853896/*, (Erişim tarhi: 17.07.2020).

MORGAN, Steve, "Cyber Crime Costs Projected To Reach $2 Trillion by 2019", (17.01.2016), *https://www.forbes.com/sites/stevemorgan/2016/01/17/cyber-crime-costs-projected-to-reach-2-trillion-by-2019/#479eef553a91*, (Erişim tarihi: 13.08.2020).

NATO, *A New NATO For A New Century*, (05.11.2008), https://www.nato.int/cps/en/natolive/opinions_25558.htm, (Erişim tarihi: 25.08.2020).

NATO, *Kuzey Atlantik Antlaşması*, (09.12.2008), https://www.nato.int/cps/fr/natohq/official_texts_17120.htm?selectedLocale=tr, (Erişim tarihi: 25.08.2020).

NATO, *The Alliance's New Strategic Concept*, (26.08.2010), https://www.nato.int/cps/en/natohq/official_texts_23847.htm?&utm_source=twitter &utm_medium=smcweb&utm_campaign=23847, (Erişim tarihi: 29.08.2020).

NATO, *North Atlantic Cooperation Council (NACC*), (30.01.1017), https://www.nato.int/cps/en/natolive/topics_69344.htm, (Erişim tarihi:30.08.2020).

NATO, *NATO's Enlargement*, (04.07.1997), https://www.nato.int/docu/comm/1997/970708/ infopres/e-enl.htm, (Erişim tarihi: 01.09.2020).

NATO, *Washington Summit*, (06.11.2008), https://www.nato.int/cps/en/natohq/news_27286.htm?selectedLocale=en, (Erişim tarihi: 01.09.2020).

NATO, *Riga Summit Declaration*, (27.02.2009), https://www.nato.int/docu/pr/2006/p06-150e.htm, (Erişim tarihi: 30.09.2020).

NATO, *Riga Summit Declaration*, (08.05.2014), https://www.nato.int/cps/en/natohq/official_texts_37920.htm?selectedLocale=en, (Erişim tarihi: 06.09.2020).

NATO, "Aktif Katılım, Modern Savunma: Kuzey Atlantik Antlaşması Örgütü Üyelerinin Savunması ve Güvenliği için Stratejik Kavram", *NATO Public Diplomacy Division*, Brüksel 2010, *https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120207_strategic-concept-2010-tur.pdf*, (Erişim tarihi: 20.08.2020).

NATO, *Chicago Summit Declaration*, (01.08.2012), https://www.nato.int/cps/en/natohq/official_texts_87593.htm?selectedLocale=en, (Erişim tarihi: 09.09.2020).

NATO, *Cyber Defence*, (25.09.2020), https://www.nato.int/cps/en/natohq/topics_78170.htm, (Erişim tarihi: 30.09.2020).

NATO, *Cyber Defence Pledge*, (08.07.2016), https://www.nato.int/cps/en/natohq/official_texts_133177.htm?selectedLocale=en, (Erişim tarihi: 06.10.2020).

NATO, *Joint Statement of the NATO-Ukraine Commission*, (04.09.2014), https://www.nato.int/cps/en/natohq/news_112695.htm?mode=pressrelease, (Erişim tarihi: 09.09.2020).

NATO, *Wales Summit Declaration*, (30.08.2018), https://www.nato.int/cps/en/natohq/official_texts_112964.htm, (Erişim tarihi: 09.09.2020).

NATO, "NATO's Readiness Action Plan", Fact Sheet, *Public Diplomacy Division*, Temmuz 2016, *https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2016_07/20160627_1607-factsheet-rap-en.pdf*, (Erişim tarihi: 09.09.2020).

NATO, "Warsaw Summit Key Decisions", Fact Sheet, *Public Diplomacy Division*, Şubat 2017,

https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2017_02/20170206_1702-factsheet-warsaw-summit-key-en.pdf, (Erişim tarihi: 09.09.2020).

NATO, *Warsaw Summit Communiqué*, (29.03.2017), https://www.nato.int/cps/en/natohq/official_texts_133169.htm, (Erişim tarihi: 10.09.2020).

NATO, *Joint statement of the NATO-Ukraine Commission at the level of Heads of State and Government*, (09.07.2016), https://www.nato.int/cps/en/natohq/official_texts_133173.htm?selected Locale=en, (Erişim tarihi: 10.09.2020).

NATO, *Brussels Summit Declaration*, (30.08.2018), https://www.nato.int/cps/en/natohq/official_texts_156624.htm, (Erişim tarihi: 11.09.2020).

NATO, "Brussels Summit Key Decisions 11 – 12 July 2018", Fact Sheet, *Public Diplomacy Division*, Kasım 2018, *https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_2018_11/20181105_1811-factsheet-key-decisions-su.pdf*, (Erişim tarihi: 10.10.2020).

NATO, *Bucharest Summit Declaration*, (08.05.2014), http://www.nato.int/cps/en/natolive/official_texts_8443.htm, (Erişim tarihi: 01.10.2020).

NATO, *London Declaration*, (04.09.2019), https://www.nato.int/cps/en/natohq/official_texts_ 171584.htm, (Erişim tarihi: 11.10.2020).

NATO, *Secretary General appoints group as part of NATO reflection process*, (09.06.2020), https://www.nato.int/cps/en/natohq/news_174756.htm, (Erişim tarihi: 11.10.2020).

NATO, *Press conference by NATO Secretary General Jens Stoltenberg following the meeting of the North Atlantic Council at the level of Defence Ministers*, (08.11.2017), https://www.nato.int/cps/en/natohq/opinions_148417.htm, (Erişim tarihi: 11.10.2020).

NATO, *Signing Ceremony to Initiate a Study on NATO Network Enabled Capability (NNEC*), (03.11.2008), https://www.nato.int/cps/us/natohq/news_20084.htm?selectedLocale=en, (Erişim tarihi: 30.09.2020).

NATO, *Strasbourg / Kehl Summit Declaration*, (08.05.2014), https://www.nato.int/cps/en/natolive/news_52837.htm, (Erişim tarihi: 02.10.2020).

NATO, *Strategic Concept 2010*, (03.02.2012), https://www.nato.int/cps/en/natohq/topics_ 82705.htm, (Erişim tarihi: 02.10.2020).

NATO, *Defending the networks: The NATO Policy on Cyber Defence*, https://www.ccdcoe.org/uploads/2018/10/NATO-110608-CyberdefencePolicyExecSummary.pdf, 2011, (Erişim tarihi: 03.10.2020).

NATO, *NATO Rapid Reaction Team to fight cyber attack*, (13.03.2012), https://www.nato.int/cps/en/natolive/news_85161.htm, (Erişim tarihi: 06.10.2020).

NATO, *NATO launches Industry Cyber Partnership*, (18.09.2014), https://www.nato.int/cps/en/natohq/news_113121.htm, (Erişim tarihi: 07.10.2020).

NATO, *NATO and the European Union Enhance Cyber Defence Cooperation*, (10.02.2016), https://www.nato.int/cps/en/natohq/news_127836.htm, (Erişim tarihi: 09.10.2020).

NATO, *Rome Declaration on Peace and Cooperation*, (27.10,2000), https://www.nato.int/docu/comm/49-95/c911108a.htm, (Erişim tarihi: 30.08.2020).

NATO, *Allied Command Operations (ACO)*, (23.10.2020), http://www.nato.int/cps/en/natolive/topics_52091.htm, (Erişim tarihi: 06.12.2020).

NATO, *Statement by the North Atlantic Council concerning malicious cyber activities*, (03.01.2020), https://www.nato.int/cps/en/natohq/official_texts_176136.htm?selectedLocale=en, (Erişim tarihi: 14.10.2020).

NATO, *NATO Communications and Information Agency (NCI Agency)*, https://www.nato.int/cps/en/natohq/topics_69332.htm, (Erişim tarihi: 01.12.2020).

NATO, *Men in black – NATO's cybermen,* (24.04.2015), https://www.nato.int/cps/en/natolive/news_ 118855.htm, (Erişim tarihi: 02.12.2020).

NATO, *Joint declaration by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organization,* (05.12.2017), https://www.nato.int/cps/en/natohq/official_texts_133163.htm, (Erişim tarihi: 16.12.2020).

NATO, *Joint Declaration on EU-NATO Cooperation by the President of the European Council, the President of the European Commission, and the Secretary General of the North Atlantic Treaty Organizatio*n, (10.07.2018), http://www.nato.int/cps/en/natohq/official_texts_156626.htm, (Erişim tarihi: 19.12.2020).

NATO, *NATO and EU Press Ahead With Cooperation On Cyber Defence*, (25.11.2016), https://www.nato.int/cps/en/natohq/news_138122.htm, (Erişim tarihi: 17.12.2020).

NATO, *NATO Handbook,* Public Diplomacy Division, Brüksel 2006, https://www.nato.int/docu/handbook/2006/hb-en-2006.pdf, (Erişim tarihi: 25.08.2020).

NATO, *Framework For Collaborative Interaction (FFCI),* https://www.act.nato.int/ffci, (Erişim tarihi: 24.12.2020).

NATO, *The Atlantic Charter*, (02.07.2018), https://www.nato.int/cps/bu/natohq/official_texts_ 16912.htm, (Erişim tarihi: 01.01.2021).

NATO, *The Alliance's Strategic Concept*, (25.06.2009), https://www.nato.int/cps/en/natolive/official_texts_27433.htm, (Erişim tarihi 11.12.2021).

NATO, "NATO 2012 Chicago Summit Guide- NATO's 25th summit meeting", 20-21 Mayıs 2012,

https://www.nato.int/nato_static_fl2014/assets/pdf/pdf_publications/20120905_SummitGuideChicago2012-eng.pdf, (Erişim tarihi: 06.10.2020).

NATO, *Partnership for Peace Programme*, (23.03.2020), https://www.nato.int/cps/en/natohq/topics_50349.htm, (Erişim tarihi: 03.02.2021).

NATO, *Brussels Summit Communiqué*, (14.06.2021), https://www.nato.int/cps/en/natohq/news_185000.htm, (Erişim tarihi: 20.09.2021).

NATO, *About Us*, https://ncisg.nato.int/about-us, (Erişim tarihi: 08.12.2020).

NATO, *FRAMEWORK FOR COLLABORATIVE INTERACTION (FFCI)*, https://www.act.nato.int/ffci, (Erişim tarihi: 25.12.2020).

NATO CCD COE, *EU Cyber Defence Policy Framework Presents More Than 40 Action Measures*, https://ccdcoe.org/incyder-articles/eu-cyber-defence-policy-framework-presents-more-than-40-action-measures/, (Erişim tarihi: 08.10.2020).

NATO CCD COE, *About Us*, https://ccdcoe.org/about-us/, (Erişim tarihi: 04.12.2020).

NATO CCD COE, *The Virtual Battlefield: Perspectives on Cyber Warfare (Proceedings 2009)*, https://ccdcoe.org/library/publications/the-virtual-battlefield-perspectives-on-cyber-warfare-proceedings-2009/, (Erişim tarihi: 07.12.2020).

NATO CCD COE, *CyCon*, https://ccdcoe.org/cycon/, (Erişim tarihi: 09.12.2020).

NATO CCD COE, *Locked Shield*, https://ccdcoe.org/exercises/locked-shields/, (Erişim tarihi: 10.12.2020).

NATO CCD COE, *France Wins Cyber Defence Exercise Locked Shields 2019*, https://ccdcoe.org/news/2019/france-wins-cyber-defence-exercise-locked-shields-2019/, (Erişim tarihi: 10.12.2020).

NATO CCD COE, *NATO Summit Updates Cyber Defence Policy*, https://ccdcoe.org/incyder-articles/nato-summit-updates-cyber-defence-policy/, (Erişim tarihi: 11.10.2020).

NATO CCD COE, *NATO Recognises Cyberspace as a 'Domain of Operations' at Warsaw Summit*, https://ccdcoe.org/incyder-articles/nato-recognises-cyberspace-as-a-domain-of-operations-at-warsaw-summit/, (Erişim tarihi: 08.10.2020).

NATO CCD COE, *NATO Team Wins the Locked Shields Cyber Defence Exercise*, https://ccdcoe.org/news/2013/nato-team-wins-the-locked-shields-cyber-defence-exercise/, (Erişim tarihi: 09.12.2020).

NATO Communications and Information Agency, *NATO launches Industry Cyber Partnership*, (18.09.2014), https://www.ncia.nato.int/about-us/newsroom/nato-launches-industry-cyber-partnership.html, (Erişim tarihi: 22.12.2020).

NATO Communications and Information Agency, *Business Leaders Discuss NATO Industry Cyber Partnership*, (28.04.2015), https://www.ncia.nato.int/about-us/newsroom/business-leaders-discuss-nato-industry-cyber-partnership.html, (Erişim tarihi: 23.12.2020).

NATO Communications and Information Agency, *Three NATO Industry Cyber Partnership agreements signed at NIAS'19*, (17.10.2019), https://www.ncia.nato.int/about-us/newsroom/three-nato-industry-cyber-partnership-agreements-signed-at-nias19-.html, (Erişim tarihi:24.12.2020).

NCI Agency, *NATO's Cyber Security Centre*, https://www.ncia.nato.int/what-we-do/cyber-security.html, (Erişim tarihi: 05.12.2020).

NCI Agency, *NATO's Cyber Defenders win Exercise Locked Shields 2015*, (28.04.2015), https://www.ncia.nato.int/about-us/newsroom/natoe28099s-cyber-defenders-win-exercise-locked-shields-2015.html, (Erişim tarihi: 09.12.2020).

NICHOL, Jim, "Russia-Georgia Conflict in South Ossetia: Context and Implications for U.S. Interests", *Congressional Research Service*, Ağustos 2008,

https://www.everycrsreport.com/files/20080813_RL34618_af7d22e7f33f1eadc090b329791f1bbc6fad71e4.pdf, (Erişim tarihi: 01.10.2020).

NYE, Joseph S., "The World Needs New Norms On Cyber-Warfare," (01.10.2015), *https://www.washingtonpost.com/opinions/the-world-needs-an-arms-control-treaty-for-cybersecurity/ 2015/10/01/20c3e970-66dd-11e5-9223-70cb36460919_story.html*, (Erişim tarihi: 15.08.2020).

NYE, Joseph S., "Cyber Power", *Harvard Kennedy School- Belfer Center for Science and International Affairs,* Mayıs 2010, *https://apps.dtic.mil/sti/pdfs/ADA522626.pdf*, (Erişim tarihi: 02.10.2020).

OBE, James S., "NATO and Russia: 'Refresh' but no Transformation", *https://www.chathamhouse.org/media/comment/view/163647*, Erişim tarihi: 08.09.2020).

PAPAIOANNOU, Alexandros, "Strengthening EU-NATO Relations", (16.07.2019), *https://www.nato.int/docu/review/articles/2019/07/16/strengthening-eu-nato-relations/index.html*, (Erişim tarihi: 12.12.2020).

PEDLOW, Gregory W., "NATO STRATEGY DOCUMENTS 1949-1969", *https://www.nato.int/docu/stratdoc/eng/intro.pdf*, (Erişim tarihi: 11.12.2021).

PINDJÁK, Peter, "Deterring hybrid warfare: a chance for NATO and the EU to work together?", (18.11.2014), *https://www.nato.int/docu/review/articles/2014/11/18/deterring-hybrid-warfare-a-chance-for-nato-and-the-eu-to-work-together/index.html*, (Erişim tarihi: 22.01.2021).

PKHALADZE, Nodar, "A Look Back on the 2018 NATO Brussels Summit", Politika Raporu, *Institute for Politics and Society*, Ağustos 2018, *https://www.politikaspolecnost.cz/wp-content/uploads/2018/08/The-2018-NATO-Brussels-Summit-IPPS.pdf*, (Erişim tarihi: 11.09.2020).

PLANTERA, Federico, "NATO CCDCOE – Expertise and cooperation make our cyber space safer", (October 2018), *https://e-estonia.com/nato-ccdcoe-expertise-cyber-space-safer/,* (Erişim tarihi: 05.12.2020).

RASMUSSEN, Anders F., "Press Conference following the meeting of the North Atlantic Council at the level of Heads of State and Government during the NATO Wales Summit", (05,09.2014), *https://www.nato.int/cps/en/natohq/opinions_112871.htm*, (Erişim tarihi: 05.10.2020).

RID, Thomas, "Think Again: Cyberwar", (27.02.2012), *https://foreignpolicy.com/2012/02/27/think-again-cyberwar/,* (Erişim tarihi: 12.07.2020).

ROBINSON, Neil, "NATO: Siber Savunmada Vites Değiştiriyor", (08.06.2016), *https://www.nato.int/docu/review/tr/articles/2016/06/08/nato-siber-savunmada-vites-degistiriyor/index.html*, (Erişim tarihi: 15.08.2020).

SHAPE Public Affairs Office, *Exercise Cyber Coalition 2020 Underway*, (16.11.2020), https://shape.nato.int/news-archive/2020/exercise-cyber-coalition-2020-underway, (Erişim tarihi: 11.12.2020).

SHARMA, Himanshu, "NATO Conducts Cyber Coalition Exercise Virtually", (07.11.2020), *https://www.newdelhitimes.com/nato-conducts-cyber-coalition-exercise-virtually/*, (Erişim tarihi: 16.12.2020).

SMITH, James F., "Richard Clarke on Cyber Threats: Defense is Key", (21.09.2010), *https://www.belfercenter.org/publication/richard-clarke-cyber-threats-defense-key*, (Erişim tarihi: 07.08.2020).

SMITH, Michael ve Peter WARREN, "Nato Warns of Strike Against Cyber Attackers", (06.06.2010), *https://www.thetimes.co.uk/article/nato-warns-of-strike-against-cyber-attackers-97qkr5lbtwp*, (Erişim tarihi: 08.01.2021).

STOLTENBERG, Jens, "The Secretary General's Annual Report 2019", *https://www.nato.int/nato_static_fl2014/assets/pdf/2020/3/pdf_publications/sgar19-en.pdf*, (Erişim tarihi: 26.12.2020).

STOLTENBERG, Jens, "NATO Will Defend Itself", (29.08.2019), *https://www.nato.int/cps/en/natohq/news_168435.htm?selectedLocale=en*, (Erişim tarihi:25.12.2020).

TAYLOR, Claire, "NATO: The Prague Summit and Beyond", Research Paper 03/05, *House Of Commons Library*, Ocak 2003, *https://researchbriefings.files.parliament.uk/documents/RP03-05/RP03-05.pdf*, (Erişim tarihi: 06.09.2020).

TAYLOR, Claire, "NATO Summit 2010", SN/IA/5788, *House Of Commons Library*, Aralık 2010, *https://researchbriefings.files.parliament.uk/documents/SN05788/SN05788.pdf*, (Erişim tarihi: 08.09.2020).

TAYLOR, Trevor, "NATO and Central Europe", (10.04.2002), *https://www.nato.int/docu/review/1991/9105-4.htm*, (Erişim tarihi: 28.08.2020).

The European Union Agency for Cybersecurity, "Overview Of Cybersecurity And Related Terminology", *European Union Agency For Network and Information Security*, Versiyon 1, Eylül 2017, *https://www.enisa.europa.eu/publications/enisa-position-papers-and-opinions/enisa-overview-of-cybersecurity-and-related-terminology*, (Erişim tarihi: 12.08.2020).

The Guardian, *Ground Zero stops burning, after 100 days*, (20.12.2001), https://www.theguardian.com/world/2001/dec/20/september11.usa, (Erişim tarihi: 13.12.2021).

The New York Times, *Text: Obama's Remarks on Cyber-Security*, (29.05.2009), https://www.nytimes.com/2009/05/29/us/politics/29obama.text.html, (Erişim tarihi: 13.08.2020).

The North Atlantic Council, *Washington Summit Communiqu*, (24.04.1999), https://www.nato.int/docu/pr/1999/p99-064e.htm, (Erişim tarihi: 01.09.20209).

U.S. Department of State, *NATO Summits and Meetings*, https://2017-2021.state.gov/nato-summits/index.html, (Erişim tarihi: 11.10.2020).

VÄLJATAGA, Ann, "Tracing Opinio Juris in National Cyber Security Strategy Documents" *NATO Cooperative Cyber Defence Centre of Excellence*, Tallinn 2018, *https://ccdcoe.org/uploads/2019/01/Tracing-opinio-juris-in-NCSS-2.docx.pdf*, (Erişim tarihi: 04.12.2020).

VERREKIA, Bridget, "Digital Diplomacy and Its Effect on International Relations*", Independent Study Project Collection,* Bahar 2017, *https://digitalcollections.sit.edu/cgi/viewcontent.cgi?referer=https://scholar.google.com.tr/&httpsredir=1&article=3619&context=isp_collection*, (Erişim tarihi: 17.08.2020).

VERTON, Dan, "Serbs launch cyberattack on NATO", (04.04.1999), *https://fcw.com/1999/04/serbs-launch-cyberattack-on-nato/195288/*, (Erişim tarihi: 15.12.2021).

WHEATCROFT, Geoffrey, "Who Needs NATO?", *https://www.nytimes.com/2011/06/16/opinion/16iht-edwheatcroft16.html*, (Erişim tarihi: 24.08.2020).

WHITTAKER, Francis, "What Is WikiLeaks? Everything you need to know", (30.04.2018), *https://www.nbcnews.com/storyline/smart-facts/what-wikileaks-everything-you-need-know-n869556*, (Erişim tarihi: 25.07.2020).

WORSTALL, Tim, "Stuxnet Was a Joint US/ Israeli Project", (01.01.2012), *https://www.forbes.com/sites/timworstall/2012/06/01/stuxnet-was-a-joint-us-israeli-project/?sh=7bef79ab7a8a*, (Erişim tarihi: 07.01.2021).

ZOLOTUKHINA, Elizabeth ve Christian OSTERMANN, "The Evolution of NATO: the 2010 Strategic Concept and Beyond", (21.05.2010), *https://www.wilsoncenter.org/event/the-evolution-nato-the-2010-strategic-concept-and-beyond*, (Erişim tarihi: 08.09.2020).