T.C.
İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER ENSTİTÜSÜ SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER ANABİLİM DALI

YÜKSEK LİSANS TEZİ

NATO'NUN GÜVENLİK ALANINDA YENİ BİR BOYUT: SİBER GÜVENLİK

Gizem SOMUNCU

2501110471

TEZ DANIŞMANI

Dr.Öğr.Ü. Gizem BİLGİN AYTAÇ

İSTANBUL–2018

T.C. İSTANBUL ÜNİVERSİTESİ
SOSYAL BİLİMLER
1982 ENSTİTÜSÜ

Y Ü K S E K L İ S A N S
T E Z O N A Y I

ÖĞRENCİNİN

Adı ve Soyadı : **GİZEM SOMUNCU** Numarası : **2501110471**

Danışman :**DR. ÖĞR. ÜYESİ GİZEM BİLGİN AYTAÇ**

Anabilim/Bilim Dalı : **SİYASET BİLİMİ VE ULUSLARARASI İLİŞKİLER**

Tez Savunma Tarihi : **16.04.2018** Tez Savunma Saati : **13:00**

Tez Başlığı : **NATO'NUN GÜVENLİK ALANINDA YENİ BİR BOYUT: SİBER GÜVENLİK**

TEZ SAVUNMA SINAVI, Lisansüstü Öğretim Yönetmeliği'nin **36. Maddesi** uyarınca yapılmış, sorulan sorulara alınan cevaplar sonunda adayın tezinin **KABULÜ'NE** OYBİRLİĞİ / ~~OYÇOKLUĞUYLA~~ karar verilmiştir.

JÜRİ ÜYESİ	İMZA	KANAATİ (KABUL / RED / DÜZELTME)
1- PROF. DR. BURAK SAMİH GÜLBOY		
2- DR. ÖĞR. ÜYESİ GİZEM BİLGİN AYTAÇ		KABUL
3- DR. ÖĞR. ÜYESİ CAN KAKIŞIM		KABUL

YEDEK JÜRİ ÜYESİ	İMZA	KANAATİ (KABUL / RED / DÜZELTME)
1- PROF. DR. LEVENT ÜRER		
2- DR. ÖĞR. ÜYESİ PINAR ERKEM GÜLBOY		KABUL

ÖZ

NATO'NUN GÜVENLİK ALANINDA YENİ BİR BOYUT: SİBER GÜVENLİK

Gizem SOMUNCU

Soğuk Savaş sonrası yıllarda bilgi ve iletişim teknolojilerindeki ilerleme, 1648 Westphalia ile çizilen coğrafi sınırları daha geçirgen bir hale sokmuştur. Bu değişim ile beraber yeni tehditler karşısında ortodoks güvenlik paradigması yetersiz kalmaya başlamıştır. Özellikle internetin küresel kullanım oranındaki artış, siber güvenlik kavramının ulusal ve uluslararası güvenlik açısından öncelikli hale gelmesine neden olmuştur. Çünkü siber tehditler kişisel, kurumsal, ulusal hatta uluslararası olmak üzere zincirleme sonuçlar doğurmaktadır. Kişisel verilerden, bankacılık işlemlerine kadar geniş yelpazede gerçekleştirilen siber saldırılar ile devletler, bu "yeni alandaki yeni soruna" karşı "yeni stratejiler" geliştirmek ve işbirliği yolları bulmak zorunda kalmaktadır. Her seviyede aktörün siber tehditin muhatabı olması devlet merkezli, nihai hedefin devletin güvenliği olduğu anlayışın değişerek devlet dışı aktörlerin rollerinin önem kazanmasına neden olmuştur. Siyasi, ekonomik, askeri, entegrasyonlara ek olarak teknolojik entegrasyon çok boyutlu güvenlik anlayışının gelişmesine katkıda bulunduğundan devletler için küresel siber saldırılara karşı ulusal güvenliğin sağlanması maksadıyla uluslararası ittifaklar içinde olma ihtiyacı artmaya başlamıştır. Bu çalışmada anonim ve gelişen teknoloji ile her gün değişen, dinamik siber tehditler kapsamında ihtiyaç duyulan ittifakın somut halini teşkil eden, 29 üye ve 39 ortak ülkeyi aynı çatı altında birleştiren NATO'nun uyguladığı siber güvenlik stratejisi incelenerek aynı dinamiklik de kolektif güvenliğin uygulanma "imkânı" tartışması yapılacaktır.

Anahtar Kelimeler: Güvenlik, özgürlük, siber güvenlik, ulusal güvenlik, NATO, kolektif güvenlik

ABSTRACT

A NEW DIMENSION IN NATO'S SECURITY DOMAIN: CYBERSECURITY

Gizem SOMUNCU

Geographical boundaries drawn with 1648 Westphalia have become permeable as a result of progress in information and communication technologies in the post-Cold War years. Along with this change, the orthodox security paradigm has become insufficient in the face of new threats. The concept of cybersecurity has become a priority in terms of national and international security as a result of increment in the global usage of the internet. Because cyber threats have consequences which are linked to personal, institutional, national and international actors. Cyberattacks, ranging from personal data to banking operations, have to be dealt by the governments. Also new strategies against this “new problem in the new area” must be developed and ways to cooperate should be found. The security understanding, in which the state is centered and the security of the state is the ultimate goal, has changed because the cyberthreat targets actors of all levels. Now the roles of non-state actors are gaining importance. The integration of technology along with policy, economy and military has contributed to the development of multidimensional security. As of today necessity of being in an international alliance to provide national security against global cyberattacks, is inevitable. In this study the struggle between dynamic cyberthreats which are changing every day with anonymous and developing technology and the cybersecurity strategy implemented by NATO will be examined. Also possibility of applying collective security in the same dynamism within the scope the threat will be debated .

Keywords: Security, freedom, cybersecurity, national security, NATO, collective security

ÖNSÖZ

İlerleyen teknoloji ve küreselleşme ile değişen değerler uluslararası aktörlerin tehdit ve güvenlik algılarını etkilerken, etkilenen aktörlerin konu kapsamında aldığı önlemler eski fakat hala geçerliliğini koruyan güvenlik-özgürlük ikilemini de beraberinde getirmektedir. Bireysel güvenlik, devlet bekası, bireyin özgürlüğü, ulusal güvenlik, uluslararası güvenlik, ittifak, kolektif güvenlik vb. kavramların tekrar ele alınmasını gerekli kılmaktadır.

Bu çalışmada söz konusu alanları tekrar inceleme ve araştırmama neden olan, fikir veren arkadaşım Bülent AKKUŞ'a, müteakiben yöntem ve içerik konusunda yol gösteren, destek olan Hocam Prof.Dr. Burak Samih GÜLBOY'a ve süreci bu kadar uzatıp çalışmamdan kopmuş olmama rağmen beni tekrar harekete geçiren ve sonuna kadar destek olan tez danışmanım, adaşım, Hocam, Dr.Öğr.Ü. Gizem BİLGİN AYTAÇ'a az geleceğini bilerek teşekkürlerimi sunmayı önemli bir vazife bilirim.

Bana bütün eğitim hayatım boyunca maddi ve manevi yardımlarını esirgemeyen, her zaman her konuda olduğu gibi bu süreçte de bana güvenip destek olan aileme sonsuz teşekkürler.

Gizem SOMUNCU

Ankara, 2018

İÇİNDEKİLER

Sayfa

TABLOLAR LİSTESİ

ŞEKİLLER LİSTESİ

KISALTMALAR LİSTESİ

AGİK : Avrupa Güvenlik ve İşbirliği Konferansı

AGSK : Avrupa Güvenlik ve Savunma Kimliği

AKKA : Avrupa Konvansiyonel Kuvvetler Antlaşması

ARPA : Advanced Research Projects Agency

ARPANET : ARPA Network

BİO : Barış İçin Ortaklık

BM : Birleşmiş Milletler

CADO : Comprehensive All-Domain Operations

CCDCOE : Cooperative Cyber Defence Centre of Excellence

CD-CSC : Cyber Defence Coordination and Support Center

CDMA : Cyber Defense Management Authority

CDMB : Cyber Defence and Management Board

CMDB : Cyber Defence Management Board

DDOS : Distributed Denial of Service

DoS : Denial of Service

FBI : Federal Bureau of Investigation

FTP : File Transfer Protocol

http : Hypertext Transfer Protoco

IETF : Internet Engineering Task Force

IoT : Internet of Things

IP : İnternet Protokol

ISO : International Standards Organization

MILNET : Military Network

MJOT	**:** Major Joint Operation
NASA	**:** National Aeronautics and Space Administration
NATO	**:** North Atlantic Treaty Organization
NC3A	**:** NATO Consultation, Command and Control Agency
NCI	**:** NATO Communications and Information
NCIA	**:** NATO Communications and Information Agency
NCIRC	**:** NATO Computer Incident Response Capability
NCIRCTC	**:** NATO Computer Incident Response Capability Technical Centre
NCISGCD	**:** NATO Communications and Information Group Cyber Defence
NCSA	**:** NATO Communications and Information Systems Services Agency
NCW	**:** Network-Centric Warfare
NDPP	**:** NATO Defence Planning Process
NICP	**:** NATO Industry Cyber PArtnership
NMG	**:** NATO Mukabele Gücü
NNEC	**:** NATO Network Enabled Capability
NSA	**:** National Security Agency
RRT	**:** Rapid Reaction Team
SHAPE	**:** Supreme Headquarters Allied Power Europe
SSCB	**:** Sovyet Sosyalist Cumhuriyetler Birliği
TCP	**:** Transmission Control Protocol
URL	**:** Uniform Resource Locator
VP	**:** Varşova Paktı

"Yakın gelecekte çıkabilecek büyük bir savaşta ilk mermi internette atılacaktır."

Rex HUGHEZ (NATO Güvenlik Danışmanı)

GİRİŞ

Bilgi teknolojilerindeki gelişmeler ve bu teknolojilerin hayatın her noktasında kullanımının artması ile ağlar üzerinden karşılıklı etkileşim içerisinde bulunulması yeni tehditleri de beraberinde getirmektedir. Çağımızda internetin sosyal hayatta olduğu kadar askeri - politik alanda da gelişme gösteren bir araç olarak ortaya çıkması yeni bir güvenlik parametresi olarak siber güvenlik kavramını gündeme getirmiştir. İnternetin küresel kullanım oranı, siber güvenlik kavramının ulusal ve uluslararası güvenlik açısından öncelikli hale gelmesine neden olmuştur. Çünkü siber tehditler kişisel, kurumsal, ulusal hatta uluslararası olmak üzere geniş yelpazede zincirleme sonuçlar doğurmaktadır.

Üç bölümden oluşan bu çalışmanın konu kapsamındaki araştırma ve tartışmaların ortaya konulmaya çalışıldığı ilk kısmı olan II. Bölümde, değişen uluslararası ilişkiler ve güvenlik anlayışına bağlı olarak aktörlerin bu değişimden nasıl etkilendiği ifade edilmeye çalışılmıştır. Devamında Soğuk Savaş sonrası değişen güvenlik algısının günümüzde en çok tartışılan problemlerinden biri olarak ifade edebileceğimiz siber tehdit ve söz konusu kavram ile ilintili diğer ifadelerin tanımları üzerinden sistem için hala en önemli aktör kabul edilen devletin, devlet-birey, devlet-devlet, devlet-uluslararası örgütler vb. konumu açıklanmaya çalışılmıştır. Uluslararası ilişkiler kuramlarından örnekler ile özellikle devlet-birey arasındaki güvenlik-özgürlük ikileminin yarattığı ve yaratabileceği olumsuz durumlar örneklendirilmeye çalışılmıştır. Sosyal medya üzerinde kişisel veriler kullanılarak ya da bankacılık işlemleri ile gerçekleştirilen dolandırıcılık faaliyetleri bireyleri etkileyen bir siber olay olurken, bir devlet kurumunun verilerinin ele geçirilmesi daha geniş bir kitleyi etkilemekte hatta ulusal güvenliği tehdit eder bir hal almaktadır. Söz konusu örnekler üzerinden de anlaşılabileceği gibi tehdidin etki kapasitesinin yüksek olması devletlerin konu kapsamında gerekli tedbirleri almasını da zorunlu kılmaktadır. Ulusal güvenliğe yönelik alınan tedbirler ile güvenlik kapsamında bireylerin özgürlüğüne müdahale veya özgürlüğünden vazgeçilmesi durumunun ortaya çıkması ise konu kapsamındaki ana tartışma noktasını oluşturmaktadır. Aynı bölümde bu kapsamda uluslararası

ilişkiler kuramlarından örnekler ile özellikle devlet-birey arasındaki güvenlik-özgürlük ikileminin yarattığı ve yaratabileceği olumsuz durumlar örneklendirilmeye çalışılmıştır. Ayrıca söz konusu siber tehdidin ulusal ve uluslararası güvenlik açısından riskleri kapsamında var olan uluslararası mevzuatın durumu, kapsamı ve eksiklikleri tartışılmaya çalışılmıştır. Küreselleşmenin etkisine ilave olarak siber alanın yapısı gereği anonim ve dinamik olması nedeniyle devletlerin savunma yeteneklerini sürekli geliştirmelerine rağmen alınan tedbirlerin yetersiz kalması durumu da uluslararası ittifaklara olan ihtiyacı daha da artırmaktadır.

Özellikle küreselleşme ile gündeme gelen yeni tehditler doğrultusunda üçüncü bölümde Soğuk Savaş sonrası varlığını devam ettiren ve kendini değişen güvenlik ortamına adapte etmek maksadıyla çalışan NATO'nun (North Atlantic Treaty Organization) devletler açısından "kolektif siber güvenlik" için önemli bir örgüt olduğu ifade edilmeye çalışılmıştır. NATO, Soğuk Savaş'ın başlangıcından günümüze kadar mevcudiyetini koruyan ve kolektif güvenliği amaç edinen bir ittifak iddiasındadır. İttifak, üyelerinin güvenliği için değişen güvenlik paradigmalarına göre kendini revize etmektedir. Bu kapsamda değişen ihtiyaçlar doğrultusunda da siber güvenlik çalışmalarını genişletmeye devam etmektedir. Ancak güvenlik önlemleri konusunda çözüm yollarının geliştirilmesi söz konusuyken herhangi bir siber saldırı karşısında kolektif güvenliğin en önemli ifadesi olan Kuzey Atlantik Ortaklık Antlaşmasının 5. Maddesi kapsamında nasıl ve ne şekilde bir reaksiyon verileceği netleşmiş değildir. İlgili bölümde önce NATO'nun Soğuk Savaş sürecinde kendi güvenlik anlayışını tanımlaması açıklanmaya çalışılacak olup müteakiben Soğuk Savaş sonrası, küreselleşme ile gündeme gelen yeni tehditlerden biri olan siber tehdit kapsamında alınan kararlar, oluşturulan yapılar tanıtılmaya çalışılacaktır. Ancak NATO'nun üyeleri için güvenlik açısından önemli bir garanti olarak gördüğü 5. Maddenin siber saldırı karşısındaki reaksiyonu doğrultusunda hala net bir sonuca varılamadığı hususu tartışılacaktır. Çünkü siber saldırının anonim yapısı gereği savunma veya karşı saldırıya yönelik uluslararası hukukta tam karşılığının oluşturulmaması meşru savunma zemininin oluşturulmasını engellemektedir. Geçerli olan savaş kavramlarının, standart siber karşılıkları henüz formüle edilememiş ve herhangi bir siber savaş durumunda ulusal ve uluslararası sorumluluklar belirlenememiştir. Bu nedenle söz konusu saldırıya karşı savunma durumunda davranış normlarının düzenlenmesi ihtiyacı halen devam etmektedir. Bu düzenlemelerin eksikliği nedeniyle

de güvenlik-özgürlük dengesi tartışmaları siber güvenlik alanında etkinliğini korumaktadır.

Bu doğrultuda NATO üyelerinin siber güvenliklerini sağlamak maksadıyla yaptıkları düzenlemeler arasındaki farklılıklar ile uluslararası ortak kabullerin oluşturulamamış olması konu kapsamında standart bir güvenlik şemsiyesinin oluşmasının önündeki en büyük engellerden biri olarak iddia edilebilir. Bazı ülkeler yeni kurumlar oluştururken bazı ülkeler de mevcut kurumların görev alanını genişleterek çözüm bulmaya çalışmaktadır. Ancak ülkeler arasındaki kapasite farklılıkları devam ettiğinden dolayı hala ittifak içinde standart bir savunmanın oluşturulamadığı görülebilir. Buna ilave olarak devletler tarafından değerlendirilmesinde fayda görülen asıl husus ise konu kapsamında NATO zirvelerinde farklı şekilde ifade edilerek siber tehdidin varlığı kabul edilse de bu döneme kadar sadece bir defa 11 Eylül saldırıları sonrası devreye sokulmuş olan 5.Maddenin siber saldırı sonrası kolektif güvenlik maksadıyla devreye geçirilebileceği konusuna şüphe ile yaklaşılmasıdır.

BİRİNCİ BÖLÜM

DEVLET VE SİBER GÜVENLİK

Güvenlik kavramı genel olarak tehdit, tehlike ve korku durumunun, hissinin ve algılamasının olmaması olarak tanımlanabilir.[1] Bu tanımda bahsedilen algı, kişi/organizasyon maksadının değişmesi ya da gelişen durumlara göre revize edilmesi sonucu değişkenlik göstereceği için güvenlik algısı ve maksat arasında kuvvetli bir bağ mevcuttur. Maksadın değişmesi ile yeni güvenlik arayışları gündeme gelebilmektedir. Bilgi toplumu kavramı ile güvenlik tanımının değişmesi de bu duruma örnek olarak verilebilir.

Güvenlik kavramı genel olarak uluslararası ilişkiler disiplininde farklı aktörler çerçevesinde ele alınan bir kavramdır. Birey, toplum, devlet, uluslararası sistem ve devletlerden oluşan bölgesel ittifaklar, uluslararası kuruluşlar vb. şeklinde günümüzde gittikçe çoğalan bu aktörler, analiz düzeyi olarak da ifade edilmektedir.[2] Bu aktörlerdeki çeşitlilik güvenlik algısının da çeşitlenmesine neden olmaktadır.[3] "18.yy'da kimin güvenliği sorusunun cevabında referans objesi devlet iken günümüzde cevap bireyden, askeri yapıdan, çevre güvenliğine kadar çeşitlilik göstermektedir."[4] Zaman ilerledikçe ve konjontür değiştikçe uluslararası ilişkileri etkileyen ve uluslararası ilişkilerden etkilenen aktörler de çeşitlenmektedir. Bu çeşitlenme güvenlik anlayışının değişmesine ve güvenliği sağlamak için aktörlerin geliştirdiği yöntemlerin de sürekli yenilenmesine neden olmaktadır.

I. TEMEL KAVRAMLAR

Bir tehdit söz konusuyken alınabilecek önlemler kapsamındaki en büyük problemlerden birisini kavram karmaşası oluşturmaktadır. Yukarıda ifade edilen kavramların tam olarak nesnel tanımlarının belirtilmemesi bunlara karşı hem ulusal hem de uluslararası hukukun gelişmesinin önüne geçmektedir. Bu sürecin uzaması

[1] Hans Günter BRAUCH, "**Güvenliğin Yeniden Kavramsallaştırılması: Barış Güvenlik, Kalkınma ve Çevre Kavramsal Dörtlüsü**" (Çev.Zeynep ARKAN), Uluslararası İlişkiler, Cilt 5, Sayı 18, 2008,s.2-3

[2] J.D SINGER, **The Level of Analysis Problem in International Relations,** (der. K. Knorr, S. Verba), The International System:Therotical Essays, Princeton University Press, 1961, s.80

[3] Beril DEDEOĞLU, **Uluslararası Güvenlik ve Strateji,** İstanbul, Derin Yayınları, 2003, s.9

[4] Fatih DEDEMAN, **Geleceğin Güvenlik Ortamının Şekillenmesinde Hibrit Savaş Modelinin Değerlendirilmesi,** Güvenlik Bilimleri Dergisi 5, 2016, s.142

hem vatandaşların hem de devletlerin bu sorundan muzdarip kalmalarını neden olmaktadır.

İnternet; Soğuk Savaş'ın silahlanma yarışının günümüze bıraktığı miras olarak ifade edilebilir. İnternetin oluşturulma süreci; 1957 yılında Sovyet Sosyalist Cumhuriyetler Birliği (SSCB) tarafından Sputnik 1 ve 2 uydularının yörüngeye yerleştirmesi neticesinde ABD, 1958 yılında National Aeronautics and Space Administration'ın (Ulusal Havacılık ve Uzay Dairesi-NASA) kurulumu ile başlamaktadır. Müteakiben yine ABD tarafından askeri teknoloji açısından üstünlüğünü devam ettirmek amacıyla Advanced Research Projects Agency (İleri Araştırma Projeleri Ajansı-ARPA) kurulmuştur. ARPA, dönemin en önemli tehdidi olan nükleer savaş olasılığına karşı iletişimin sürekliliğini sağlayacak bilgisayar ağı üzerine çalışmalar yapmıştır.[5] Söz konusu çalışmalara ek olarak ABD Savunma Bakanlığı farklı yerlerdeki bilgisayarlar arasında bilgi alışverişi sağlayan ağları geliştirmek maksadıyla üniversiteler ile ortak çalışmalar yapmaya başlamıştır. Söz konusu çalışmalar ile ilk defa 1965 yılında farklı yerlerdeki bilgisayarlar arasında veri paylaşımı yapan ilk ağ oluşturulmuştur. ARPA Network (ARPANET) projesi ile 1968'de dört üniversite arasında bağlantı kurmak hedeflenmiş, bu hedef doğrultusunda yapılan çalışmalar ile 1969 yılında söz konusu bağlantı bu dört üniversite arasında sağlanmıştır.[6] ABD Savunma Bakanlığı tarafından ARPANET, MILNET (Military Network) ve ARPANET olarak ikiye ayrılmıştır. Müteakiben ticari olarak kullanılmaya başlanılan ARPANET 1990 yılında kapatılmıştır.1990 yılında İsviçre'de yer alan Araştırma Merkezinde oluşturulan yeni ara yüz "Hiper Text Transfer Protokolü (http)" ve dokümanları tanımlama sistemi (URL) ile "World Wide Web – www" icat edilmiştir.[7] Temel olarak "internet adem-i merkezi bir yapıya sahiptir" denilebilir. Bu da temsil, güç ve meşruiyetinin tartışılabileceği bir geleneksel yönetimin söz konusu olmadığının göstergesidir. "İnternette var olan her hareket bir İnternet Protokol (IP) adresinden yönlendirilen bir veridir."[8] Söz konusu adres, internete erişim sağlanan coğrafi konum, kullanılan araç gibi bilgileri sağlamaktadır. Dosya aktarım

[5] Debra L.SHINDER, **Scene of the Cybercrime:Computer Forensics Handbook,** USA, Syngress Publication, 2002,s.58-60

[6] Romualdo PASTORSATORRAS, Alessandro VESPIGNANI,**Evolution and Structure of the Internet: A Statistical Physics Approach,**Cambridge University Press, Cambridge, 2004, s.4

[7] P.W.SINGER, Allan FRIEDMAN,**Siber Güvenlik ve Siber Savaş,** Çev: Ali ATAV, Buzdağı Yayınevi,2015,s.37

[8] P.W.SINGER, Allan FRIEDMAN,**Siber Güvenlik ve Siber Savaş,**s.54

protokolü (File Transfer Protocol-FTP) ve Aktarım Denetim Protokolü (Transmission Control Protocol-TCP) ile birçok kullanıcı aynı anda ağa bağlanır hale gelmiştir. Çok farklı amaçlar tarafından kurulan söz konusu yapı şu an kuran kurum ve amacının dışında, dünya üzerindeki mesafeleri ortadan kaldırarak farklı konularda ortak noktaları olan insanların iletişim halinde kalmasını sağlamaktadır. Bu duruma Soğuk Savaşın bitmesi de etki olarak gösterilmektedir. Söz konusu dönemin sona ermesi ile ortadan kalkan yasakların etkisi ve internetin askeri alan kullanımı dışına çıkması, kullanıcı sayısının artması ile verilerin paylaşıldığı sanal bir alan, siber alan oluşmuştur.[9] Bu oluşum ile artan bilgi ve veri paylaşımı beraberinde problemler de getirmiştir.

Günümüzün en çok kullanılan kavramlarından biri siber alan haline gelmiştir. **Siber** ifadesi sibernetik kökeninden gelmektedir. Yönetici manasına gelen Yunanca "kybernetes"e uzanır. İlk defa "hayvanlarda ve makinelerde iletişim ve kontrol bilimi" sibernetik kelimesinin kısaltması olarak 1948 yılında Amerikalı bilim adamı Norbert WEİNER tarafından kullanılırken[10] **siber uzay** ise, William GIBSON tarafından ilk defa 1984 yılında "Neuromancer" adlı bilimkurgu romanında kullanılmıştır.[11] Genel anlamı ile siber alan, her türlü yazılım, donanım ve iletişim alt yapısından meydana gelen ve birbirine bağlı ya da bağımsız bilgi sistemlerinin oluşturduğu sayısal ortamdır. Siber alan, kritik alt yapı[12] olarak değerlendirilen enerji, su kaynakları, finans, sağlık, ulaşım ve haberleşme gibi altyapıların bağımlı olduğu ve gittikçe de daha da bağımlı hale geldiği bir alan olarak ifade edilebilir. Söz konusu alan ABD Ulusal Güvenlik Stratejisi tarafından; 2003 yılında siber alan, kritik altyapılarımızın çalışmasını sağlayan birbirine bağlı yüzbinlerce bilgisayar, sunucu, yönlendirici, anahtar ve fiber optik kablolardan oluşan alan, 2006 yılında iletişim ağı ile birbirine bağlanan sistemlerde veri saklama, değiştirme ve iletme amacıyla elektronik ve elektromanyetik spektrumun kullanıldığı alan, 2010 yılında ise internet, iletişim ağları,

---

[9] Manuel CASTELLS, **The Rise of the Network Society,** West Sussex, Wiley- Blackwell, 2010, s. 403

[10] Jason WHITTAKER, **The Cyberspace Handbook,**Oxon, Routledge, 2004, s.4

[11] William GIBSON, **Neuromancer,** (Çev.Melike ALTINTAŞ), İstanbul, Gündüz Yayınları, 1984,s.77

[12]**"kritik altyapılar** "zarar görmesi veya yok olması halinde, vatandaşların sağlığına emniyetine, güvenliğine ve ekonomik refahına veya kamu hizmetlerinin etkin ve verimli işleyişine ciddi boyutta olumsuz etki edebilecek fiziksel ve teknolojik tesisler, şebekeler, hizmetler ve varlıklar" Summaries of EU Legislation," European Programme for Critical Infrastructure Potection",(Çevrimiçi) http://europaeu/legislation_summaries/justice_freedom_security/fight_against_terrorism/133260_en.htm, 17 Temmuz 2013

bilgisayar sistemleri, gömülü işlemci ve kontrol birimlerini içeren, bilgi teknolojileri altyapılarından meydana gelen, birbirine bağımlı ağların oluşturduğu bilgi ortamındaki küresel bir alan olarak tanımlanmıştır. 2011 yılında da NATO tarafından; bilgisayarlar ve bilgisayar ağlarının ortaya çıkardığı, insanlar ve bilgisayarların bir arada bulunduğu ve çevrimiçi faaliyetlerin tüm yönlerini içeren sayısal bir dünya olarak ifade edilmiştir.[13]

Siber uzay ise; en başta dijital verilerin oluşturulduğu, saklandığı ve paylaşıldığı bilgi ortamıdır. Fakat sadece sanal değildir.[14] Anlaşılacağı üzere siber uzay sadece internetten ibaret olarak düşünülmemelidir. Kapalı ağlar, enerji dağıtım ağları, elektronik komuta sistemleri, insansız hava araçları vb. birçok sistem bu alanın parçalarını oluşturmaktadır.[15] Söz konusu yapı, teknoloji ve onun kullanıcıları ile paralel olarak sürekli değişmektedir. Cep telefonlarının bilgisayarlarla yarışacak boyutta artan işlemci gücü ve kabiliyetleri ve son dönemde ortaya çıkan Nesnelerin İnterneti (Internet of Things-IoT) kavramıyla siber alanın sınırları bilgisayarların dışına çıkarak evlerimize, arabalarımıza kadar uzanmıştır. Bir zamanlar sadece iletişim, müteakiben ticaret aracı iken günümüzde gıda, bankacılık, sağlık, ulaşım, enerji vb. altyapı sektörlerini kapsayan bir hal almıştır. Devletler tarafından hem kendi kurumları ile olan ilişkiler hem de özel kurumlar ile yürüttüğü ilişkiler siber uzaya taşınmış ve artarak da bu taşımaya devam edilmektedir.

Söz konusu alan içinde kötücül yazılım, botnetler, DDOS (Dağınık Servis Engelleme Saldırısı) saldırıları, virüsler truva atları[16], bilgisayar sistemleri zayıflıkları, ağ savunmasızlık problemleri, ihlaller, bilgi hırsızlıkları, kimlik hırsızlıkları vb.

---

[13] Hasan ÇİFTÇİ,**Her Yönüyle Siber Savaş,** Tubitak Popüler Bilim Kitapları, 2013, s.3-4
[14] P.W.SINGER, Allan FRIEDMAN,**Siber Güvenlik ve Siber Savaş,** ,s.29
[15] Hasan ÇİFTÇİ,**Her Yönüyle Siber Savaş,s.5**
[16] Botnet (robot network), robot ağ adı verilen programların ifade eder. Botnet, bir veya birden fazla bilgisayarı uzaktan kontrol altına alan programa verilen isimdir. Bu tip saldırı altında olan bilgisayar kullanıcıları genellikle donanıma zararlı bir yazılım yüklendiğinden haberdar olmazlar. DoS (Denial of Service) saldırısı,'hizmet engelleme' kelimelerinin birleşimiyle tanımlanan bir eylemdir. DoS saldırılarında kullanılan yazılımlar, belirli ağ kaynaklarına yetkili erişimi engelleyen programlardır. Mantık bombası (logic bomb), belli bir programın içine kasıtlı olarak zararlı bir kod yerleştirilmesi işlemine verilen isimdir. Mnatık bombası genellikle hedef alınan bilgisayar veya ağlardaki bilgileri yok etmek veya kulanılamaz duruma getirmek için kullanılır. Truva atı (Trojan horse), kullanıcıların çalıştırmak istedikleri program gibi davranan yazılımlara verilen isimdir. Mantık bombasına benzer bir sistemle çalışır. Virüs, hedef bilgisayar veya ağlara zarar vermek için yazılan bir uygulamadır (application). Virüsler bilgisayar dosyalarına girerek kendi kendisini çoğaltabilirler. Solucan (worm) ise kendi kendisini yayabilen virüs programıdır. Bu programlar genel olarak, ağlara karşı DoS saldırısı gerçekleştirmek veya virüs sokmak için 'arka kapı' (back door) olarak bilinen sistem açıkları yaratmak için kullanılırlar. Zararlı programların türleri ve tanımları hakkında resmi bir tasnif çalışması için bkz.: United States General Accounting Office, **Critical Infrastructure Protection, Challenges and Efforts to Secure Control Systems**, (March 2004).

problemler günümüzde hem bireysel hem ulus-devlet hem de ulus-ötesi seviyelerde tartışılmaktadır.[17] Sayılan durumlar sanıldığının aksine çoğu zaman anlaşılmadan ve çok masum şekilde bizi etkilemektedir. 2007 yılında Estonya'da meydana gelen siber saldırı örneği üzerinden inceleme yapılırsa aslında basit, kolay ve hızlı gerçekleşen saldırı sürecinin, gittikçe internete bağlı hizmetleri artıran bir ülkede ne kadar büyük etkileri olduğu görülebilir.

Söz konusu saldırı DDoS'a örnektir. Bu saldırı türünde binlerce bilgisayar eş zamanlı olarak ağlara saldırı düzenleyerek çökmelerine neden olmaktadır. Bu esnada bilgisayar sahibi bir yavaşlama hisseder ancak saldırı işlemi arka planda devam eder. Söz konusu saldırıların başlangıcı masum gözüken girilmiş bir internet sitesi ya da bir elektronik posta olabilir. Söz konusu enfeksiyonun başka bilgisayarlara da sıçraması ile solucanlar ortaya çıkar.[18]

Bu problemler siber saldırı olarak ifade edilmektedir. Buradan hareketle **siber saldırı**; devletler ya da yasal olmayan kuruluşlar, terörist gruplar, şirketler veya bireyler tarafından yazılım, donanım, bilgi ya da bilgisayar sistem ve ağları ile altyapıya karşı yapılan kasıtlı müdahaleler şeklinde tanımlanabilir.[19] Bu müdahaleler söz konusu alanlarda imhalara, bozulmalara, gerilemelere ve girişin kabul edilmemesine neden olmaktadır. Siber uzayda gerçekleştirilen bir saldırı herhangi bir kısıtlamaya maruz kalmadan çok hızlı bir şekilde, aynı anda birçok hedefi etkileyecek bir saldırıya dönüşebilmektedir. Sorun şu ki siber saldırı alanı büyük ve gittikçe de büyümektedir. Söz konusu büyüklüğe göre oyuncular ne kadar küçük ise o kadar avantajlı hale gelmektedir.[20]

Siber saldırı ifadesi tam olarak literatürde, devletlerin ulusal mevzuatında veya uluslararası hukuk kaynaklarında açıkça tanımlanmış ve hala üzerinde uzlaşma sağlanmış mutlak bir kavram değildir. Konu kapsamındaki ilk kavramsallaştırmalardan biri olarak 1983 tarihli Avrupa Ekonomik Topluluğu Uzmanlar Komisyonu'nun **bilgisayar suçları** ifadesi; "bilgileri otomatik işleme tabi

---

[17] PeterJ. Denning and Dorothy E.Denning,**"The Profession of IT Discussing Cyber Attack"**, Viewpoints,September 2010 Vol.53 No.9,S.29 (çevrimiçi) http://calhoun.nps.edu/bitstream/handle/10945/35515/cacmSep10.pdf?sequence=1

[18] Richard CLARKE, Robet K. KNAKE, **Siber Savaş Ulusal Güvenliğe Yönelik Yeni Tehdit**, Çev. Murat ERDURAN, İstanbul Kültür Üniversitesi, İstanbul,2011 s. 14-15

[19] Hasan ÇİFTÇİ, **Her Yönüyle Siber Savaş,** s.133

[20] Kenneth GEERS, **Strategic Cyber Security: Evaluating Nation-State Cyber Attack Mitigation Strategies with DEMATEL**,Tallinn University Of Technology Faculty of Information Technology Department of Informatics PhD Thesis, 2010, s.15

tutan veya verilerin nakline yarayan bir sistemde kanuna, ahlaka aykırı olarak veya yetki dışı gerçekleştirilen her türlü davranış" kabul edilebilir.[21]

Siber saldırı, düşmana karşı askeri avantaj sağlayabilecek bir aktivite kategorisine sokulmaktadır. Ancak asıl problem, bu askeri yapıların tek başına değil sivil altyapılar ile bağlantılı olmasıdır. Bu durum yaşanan saldırıların etkisinin askeri yapılar üzerinde sınırlı kalamayacağını göstermektedir.[22] Sahibinin onayı olmadan bilişim sisteminin doğruluğu, uygunluğu, gizliliğini etkilemek niyetiyle veri ve bilgi, askeri yapılar dışında da siber silah haline gelmektedir.

Siber alan diğer bir adıyla siber uzay diğer dört savaş alanından farklı olarak direkt kimsenin hayatına kastetmemekte donanım üzerinden zarar vermektedir. Çok başka bir boyut olarak düşünülse de dizüstü bilgisayarlar, masa üstü bilgisayarlar, cep telefonları vb. donanımlar siber uzayın parçalarını oluşturmaktadır. Siber uzay sadece internet ve ona bağlı bilgisayarlar ile eşleştirilmemelidir. İnternet ve internete girmeyen bütün bilgisayarları ifade eder. Bunların birbirine bağlanmasını sağlayan kablolar da bu yeni savaş alanının parçalarını oluşturmaktadır.[23] Diğer harekât alanları ile karşılaştırıldığında siber alanın insan eliyle oluşturulduğu ve özel sektörün genel olarak hâkim olduğu, teknolojinin gelişimine paralel olarak sürekli geliştiği, alan içinde sahip olunan teknolojik özellikler gereği erişimin çok hızlı olduğu ve durumun tehditler açısından da aynı hızı içerdiği, kendisi dışındaki diğer harekât alanlarının tamamında harekât özelliğine sahip olduğu ve coğrafyadan bağımsız, sınırlara bağımlı olmadığı görülebilir.[24]

Özellikle uluslararası iletişimin başlıca aracı olan internet, doğası gereği dünyanın herhangi bir yerinde bağlantı sağladığı sürece, siber saldırıya her yere ulaşabilecek imkânı sunmaktadır. Herhangi bir sınır söz konusu değildir. İnternet için ulusal sınırlar sadece hukuki yapılar tarafından dikkate alınmaktadır. "İnternetin bu

---

[21] Tezcan ÖZKAN, "**Siber Terörizm Bağlamında Türkiye'ye Yönelik Faaliyet Yürüten Terör Örgütlerinin İnternet Sitelerine Yönelik Bir İçerik Analizi**", Yüksek Lisans Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Ağustos 2006, s.67

[22] Rain OTTIS, **"Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability"**, In Proceedings of the 8th European Conference on Information Warfare and Security, Lisbon, Academic Publishing Limited,s.178

[23] Richard CLARKE, Robet K. KNAKE (Çev. Murat ERDURAN,s. 43-44

[24] Hasan ÇİFTÇİ,**Her Yönüyle Siber Savaş,**s. 8-9

dinamik yapısı karşısında ulusal hukukun sınırlandırılması, bu belirli sınırlar içinde soruşturma ve kovuşturmanın belirli bir süre alması, süreci olumsuz etkilemektedir."[25]

En mahrem alanlara kadar giren ve hayatın en büyük parçası haline gelen teknolojik gelişmeler, terörist araçların çeşitliliğini arttırmış, ulaşılabilir kılmıştır. Devletler için de, vatandaşları ile yürüttüğü işlemlerin merkezi hale gelmeye başlaması nedeniyle siber alan, bireylerin bilgilerinin gizliliği açısından terörist faaliyetler açısından tehdit taşımaktadır.[26] Teknolojik terör, teröristlerin yakalanma riskini azaltmakla beraber bilgisayarları eyleme karşı korunmasız kılmaktadır. Tehdidin her gün değişikliğe uğrayan yapısı ise tedbirleri ve savunmayı engelleyen önemli bir detay haline gelmiştir. İnternet, uluslararası sistemin aktörleri olan devlet, toplum, örgüt ve bireyleri birbirine daha da bağlamıştır.

Birey ve devletin, bir üst otoritenin olmadığı siber alanda eşit aktörler haline geldiği görülmektedir. İki aktör arasında birbirinden bağımsız hareket ve kararı daha da zorlaştırmış, her birini etkileyen bir durumu diğeriyle de bağlantılı hale gelmiştir. Vatansever hacker tanımları oluşmaya başlamıştır. Anonimliğin getirdiği avantaj ile hükümetlerin resmi olarak müdahil olmadan, istedikleri doğrultuda uluslararası etkiler yaratılmasından faydalandığı da görülmekte fakat ispatlamasında güçlükler yaşanmaktadır.

Teknolojik gelişmelerin artması, bilişim sistemlerindeki yenilikler savaş kavramında da farklı tanımlamalar yapmayı zorunlu kılmıştır.[27] Örneğin; ABD Başkanı Bush döneminde siber güvenlik danışmanlığı yapmış olan Richard CLARKE tarafından **"**Bir devletin başka bir devletin bilgisayar sistemlerine ve ağlarına sızarak hasar veya kesinti yaratmak üzere hareket etmesi"[28] siber savaş olarak tanımlanmıştır. Ayrıca kendisi, "basit bir elektromanyetik spektrumun dost unsurlarca etkin kullanımının sağlanması ve düşman tarafından kullanılmasının önlenmesi maksadıyla icra edilen elektronik destek, elektronik saldırı ve korunma yollarını kapsayan **elektronik harp"** tanımı ile[29] "Barış, kriz, asimetrik tehdit ve savaş dönemlerinde sivil ya da askeri ayrımı yapılmaksızın karşı tarafın sahip olduğu altyapı

[25] Bülent AKKUŞ, **Özgürlük ve Güven(sizlik) İkileminde Siber Uzay- Yeni Dünya İçin Toplum Sözleşmesi Denemesi,** Milenyum yayınları, 2016,s.135
[26] Michaek G. SOLOMON, Mike CHAPPLE, **Information Security Illuminated**, Jones and Barlett Publishers, USA, 2005 s. 1-5
[27] Ali Bülent UŞAKLI, **Savaşın Dönüşümü ve Teknoloji,**Lalezar Kitabevi,Ankara, 2008, s.132
[28] Richard CLARKE, Robet K. KNAKE ,s.8
[29] Ae.s.132

sisteminin çalışmasını engellemek, sisteme zarar vermek gibi süreçleri içeren bir harp türü olarak **bilgi savaşını"** da açıklamıştır. Bu tür, asıl savaşın başlamasından önce düşmana karşı bilgi üstünlüğü ile fiziki bir güç kullanmadan askeri veya politik amaçlara ulaşmayı hedeflemek olarak ifade edilmektedir.[30] Psikolojik harekât olarak da tanımlanan bu harp ile medya ve teknolojileri ile karşı tarafın karar mekanizmasını etkileyerek ya da halkı etki altına alarak sonuca ulaşılabildiği görülmektedir.

Yaşanabilecek sıkıntılar üzerinden siber tehdit oluşturan milisler yine genel olarak internet aracılığı ile iletişim kurmakta yine internet üzerinden idare sağlamaktadır. İnternet üzerinden yapılan işlemlerin onlar için sağladığı kolaylıklardan biri olan kimliğini saklayabilme özelliğinden faydalanmaktadırlar.[31] Siber tehdit ve saldırı teknik terimler üzerinden ifade edilebildiği gibi teröristler tarafından manipülasyon aracı olarak da kullanılmış kafa kesme sahneleri paylaşılarak psikolojik savaş aleti olmuş, ya da devletler için tehdit olan terörist gruplar tarafından propagandalarını daha geniş kitlelere iletebildikleri temin aracı ya da "on-line" eğitim merkezi olarak bomba üretimi ve yerleştirilebileceği yerlere yönelik paylaşımın yapılabileceği uygun bir zemin olarak da kullanılmıştır.[32] Ayrıca terör örgütleri benimsedikleri ağ tabanlı örgüt yapısı ile örgüt içi iletişim koordinasyon sağlamakta, eylemlerini oluşturdukları bu ağ üzerinden planlayıp icra etmektedirler.[33]

Siber terörizm kavramını ifade edebilmek için farklı tanımlar görülmektedir. Bunlardan birisi, "belirli bir politik ve sosyal amaca ulaşabilmek için bilgisayar veya bilgisayar sistemlerinin bireylere ve mallara karşı bir hükümeti veya toplumu yıldırma, baskı altında tutma amacıyla kullanılmasıdır".[34] FBI ise, "alt-ulus grupları veya gizli örgütler tarafından savaşçı olmayan hedeflere karşı şiddetle son bulan bilgi, bilgisayar sistemleri, bilgisayar programları ve verilere karşı önceden planlanmış siyasi güdümlü saldırı" şeklinde tanımlamıştır.[35] Diğer bir tanım Stanford Taslağı olarak bilinen belgede yapılmıştır. Siber terör söz konusu belgede "hukuken yetkili kılınmış

---

[30] A.e.s.133

[31] Rain OTTIS, **" A Systematic Approach to Offensive Volunteer Cyber Militia"** Faculty of Information Technology PhD Thesis,2011, TUT Press, S.34

[32] Richard CLARKE, Robet K. KNAKE,s.69

[33] Andrew KOYBKO, **"Hybrid Wars The Indirect Adoptive Approach to Regime Change"** Moscow Peoples' Friendship University of Russi,2015,s.159-161

[34] Cybercrimes:Infrastructure Threats from Cyberterrorist", Cyberspace Lawyer, 4 No:2, Cyberspace Law 23'den aktaran Mehmet ÖZCAN, "Siber Terörizm ve Ulusal Güvenliğe Tehdit Oluşturma Boyutu" s.6, (Çevrimiçi) http://www2.cbu.edu.tr/kalac/dokumanlar/siber.pdf 13.Kasım 2015

[35] P.W.SINGER, Allan FRIEDMAN,**Siber Güvenlik ve Siber Savaş,** s.134-135

görevlilerinin eylemleri dışında, siber sistemlere karşı girişilen ve kişi veya kişilerin ölümü ya da yaralanması, kamu düzeninin bozulması veya önemli ekonomik zararlara neden olması muhtemel olan şiddet, bozma ve engelleme eylemlerinin kasıtlı şekilde yapılması ve yapılacağı tehdididir." şeklinde tanımlanmıştır.[36] Kavram dar veya geniş anlam olarak değerlendirildiğinde tartışmalı olarak ifade edilebilir. Dar anlamı ile sadece insanların can ve mallarını tehdit eden saldırı iken geniş anlamı ile dar anlamına ilave olarak sosyal, dini, ideolojik, politik vb. farklı amaçlar ile gerçekleştirilebilen bir saldırı olabilmektedir.[37]

II. KÜRESELLEŞME İLE DEVLET VE GÜVENLİK İKİLEMİ

Günümüzün internetinin yarattığı etki gibi matbaa da Reform hareketi ile Avrupa'da savaşların başlamasına neden olarak değişimi başlatmıştır. Bu değişim ile derebeylikler, imparatorluklar gibi eski yönetim yapıları yerini yeni ulus-devlete bırakmıştır. Ulus-devlet, egemen, hükümranlık alanının mutlak sahibi, bu konuda tekel şeklinde ifade edilebilir.[38] 1648 tarihli Westphalia anlaşması ile dinsel aidiyet yapısı yerini topraksal (teritoryal) ve daha seküler aidiyete bırakmaya başlamıştır. Teritoryal aidiyette, devlet egemenliğini belirli bir toprak üstünde yaşayan halka dayandırmaktadır. Meşruiyetini ve varlık sebebini bu toprak üzerindeki ulustan aldığı kabul edilmektedir.[39] Ortodoks uluslararası ilişkiler kuramı çerçevesinde yapılan bu tanımlar ile anarşik olarak ifade edilen uluslararası sistemin temel öznesi olarak uluslararası hukuk da ulus-devlet üzerinden şekillendirilmiştir.

Güvenlik anlayışı ise, insan topluluğunun güvenliği ile beraber anılmaya başlanmıştır. Sınırların belirgin olduğu bu süreçte devletin, hem en önemli güvenlik sağlayıcı hem de güvenliğinin sağlanması gereken özne olarak görülmesi doğaldır. Bu noktada güvenlikten kasıt devletin sınırlarının tehlikelerden korunması, iç ve dış egemenliğinin devamlılığının sağlanması ve diğer devletler tarafından kabul görmesidir. "Modernist-realist-pozitivist bakış açısıyla ülkeler sistem içerisinde belli

[36] Mehmet ÖZCAN, "**Siber Terörizm ve Ulusal Güvenlik: İnternet ve Hukuk"** İstanbul Bilgi Üniversitesi Yay.2002,S.309
[37] Hasan ÇİFTÇİ, **Her Yönüyle Savaş,** S.6
[38] Nuri YURDUSEV, '**Uluslararası İlişkiler' Öncesi,** Devlet, Sistem ve Kimlik, İletişim Yayınları, İstanbul,2006, s.20
[39] Faruk YALVAÇ, **Devlet**, (der. Atila ERALP), Devlet ve Ötesi Uluslararası İlişkilerde Temel Kavramlar, İletişim Yayınları, İstanbul, 2006, s.18

seçeneklere sahip aktörler olarak görülmektedir."[40] Ayrıca klasik realizm tarafından devletlerin iç ve dış siyaset alanları arasındaki fark belirginleştirilip kendisini oluşturan bireylerin çıkarları ve tehdit algıları devlet ile bütünleştirilmiş şekilde kabul görmektedir. Bu da devletin güvenliği eşittir bireylerin güvenliği anlayışı demektir.[41]

Küreselleşme ile beraber ulus-devletlerarası geçişkenlik artmaya başlamıştır. Bu sürecin "devlet kurumunu yıprattığı ve/veya dönüştürdüğü,"[42] devletlerarası sistemi ve geleneksel düzeni değiştirdiği iddia edilmektedir.[43] Küreselleşme; "uzak topraklar üzerindeki efendiliğin yeni versiyonu, yani küresel seçkinlerin, yurt temelli kapalı birimlerin politik ve kültürel gücünden bağımsızlaşması ve bunun sonucunda politik ve kültürel gücün etkisini yitirmesi" olarak da ifade edilmektedir.[44]

İnsanların ve toplumun güvenliği devletin güvenliği ile beraber anılır olmaya hatta daha fazla önem kazanmaya başlamıştır. Küresel değerler çerçevesinde desteklenen ve genel ahlaki çerçevede değerlendirilen güvenlik kavramı gündemdedir. Eski yönetim şekillerinin başına gelen şekilde ulus-devletler de yeni aktörler ve teknolojilerin karşısında zorlanmaktadır. Yeni küresel tehditlerin yükseldiği görülmektedir. Ulusal güvenlikten uluslararası güvenliğe geçilmiştir denilebilir. Yani devletlerarası işbirliğinin gündeme geldiği bir döneme geçildiğinden bahsedilebilir. Var olan yeni dönem birey için özgürlükler açısından doğa durumuna[45] dönüş olarak da ifade edilmektedir. Ancak ilerleyen teknolojik gelişmeler ile kişi hak ve özgürlüklerine karşı tehdidin arttığı ve bu tehditlere karşı güvenlik adına da devlet tarafından sınırlamalar yapılarak doğa durumuna geçişin söz konusu olmadığı söylenilebilir.

---

[40] Cem KARADELİ (der.),**Küreselleşme ve Alternatif Küreselleşme,** Ankara, Phoenix Yayınevi, 2005,s.15

[41] Oktay F. TANRISEVER, **Devlet**, (der. Atila ERALP), Devlet ve Ötesi Uluslararası İlişkilerde Temel Kavramlar, İletişim Yayınları, İstanbul, 2006, S. 108-110

[42] Cem KARADELİ (der.),**Küreselleşme ve Alternatif Küreselleşme,** s.13

[43] James N.ROSENOU, **"The Complexities and Contradictions of Globalization"** Current History, Vol.96 No.613,1997,s.361

[44] Zygmunt BAUMAN, **Küreselleşme Toplumsal Sonuçları,** (Çev. Abdullah YILMAZ), Ayrıntı Yayınları, İstanbul,1999,s.11

[45] Sözleşmeci düşünürler tarafından;
Doğal durum; İnsanların, hukuk ve devlet mekanizmasının olmadığı sınırsız özgürlük dönemini ifade eder. Bunun devamında ise "toplum sözleşmesi" olarak ifade edilen insanların güvenlik ihtiyaçları çerçevesinde özgürlüklerinin bir kısmından vazgeçerek belli kurallar dahilinde bir üst otoritenin devlet mekanizmasının bireylerin rızaları ile oluştuğu kabul edilir. Bkz.Filiz ZABCI," John Locke: Liberalizmin Düşüncedeki Öncüsü", **Kral Devletten Ulus Devlete,** Mehmet Ali AĞAOĞULLARI, Filiz ZABCI ve Reyda ERGÜN, 2. Baskı, Ankara, İmge Kitabevi, 2009, s.164, Mehmet Ali AĞAOĞULLARI, "Thomas HOBBES: Ölümlü Tanrı", **Kral-Devlet ya da Ölümlü Tanrı,** Mehmet Ali AĞAOĞULLARI ve Levent KÖKER, 4. Baskı, Ankara, İmge Kitabevi, 2009, s.183, Jean-Jacques ROUSSEAU, **Toplum Sözleşmesi,** (Çev. Vedat GÜNYOL), Türkiye İş Bankası Kültür Yayınları, İstanbul, 2010, s.13-15

Diğer taraftan ise yine aynı gelişmelerin devlet açısından meşru güce sahip olduğu iktidar alanını belirleyen sınırların aşınması anlamına geldiği ifade edilebilir. Çünkü siber uzay, zaman ve mekândan bağımsız bir "doğa durumu" olarak görülebilir. Bu nedenle doğa durumunun içindeki bireylerin güvenliklerinin teminatı olarak görülen toplum sözleşmesi kavramı[46], "üst otoritenin olmadığı sınırsız siber alan için de gerekmektedir" düşüncesi temel tartışma noktalarından biri haline gelmektedir.[47]

Sözleşmeci düşünürlerden Thomas HOBBES tarafından, oluşturulan devletin tek ve en önemli görevi güvenliği sağlamak olarak ifade edilmiş[48] ve devlet olmadıkça herkesin daima savaş, çatışma halinde olacağı iddia edilmiştir.[49] Günümüz şartlarında bu görüş, egemenin internet üzerinde güvenlik gerekçeli sansürü benimsediğini söyleyebilir. Fakat birey güvenle özgürlüğe ulaşmak istemektedir. Devlet de öncelikli olarak güvenliği sağlamayı hedeflemektedir.

Siber uzayda bireyler için, güvenle özgürlüğe ulaşmak ana ortak nokta iken güvenliğin sağlanması durumunda çoğu zaman olumsuz etkilendiği söylenen özgürlük tartışmanın temeli olmaktadır.[50] Bireylerin rızası ile oluşturduğu bir üst otorite olan devletin, sahip olduğu hakları bireylerden bağımsız olarak güvenlik bahanesi ile özgürlükleri geri plana atarak kullanması kendiliğinden oluşan dengenin bozulması olarak görülmektedir.[51] John LOCKE tarafından bu durum, "devletin amacının bireyin haklarını korumak olduğu ve nitekim bunda başarısız olur ya da bu yetkisini bireylerin haklarını ihlal etmek için kullanırsa sözleşme hükümsüz olur" şeklinde ifade edilmiştir.[52]

---

[46] Toplum sözleşmesi kuramları; doğa durumunda özgür ve eşit barış içindeki bir durumda iken birey denetlenemez bir özgürlüğe sahipti. Fakat kendi haklarını savunurken başkasının haklarına zarar vermekteydi. Tehditlerin oluşması ile oluşan kaos ortamında bireylerin kendi özgürlüklerini korumak ve güvenliklerini sağlamak maksadıyla bencil çıkarlarından vazgeçmelerini, devlet ve hukuku oluşturma nedenlerini ortaya koymaktadır. Ya da özgür ve eşit barış içindeki bir durumda iken birey denetlenemez bir özgürlüğe sahipti. Fakat kendi haklarını savunurken başkasının haklarına zarar vermekteydi.

[47] Bülent AKKUŞ, s.14-25

[48] Thomas HOBBES, **Yurttaşlık Felsefesinin Temelleri,** (Çev. Deniz ZARAKOLU), İstanbul, Belge Yayınları, 2007, s.172

[49] Der. Howard WILLIAMS, Moorhead WRIGHT, Tony EVANS, **Hobbes,** Uluslararası İlişkiler ve Siyaset Teorisi Üzerine Bir Derleme, Siyasal Yayınevi, Ankara, 2007, s.135-137

[50] Haydar Burak GEMALMAZ, **Sanal Dünyalarda Özgürlük ve İktidar**, İstanbul, Beta Yayıncılık, 2011, s. 2

[51] NETANEL, Neil Weinstock, **Cyberspace Self-Governance: A Skeptical View From Liberal Democratic Theory**, 88 Cal. L. Rev. 395 (2000). http://scholarship.law.berkeley.edu/californialawreview/vol88/iss2/8

[52] Donald G. TANNENBAUM, David SCHULZ, **Siyasi Düşünce Tarihi ve Fikirleri,** (Çev.Fatih DEMİRCİ), Ankara, Adres Yayınları, 2011, s.137

Bu görüşlere karşın sistem içerisinde tek etkili ve yetkili aktör olarak devleti tanıyan klasik realistler tarafından da devletin müdahaleci yapısı olumlanmaktadır. Aktör tartışmaları çerçevesinde davranışsalcılar tarafından ise, ulus adına meşru otoritenin kullanılmasının devlet ile eşleştirilemeyeceği, bireyin hakları ve özgürlükleri çerçevesinde resmi iktidara karşı sahip olduklarını korumak adına uluslararası arenada çabalayabileceği kabul edilmektedir. Çoğulcuların görüşleri de bu kapsamda uluslararası sistem içindeki farklı aktörlerin varlığı ile gücün artık sadece devlet tekelinde olduğu gerçeği dışında yeni aktörlerin de dikkate alınması yönündedir.[53] Bu kapsamda Realizm ve Neorealizmin devlet anlayışına karşı Konstrüktivizim, Eleştirel Teori ve Post Yapısalcıların ortak eleştirileri vardır. Söz konusu teoriler küreselleşmenin devletlerin başa çıkamayacağı kadar kapsamlı olduğunu, devlet dışı aktörlerin sayısının arttığını sistem içinde etkin ve yetkin tek aktörün artık devlet olarak kabul edilmesinin doğru olmadığını savunur. Ayrıca İnşacılar tarafından da iletişimin artması ile kimlikler yeniden inşa edileceğinden güvenlik sorunlarının da geleneksel yöntemler ile çözülemeyeceği ifade edilmektedir.

Ancak bahsedilen bu dönüşüm içinde değişmediği iddia edilen bir husus vardır ki o da devletlerin direkt silahlı çatışma aşamasına gelmeden dolaylı bir güç kullanmayı tercih etmeleridir.[54] Bu durumu FOUCAULT "Politika, savaşın başka araçlarla sürdürülmesidir" şeklinde ifade ederek var olan güç ilişkileri devam etse de bunların tarih sahnesine zuhur ettiği savaşların günün koşullarına göre değişmesini dile getirmiştir.[55]

Tehdit ve güvenlik açısından incelendiğinde devlet-vatandaş ve güvenlik bağı da meşruiyet kapsamında önemli bir tartışma noktası haline gelmektedir. Çünkü vatandaş olarak bireyler, siber alanda kişisel güvenlik talep ederken devlet tarafından güvenlik kaygıları doğrultusunda getirilecek bir düzenlemeyi de kendi özel alanlarına müdahale olarak görebilmektedir. Bu ikilem devletlerin siber savunma kapsamında ulusal adım atmasının önündeki en büyük engeli teşkil etmektedir. "Devletin bilişim sektörüne düzenleme getirmesi zorunluluğu gerekli görülse de herkesin karşı çıktığı bir olgudur."[56] Çin'de var olduğu için tartışılan sansür, internetin devlet servis

[53] Erhan BÜYÜKAKINCI, **Küreselleşme Üzerine Kuramsal Tartışmalar: Merkezi Devlet ve Yeni Aktörler,**(Der**.:** Cem KARADELİ),Küreselleşme ve Alternatif Küreselleşme**,** Ankara, Phoenix Yayınevi, 2005 s.27-29
[54] Ali Bülent UŞAKLI, **Savaşın Dönüşümü ve Teknoloji,** ,s. 172
[55] Çetin VEYSAL, **Savaşın Felsefesi,** İstanbul, Etik Yayınları,2006,s.256
[56] Richard CLARKE, K. KNAKE,,s.67

sağlayıcısı üzerinden “intranet” gibi bir iç sistem olarak kullanılmasından kaynaklanmaktadır. Ağın güvenliğinden devlet sorumludur. Güvenlik olarak çok avantajlı olan bu durum özgürlükler açısından değerlendirildiğinde uluslararası kamuoyu tarafından tartışılmaktadır.[57] Bu tartışmalarda ulaşılan sonuç ise çoğu zaman devletin siber güvenliği devralmasının mümkün olmadığı aynı zamanda sıfır müdahil olma gibi bir şansının da olmadığı şeklindedir.[58]

Bireysel veri gizliliğinin günümüzde artan önemi ile şeffaflık da paralel olarak artmaktadır. Başat arama motoru olarak ifade edebileceğimiz Google tarafından arama verilerinin, sunucularında depolanmakta olduğu ve bu verilen üçüncü kişilerle paylaşılması durumu gündemde olan veri gizliliği tartışmalarından biridir. Google bilgisayarınızdaysa örneğin internet tarayıcınızın açılış sayfası ise hangi saatlerde internette çevrimiçi olunduğu, hangi anahtar kelimelerle arama yapıldığı, hangi örün sayfalarına girildiği artık Google sunucularında kayıt altındadır. Sadece “gmail”in 1.2 milyar kullanıcı hesabına sahip olduğu düşünülürse insanlar hakkında elde edilen verilerin büyüklüğü, istihbari bilgilerin değerinin ne kadar önemli olduğu tahmin edilebilir. ABD merkezli Google’ın Ulusal Güvenlik Ajansı (National Security Agency-NSA) ile Rusya merkezli Yandex’in Rusya ile sıkı ilişkiler içinde olduğu, kayıt altına aldığı tüm bilgileri bağlı olduğu ülkenin devlet kurumlarının kullanımına açabildiği iddiaları ortaya atılmaktadır.

Buna ek olarak kişisel güvenlik açısından diğer bir tehdidin sosyal medya ağları olduğu ifade edilmektedir. Örneğin Facebook üzerinden kişinin gönüllü olarak paylaştığı ve sakladığı veriler, paylaşan kişi hakkında bilgi edinmek ve edinilen bilgileri illegal amaçlara dönük olarak kullanmak için oldukça uygun bir ortam sağlamaktadır.

Siber uzayın “sınırsızlığı” her aktör için güvenlik konusunda tedirginlik yaratmaktadır. Bu kapsamda devletler tarafından ulusal bilgi güvenliği amacıyla Çin tarafından alınan önlemler gibi yasala çıkarılması durumu ise devletin birey özgürlükleri üzerindeki olumsuz etkilerini artırmaktadır. Çoğu hukukçu tarafından bu durum bireyin internete erişim hak ve özgürlüklerinin ellerinden alınması olarak ifade edilmektedir. Birey hem devletler hem de kötü niyetli gruplar tarafından etrafı sarılmış

[57] Richard CLARKE, K. KNAKE,s.74
[58] P.W.SINGER, Allan FRIEDMAN, s. 267

halde hem de devlet kontrolü ile özgürlükleri, mahremiyeti elinden alınmış olarak farklı aktörler tarafından tehdit altında bulunmaktadır.[59]

Sosyal ağlar bireyler için tehdit içerirken yine aynı sosyal ağlar devletler için de karşıt grupların oluşturulduğu, organize edildiği alanlar haline gelmektedir. Bu durumun uluslararası alandaki örneği Arap Baharı olarak gösterilebilir. İnsanların sosyal medya üzerinden iletişim sağlayarak devlet karşıtı toplantılar, gösteriler organize ederek hükümete müdahaleye kadar gidecek süreçler yarattığı söz konusu örnek üzerinden görülebilmektedir. Ulusal olarak ise aynı duruma "Gezi Olayları" verilebilir. Her iki örnekte de "Politik hedeflere ulaşabilmek için bilgi paylaşımı vasıtasıyla örgütlenme, propaganda faaliyetleri"[60] gerçekleştirildiği ifade edilebilir. Bu durum "politikanın başka araçlarla devamı" kavramının somutlaşmış hali olarak görülebilir. İfade edilen örnekler devletlerin söz konusu iletişim alanlarına müdahalesini yine kendisinin bekası üzerinden şekillendirmesine neden olmaktadır. İnternetin yavaşlatılması veya kullanımının sınırlandırılması belirtilen örnekler üzerinden düşünüldüğünde bireylerin özgürlüklerinin sınırlandırılması olarak görülebilecekken, yine aynı süreçte terör örgütlerinin iletişiminin engellenmesi açısından bireyin güvenliğinin sağlanması olarak da ifade edilebilir. Ancak "BM Küresel Terörle Mücadele Stratejisi, Avrupa Konseyi Bakanlar Komitesi İnsan Hakları ve Terörle Mücadele Rehber İlkeleri" ile "Avrupa Birliği Terörle Mücadele Stratejisi"nde, devletlerin terörler mücadele ederken insan hak ve özgürlüklerini ihlal etmemesi gerektiği ifade edilmiştir.[61]

Terör örgütleri, örgüt içi iletişim ve koordinasyonlarını internet üzerinden sağlarken internetin sağladığı anonimlikten faydalanarak eylemlerini de oluşturdukları ağ yapısı üzerinden planlamaktadırlar. ABD tarafından geliştirilen örtülü faaliyetler[62] kavramı da bu belirsizliğin nasıl kullanıldığını göstermek açısından faydalı olmaktadır.

---

[59] Sevgi KESİM GÜVEN, **Gözetim Toplumu ve Toplumsal Meşruiyet,** Mimar Sinan Güzel Sanatlar Üniversitesi Sosyal Bilimler Enstitüsü Sosyoloji Anabilim Dalı Genel Sosyoloji ve Metodoloji Programı Doktora Tezi, 2007, s. 152-155

[60] Andrew KORYBKO,s.33

[61] Duygu Çağla BAYRAM, **"İnsan Güvenliği ve Terörizm"** Yüksek lisans Tezi, Karadeniz Teknik Üniversitesi Sosyal Bilimler Enstitüsü Anabilim Dalı Uluslararası İlişkiler Yüksek Lisans Programı, Trabzon, 2016,s.46

[62] "Düşman devlet veya grupların etkilenmesi veya yabancı devlet ya da grupların desteklenmesi maksadıyla devlet tarafından icra edilen, ancak planlama ve operasyon safhalarında devletin sorumluluğunun tespit edilemeyeceği, faaliyetin açığa çıkması durumunda makul bir şekilde inkâr edilebileceği ve sorumluluk yüklenilemeyeceği faaliyetler" Fatih DEDEMAN, s.150-161

Liberalizm bireysel hak ve özgürlükler ile özel alan bağımsızlığı görüşünü getiren bir ideoloji olmuş ve kabul görmüştür. Devletin özel alana olan müdahalesine karşı olan liberalizm, devletin sorumluluğunu güvenlik ve düzen sağlamak şeklinde belirlemiştir. İşte bu nedenle siber uzaya yönelik sansürlemeler liberaller tarafından devletin varoluş sebebi olan halkının güvenliğini sağlamak maksadıyla, özgürlüğünü de koruması gerçeğinin unutulduğu şeklinde ifa edilmektedir.[63] Ulus-devlet, güvenlik üzerinden sahip olduğu kontrol mekanizmaları ile vatandaşları üzerinde daha etkin olarak kendi ihtiyaçları doğrultusunda bireyler oluşturmaktadır.[64] Bu kontrol ve gözlem FOUCAULT tarafından panoptikon metaforu ile açıklanmaya çalışılmıştır.[65] Bu durum siber alanda var olan sistemler ve teknolojiler ile devletler için çok daha kolay hale gelmektedir. Örneğin web sitelerindeki çerezler[66], internet kullanıcısının daha önce giriş yaptığı internet sitelerini gelecekte yapacağı aramalara yönelik arşivlemektedir. Bu durum kullanıcı için zaman kazanma açısından faydalı olsa da kişinin sahip olduğu bilgilerin takip edilebilir olması gibi tehditleri beraberinde taşımaktadır. Ayrıca kişinin teknoloji ile gittikçe özgürleştiği ifade edilirken aslında gittikçe mahremiyetini kaybettiği ve çok daha rahat izlenip kontrol edilebilir hale geldiği şeklinde yorumlanabilir. Söz konusu çıkarım, artan sosyal medya ağlarında kişilerin fotoğraflarından, bulundukları yere, beraber vakit geçirdiği insanlardan ailelerine kadar değişen sosyal, ekonomik, medeni durumları gibi birçok özelini gönüllü olarak paylaşmalarına dayanılarak yapılabilir.

"Çok fazla kişinin pek az kişiyi gözlediği bir durumdan pek azın çok fazlayı gözlediği bir duruma geçiş" söz konusu olmaya başlamıştır."[67] "Siber uzay panoptikonu" ile artık gözlenmekten kaçış gittikçe imkânsızlaşmaktadır. Söz konusu kontrol de en rahat devletler tarafından yine bireylerin lehine yapıldığı iddia edilerek yapılmakta ve yapılmaya çalışılmaktadır. "Tehdidin güvenlikleştirmesi ile alınan tedbirlere meşruluk kazandırılmaktadır. Böylece kamusal bir sorun siyasi alana girince devleti ilgilendirir, devlet için güvenlik sorunu haline gelir. Kendine güvenlik

---

[63] Bülent AKKUŞ, s.72

[64] Michel FOUCAULT, **Hapishanenin Doğuşu**, (Çev. Mehmet Ali KILIÇBAY), İmge Kitabevi, 2006, s.290-294

[65] Panopticon, izlenen kişinin izlendiğini, takip edildiğini bilmeyen kişinin belirsizlik, görünmezlik üzerinden kontrol amaçlı tasarlanmış sistemde kurallara uygun hareket etmesini sağlamaktadır.

[66] "cookies" olarak da bilinen çerezler kişinin geçmişte internet üzerinde yaptığı hareketleri saklayarak yeniden yapılacak bir işlem de hafızadan faydalanılmasını sağlamaktadır.

[67] Thomas MATHIESEN, **The Viewer Society: Michel Foucault's "Panopticon' revisited,** Theoretical Criminology, 1997, 1: 215 London: Sage, s.220-225

sorunu bulan devlet, önlemler alınması gerekliliği doğrultusunda hareket eder."[68] Böyle bir durumda da "Devlet, meşruluğunu kendinden değil halktan aldığı olgusunu gözden kaçırmaktadır."[69] Devletin güvensizliği bireyin güvensizliğinin önüne geçmeye başlamaktadır.[70] Bu ikilemlerin beraberinde "siber güvensizlik alanı" yaratacağı ve siber alanın özelliği gereği aktörlerin kendini sınırları belli olmayan bir çatışma içinde bulacağı yönünde görüşler oluşmaktadır.[71] Yani "özgürlük güvenliğe ya da güvenlik özgürlüğe feda edilmemelidir."[72]

Söz konusu ikilemlerden olumsuz etkilenmemek maksadıyla ulusal siber güvenliğin sağlanmasına yönelik olarak yürütülecek çalışmalarda esas alınması gereken temel ilkeler aşağıdaki şekilde sıralanabilirse devlet-birey arasındaki güvenlik-özgürlük dengesi sağlanabilir.[73]

- Uluslararası sözleşmelerle teminat altına alınmış temel insan hak ve hürriyetlerinin korunması,
- Demokratik toplum düzeninin gereklerine uyulması,
- Alınacak tedbirlerin Ölçülülük İlkesine göre belirlenmesi,
- Karar alma süreçlerine tüm paydaşların katılımını sağlayacak kapsayıcı bir yaklaşımın benimsenmesi,
- Siber güvenliği hukuki, teknik, idari, ekonomik, politik ve sosyal boyutları ile ele alan bütüncül bir yaklaşımın benimsenmesi,
- Geliştirilecek çözümlerde güvenlik ile kullanılabilirlik arasında denge kurulması,
- Diğer ülke mevzuatlarının göz önünde bulundurulması ve mümkün olabildiğince uyumluluğun sağlanması,
- Uluslararası işbirliğinin sağlanması.

---

[68] N.MİŞ, **"Güvenlikleştirme Teorisi ve Siyasal Alanın Güvenlikleştirilmesi"** Akademik İncelemeler Dergisi, 6 (2), 2011, s.348

[69] Jean-François LYOTARD, **Post Modern Durum-Postmodernizm,** (Çev. Ahmet ÇİĞDEM), Ara Yayıncılık, İstanbul,1990, s.43

[70] Gizem BİLGİN AYTAÇ,**"ÜÇÜNCÜ DÜNYA GÜVENLİĞİ VE İNSANİ MÜDAHALE İnsan Güvenliğinden Irak Müdahalesine Eleştirel Güvenlik Yaklaşımları"** Dezanj Yayınları, İstanbul,2014,s.91

[71] Fulya GÖKCAN HİSARLIOĞLU, (Ed. Mustafa AYDIN), **Güvenlik Çalışmaları Serisi 1-10**,Kitap İncelemesi İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2012, s.175

[72] Duygu Çağla BAYRAM, s.48

[73] M. Ünver, C. Canbay, A.G. Mirzaoğlu, "**Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler**", Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı, Sf.22-52, 2009.

III. GÜVENLİK İÇİN YENİ TEHDİT "SİBER OLAN"

Siber terörizmi, internet üzerinden işlenen diğer suçlarla karşılaştırdığımızda bu şekilde terörizm olarak adlandırılmasına neden olan özelliği, mağdurun özellikle çoğu zaman siyasi bir amaçla devlet olmasıdır.[74] Sanal ortam, bu faaliyet için hem araç hem de söz konusu faaliyetin cereyan ettiği mecrayı oluşturmaktadır. Bu belirsiz tehdit Soğuk Savaş örneği ile karşılaştırıldığında, Soğuk Savaş'ta her iki blok için de tehdidin kim olduğu, tehdidin kaynağı, bu tehdide nasıl bir karşılık verilebileceği vb. bilinmekteyken, aynı durum günümüzde tehditlerden biri olarak kabul edilen siber terör için "anonimlik" özelliği nedeniyle söylenilememektedir. Küresel olarak internetin hızla gelişmesi, askeri, siyasi, ticari vb. alanlarda kullanılması ile günümüzde ülkelerin altyapıları ve savunma sanayilerinin bu teknoloji ile yönlendirilmekte olması bu bağımlılığın herhangi bir saldırı durumunda devletleri çok zor duruma düşüreceği genel kabul görmektedir. Çünkü internet kendi içinde zafiyetleri barındırmaktadır. Bunlar; kablolu ve kablosuz şekilde internete bağlanmayı sağlayan adresleme sistemleri, tek başına yetkiye sahip olan bir kurum üzerinden yönetişimin olmaması, elektronik posta sağlayıcıların işletim sistemlerinin açık ve şifresiz olması nedeniyle iletişimin görülebilir olması, kötü yazılımların çok rahat bir şekilde internet üzerinde dolaşabiliyor olması…[75]

Siber uzay yeni bir boyut olarak ele alınmakta fakat birçok bileşenden oluştuğu göz ardı edilmektedir. Örneğin ayrı bir boyut olmakla beraber bağlanmayı sağlayan kablolar, fiber optik kablo demetleri egemen ülkelerin topraklarında yerleşik haldedir. Bu nedenle de söz konusu ağlar kapsamında egemenlik sorun ve tartışmaları gündemden düşmemektedir. Siber uzayın tamamına kimse sahip olmadığı için güvenliğinden de kimse sorumlu olamaz düşüncesi siber savunma konusunda keskin adımlar atılmasının önüne geçmektedir.[76]

Söz konusu tehdidin bu kadar tartışılmasının en büyük nedenlerini sahip olduğu özelliklerin daha önceki dönemlerdekilerden farklı olması oluşturmaktadır. Siber saldırı, saldırganın kimliğini gizlemesine imkân vermekte, inkâr edilebilirlik

---

[74] Ali Murat KÖKNAR, " **Sanal Ortamda Terörizm**", TC Dışişleri Bakanlığı Bilişim ve İnternet Teknolojilerinin Ceza Hukuku Açısından Doğurduğu Yeni Sorunlar Semineri Bildirisi, Bursa 24 Mart 2011, s.66

[75] Richard CLARKE, Robet K. KNAKE,s. 46-47

[76] Richard CLARKE, Robet K. KNAKE,s. 137

yaratmakta, sınır gözetmeksizin dünyanın her yerinden gerçekleştirilebilmekte, saldırıyı yapanlar açısından düşük risk içermekte, siber saldırıda konvansiyonel silahlarla kıyaslandığında siber silahların çok daha ucuz ve oldukça etkili olduğu görülmektedir. Bu durum da siber alandaki risk ve tehditlerin asimetrik karakterini ortaya koymaktadır.

Devlet dışı unsurlar veya güçsüz devletler siber uzayın kendilerine tanıdığı imkânlar ile "oyun" içinde çok kolay yer alabilmektedir. Asimetrik tehdit kapsamında ülkeler kendi güvenlikleri için siber alana hâkim olma ve bu ortamda yapılabilecek asimetrik müdahalelerde güçlü bir pozisyonda bulunma istekleri nedeniyle siber ordular oluşturmaya başlamıştır. Bu oluşumlar siber alanın doğurduğu tehditlerin ulusal boyutta, ülke güvenliği açısından önem kazandığını göstermektedir. Eski Pentagon yetkilisi ve Harvard Kennedy Okulu Dekanı olan Joseph NYE tarafından bu durum eski ve yeninin sistem içinde beraber var olmasının getirdiği özellik nedeniyle "hükümetler hala internetteki büyük köpeklerdir ama küçük köpekler ısırır." diyerek tehditleri tanımlamıştır.[77] Bu durum uluslararası hukukta kuvvet kullanımı ve buna bağlı olarak meşru müdafaa hakkıyla ilgili yeni soruların ortaya çıkmasına neden olmuştur.[78]

Küreselleşme ile beraber tehditlerin belirginliği tahmin edilebilirliği daha belirsiz hale gelmeye başlamıştır. Yeni güvenlik tehditleri değişken, belirsiz, tahmin edilemez olarak tanımlanmaktadır. Terörizm, siber saldırı, kitle imha silahları vb. tehditlerin çeşitlendiğini, karmaşıklaştığını ve ulus-devlet dışı unsurlardan kaynaklanır hale geldiğini göstermektedir. Tehditlerin bu sayılan özellikleri nedeniyle de güvenliğin artık çok boyutlu hale gelmesi gerekliliği ortaya çıkmış ve eskiden birbirinden ayrı politikalar ile ele alınan bireysel, ulusal, uluslararası güvenlik arasındaki belirgin sınırlar ortadan kalkmaya başlamıştır.

Sosyal, siyasi ve ekonomik olaylar artık sadece ulusal boyutta değil tüm dünyayı etkileyecek boyuta taşınmıştır. Savaşın, tehdidin tarafları olan devletlerin yanına ittifaklar hükümet dışı örgütler ve terör örgütlerinin de eklendiği görülmektedir.[79] Dünyanın herhangi bir noktasında yaşananların etkisi farklı herhangi bir noktada hissedilir hale gelmiştir. Küreselleşme ile devlet tek ekonomik, siyasi ve

[77] P.W.SINGER, Allan FRIEDMAN,s. 207
[78] Şener ÇELİK, **Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme,** Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt:15, Sayı:1, 2013, s.137
[79] Ali Bülent UŞAKL, s.180

askeri güç merkezi olmaktan çıkmıştır. Farklı dinamikler devletin kontrolünün dışındaki alanlarda faaliyette bulunmaya başlamıştır. Bu faaliyetler ile devlet politikaları da kamuoyunu etkileyebilir hale gelmiştir. Teknolojik altyapının yani ulaşım ve haberleşme imkânlarının gelişmesi, savaşların etkilediği alanın genişlemesine küresel çapta etkilerinin hissedilmesine neden olmuştur.[80] Ulus-devletlerin sınırları dışına taşan durumların artması uluslararası kuruluşlara ihtiyacının artmasına neden olmuştur. Bu şartlar altında uluslararası sistemde güvenliği sağlama maksadıyla ortak çıkarı kabul etmeyen realist paradigmaya ters olacak şekilde kolektif güvenlik kavramı oluşmaya başlamıştır. İngiliz Okulu tarafından ülkeselliğin çözülmesi ile yani sınırların eski anlamını yitirmesi ile uluslararası toplum yaklaşımının oluştuğu devletin de bu sistemin bir üyesi haline geldiği ifade edilmektedir.[81] Bireyin güvenliği onu oluşturan topluluktan bağımsız olarak görülemez.[82]

Teknoloji risklerinin siyasal ve bilimsel olarak idaresiyle ilgili sorunlar, aktüel ve potansiyel olarak kullanılan teknoloji risklerinin idaresiyle (doğa, toplum ve kişisellik alanlarında) ilgili sorunlar tarafından gölgede bırakılmaktadır. Teknolojik gelişmenin riskleri coğrafi alan kapsamında belirli alanlarda meydana gelebildiği gibi, belirli alanları kapsamayan daha geniş olabilecek şekilde ya da evrensel biçimde oluşabilmektedir. Yeni tehdit zaman ve mekândan bağımsız "siber olan" her şey haline gelmeye başlamıştır. Bu gelişme ile eşleştirilebilecek diğer bir problem de yaşanabilecek olumsuzlukların artık öngörülmesinin de zorlaşması olarak ifade edilmektedir. Risklere maruz kalan ve risklerden istifade edenler arasında çelişkiler gelişmeye başlamıştır. Bilginin önemi artmakla beraber bilgiye şekil verme, kitle iletişimi altında bilgiyi yayma araçları üzerindeki tasarruf da artmaktadır. Bu nedenle içinde bulunulan toplum bilgi, medya, bilim toplumu olarak ifade edilebilir. Değişen toplum ile devlet de "uluslararası toplumu hem şekillendiren hem de onun tarafından şekillenen hale gelmiştir."[83]

Dönüşen toplum beraberinde yeni tehditleri, riskleri de getirmiştir. Bunun için gerekli olan bilinç ve siyasi örgütlenme biçimleri eksik olsa da, tehlike dinamiklerini harekete geçiren yeni tehditler ulus-devlet sınırlarının olduğu gibi uluslararası

---

[80] Mehmet Tanju AKAD, **Savaş Tarihinin Dönüm Noktaları**, İstanbul, Kastaş Yayınevi, 2005,s.11

[81] Barry BUZAN, **"From International to World Society?: English School Theory and the Social Structure of Globalization"** Cambridge University Press, Cambridge,2004,s.11

[82] Gizem BİLGİN AYTAÇ, s.81

[83] Andrea BIRDSOLL, **"The International Politics of Judicial Intervention: Crating a More Just Order"** London: Routledge,2009,s.17

örgütlerin de aleyhine olmaktadır. Sun TZU "Yüz savaşta yüz zafer çok büyük bir başarı değildir. Asıl hüner düşmanı hiç savaşmadan ele geçirmektir." diye 6.yüzyılda günümüz siber saldırı ve savunmasının bir çeşit tanımını yapmıştır.

Tarih boyunca askeri gelişmelerin sonuçlarının dünya düzenini şekillendirdiği görülmüştür. Silahlar, toplar, hava gücü, nükleer silah gibi... Siber uzay, siber tehdit de günümüzün değişen koşullarında güvenlik algılarını şekillendirmektedir. Siber uzay; kara, hava, deniz ve uzaydan sonra beşinci savaş alanı olarak tartışılmaya başlanmışken bilgisayar ve internet güvenliğinde uzman firmalar tarafından yapılan açıklamalarda küresel ölçekli siber saldırıların sayısı 2011 itibarıyla 946 milyonu bulduğu ifade edilmiştir.

Soğuk Savaş dönemi tehdit ve güvenlik açısından birkaç noktaya dayanmaktaydı. Kimin saldıracağının bilinmesi, saldırının nereden geleceğinin bilinmesi, dehşet dengesi kapsamında karşılık verilebilirlik vb. Fakat internetin yaygınlık kazanması ile beraber mekân-sınır kavramı ortadan kalkmış iletişim yeni bir boyut kazanmıştır. Askeri hedefler hedef olmaktan çıkmış, onunla oluşturulan taktik ve stratejiler geçerliliğini kaybetmeye yüz tutmuştur.

İnternetin sağladığı "küresel bağlanmışlık (interconnectedness)"[84] olumlu sonuçlar doğurduğu gibi olumsuz etkileri de beraberinde getirmiştir. Yeni suç türleri, terörizmin yeni bir boyutunu da gündeme taşımıştır. Örneğin vatansever içerikli ve politik altyapıya sahip siber olaylar devletleri ve uluslararası organizasyonları ulusal ve uluslararası kapsamda güvenliklerini gözden geçirmeye yöneltmektedir. Buna bağlı olarak da siber güvenlik gündeme gelmiştir.

Siber güvenlik "siber ortamda, kurum, kuruluş ve kullanıcıların varlıklarını korumak amacıyla kullanılan araçlar, politikalar, güvenlik kavramları, güvenlik teminatları, kılavuzlar, risk yönetimi yaklaşımları, faaliyetler, eğitim, teknolojiler bütünü olarak tanımlanmaktadır."[85] Yakın bir zamana kadar bireysel ve kurumsal sorunlara yol açan siber saldırılar artık kamu ve ülke güvenliğini tehdit edebilecek boyutlara gelmiştir. Der DERIAN bu durumu; "taklit (imitasyon) ve simülasyona ait yeni teknolojiler ile izleme yetenekleri ve hızın artması ile gerçek ve sanal savaş arasındaki alanın (gap), coğrafi mesafelerin ve kronolojik sürenin kısalması (collapse)" olarak

[84] Mary KALDOR, **New and Old Wars: Organized Violence in a Global Era**, Cambridge, Polity Press, 1998, s.3
[85] Hasan Çiftçi, **Her Yönüyle Siber Savaş,**S. 6

ifade etmiştir. Gerçekleşen bu değişimler ile savunma sanayi teknolojileri sayesinde savaşın niteliği ve tanımı günden güne değişmeye başlamıştır.[86] Geleneksel savaş metodundaki değişimler ile "farklı savunma (ya da saldırı) yöntemlerini bir arada kullanabilen ve aynı anda düzenli/düzensiz savaş icra edebilme kabiliyetine sahip olan stratejilere doğru ilerlemektedir."[87] Ülkeler kendilerini bu duruma hazırlamaya başlamış hatta geç bile kalmıştır. Örneğin ABD ulusal güvenlik perspektifi ile 2009 yılında Birleşik Siber Komutanlık bünyesinde siber muharebe birimi kurmuştur. Söz konusu birimin silahlı kuvvetler bünyesinde kurulması internetin de kurucusunun ABD Savunma Bakanlığı olduğu düşünüldüğünde sonuç çok şaşırtıcı görünmemektedir.[88]

Tehditlere yönelik önlem ve karşılık gündeme geldiğinde ise bunun standartlarının ne olacağı sorulduğunda verilen cevap ile hukuk tartışmaları gündeme gelmektedir. Hukukun temel amacı en genel haliyle toplumsal düzen sağlamak olarak ifade edilebilir. İnsanların gündelik hayatları için toplumsal düzeni sağlayan hukuka ihtiyaç duyması gibi uluslararası toplum içinde de ihtiyaç duyulmaktadır.

Ulusların ilişkilerinde sürekli olarak yer alan değişikliklere rağmen, uluslararası politikanın temel yapısı hala anarşik olarak ifade edilebilir. Her devlet, diğerleriyle işbirliği yapsa da yapmasa da öncelikli olarak kendini korumaya çalışmaktadır. İşte bu anarşik yapı ve koruma içgüdüsü çerçevesinde hukuk önemini korumaktadır. Örneğin uluslararası anlaşmaların varlığı ülkelerin hukuk dışı trafiği bloke etmelerini zorunlu hale getirebilmektedir. "Devlet artık bazı egemenlik yetkilerini AB gibi ulus üstü yapılara devredebilmekte sınırlı etkiler ile karşılaşabilmektedir."[89] Uluslararası örgütleri var eden ve devamlılığını sağlayan uluslararası hukuk ve onun kabulleri çerçevesinde hareket etmeye çalışan diğer bir örgüt olan NATO da, bu tartışmalar içinde kalan en önemli örgütlerden biri haline gelmiştir. Soğuk Savaş dönemi ve sonrasındaki stratejilerinin dayandığı meşru nedenler her zaman tartışma konusu olmuştur. Günümüzde siber güvenlik anlayışı çerçevesinde müdahale kavramı da hukuki açıdan tartışılmaya başlanmıştır. Çünkü var olan tartışmalar, kan akıtmadan

---

[86] James Der DERİAN, "**Virtuous War/Virtual Theory**", International Affairs, Cilt 76, No.4, Ekim 2000, s.771–788.
[87] Salih BIÇAKCI, "**Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu**", Uluslararası İlişkiler, Cilt 9, Sayı 34 (Yaz 2012), s. 205-226.
[88] Richard CLARKE, Robet K. KNAKE,s. 28
[89] Trudy JACOBSEN,**"The End of Westphalia? Re-envisioning"** Hampshire,Ashgate Publishing,2008,s.5-6

başlayan siber saldırıların etkilerinin zamanla sadece siberde kalmayarak ateşli silahlar ile karşı karşıya gelinen bir çatışmaya dönüşebileceği yönündedir.[90]

Uluslararası olarak yapılabileceklerin başında ortak bir tanım, politika, hukuk çalışması gelirken olası bir durumda yapılacakların uluslararası normlar çerçevesinde belirlenmesine ihtiyaç duyulmaktadır. Siber tehdide karşı yapılacak bir kolektif çalışma, doğası gereği tamamen savunmaya yönelik olacaktır.[91] Bu kapsamda yapılan ilk uluslararası sözleşme; "Avrupa Konseyi Siber Suçlar Sözleşmesi"dir. Söz konusu sözleşme 23 Kasım 2001 tarihinde imzaya açılıp 01 Temmuz 2004 tarihinde yürürlüğe girmiştir.[92] Sözleşme, imzalayan ülkelere siber suç olarak Sözleşme 'de belirlenen suçların işlenmesini ulusal mevzuatlarında suç olarak belirlemelerini ve ulusal düzeyde önlemler almalarını gerekli kılmaktadır. Mütekabiliyet esası ile yardımlaşma, suçluların iadesi gibi konuların düzenlendiği sözleşme ile yasal ve teknik problemleri azaltmak hedeflenmektedir.[93]

İmzalanan ilk anlaşmanın etkinliği konusunda farklı görüşler vardır. Bu görüşlerden yapılan çalışmayı başarısız olarak gören taraf, imzalayan ülkelerin Sözleşmeyi kendi çıkarları, ihtiyaçları, sınırsız bilgi paylaşımı yapılmaması doğrultusunda yorumlayarak hazırladıklarını savunmaktadır. Ayrıca özellikle siber tehdit konusunda başat olarak ifade edilen Çin ve Rusya'nın da Sözleşme 'de imzacı taraf olmaması bu görüşü güçlendirmektedir. Söz konusu ülkelere ek olarak herhangi bir siber saldırıdan en çok etkilenecek ülkelerden birinin ABD olabileceği değerlendirilirken, siber alanda silahsızlanma ya da bunların kontrol altında tutulmasına da en çok karşı çıkan ülkelerden birisi olması yine dikkat çekici olarak değerlendirilebilir.

---

[90] Richard CLARKE, K. KNAKE,s.140

[91] Christian Günter CZOSSECK, Karlis PODINS, "**An Evaluation of State- Level Strategies Against Botnets in the Context of Cyber Conflicts**",A Vulnerability-Based Model Of Cyber Weapons And Its Implications For Cyber Conflict Estonian Business School, Doctoral Thesis in Management, No.14, Talinn 2012,s.57-66

[92] Orçun KEÇECİ, **Siber Suçlar ve Siber Terörizm**, s.12, (Çevrimiçi) http://www.academia.edu/2333087/Siber_Su%C3%A7lar_ve_Ter%C3%B6rizm , 25.01.2016

[93] "Convention on Cyberspace", Council of European Treaties Series, No.185, http://conventins,coe,int/Treaty/Commun/QueVulezVous.asp?NT=185&CL=ENG,04.06. 2014

IV.SAVAŞ HUKUKU VE SİBER GÜVENLİĞİN YASAL BOYUTU

Devlet merkezli uluslararası sistemin temelinin atıldığı 1648 Westphalia anlaşmalarından itibaren aktörler arasında kuvvet kullanma tanımı, savunma ve saldırı yöntemleri çeşitli anlaşmalar ve konferanslarda gündeme gelmiş ve hep yasaklanmıştır. Özellikle 1. Dünya Savaşı sonrası sürecin bu anlamda daha etkili olduğu söylenebilir. Milletler Cemiyeti Sözleşmesi ile başlayan süreç 1928 yılında 62 ülke tarafından imzalanan savaş yolunun tercih edilmemesini içeren Briand Kellogg Paktı ile devam etmiştir. Söz konusu paktın 2. maddesine göre, "İmzacı devletler niteliği ve kaynağı ne olursa olsun, aralarındaki her türlü anlaşmazlık ve çekişmelerde barış yollarından başka bir yol izlememeyi esas aldıklarını kabul ve ilan ederler." Söz konusu maddeden de anlaşılabileceği gibi Briand-Kellogg Paktı'nı bu kadar önemli kılan özelliği kuvvet kullanmaktan kaçınma ilkesini ilk defa bu kadar yalın biçimde dile getiren bir uluslararası hukuk düzenlemesi olmasıdır."[94]

1945 yılında yürürlüğe giren ve 193 BM üyesi ülke tarafından kabul edilmiş olan BM Sözleşmesi tarafından ise, kuvvet kullanmama ilkesi "tüm üyeler, uluslararası ilişkilerinde gerek herhangi bir başka devletin toprak bütünlüğüne ya da siyasal bağımsızlığına karşı, gerek BM'nin amaçları ile bağdaşmayacak herhangi bir biçimde kuvvet kullanma tehdidine ya da kuvvet kullanılmasına başvurmaktan kaçınırlar." şeklinde ifade edilmiştir.[95]

Buna karşın BM Sözleşmesi kuvvet kullanımı tanımına ek olarak kuvvet kullanma yöntemi kapsamında hükümleri de içermektedir. En başta kuvvet kullanımını iki durum ile sınırlayarak tanımlamaya başlamıştır. Bunlardan ilki "Güvenlik Konseyi Kararı ile Kuvvet Kullanımıdır". BM Sözleşmesinin 7. Bölüm 39. Maddesine göre uluslararası barış ve güvenliği temin için bu duruma karşı herhangi bir saldırı gerçekleştirildiğinde yapılacak herhangi bir yaptırıma yönelik BM Güvenlik Konseyi karar merciidir. Devamında 41. Madde ile ise Konsey saldırgan devleti diplomatik ve ekonomik vb. açılardan bazı ambargolara maruz bırakabilir. Söz konusu yaptırımların yetersiz kalması durumunda yine sözleşmenin 42. Maddesi gereği kuvvet kullanımına karar verilebilir.

---

[94] Şener Çelik, s.153

[95] BM Sözleşmesi madde 2 (4), Charter of the United Nations, " Chapter I: PURPOSES AND PRINCIPLES", http://www.un.org/en/documents/charter/chapter1.shtml, (Erişim: 27 Haziran 2012)

Bunlara ek olarak kuvvet kullanımına müsaade eden diğer bir hüküm ise meşru müdafaa hakkını tanımlayan 51. Maddedir. Meşru müdafaa üç durumun olması durumunda hak olarak tanınmıştır. Kuvvet ise "fiziksel saldırıları ve ekonomik, diplomatik ve propagandaya yönelik eylemler" gibi zorlayıcı önlemlerin tümünü ihtiva eden geleneksel kavramları içerecek şekilde tanımlanmıştır."[96] Bu perspektiften siber silahların herhangi bir saldırı kapsamında yardımcı silah olarak kullanılabildiği gibi asıl silah olarak da kullanılabileceği öne sürülebilir. Bu saldırılarda aşağıda sıralanan ve güvenliği en çok önemsenen hususlar karşısında tedbir ihtiyacı önemini giderek artırmaktadır.

1. Vatandaşların ve onların yurt dışındaki mülklerinin korunması,
2- Ulusun politik bağımsızlığının korunması
3- Ülkenin toprak bütünlüğünün korunması.[97]

BM tarafından uygulanacak silahlı müdahaleler belli çerçeve içine alınmış ve uluslararası hukukun temelini oluşturan maddeler ile kuvvet kullanımı meşruiyeti ifade edilmeye başlanmıştır. Silahlı güç kullanılmasının hukuki olarak iki boyutu ifade edilmektedir. İlki; savaş açma hakkı olarak da ifade edilebilen "jus ad bellum" silahlı güç kullanmanın haklılığı, savaşın gerekçelerinin hukukuna uygunluğuna ilişkin kuralları kapsar. Söz konusu kuralların temelini BM Sözleşmesi oluşturmaktadır. Diğeri ise savaşma kuralları olan " jus in bello"dur. Jus in bello; çatışma esnasında kullanılan yöntem ve araçların hukuka uygun olarak kullanılmasını içeren yapıdır. Söz konusu kuralların temelini de Silahlı Çatışma Hukuku (Law of Armed Conflict) oluşturmaktadır.[98]

Fakat siber alan, siber saldırı, siber güvenlik kavramları ile konvansiyonel savaş, topyekûn savaş gibi günümüzde yapısı değişen savaş niteliklerine göre belirlenen söz konusu maddelerin yetersizliği ve yeni düzenlemelerin ihtiyaç olduğuna yönelik yeni tartışmalar gündemdedir. Çünkü BM Genel Kurulunun 3814 sayılı ve 1974 sayılı kararına göre saldırı; "bir devletin diğer devletin egemenliğine, ülke bütünlüğüne veya siyasi bağımsızlığına karşı veya bu tanımda belirtildiği üzere BM Sözleşmesi ile bağdaşmayan diğer herhangi bir silahlı kuvvet kullanılması" olarak tanımlanmaktadır. Tanımdan da anlaşılacağı gibi saldırı kavramı silahlı güç ile

[96] Michael GERVAİS, **Cyber Attacks and the Laws of War,** Berkeley Journal of International Law, Vol.30, Issue 2 (2012),s.536
[97] Hasan ÇİFTÇİ. **Her Yönüyle Siber Savaş,** s.97
[98] Hasan ÇİFTÇİ. **Her Yönüyle Siber Savaş,** s.96

eşleştirilmiş ve meşru müdafaa hakkının ancak buna bağlı olarak doğabileceği anlaşılmaktadır. Bu perspektiften değerlendirildiğinde siber saldırıların meşru müdafaa kapsamında değerlendirilemeyeceği tartışılmaya başlanmıştır.

Buna karşı olarak siber alanda kullanılan yöntemlerin de kullanan aktörler tarafından silah olarak değerlendirilebileceğini savunan görüşler de mevcuttur.[99] Bu görüş Cenevre Sözleşmelerinin 1. Protokolünde saldırının "hasma karşı şiddet eylemleri" olarak ifade edilmesinden yola çıkmaktadır. Çünkü bu tanım içerisinde silahlı bir müdahaleye direkt bir atıf bulunmamaktadır. Fakat dikkat edilmesi gereken başka bir husus var ki o da siber saldırıların hedefinin bireyler olması neticesinde mağdur olan devlet, saldırganların devlet desteği olmaması durumunda meşru müdafaa hakkından bahsedemez.[100]

Ancak sivillere uygulanan siber saldırı yine Cenevre sözleşmelerinin "sivillerin korunması" ve BM tarafından hedef ayırt etmeyen silahlar konulu protokoller kapsamında değerlendirilebilir. Nitekim buna ek olarak BM tarafından siber suçlara karşı iki karar alınmıştır. İlk karar ile uluslararası bir bilinç yerleştirmek maksadıyla siber güvenlik kapsamında dokuz kıstas[101] tanımlanmıştır. 58/199 (2004) numaralı ikinci karar ile ise üye devletler kritik altyapıların korunması için siber güvenlik konusunda bilinçlenmeye teşvik edilmektedir.[102]

NATO tarafından ise bu husus NATO Kolektif Siber Savunma Mükemmeliyet Merkezi (Cooperative Cyber Defence Centre of Excellence (CCDCOE) tarafından Gürcistan'a gerçekleştirilen siber saldırılar neticesinde hazırladıkları Yasal Dersler dokümanında ele alınmıştır. Söz konusu dokümanda siber savaş, "uluslararası hukukta ifade edilen savaş kavramı ile beraber anılarak bu hukuk kurallarının siber saldırı başlatmak veya siber savaş esnasında uyulmasına dikkat edilmesinin gerektiği, siber saldırı neticesinde de yaralanma ölüm vb. hasarlar oluşuyorsa siber terörizmin de Silahlı Çatışma Hukukunun bir parçası olarak ele alınabileceği, 11 Eylül saldırıları sonucunda silahlı çatışmanın taraflarının devletler olması şartının

[99] D.BLAKE, J.S.IMBURGIA, **Bloodless Weapons? The Need To Conduct Legal Reviews Of Certain Capabilities And The Implications Of Defining Them As "Weapons",** The Air Force Law Review Articles, Vol.66,2010, s.160
[100] Hasan ÇİFTÇİ, **Her Yönüyle Siber Savaş,** s.99
[101] 57/239 (2002); farkındalık, sorumluluk, mukabele, ahlak, demokrasi, risk değerlendirmesi, güvenlik tasarım ve gerçekleştirimi, güvenlik yönetimi ve yeniden değerlendirme.
[102] Hasan ÇİFTÇİ, **Her Yönüyle Siber Savaş,** s.109

değişerek devletler tarafından desteklenen grupların da olabileceğinin görüldüğü ve BM ile NATO tarafından kabul edildiği" hususlarına yer verilmiştir.[103]

2012 yılında CCDCOE internet sitesinde yayımlanan Talin El Kitabı ile jus ad bellum ve jus in bello kuralları siber alana uyarlanmıştır. 95 maddelik söz konusu Kitapta;

- Bir devlet egemen olduğu bölgede siber altyapı ve faaliyetleri kontrol edebilir.

- Bir devlet, kendisiyle ilişkilendirilebilecek bir siber eylem için uluslararası alanda yasal sorumluluk taşır.

- Uluslararası hukuka uymayan bir eylem yüzünden zarar gören bir devlet, sorumlu devlete karşı siber önlemler alabilir.

- Bir siber saldırı çapı ve etkileri itibariyle, siber olmayan bir harekâtın çapı ve etkisine denk bir etki yaratıyor ise, o siber saldırı "kuvvet kullanımı" anlamına gelir.

- Ölçüsü ve etkileri açısından silahlı saldırı olarak nitelendirilebilecek bir siber saldırıya karşı, mağdur devletin meşru müdafaa hakkı saklıdır.

- Sivillere ve sivil altyapılara karşı siber saldırı yapılamaz.

- Hem askeri hem de sivil amaçlarla kullanılan nesnelere siber saldırı yapılabilir.

- Bir devlette yerleşik siber altyapı aracılığıyla siber harekâtın yönlendirilmiş olması, bu devlete siber harekâtı atfetmek için yeterli değildir.

- Bir devletin hudut bütünlüğüne, siyasi bağımsızlığına tehdit oluşturan veya kuvvet kullanımı içeren ya da BM'nin amaçlarıyla uyumsuz olan bir siber harekât hukuksuzdur.

- Uluslararası organizasyonlar veya bölgesel nitelikli kuruluşlar, Birleşmiş Milletler Güvenlik Konseyi tarafından yetkilendirilmeyi ya da

[103] Cooperative Cyber Defence Centre of Excellence, **Cyber Attacks Against Georgia: Legal Lessons Identified**",2008

görevlendirilmeyi müteakip, siber harekâtlara karşılık ya da siber harekât içeren yaptırım niteliğinde eylemler icra edebilir.[104] maddeleri bunlardan bazılarıdır.

BM Şartı'nın 2. Maddesinin 4. Fıkrası uluslararası hukukun kuvvet kullanma yasağı kapsamında temel düzenleme olarak görülmekte ve silahlı saldırı olması durumunda meşru müdafaa hakkını kabul etmektedir. Yukarıda maddeleri sayılan El Kitabı, siber saldırının da bir kuvvet kullanma çeşidi olduğunu ifade etmektedir.[105] Bu noktadan hareketle herhangi bir siber saldırı karşısında uluslararası hukuka uygun karşılık verilebilmesi için saldırının haksız olarak mağdur ülkenin iktisadi sosyal, kültürel ya da dış politikasına baskı içermesi gerekir çıkarımı yapılabilir. Fakat asıl problem yapılacak uygulamadan ziyade saldırının kaynağının tespiti olduğundan saldırı fiilinin devlete atfedilir ajanları tarafından yapıldığının ispatı gerekmektedir.[106] Nitekim Estonya örneğinde de ana sorunu saldırının kaynağının ispatı sorunu oluşturmuştur.[107] Bu anonimlik devam ettiği sürece (hala standart tanımlar üzerinden uzlaşılamamış olsa dahi) uluslararası hukuk düzenlemeleri savunma için yetersiz kalmaya devam edecektir.

---

[104] Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı, http://www.mgk.gov.tr/index.php/siber-savasa-uygulanacak-hukuk-hakk-nda-tallinn-el-kitab-uluslararas-siber-guevenlik-hukuku#, (Erişim: 15 Mart 2015)

[105] Michael N. SCHMITT, **Tallinn Manual on the International Law Applicable to Cyber Warfare,** International Group of Experts Invited by the NATO Cooperative Cyber Defence of Excellence, 2012

[106] Özgür MUMCU, **Jus ad Bellum ve Jus in Bello Açısından Siber Saldırı Kavramı,** Geleceğin Savaşları ve Silahları, Uğur Mumcu Araştırma Gazetecilik Vakfı Yayınları, Ankara, 2014, s.177-182

[107] Ennenen TIKK, Kadir KASKA, Liis VIHUL, **International Cyber Incident- Legal Considerations,** Cooperative Cyber Defence Centre of Excellence, Talinn, 2010, s.20

İKİNCİ BÖLÜM

NATO GÜVENLİK ALANINDA YENİ BİR BOYUT: SİBER GÜVENLİK

I. SOĞUK SAVAŞ DÖNEMİ NATO VE GÜVENLİK ALANI

İkinci Dünya Savaşı'nın sona ermesiyle beraber dünya siyasetinde etkili olan Avrupa devletleri, yaşadıklarının etkisiyle geri planda kalırken iki yeni gücün devreye girdiği görülmüştür. Birleşik Devletler ve Sovyetler Birliği, 1945 sonrası oluşan çift kutuplu sistemin başat aktörleri olmuştur. Doğu Bloğu ve Batı Bloğu şeklinde birbirini ötekileştiren iki farklı yapı döneme adını vermiştir. Bu yapılar üzerinden tehdit algıları ve güvenlik tanımları geliştirilmeye başlanmıştır. Nükleer tehdit Savaş'ı "soğuk" yapan neden haline gelmiştir. Bu anlayış çerçevesinde her iki bloğun üyeleri kendilerine bir güvenlik şemsiyesi oluşturmuşlardır. NATO, Batı Bloğunun güvenlik teminatı, Sovyetler Birliği'ne karşı koruma garantisi olurken demokrasi, liberalizm gibi değerlerin de temsilcisi ve güvencesi haline gelmiştir. Hem üyeleri hem de üye namzetleri için Kuzey Atlantik Örgütü'nü bu dönemden sonra her türlü tehdit için önemli ve çekici kılan en önemli özelliği 5. Madde haline gelmiştir. Üyelerine güvenlik garantisi sağlayan bu madde Örgütün Soğuk Savaş boyunca "güvenlik alanının" hem kendisi hem de koruyucusu olmuştur.

5.maddenin içeriği; üye ülkelerden birine herhangi bir saldırı olmasında toplu halde karşı saldırı gerçekleştirilmesi üzerine oluşturulmuştur. "Taraflar, bir ya da birden fazlasına Avrupa ya da Kuzey Amerika'da yapılacak silahlı saldırıyı kendilerinin tamamına karşı yapılmış olarak değerlendirecektir." diyen 5.madde topyekûn savunmanın ana hatlarını ifade etmektedir.[108] Taraf olan ülkeler barış ve güvenliği BM Antlaşmasına uygun olarak korumayı ve Kuzey Atlantik bölgesinde istikrarı sağlamayı hedef olarak göstermiştir.

1967 yılında ABD ve Kanada'nın da dâhil olduğu 33 ülkenin katılımıyla Avrupa Güvenlik ve İşbirliği Konferansı (AGİK)[109] Fransa tarafından gerçekleştirilmiştir. NATO

[108] P.W. SINGER, Allan FRIEDMAN, **Siber Güvenlik ve Siber Savaş, s**.166

[109] Avrupa'nın bölünmüşlüğüne son verilmesi, güvenlik ve istikrarın sağlanması ve katılan devletlerarasında bu amaca yönelik işbirliğinin geliştirilmesi düşüncesiyle kurulmuş teşkilattır. Görevi Doğu ve Batı arasında çok taraflı bir müzakere ve diyalog forumu olarak belirlenmiştir. 1975'den 1990'a kadar AGİT, yeni yükümlülüklerin ele alındığı ve uygulamaların gözden geçirildiği bir dizi konferans ve toplantılar şeklinde devam etmiştir. 1990 yılında yapılan Paris

üyeleri ile daha gelişmiş bir işbirliği gündeme gelmiştir. Böylece Avrupa'nın savunması ile ilgili konuların NATO dışında tartışılabileceği ikinci bir alan söz konusu olmuştur.

1979 yılında SSCB tarafından gerçekleştirilen Afganistan işgali Sovyetler Birliği'nin ekonomik olarak zor durumda kalmasına neden olmuş ve dolayısıyla SSCB'yi silahlanma yarışında ABD'nin gerisinde bırakmıştır. SSCB, 1987 yılında ''glasnost'' (açıklık) 1988 yılında ''perestroyka'' (yeniden yapılanma) hareketlerini başlatmıştır. 1991 yılında Paris'te iki tarafında katıldığı toplantıda Soğuk Savaşın bittiğini ilan eden Paris Yasası imzalanmıştır.

İdeolojik kutuplaşmanın sona ermesinden önce birlikte o dönemde yüksek politika (high politics) konusu olarak güvenlik, sadece askeri stratejik açıdan tek boyutlu ele alınmaktayken artık günümüzde önceden alçak politika (low politics) olarak nitelenen birçok alan uluslararası politikanın içeriğini oluşturmaktadır. Yeni sistemde ortak güvenlik söz konusudur. "Diğer ülkeleri kendi güvenliği için tehdit olarak algıladığı sürece hiçbir ülke güvenlikte değildir." anlayışı hâkimdir.

II. SOĞUK SAVAŞ SONRASI NATO'NUN GÜVENLİK ALANI

1989 yılında Doğu Blokunun kaybıyla uluslararası sistem ve özellikle Batı Bloku bu beklemediği durum karşısında meşruiyet kaynağını kaybetmiştir. Bu andan itibaren NATO yıllardır her türlü stratejisini şekillendirdiği güvenlik anlayışını, ona göre oluşturduğu tehdit algısı kaynağını kaybetmiştir. Bu beklenmedik sonun iyimser bakış açısını en iyi yansıtanlardan biri Fukuyama olmuştur. Tarihin Sonu tezine göre; mücadele sonucu Batı tarzı liberalizm ve demokrasi kavramlarının nihai bir yönetim biçimi olarak varlığı kanıtlanmıştır. Fakat diğer taraftan 1989'a kadar sahip olduğu meşru düşmanı kaybeden NATO, sahip olduğu güç temelinde varlığına neden oluşturacak, devamlılığını sağlayacak değişiklikleri gündeme getirme ihtiyacı duymuştur. Sahip olduğu güç tekeline meşruiyet kaynağı oluşturarak yeni bir kimlik arayışına girmiştir. Bu amaçlar sonucunda "Stratejik Kavram" değişikliği gündeme getirilmiş ve uygulanmıştır. Yeni görev alanları belirlenmeye başlanmıştır. Ayrıca yeni bağımsız devletlerin de uluslararası arenaya dâhil olması ile NATO genişleme

Zirvesi soğuk savaş sonrası dönemde ortaya çıkan tehlikeleri karşılamayı amaçlayan bir kurumsallaşmanın başlangıcını işaret etmiştir.

stratejisini tekrar gündeme getirmiştir. Böylece eski Doğu Blok'undan olan bu yeni devletlerle önce diyalog, sonra işbirliği sağlayacak çeşitli organizasyonlar meydana getirilmiştir.[110] Yani Soğuk Savaş sonrası NATO bir sona gelmemiş, fakat Soğuk Savaş dönemi görevlerinin sonuna gelmiştir.

NATO, Sovyetler Birliği'nin yıkılmasında sonra kendine yeni misyonlar edinerek varlığını devam ettirmiştir. Stratejileri yumuşamış kendine belirlediği görevler çeşitlenmiştir. Artık bir bloktan gelebilecek saldırılara karşı koymayı değil küresel olarak dünya barışının korunmasını görev edinmiştir. NATO'nun tehdit olarak belirlediği unsurlar da değişime uğramıştır. Görev alanları yeniden tanımlanmıştır. Varlık nedeni ve genişleme stratejisinin sebebi üzerine bu dönemden sonra verilen yanıt Soğuk Savaş sonrası barış ve düzenin korunmasının yanı sıra eski komünist ülkeleri de Batılı sisteme dâhil ederek demokrasinin yerleşmesini sağlamak şeklinde gösterilmiştir. Bu dönemde, aşırı milliyetçilik, etnik ve bölgesel çatışmalar, kitle imha silahları, uyuşturucu ticareti vb. NATO için yeni varoluş sebepleri haline gelmiştir. Bu sebepler devamında NATO'nun kavram değişikliğine gitmesine neden olmuştur. Bunun ilk adımı olarak 1990 yılında yapılan Londra Zirvesi gösterilebilir.

Sadece Avrupa'da değil Avrupa dışında da istikrarı bozucu gelişmeleri tehdit olarak belirlemiştir. BM tarafından yürütülen uluslararası jandarmalığı üstlenerek barış ve güvenliğin teminatı haline gelmeyi hedeflemiştir. Avrupa güvenliği için almak istediği sorumluluk hem siyasi hem askeri alanda olmuştur. Siyasi alanda Doğu Avrupa devletleriyle işbirliği içine girmiş, askeri boyutta ise özellikle Balkanlarda faaliyetlerde bulunmuştur.

7-8 Kasım 1991'de Roma'daki Zirve ile daha da belirginleşen değişen güvenlik anlayışı "yeni strateji kavramı" adı altında kabul edilmiştir. "Yeni Stratejik Kavram" ile elde edilmek istenen, acil ve tehlike arz eden durumlarda, en kısa sürede ve etkili olarak sorun olan bölgeye yerleştirebilecek bir askeri güç yapılandırılmasıdır. Sadece Avrupa değil Avrupa dışında da istikrarı bozacak durumlar tehdit olarak belirlenmiş böylece ilgi alanı genişlemiştir.[111]

Askeri, siyasi ve ideolojik algılarda değişiklikler meydana gelmiştir. Bu değişikliklerin meydana geldiği zemin üzerine NATO da yeni ilkeler benimsemiştir.

[110] Mehmet HASGÜLER, Mehmet B. ULUDAĞ, **NATO,** Devletlerarası ve Hükümetler-dışı Uluslararası Örgütler, Nobey Yayın, Ankara, 2005,s. 204-209
[111] Derya Gonca PEKSARI, s.53

Ancak konjonktür değişse de temel amaç üye ülkelerin güvenliklerini korumak olarak devam etmektedir.

1991 yılında Roma Zirvesi'nde "Yeni Stratejik Kavram" belirlenmiştir. NATO tarihinde ilk defa bir stratejik kavramı kamuoyuna açık şekilde sunmuş, strateji uzmanlarının, halkın, gazetecilerin eleştirisine açık hale getirmiştir. Bu tarihten 1992'de "Yeni Stratejik Kavram" kabul edilene kadar geçen dönemdeki strateji "Geçiş Dönemi Stratejisi" olarak adlandırılmaktadır. NATO bu strateji ile bundan böyle üyelerini sadece saldırıya değil etnik, dinsel, bölgesel sorunlar, insan hakları ihlalleri, terörizm vb. risk faktörlerini de göz önüne alarak koruyacağını belirtmiştir. Yeni Kavram ile kriz yönetimi ve barışın korunması amaçlanmıştır. Hedeflere önleyici diplomasi ile ulaşılacağı öngörülmüştür. Bu bildirinin SSCB'nin artık eski düşman olduğunu Soğuk Savaş'ın sonu olduğunu ilan eder nitelikte olduğu değerlendirilebilir. NATO bu şekilde kendini yeni koşullara adapte etmeye çalışmıştır. Bu dönemden itibaren de en büyük sorunlardan biri olarak terör kavramı dile getirilmeye başlanmıştır. Ancak terörün Devletler Hukukunda tanımı konusunda kesin bir fikir birliğine varılmamıştır. Yeni tehdit algıları çerçevesinde işbirliğini artırmayı hedefleyen NATO kendisi içinde oluşturduğu birçok yapı ile üye olmayan devletler ile de iletişimini artırmıştır.

1991'den sonra NATO'nun benimsediği yeni ittifak anlayışının somut göstergeleri; Barış İçin Ortaklık (BİO), Avrupa Güvenlik ve Savunma Kimliği (AGSK), AKKA, Kurucu Senet, kitle imha silahlarının yaygınlaşmasını önlemeye yönelik çalışmalar, Euro-Atlantik Ortaklık Konseyi vb. olmuştur. Ayrıca koşulların değişmesi ile meydana gelen başka oluşumlar da söz konusudur.

NATO değişen dünya koşullarında varlığını sürdürürken Doğu Avrupa'nın yeni ülkeleriyle de ortak bir güvenlik kurumu haline gelmiştir. 1999 yılında Washington Zirvesinde "Yeni Stratejik Kavram" kabul edilmiştir. Kavram' da Transatlantik bağının korunacağı, Kurucu Senet çerçevesinde de Rusya ile ilişkilerin daha yakın şekilde süreceği belirtilmiştir. Bu zirve NATO'nun tekrar hayata geçirildiği bir zirve olmuştur. Örgüt bundan böyle sadece doğrudan saldırıya karşı değil aynı zamanda Kavram 'in 20-24.maddelerindeki sayılan etnik, dinsel rekabet, bölgesel uyuşmazlıklar, insan hakları ihlalleri, devletlerin dağılması, kitle imha silahlarının yayılması, terörizm gibi risklere karşı da koruyacaktır. Ayrıca dile getirilen ''Avrupa Atlantik'' kavramıyla Baltık, Balkanlar, Karadeniz, Ukrayna ve Rusya'nın içine alındığı bir anlam ifade edilerek Avrupa kıtası içinde bölünmüşlüğün ortadan kalkması hedeflenmiştir.

NATO'nun sabit tehdit odağını kaybetmesi ile uzun süre yeni bir ''öteki'' arayışına girilmiştir. Bu arayışın sonuca ulaştığı tarih 11 Eylül 2001 olmuştur. Yani aranan kan bulunmuştur. İki kutuptan birinin kaybolması ile realist kuramın temelini oluşturan uluslararası sitemin anarşi olgusuyla nitelediği yapı tekrar sisteme hâkim olmuştur. Sistemi dengeleyecek güç ve güçlerin belirsizliği anarşiyi gündeme getirmiştir. Yaşanan terör olayı güvenlik ortamının tehditlerinin belirsizliğini ortadan kaldırmıştır. NATO 52 yıllık tarihinde ilk kez bir terör olayını 5.madde kapsamına alarak ABD'ye destek vermiştir. Böylece tek bir NATO ülkesine yapılan saldırı hepsine yapılmış sayılır anlamına gelen 5.maddenin uygulaması ilk olarak 11 Eylül sonrası gerçekleştirilmiştir. ABD, NATO'yu belli bir alanı değil belli bir kavramı savunan bir örgütlenme haline getirmek istemiştir. Güvenlik kavramı tekrar askeri bir yapı halini almıştır. Kısacası Soğuk Savaş sonrası dönem 11 Eylül ile son bulmuştur.

Bunun neticesinde, 2002 yılında gerçekleştirilen NATO'nun Prag Zirvesi'nde görüşülen önemli konulardan biri terörizm olmuştur. NATO'nun "Stratejik Kavramı" temel alınarak terörizm ve kitle imha silahlarının yayılmasıyla mücadele amaçlı hazırlanan önlemler paketi sunulmuştur. İttifak liderleri radikal dincilik, uluslararası terörizm ve sınır ötesi suç ağlarını göz önüne alarak NATO'nun çalışma yöntemlerinde bazı değişiklikler yapmaya karar vermiştir. NATO Mukabele Gücü'nün (NMG) oluşturulması kararı alınmıştır. Kara, hava, deniz unsurlarını içerecek, ihtiyaç duyulduğunda NATO'nun en yüksek karar makamı olan Kuzey Atlantik Konseyi kararıyla hızla harekete geçebilecek bir yapı oluşturulması amaçlanmıştır. Ayrıca genişleme stratejisine devam edilerek Slovakya, Letonya, Slovenya, Estonya, Litvanya, Romanya ve Bulgaristan'ın ittifaka üyelikleri kabul edilmiştir. 2004'te üyelikleri resmen gerçekleştirilmiştir.[112]

11 Eylül saldırıları sonrasında terörizmle mücadele konusunda yeni sorumluluklar alan NATO görev alanının oldukça uzağında Afganistan'da istikrar ve güvenliği sağlama görevi üstlenmiştir. Böylece NATO "Yeni Stratejik Kavram"ında belirtildiği gibi hayati çıkarlarının riske girdiği durumlarda Avrupa dışında dahi olsa kriz yönetimi ve barışı koruma operasyonlarının uygulanmasında herhangi bir tereddüt göstermeyeceğini ortaya koymuştur. Afganistan'da Taliban militanlarına karşı

[112] NATO, (2003) "**The Prague Summit and NATO's Tranformation**", North Atlantic Treaty Organisation, s.1-50

başlatılan askeri operasyonların da NATO'ya devredilmesiyle birlikte NATO'nun müdahale alanının Avrupa coğrafyasının dışına taşındığı görülmüştür.

Kutuplardan birinin kaybolması ile ayakta kalan kutbun lideri olan Amerika'nın başkanı Bush ''yeni bir dünya düzeninden'' bahsetmeye başlamıştır. ABD Genelkurmay Başkanı 1992 yılında yaptığı bir konuşmasında Soğuk Savaş dönemi sonrasını, 1815 sonrası döneme benzeterek o dönemde oluşan Avrupa Ahengi gibi bir barış ortamının yaratılabileceğini dile getirmiştir. Hatta bunu "o dönemin kralları bunu savaştan bıkarak yapabiliyorsa biz başkanlar, başbakanlar, parlamentolar ve halklar özgürlük temelli bir barış yapabiliriz." diyerek vurgulamıştır. 1989 yılı sonrası yaşanan gelişmelerde Moskova hem NATO'nun hem VP'nin feshedilmesinden yana tavır takınmıştır.

III. NATO'NUN SİBER GÜVENLİK KARŞISINDA KURUMLAŞMASI VE GÜVENLİK ALANI TANIMLAMASI

NATO'nun varlığını devam ettirmesi için sorumlulukları da değişmeliydi. Fakat temel amaç olarak üyelerin güvenliğinin sağlanması vurgulanmaya devam etmektedir.[113] Ülkeler ve uluslararası örgütler için yeni riskler ortaya çıkmıştır. Risk ortamı devamında fırsatları da doğurmuş, Soğuk Savaş'tan galip çıkan blokun temsilcisi olarak ifade edilebilecek olan ve aslında bölgesel bir örgüt olan NATO, günün koşullarını göze alarak yenilenme ve adaptasyon süreci içine girmiştir.

Üyelerine yönelebilecek "herhangi bir" saldırı tehdidine karşı ortak savunma ve caydırıcılık sağlanması kararı alınmıştır. Böylece varlık nedeni ortadan kalktığı için yok olması beklenen ittifak devamının gerekliliğini yeni tehdit tanımları yaparak bunlara karşı üye ülkeleri savunma görevi olarak ifade etmiştir.

Çağın getirdiği teknolojik tehditler de ittifakın gündemine girmeye başlamıştır. Yeni Kavram'ın kabulü ile beraber çözülmesi gereken yeni sorunlar da devreye girmiştir. 5. Maddenin tanımlanmasının ve hangi durumlarda devreye gireceği sorunu belirsizleşmeye başlamıştır. Silahlı bir saldırıya karşı devreye sokulacak olan bu maddenin siber saldırıların, hayati zararlar verebilecek tehlikeli maddelerin

[113] Derya Gonca PEKSARI, "**NATO'nun Değişen Konsepti**", Edt: Enver BOZKURT, Asil Yay,2007,s.2

kullanılması ve enerji kaynaklarının kesilmesi gibi tehditler karşısında nasıl kullanılacağı günümüzde hala belirsiz olarak kabul edilmektedir.

Buna rağmen NATO, Cyber Defence and Management Board (CDMB) ve Military Authorities ve Communications and Information Agency gibi oluşumlar meydana getirmiştir. Bilginin yeterince hızlı ve güvenle paylaşılmadığı takdirde üye ülkelerin muhtemel NATO harekâtlarına katılımının mümkün olmayacağı anlayışı üzerine bu çalışmalar başlatılmıştır. Üye ülkelerin ağ yapısı ve askeri potansiyel farkı nedeniyle NATO Ağ ile Etkinleştirilmiş Güç Programı (Network-Enabled Capability-NNEC) ve Ağ Merkezli Savaş (NCW) için bilişim alt yapısı önemli hale gelmiştir. Bu nedenle Soğuk Savaş'ta NATO iletişim ve Enformasyon Sistemleri Ajansı (NCIA) ve Avrupa İttifak Güçleri Büyük Karargâhları Avrupa Müttefik Kuvvetleri Yüksek Karargâhı (Supreme Headquarters Allied Powers Europe-SHAPE) Teknik Merkezleri 1 Haziran 1996 yılında kurulan NATO Danışmanlık Komuta- Kontrol Ajansına NC3A'ya bırakılmıştır. Amacı, teknolojik gelişmeleri takip etmek olarak belirlenmiştir. Ayrıca, NATO operasyonlarında araştırmadan takibe, hava komuta-kontrolden füze savunmasına, elektronik harpten erken uyarı ve kontrol sistemlerine, iletişimden bilişim sistemlerine kadar birçok sahada görev yapmaktadır. NATO İstişare, Kumanda ve Kontrol Ajansı (NATO Consultation, Command and Control Agency-NC3A) yapılanması içinde siber güvenlik ve bilgi paylaşımının sağlanması için faaliyet gösteren bir bölüm de yer almaktadır.

Dönemin özellikleri ve yaşanan gelişmeler neticesinde örgüt kendini revize etmeye çalışmaktadır. NATO içerisindeki yapılar, üye ülkelerin politikalarını temel görevleri yerine getirebilecek şekilde koordine etmelerine olanak sağlar. Bu yapılar politik, ekonomik ve askeri olmayan diğer konular üzerinde olduğu kadar, ortak savunma için müşterek planların tasarlanması; askeri kuvvetlerin görev yapabilmesi için gerekli altyapı ve tesislerinin kurulması; müşterek eğitim programları ve tatbikatların düzenlenmesi konularında daimi bir danışma ve işbirliği olanağı sunar."[114]

Söz konusu yapıların, dönemin değişen özellikleri ile değişen tehdit yapılarına uygun olarak NATO tarafından ortaya çıkması muhtemel hibrit çatışmaların en önemli unsuru olan siber savaş kabiliyetini edinmek üzere toplantılar düzenlenmeye başladığı görülmektedir. "İlk aşamada askeri komuta-kontrol ağları ve sistemi siber

[114] Mehmet Ada, Hüseyin ÇAKIR, **Kuzey Atlantik Antlaşma Örgütü'nün (NATO) Siber Güvenlik Stratejisinin İncelenmesi**, Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 2017, s.637

savaş kavramının gereklerine göre düzenlenmeye başlanmıştır. NATO'nun 1998'de düzenlediği "Harekât Sistemlerine Enformasyon Teknolojilerinin Uygulanması" ve 1999'da düzenlediği " 21. Yüzyılda NATO Enformasyon Sistemlerini Korumak" başlıklı toplantıları, NATO'nun yeni döneme uyum sağlama çabasının yansımaları olarak kabul edilebilir".[115] Çünkü o yıl, Sırp hedeflerinin bombalanmasında Sırp hackerler tarafından NATO karargâhına ve üye ülkelerin askeri haberleşme sistemlerine yönelik siber saldırılar söz konusu olmuştur. NATO, Kosova'da yaşanan çatışmalar esnasında Sırp hackerler tarafından web sitelerine yapılan saldırılarla, siber tehdide maruz kalmaya başlamıştır.

1999 tarihli "Stratejik Kavram" belgesinde, teknolojinin hızla yayılmasının tehdit grupları açısından silah üretim bilgilerine erişmelerini sağlayabileceği ve bunun da karmaşık bir rakip silahlı güç oluşturacağı vurgulanmıştır. Söz konusu Belgeden, NATO'nun artık sadece devletleri değil devlet-dışı aktörleri de tehdit algısına dâhil ettiği anlaşılabilmektedir. NATO'nun Hibrit Savaş kavramını benimsediği ve tehditleri de bu çerçevede tanımladığı görülmektedir: "İlaveten, devlet ve devlet-dışı hasımlar ittifakın bilgi sistemlerine artan güveni bu tür sistemleri bozmak için düzenlenen enformasyon operasyonlarıyla sömürebilirler. Bu tür stratejileri NATO'nun geleneksel silah gücü üstünlüğüne karşı gelmek için kullanabilirler[116]

Aynı yıl Washington Zirvesi Bildirisinde "İttifak'a karşı geniş çaplı bir saldırı ihtimalinin kısa vadede gerçekleşebileceği, ittifak üyelerinin güvenliklerinin, askeri ve askeri olmayan tahmini güç birçok risklerle karşı karşıya bulunduğunu bildirilmiştir.[117] İttifakın sorumluluk alanı genişletilmiştir. Tehditler, artık yalnızca ulus-devlet seviyesinde değil ulus-altı gruplardan da beklenir ve gelir olmuştur. Değişen ve gelişen düşman, tehdit kavramları devamında ülkelerin de güvenlik politikalarının değişmesine neden olmuştur. Bu değişim global manada etkisini göstermeye başlamış uluslararası örgütler de bu değişime ayak uydurmaya başlamıştır. NATO'nun yeni güvenlik stratejisinin belirlendiği 1999 Zirvesinden hemen sonra, devlet ve hükümet başkanlarının katılımıyla Washington'da düzenlenen "21. Yüzyılda İttifak" başlıklı toplantıda, ittifak üyesi ülkelerin savunma imkân ve kabiliyetlerinin

---

[115] Salih BIÇAKCI, "**Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu**", s. 205-226.

[116] "The Alliance's Strategic Concept, 24 Nisan 1999", 23. madde, http://www.nato.int/cps/en/natolive/official_texts_27433.htm (Erişim Tarihi 12 Aralık 2011).

[117] Mustafa PULAT, " **Avrupa Güvenlik ve Savunma Politikası", Gazi Üniversitesi Sosyal Bilimler Enstitüsü Uluslararası İlişkiler Anabilim Dalı, Ankara: Yayınlanmış** Yüksek Lisans Tezi,2002, S.38

artırılması için stratejik tertiplenebilme ve hareket kabiliyetinin yükseltilmesi gerekliliği vurgulanmıştır. Bu çerçevede etkili enformasyon sistemlerine sahip olunmasının savunma gücünü arttıracağı dile getirilmiştir.[118]

Artık tehdidin açık bir "gönderici adresinin" kalmaması, bilim ve teknoloji de büyük ölçüde yaşanan gelişmenin uluslararası ilişkileri nasıl etkilediğinin göstergesi olmuştur. Uluslararası ilişkilerin önde gelen aktörlerinden olan NATO'da hem tehdit hem önlem açısından payına düşeni almıştır. Terör eylemlerinin arttığı dönem olarak kabul edilebilecek Soğuk Savaş sonrası asıl kırılma 11 Eylül ile gerçekleşmiştir.

11 Eylül sonrası, teknolojik gelişmeler de değerlendirildiğinde dijital 9/11 korkusu oluşmuş, devamında 2002 yılında Prag Zirvesinde de bu konular ele alınarak NATO'nun siber saldırılara karşı savunma birimi olarak kurulan Yükselen Güvenlik Tehditleri Bölümü'nde de siber güvenlik; terörizm ve kitle imha silahlarıyla birlikte beş önemli tehditten biri kabul edilmiştir. Ayrıca Prag Yetenek Taahhütlerinin bir parçası olarak NATO'nun yeteneklerinin siber saldırılara karşı koruyabilecek şekilde geliştirilmesi konusunda çağrıda bulunulmuştur. Bu açılardan Zirve, siber güvenlik algısı ve strateji mantığının değişiminde bir başlangıç olarak görülmektedir.

Müteakiben NATO Ağ ile Etkinleştirilmiş Güç Programı (Network-Enabled Capability-NNEC) başlatılmıştır. Programın amacı; NATO'nun askeri ve sivil unsurlarının enformasyon altyapısı aracılığıyla birleştirmesi olmuştur. Anlayış, bilginin yeterince hızlı ve güvenle paylaşılmadığı takdirde üye ülkelerin muhtemel NATO harekâtlarına etkin katılımının mümkün olmayacağı üzerine inşa edilmiştir.[119]

Bir önceki yüzyılın etkin riski olan konvansiyonel tehdidin yerini alan farklı tehditler özellikle 2002 Prag Zirvesi'nde tekrar ele alınarak Örgüt 'ün bu tehditlere yönelik alacağı önlemler ve yapacağı uygulamaları yenilemek açısından kararlar alınmıştır. Artık tehdit algısı konvansiyonelden ziyade asimetrik olarak kabul edilmiş, bu da NATO için yeni bir vizyon haline gelmiştir.

Örgütün savunma kabiliyetlerini artırmak, zararlı yazılımlarla mücadele etmek, saldırı tespiti ve olaylara müdahale ile siber tatbikatlar icra etmek maksadıyla NATO

---

[118] "An Alliance for the 21st Century' Washington Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Washington, D.C. on 24th April 1999" http://www.nato.int/cps/en/natolive/official_texts_27440.htm (Erişim Tarihi 13 Aralık 2011).

[119] The Prague Summit and NATO's Transformation, 2003 http://www.nato.int/docu/rdr-gde-prg/ rdr-gde-prg-eng.pdf (Erişim Tarihi 14 Aralık 2011).

Bilgisayar Olaylarına Müdahale Yeteneği (NATO Computer Incident Response Capability-NCIRC) programı oluşturulmuştur. Programın içeriği ile üç farklı aşama benimsenmiştir.

1- NCIRC'nin başlangıç seviyesi yeteneklere kavuşturulması (2003-2006)
2- Bilgi güvenliği kapsamında projelerin geliştirilmesi maksadıyla NCIRC'nin tam harekât yeteneğine ulaştırılması (2006-2012)
3- Yasal mevzuatı içeren siber savunma çözümleri oluşturmak. (2012-…)[120]

Müteakiben kurulan NATO Muhabere ve Bilgi Ajansı Bilgisayar Olaylarına Müdahale Teknik Merkezi (NCIA NCIRC TC) NATO'nun genel yapısı içerisinde teknik seviyede günümüzde muhabere ve bilgi sistemlerine ait tedarik, idame ve işletme görevlerini yürütmektedir.

Şekil 4.1 : NCIA Ajansı

Siber Savunma Birimi, NCIA Genel Müdürüne bağlı görev yapan Alt Yapı Servisleri Direktörlüğü altında hizmet sağlamaktadır. 29 NATO üyesi ülkenin siber savunması, merkezi olarak NCIA NCIRC Harekât Şubesi tarafından yürütülmektedir. Harekât Şubesi, siber saldırılar ve bilgisayar olayları ile ilgili önleme, tespit etme, tedbir alma ve düzeltme faaliyetlerini yürütmektedir. NATO bünyesinde kesintisiz siber güvenliğin sağlanması görevini yürütmektedir. Takip ettiği diğer bir husus NATO web sitelerinin

[120] NATO CIS Cervices Agency, "**NATO Cyber Defence Management**", 2011.

faaliyetlerinin takibi olup birçok saldırının hedefi olan NATO web sitesinin güvenlik takibini yapmaktadır.

Tehditlerin niteliği değiştikçe uygulanan metotlarda da değişim gündeme gelmiştir. NATO'da kendini buna göre uyarlamaktadır. Siber savunmanın ulusal sınırları aşan doğası nedeniyle NATO'nun siber savunma kapasitesini artıracak yeni küresel ortaklıklar ittifak tarafından desteklenmektedir. NATO hâlihazırda bilgi teknoloji firmaları olan Microsoft, Google ve IBM, Uluslararası Standartlar Birliği (International Standards Organization-ISO) ve Internet Mühendisliği Görev Kuvveti (Internet Engineering Task Force (IETF) ile işbirliği yürütmektedir.[121]

NATO'nun siber güvenliği yeni bir askeri alan olarak gördüğü ve buna yönelik savunma stratejisi oluşturmaya çalıştığı görülmektedir. Bu durum NATO'nun zirvelerinde dile getirilmektedir. Zirve bildirgelerinde, genişleyen güvenlik yelpazesi ile NATO'nun 29 üye ülkesinin hem siyasi hem de askeri liderlerinin ağ güvenliği ile kendi ülke güvenlikleri arasında direkt bir ilişki olduğu anlaşılırken bunun düşmanca eylemlere karşı korunması gerektiğinin kabul edildiği yorumu yapılabilir. Hatta söz konusu tehdit karşısında önlem almak isteyen dokuz NATO üyesi (ABD, Almanya, İngiltere, Fransa, Hollanda, İspanya, İtalya, Kanada, Norveç) 2003 yılında bilgi paylaşımı içeren bir anlaşma imzalamıştır.[122]

2004 yılında Prag Zirvesinden sonra NATO İletişim ve Enformasyon Sistemleri Servisi Ajansı (NCSA) oluşturulmuştur. Ajansın içindeki merkezlerden en önemlisi muharip unsurların "bilgi güvenliği teknik merkezi" şeklinde ifade edilebilir. Prag Zirvesi'nde alınan kararlardan biri de kritik alt yapıların terörizme karşı korunması için NATO siber savunma programının oluşturulması olmuş, NCSA siber saldırılara karşı ilk müdahaleyi yapacak unsur olarak belirlenmiştir. [123]

İttifak kendini bu şekilde döneme adapte ederken tam olarak netleşmeyen siber tehdit, 2007 yazında Estonya'da yaşanan olayların neticesinde bir tehdit olarak algılanmaya başlandı denilebilir. Üç hafta süren siber saldırı dalgası NATO'nun elektronik iletişime bağımlı toplumlarının aynı zamanda siber savunma noktasında ne

---

[121] Rex B. HUGHES, **"NATO Cyber Defence",** s.4, Nisan 2009, (Çevrimiçi) https://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf , 12.07.2014

[122] " **İnfografya: NATO'nun Siber Güvenlik Politikasında Kırılma Noktaları**" http://biltekhaber.net/infografya-natonun-siber-politikasında-kırılma-noktaları/ (Erişim: 02.12.2015)

[123] Salih BIÇAKCI, "**Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu**", s. 205-226.

kadar zayıf olduklarını göstermiştir. Estonya Savunma Bakanı Dr. Jook AAVİKSOO'nun NATO'ya ve diğer ülkelere yönelik olarak yaptığı yardım çağrısı NATO tarafından (ad hoc) yardım takımlarının görevlendirilmesi ile cevaplandırılmıştır. İttifakı siber savunma politikasını radikal biçimde ele almak ve karşı önlemlerini yeni bir düzeye taşımak noktasında harekete geçiren olay bu olmuştur denilebilir.

2007 yılında, Estonya Hükümeti ülkenin Nazi işgalinden Sovyetler Birliği tarafından kurtarılmasını temsil eden anıtın yerini değiştirmiştir. Değişim yapılan yer eskisine oranla daha geri planda ve görünürlüğü az olan bir yer olmuştur. Bu karar Estonya içindeki Rusça konuşan azınlık arasında tepki doğmasına sebep olmuştur. Bu tepkilerin devamında ise Estonya'nın önemli ekonomik ve siyasi yapılarına siber saldırıların gerçekleştiği görülmüştür. Saldırı DDoS (Distributed Denial of Service) olarak gerçekleştirilmiştir. İletişim araçlarının gelişmesi, iletişim için dijital altyapılara dayalı iletişimin artması ulus-devletler için yeni hassasiyetleri beraberinde getirmiştir. Estonya'da yaşanılan sorun bu duruma örnek oluşturan bir olay olmuştur. Uluslararası medya tarafından "ilk Siber Savaş" olarak sınıflandırılmıştır. Gayri resmi, ulus-devletten bağımsız siber milislerin ulus-devlete tehdit haline geldiğinin göstergesi olmuştur. Estonya Devlet Başkanı Toomas HENDRIK ILVES tarafından "Siber saldırılar, ulus-devletleri felce uğratmanın, zarar vermenin ve devletleri zayıflatmanın yeni saldırgan biçimidir." tanımı yapılmıştır. Beyaz Saray siber güvenlik danışmanı Howard SCHMIDT tarafından "Estonya ileri teknoloji kullanan hükümeti ve ekonomisi ile geleceğini inşa etmiş fakat bu saldırı ile işte tam da sahip oluğu bu ileri teknoloji nedeniyle dizleri üzerine çökmüştür." şeklinde yorumda bulunmuştur.[124] Resmi olarak Rus hükümeti ile bir bağı olmasa da rejimi destekleyenler tarafından kurulan 120.000 Rus üyesi olan Nashi (bizimkiler) hareketinin lideri olan dönemin Rus Parlamentosu lideri olan Sergei MARKOV'un asistanı tarafından yapılan itirafta, Estonya saldırılarının Nashi'nin de dâhil olduğu "vatansever hackleme" olarak adlandırılan bir eylem olduğu ifade edilmiştir.[125] Estonya'ya yapılan siber saldırı 22 gün sürmüş hem devler hem de özel sektör bu siber harekâttan muzdarip olmuştur.

[124] Stephen HERZOG, **Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses**, Journel of Strategic Security, Volume 4, Number 2 Summer 2011: Strategic Security in the Cyber Age, s.52
[125] P.W.SINGER, Allan FRIEDMAN, **Siber Güvenlik ve Siber Savaş,** s.153

Kosova'dan sonra Estonya saldırıları NATO için ikinci işaret olarak kabul edilmektedir. Örnek olarak kabul edilmeye başlanılan bu olay yeni ulusal stratejilerin oluşturulması ya da var olanların güncellenmesi ihtiyacını gündeme getirmiştir. Uluslararası dijital hareketlilik, siber terörizmin de dâhil olduğu ulus-devletler için tehdit alanını genişletmiştir. Bu durumun somut olarak yansıması kabul edilebilecek Estonya olayı, internetin çok güçlü bir asimetrik araç olabileceğini ve uluslararası grupların ne kadar etkin olabileceğini göstermiştir. Yaşanan saldırı sonrası NATO ve Avrupa Birliği ülkelerinde siber güvenlik ve bu gibi olaylar ile bağlantısı olabilecek ülkelere karşı nasıl bir yaptırım uygulanabilir tartışmaları başlamıştır. Yaşanan süreçte Alman yetkililer siber güvenliğin de 5. Madde kapsamına alınmasını önermiştir. Fakat kimse ölmediği ve zarar görmediği için NATO tarafından 5.madde geçerli görülmemiştir. Uluslararası kamuoyu için eğitici bir saldırı olarak kabul görmektedir. Böylece yeni teknoloji ile eskinin teknolojisi kapsamında hazırlanan uluslararası hukukun arasındaki makas görülmüştür. Carl von Clausewitz'in savaş tanımı olan "Savaş bağımsız değil, politikaların farklı araçlarla devamıdır." üzerinden gider isek savaşın siyasi yapı ile etkileşimde olduğu görülebilir. Bu doğrultuda dijital bir belirsizlikte bunun saldırı, savaş vb. olarak tanımlanmasında yine politikacıların muhakemesinin etkili olduğu söylenebilir.[126]

Estonya siber saldırısı sonrasında konuyla ilgili olarak 15 Ağustos 2007'de İngiliz raportör Lord JOPLING tarafından hazırlanan raporla, daha önce terörizm önceliğiyle yazılan 2006'daki güvenlik belgesine siber güvenlik önceliği ilave edilmiştir. Bu düzenleme, NATO'nun savaş algısının Soğuk Savaş dönemine göre ne denli farklılaştığına işaret etmektedir. Ayrıca Estonya'daki olaylar NATO'nun siber uzay politikasının üç temel ayağını belirleyen resmi bir "NATO Siber Politikasının" hazırlanmasına neden olmuş ve söz konusu Politika Ocak 2008'de kabul edilmiştir. Politikaya göre, "yerinde hizmet" adı altında talep üzerine yardım sağlanacağı aksi takdirde siber güvenliğin egemen devletlerin kendi sorumluluğu olarak kalacağı ifade edilmiştir. Ayrıca "yineleme" adı altında ise uluslararası, bölgesel ve ulusal düzeylerdeki yapıların veya yeteneklerin gereksiz yere tekrarlanmasını engellemenin amaçlandığı, güvene dayanan, erişime açılması gereken sistemle ilgili bilginin hassasiyetini ve olası zayıf noktaları göz önünde bulunduran bir işbirliğinin söz konusu olacağı belirtilmiştir.

[126] P.W.SINGER, Allan FRIEDMAN, **Siber Güvenlik ve Siber Savaş,** s. 172

Estonya saldırıları ile aynı yıl Amerikan askeri bilgisayar sistemleri, görülen en ciddi saldırıya maruz kalmıştır. Ortadoğu'daki bir askeri üste askeriyeye ait bir dizüstü bilgisayara bağlanan basit bir USB aygıtı ile casus yazılım hem gizli hem de gizli olmayan sistemlere yayıldığı görülmüştür. Bu örnekler tehdidin ne kadar ciddi olduğunun görülmesine ve uluslararası kamuoyunun dikkatinin siber tehdit-güvenlik üzerine kaymasında etkin olmuştur.

2008 yılında icra edilen Bükreş Zirvesi'nde İttifak, "siber ikilemi" zirve çerçevesine dâhil etmiştir. Çünkü NATO Siber Savunma Politikası kabul edilmiştir. Ayrıca Brüksel merkezli Siber Savunma Yönetimi benimsenmiştir.[127] Bu şekilde siber savunma operasyonlarının merkezi hale getirilmesi hedeflenmiştir. Siber güvenlik konusunun kapsamlı bir biçimde ele alındığı ve Sonuç Bildirgesi'nde özel bir yer edindiği ilk Zirve olması açısından Bükreş Zirvesi önemlidir.[128]

Bükreş Zirvesi Liderleri Bildirisi 47. Bölümde, İttifakın bilgi sistemlerini siber saldırılara karşı güçlendirme, karşı yeteneklerin geliştirilmesi kararlığı ifade edilmiştir.[129] Bükreş Zirve'si sonrasında siber güvenlik alanında iki önemli gelişme yaşanmıştır. İlk olarak Brüksel'de bir NATO Siber Savunma Yönetimi Otoritesi'nin (Cyber Defense Management Authority-CDMA) kurulmasına karar verilmiştir. NATO siber savunma fonksiyonel yapılanması içinde CDMA, ihtiyaç olması halinde hızlı ve etkili bir siber savunmanın başlatılmasından ve koordine edilmesinden sorumluyken NATO Siber Savunma Yönetim Kurulu (NATO Cyber Defence Management Board-CMDB) Örgüt'ün siber savunma politikasını hayata geçirmek, üye ülkelerin herhangi birine karşı gerçekleştirilen siber saldırı durumunda gereken önlemleri almaktan sorumlu olarak oluşturulmuştur. Diğer birimler ise NATO'nun siber savunma faaliyetlerinin koordinasyonunu sağlayan NATO Siber Savunma Koordinasyon ve Destek Merkezi (Cyber Defence Coordination and Support Center, CD-CSC) ve İttifakın siber savunma hizmetlerinin geliştirilmesi, uygulanması ve idamesinden sorumlu olan NCIRC[130] Teknik Merkezidir.[131]

---

[127] NATO, Bucharest Summit Declaration, http://www.nato.int/cps/en/natolive/official_texts_8443.htm (20 Nisan 2012)
[128] Salih BIÇAKCI, "**Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu**", s. 205-226.
[129] Rex B. HUGHES, **"NATO Cyber Defence"**,s.1
[130] NCIRC; NATO'nun siber saldırı ve suçlarla mücadele merkezi olarak tüm NATO bilgi sistemlerinin siber savunmasından sorumludur.
[131] Hasan ÇİFTÇİ, **Her Yönüyle Savaş,** s. 54

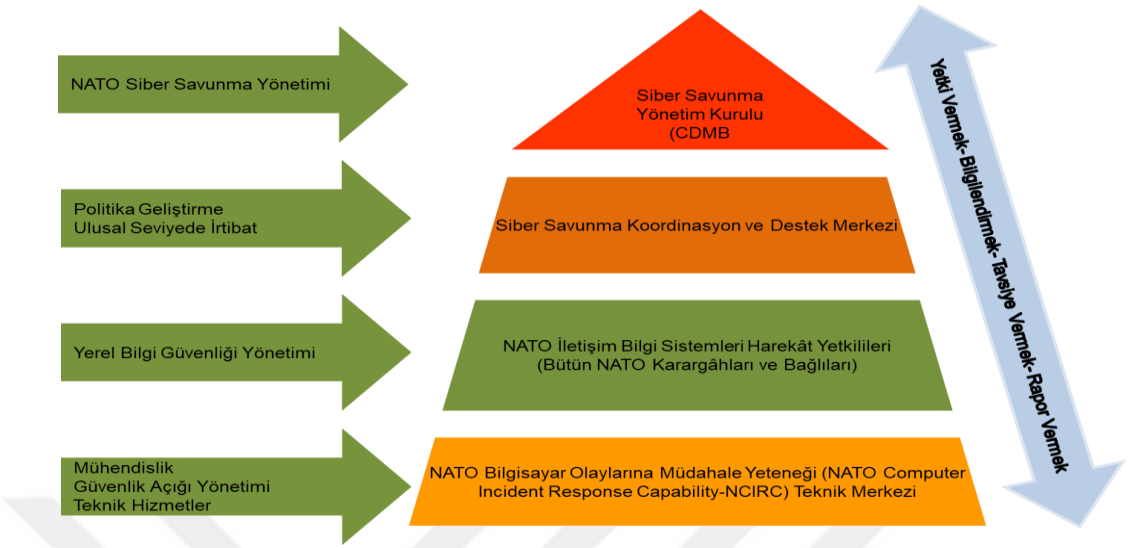
Siber savunma kapasitesini bir merkezde toplayarak harekât kabiliyetini daha arttırmak isteyen NATO, bununla yetinmeyerek Estonya Tallinn merkezli bir NATO Siber Savunma İşbirliği Mükemmeliyet Merkezi (Cooperative Cyber Defence Centre of Excellence–NATO CCD COE) kurmuştur. Brüksel'deki söz konusu merkez İttifakın siber savunma harekât kabiliyetlerine yönelik çabalarının merkezileştirilmesini temsil etmektedir. Büroyu oluşturan yapı, üyelerin bir saldırı durumunda yapılacakların koordine edildiği merkezdir. Siber savunma kapsamında NATO'nun attığı büyük adımlardan biri olan gerçek zaman harekât kapasitesi söz konusu yönetim tarafından oluşturulmuştur.

Diğer bir adım ise, Estonya merkezli Kolektif Siber Savunma Mükemmeliyet Merkezi ile siber savunma kapsamında uzun dönem doktrinel ve stratejik düşünce çalışmalarını içeren entelektüel forum olarak oluşturulmasıdır. Merkez, Estonya Savunma Bakanlığı'nın NATO'ya bu türde bir merkezin kurulması için 2007 saldırıları öncesinde teklif vermiş olmasına rağmen ancak Ekim 2008'de kurulabilmiştir. 30 personelden oluşan Merkez'in görevleri şunlardır:

1. Siberle ilgili konularda ittifak için doktrinler ve kavramlar üretmek;
2. NATO'ya üye ülkeler için eğitim kursları, atölye çalışmaları düzenlemek. Tatbikatlar yapmak;
3. Araştırmalar yapmak ve gelişmeler üzerine toplantılar düzenlemek;
4. Geçmişteki ve hâlihazırdaki saldırıları çalışarak dersler çıkarmak;
5. Devam eden saldırılarda eğer istenirse tavsiyeler vermek[132]

2008 yılından itibaren yaşanabilecek benzer durumlara hazırlıklı olmak adına ulusal ve uluslararası unsurlar arasında iş birliği ve koordinasyon süreçlerinde iç ve/veya uluslararası hukukun uygulanması yönünde analizleri de içeren NATO Siber Güvenlik Tatbikatları "NATO Cyber Coalition " adı altında icra edilmeye başlanmıştır Üye ülkeler, Nisan 2009'da Strazburg/Kehl'de yapılan zirvede yeni siber savunma stratejilerinin geliştirilmesini talep etmişlerdir. Bu tartışmalar neticesinde siber savunmanın NATO tatbikatlarına dâhil edilmesine ve NATO ile üye ülkeler

[132] 173 DSCFC 09 E bis - NATO and Cyber Defence, 2009, http://www.nato-pa.int/default. Asp?SHORTCUT=1782 (Erişim Tarihi 13 Aralık 2011).



Şekil 4.2: Siber Güvenlik Fonksiyonları

arasındaki bağın siber tehditlere karşı güçlendirilmesine karar verilmiştir. Zirvede yayınlanan bildiride yeni tehlike ve risklerle karşı karşıya kalınabilineceği dile getirilmiştir. NATO'nun oluşturduğu birimler ile Siber Güvenlik Fonksiyonları aşağıdaki şekilde ifade edilebilir:

2011 yılında üye ülkelerin savunma bakanları tarafından onaylanan Siber Savunma Siyasası ile ihtiyaç halinde üye ülkelere hızlı bir şekilde yardım etmek maksadıyla Hızlı Tepki Takımları (RRT) kurulmasına karar verilmiştir. Takımların ilgili üye ülke tarafından çağrı yapıldığında saldırıya uğrayan ülkenin komutası altında çalışması öngörülmüştür.[133] Tam anlamıyla 2012'de aktif hale gelmiş olan bu takımlar; üye ülkelerdeki uzmanlardan ve NATO çalışanlarından oluşmaktadır. Takımların ilgili üye ülke tarafından çağrı yapıldığında saldırıya uğrayan ülkenin komutası altında çalışması öngörülmektedir. Donanım ve yazılıma bağlı olarak siber tehditlerin her gün kendini yeniliyor olması ona karşı koymak için organize olan güçleri zor durumda bırakmaktadır. NATO'nun, bütün bu yeniliklere rağmen, tehdidin hızlı değişen tarzı nedeniyle karşılık vermede yeteri kadar hızlı olmadığı hala tartışılmaktadır.[134]

---

[133] NATO, "**NATO Rapid Reaction Team to fight cyber attack**", http://www.nato.int/cps/en/SID-163341AC-07A0EF3D/natolive/news_85161.htm, (Erişim: 10 Mayıs 2013)

[134] Salih BIÇAKCI, "**Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu**", s. 205-226.

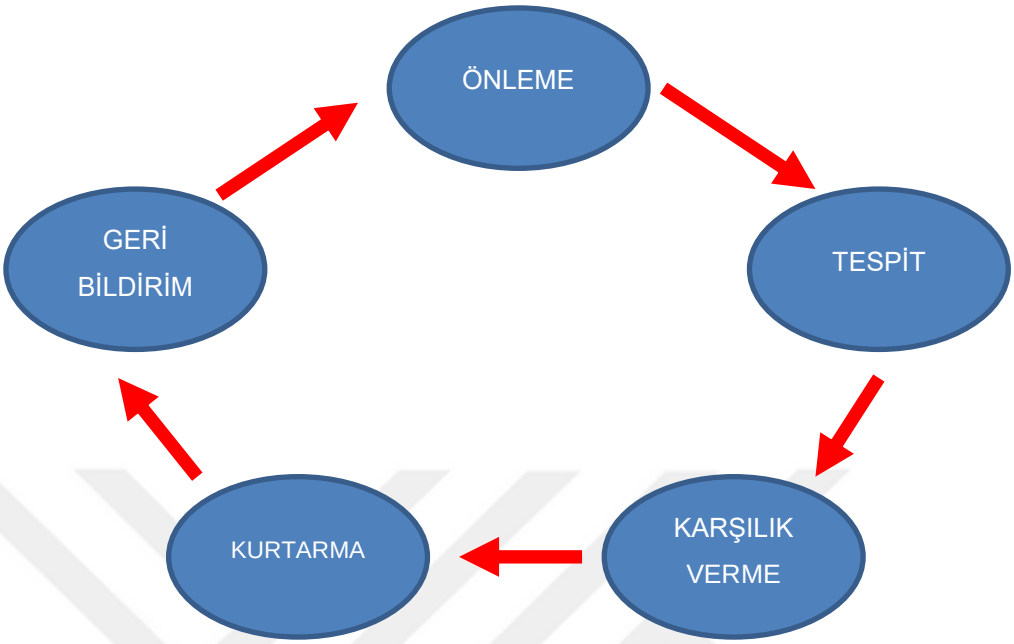
Gerçekleşebilecek herhangi bir siber saldırı, ittifak anlaşmasının 4. ve 5. Maddeleri çerçevesinde saldırı sayılacağı için meselenin ortak güvenlik kavramı şemsiyesi altında değerlendirile bilineceği, Zirve'de ifade edilen diğer bir nokta olmuştur. Ayrıca Zirveyi müteakip NATO karargâhında görevlendirilen 43 uzmanın, üye ülkelerle siber savunmanın hukuki yönleri konusunda görüşmeler yapmaya başlaması, NATO stratejisinin geliştiği yönü göstermektedir.[135] Siber güvenlik kapsamında Stratejinin altyapı teşkil edecek raporun hazırlanması maksadıyla Başkanlığını ABD eski Dışişleri Bakanı Madeleine K. ALBRIGHT'ın yaptığı bir grup oluşturulmuştur. Grup raporunu NATO Genel Sekreterine 17 Mayıs 2010'da sunmuştur. Raporda gelecek yıllarda karşılaşılacak başlıca tehditler arasında siber saldırılar da vurgulanmıştır. Zirvede ayrıca siber saldırıların hangi hukuk esaslarına göre değerlendirileceğinin belirsiz olması ve bu konudaki uluslararası hukukun gelişmemiş olması ittifak üyelerinin siber savunmasını zayıflattığı, NATO'nun bu tarihe kadar gösterdiği bütün çabalara rağmen siber savunma kapasitesinde önemli boşluklar olduğu ifade edilmiştir.[136] Bu çerçevede, ittifakın ani bir siber saldırıyla karşı karşıya kalması durumunda, Genel Sekreter ya da NATO komutanlarından birinin karşılık vermek üzere görevlendirilmesi talep edilmiştir. Böylece saldırı gerçekleşirse karşılığı verecek ekibin üst düzeyde yönetilmesi gerektiği üzerinde durulmuştur. Raporda:

- NATO'nun kritik ağları takip etme gücü arttırmalı ve tanımlanmış bütün zayıflıklar sağlamlaştırılması,
- Siber Savunma Mükemmeliyet merkezi daha fazla eğitim yaparak ittifak üyelerinin siber savunma programlarını geliştirilmesi,
- İttifak üyeleri, NATO genelindeki alıcıları ve ağ düğümlerini (node) izleyerek erken uyarı kabiliyetlerini arttırması,
- İttifak, büyük siber saldırı yaşayan ya da bu tehdidi hisseden üyelerine uzman takımı göndermesi tavsiye edilmiştir.

---

135 **"Strasbourg/Kehl Summit Declaration, 04 Nisan 2009**", http://www.nato.int/cps/en/natolive/ news_52837.htm?mode=pressrelease (Erişim Tarihi 19 Aralık 2011).

136 "NATO 2020: Assured Security; Dynamic Engagement", s.17, http://www.nato.int/strategicconcept/expertsreport.pdf (Erişim Tarihi 18 Aralık 2011).



Şekil 4.3 : NATO Siber Güvenlik Döngüsü

NATO içinde bütün bu değişim ve dönüşümler gerçekleştirilirken 2010 yılının Haziran ayında İran'ın nükleer programına saldıran "Stuxnet" adlı yazılım ile birlikte uzmanların 2001'den beri yaptığı uyarıların gerçekleştiği görülmüştür. Söz konusu saldırı soyut olarak ifade edilen tehlikelerin somutlaştığı önemli bir örnek olmuştur. Aslında NATO, ciddi boyutta bir siber saldırı ile ilk defa Kosova krizinde karşılaşmasına, İttifak'ın e-posta hesabı günlerce ziyaretçilere kapalı kalmış olmasına ve NATO web sitesi sık sık kesintiye uğramasına rağmen bu sıkıntılar bir siber saldırı olarak değerlendirilmemiştir.

Bu doğrultuda 2010 Lizbon Zirvesinde "Stratejik Kavram" yeni şekliyle kabul edilmiştir.[137] Kabul edilen Yeni Kavram'te siber saldırı tehdidi vurgulanmıştır.[138] 1999'daki Kavramte böyle bir tehdit söz konusu değildi. İttifak, 1999 yılında Washington Bildirisi'nde;

---

[137] NATO, **Lisbon Summit Declaration**, http://www.nato.int/nato_static/assets/pdf_2010_11/2010_11_11DE1DB9B73CF9BBFB52B2C94722EAC_PR_CP_2010_0155_ENG-Summit_LISBON.pdf (12 Ocak 2014)

[138] **The Allience Strategic Consept for Defence and Security of the Member of the North Atlantic Treaty Organisation by the Heads of State and Government in Lisbon: Active Engagement, Modern Defence**, http://www.nato.int/lisbon2010/strategic_concept_eng.pdf 30 Haziran 2014

- Hiçbir ülkenin bir diğerine tehdit ya da güç kullanımı ile baskı yapamayacağı, anlaşmazlıkların çözümü için demokratik kurumların geliştirilmesini sağlamak,

- Üyelerin güvenliğini, hayati menfaatlerini etkileyen konularda müttefikler arası danışmalar ve ortak endişelerin olduğu konularda forum ortamını temin etmek görev olarak sayılırken;

- Devlet ve devlet-dışı tehditlerin, İttifak'ın bilgi haber sistemlerine karşı artan güvenini, bu sistemleri bozmak üzere planlanmış olan harekâtlar söz konusu olabilir diyerek 21.yy stratejik ortamı ve getirdiği tehditler de dile getirilmiştir.[139]

2010 yılı Kavraminde İttifak için "Aktif Sorumluluk", "Modern Savunma" kavramları üzerinden siber saldırılar Avrupa- Atlantik güvenliği ve istikrarına tehdit olarak ifade edilmiştir.[140] 2010 Lizbon Zirvesi'nde ise, Haziran 2011 tarihine kadar kapsamlı siber savunma planı geliştirilmesi kararı alınmıştır.

Son yıllarda yaşanan siber saldırılar büyük servetlerin ve sıkı korunan ulusal sırların, kimliği belirsiz ve kötü niyetli kişilerin eline geçebildiğini göstermiştir. Bu tehlikeler göz önüne alınarak 2011 yılında Siber Savunma Kavrami kabul edilmiştir.

2012 Chicago Zirvesinde üzerinde durulan kilit noktalardan biri büyük bir siber saldırının sadece bilgi sistemlerini değil bu siber alan ile bir birine bağlı hükümetlerin bütün kurumlarını bunun dışında özel sektörü etkileyeceği olmuştur. NATO'nun kritik alt yapıları koruma anlayışı, ortak çaba ve dayanışma şeklinde vurgulanmıştır.[141] Bu kapsamda 2013 yılında Danimarka, Hollanda, Kanada, Norveç ve Romanya işbirliğini artırmak adına Çokuluslu Siber Savunma Kapasitesi Geliştirme Projesini başlatmıştır.

2014 yılında Galler Zirvesinde ise Genişletilmiş NATO Siber Savunma Politikası ve Siber Savunma Eylem Planı kabul edilmiş, NATO Genel Sekreteri Fogh RASMUSSEN tarafından "NATO müttefiklerini siber tehditlerin de dâhil olduğu tüm tehditlerden korumayı taahhüt etmektedir." vurgusu yapılmıştır. Zirvede ayrıca NATO ülkeleri tarafından etkileri silahlı saldırı boyutunda olan siber saldırı kapsamında ittifakın kolektif savunma şemsiyesi olan 5. Maddenin kullanılmasının talep

---

[139] Musa CEYLAN, **"YENİ NATO SOĞUK SAVAŞ'TAN SICAK SAVAŞA",** Ülke Kitapları, Kasım 1999,s.187-191

[140] Kenneth GEERS, **Strategic Cyber Security: Evaluating Nation-State Cyber Attack Mitigation Strategies with DEMATEL,** s.35

[141] **Critical Infrastructure Protection Against Terrorist Attacks**, Course Report, NATO COE DAT, Ankara,2014

edilebileceği dile getirilmiştir.[142] Söz konusu Zirve 5. Maddenin vurgulandığı ilk zirve olması açısından önemli kabul edilmektedir.

CCDCOE tarafından 2016 yılı içinde "Siber Normlar Dokümanı" hazırlanmıştır. Söz konusu normların belirlenmesi uluslararası siber güvenliğin güçlendirilmesi önemli olduğu değerlendirilebilir. Konunun uluslararası aktörleri (devletler, uluslararası örgütler, sivil firmalar, üniversiteler, vb.) bu alanda dayanışmanın gerekli olduğu konusunda hem fikir olmalarına rağmen, bugüne kadar normların oluşturulması yönünde gerekli adımların atılamadığı görülmüştür.

Yine aynı yıl NATO Siber Ortaklık (NATO Industry Cyber Partnership-NICP) çerçevesinde NATO Muhabere ve Bilişim Kurumu (NATO Communication and Information Agency-NCI) ile FORTNET firması anlaşma imzalamıştır. Özel firma ile yapılan anlaşmadan genel beklenti; NATO'nun siber savunmasını güçlendirmek, siber saldırı tehdidi altında kazanılan tecrübe bilgi ve uzmanlığın paylaşılması, siber olay durumunda etkili ve yeterli desteği sağlamak olarak ifade edilebilir

Fakat en büyük adımlardan biri olarak görülebilecek hareket, 08-09 Temmuz 2016 tarihlerinde gerçekleştirilen NATO'nun Varşova Zirvesinde, NATO üye ülkeleri kara, deniz, hava ve uzaydan sonra siber ortamın da yeni bir harekât alanı olarak resmen kabul edilmesi olmuştur. Devlet Başkanları tarafından Siber Savunma Taahhüdü imzalanmıştır. Taahhüt kapsamında NATO tarafından ülkelerin siber güvenlik seviyelerini ölçme amacıyla öz denetim kriterleri belirlemiş ve ülkelerin kendilerini değerlendirmelerini talep etmiştir.

[142] Piret PERNIK, **Improving Cyber Security NATO and EU,** International Centre for Defence Studies, Tallinn, 2014 s.2-6

Bölüm	Yer	Zaman
Siber saldırılara karşı yeteneklerimizi güçlendirmeliyiz.	Prag Zirvesi Deklarasyonu	2002
Güvenliğimize karşı gerçek tehditler; bölgesel istikrarsızlıklardan çoğalabilecek balistik füze ve nükleer teknoloji, biyolojik ve kimyasal etkenler, terörizm, **siber savaş**, organize suçlar, sınır tanımamazlık…	NATO Genel Sekreteri Konuşması, Varşova	2002
Bilgi paylaşımını ve istihbarat paylaşımının operasyonlarda gecikmemeye neden olmadan ve güvenle paylaşımı için NATO Müşterek Ağ Kapasitesini geliştirirken ana bilgi sistemlerimizin korumasını **siber saldırılara** karşı artırmalıyız…	Riga Zirvesi Deklarasyonu	2006
Klasik askeri tehditlerin içinde yeni bir çeşit tehdit belirmiştir. **Siber Saldırı… Siber Saldırılar** enerji sistemlerini, banka sistemlerini ve devlet kurumlarının hizmetlerini ele geçirebilir. Saldırılar **siber alanda** gerçekleşirken etkileri gerçek hayatta hissedilir…	NATO Konuşması, Londra	2007
NATO, ittifakın bilgi sistemlerini siber saldırılara karşı güçlendirme taahhüdünün arkasındadır. **Siber Savunma Siyasasını** oluşturduk, yapı ve yönetimini geliştirmeye devam edeceğiz. Bizim Siber Savunma Siyasamız üye ülkelerin **siber saldırıya** uğraması durumunda isteği doğrultusunda NATO ve üyelerinin bilgi sistemlerinin korunması, tecrübe paylaşımı ve kapasite desteği sağlamak ve karşılık vermesine destek olmak…	Bükreş Zirvesi Deklarasyonu	2008
Siber Savunma yeteneklerini artırmak konusunda hemfikir kalınmıştır.	Lizbon Zirvesi Deklarasyonu	2010

Siber tehditler hızlı şekilde evrilmektedir. Bu nedenle siber uzaya sürekli entegre kritik altyapı sahibi olarak modern savaşın siber boyutunu içeren NATO Doktrini oluşturulmalı ve siber saldırılara yönelik önleyici, savunan ve sonrasında iyileşmeyi içeren sistem İttifak için çok gereklidir…		
Siber saldırılar, gelişerek ve daha kompleks bir yapıda hızla artmaktadır. Lizbon Zirvesindeki taahhütlerimizi yeniden onaylıyoruz. 201 Yılında Siber Savunma Kavramini kabul ettik. NATO'nun var olan yeteneklerini ve kullanıcılarını koruma amaçlı NATO Bilgisayar Olaylarına Müdahale Yeteneği (NATO Computer Incident Response Capability-NCIRC) 2012 yılı sonunda devreye girecektir… Siber savunma önlemleri, ittifakın yapısı ve prosedürleri ile entegre edilecek, İttifakın işbirliği ve birlikte çalışabilirliğini güçlendirmek amacıyla ulusal siber savunma yetenekleri dağıtımına devam edilecektir…	Chicago Zirvesi Deklarasyonu	2012
İttifak olarak geleceğe baktığımızda siber tehdit ve saldırıların daha genel, gelişmiş ve potansiyel zarar verici olacağını görmekteyiz… Siber Saldırılar ulusal ve Avrupa-Atlantik refahını tehdit edebilir. Olaylar tek tek incelenmek üzere bir siber saldırı durumunda Kuzey Atlantik Konseyi 5. Maddeyi devreye sokabilir. Güçlü ortaklık siber tehdit ve risklere karşı önemli bir rol oynamaktadır…	Galler Zirvesi	2014

NATO'nun siber savunma eğitim ve tatbikat aktivitelerinin seviyesini artıracağız…		
NATO üye ülkeleri kara, deniz, hava ve uzaydan sonra siber ortamın da yeni bir harekât alanı olarak resmen kabul edilmiştir. Devlet Başkanları tarafından Siber Savunma Taahhüdü imzalanmıştır. Taahhüt kapsamında NATO tarafından ülkelerin siber güvenlik seviyelerini ölçme amacıyla öz denetim kriterleri belirlemiş ve ülkelerin kendilerini değerlendirmelerini talep etmiştir.	Varşova Zirvesi	2016

Tablo 4.1: İttifak'ta Zamansal Olarak "Siber" Kavramsallaşması

ÜÇÜNCÜ BÖLÜM

NATO'NUN KOLEKTİF GÜVENLİK ANLAYIŞINDA SİBER BOYUT

Alınmaya çalışılan önlemler ile saldırıların önüne geçilmeye çalışılsa da siber terörizmde saldırının nereden geldiğini tespit etmek ve nasıl bertaraf edileceğini çözümlemenin hiç kolay olmadığı görülmektedir. Ayrıca durumun vahametini ifade eden terör uzmanı Walter Laqueur " …elektronik saldırılarla daha etkili ve kalıcı zarar verme imkânı varken neden insanları veya politikacıları öldürsünler" demiştir.[143]

Mary Kaldor, iletişim araçlarının yaygınlaşmasıyla küçülen dünyamızda sığınmacı akımlarını sistemik tecavüzlerin ve ulus-ötesi suç örgütlerinin savaş ortamında görülmeye başlamasını yeni bir savaş tipi olarak kavramsallaştırmıştır. Siber alanı ve iletişim teknolojisini ayrı bir savaş alanı olarak tanımlamıştır.[144] Sanallaşan bir savaş kavramı olarak değerlendirilebilinecek bu görüş, internetin sivilleşmesinden sonra ortaya çıkan siber uzayın oluşturduğu yeni durumda asimetrik mücadeleyi de pekiştirmektedir[145]. Her ne kadar yaşanan bu tehlikenin arkasında kimlerin olacağının bulunması zor olsa da günümüzde hala siber alandaki en tehlikeli oyuncular ulus devletler olarak ifade edilmektedir. Çünkü bu şekilde bir saldırı gerçekleştirecek veya gerçekleştirmek için geçerli bir nedene sahip olabilecek "terörist gruplardan" bahsedilmemektedir. Bunun yanında teknolojinin etkisi ile organize suç ağlarının saldırı yetenekleri giderek artmaktadır. Bu noktadan değerlendirildiğinde uluslararası ortak bir terör tanımının olmaması siber olayların da terörizm kapsamına alınmasını zorlaştırmaktadır. Dolayısıyla da siber etki alanında casusluk ve sabotaj gibi noktalarda gelişmeler yaşansa da hala bir ulus devlet "üssüne" ihtiyaç olduğu gerçeği genel kabul görmektedir.

---

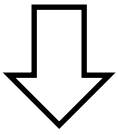
[143] Walter LAQUEUR,**"Post Modern Terorism"**, Foreign Affairs, C.75, No:5, Eylül-Ekim, 1996, s.35

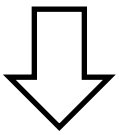
[144] Mary KALDOR,**New and Old Wars: Organised Violence in global era,** 3rd ed. 2012,Cambridge: Polity Press, s. 65,

[145] Mary KALDOR, **In Defence of New Wars**, Stability, 2013, 2(1):4, s.13 , http://dx.doi.org/10.5334/sta.at

Yeni savaş olarak da nitelenen bu yeni durum Soğuk Savaş sonrası kendi varlığına meşru dayanaklar arayan NATO'nun da "Yeni Stratejik Kavram"ına dâhil edildiği farklı Zirveler ve raporlarda görülmektedir. NATO'nun gözden geçirilmiş siber savunma politikasında siber tehditler "Yeni Stratejik Kavram" doğrultusunda 5.maddede ifade edilen toplu savunma görevini yerine getirmesi için potansiyel kaynak olarak tanımlanmaktadır. Bu düşünce Henry KISSINGER'ın NATO'yu "Kuzey Atlantik Sınırları dâhilindeki ulusların politikalarını uyumlaştıran en üst düzeyde bir siyasi yapı" olarak tanımlamasından hareketle hala varlığını devam ettirmektedir. Bu nedenle NATO varlığını konjonktüre uygun hale getirmeye çalışmaktadır. Fakat hala Siber Savaş olarak ifade edilen mücadelenin tanksız, topsuz gürültüsüz yapısı gibi özelliklerinin yanında kaynağının belirsizliği önemli bir problem olmaktadır.

Article 4 (Danışma)	Article 5 (Kolektif Savunma)
The Parties will consult together whenever, in the opnion of any of them, the territorial integrity, political independence or security of any of the parties is threatened.	- The Parties agree that armed attack against one or more of them in Europe or North America shall be considered an attack against them all and consequently they agree that, if such an armed attack occurs, each of them, in exercise of the right of individual or collective self-defence recognised by Article 51 of the Charter of the UN, will assist the Party or PArties so attacked by taking forthwith, individually and in concert with the other Parties, such actions as it deems necessary, including the use of armed force, to restore and maintain the security of the North Atlantic area. - Any such armed attack and all measures taken as a result of thereof immediately be reported to the Security Council. Such measures shall be terminated when the security Council has taken the measures necessary to restore and maintain internaitonal peace and security.





-Müttefiklere görüş ve bilgi teatisi verir. -Karar almadan ve harekete geçmeden önce konuları tartışma olanağı sağlar -Askeri çatışmayı önlemek için gerekli araçları sağlayarak önleyici diplomaside NATO'ya aktif rol verir -Herhangi bir ülke 4'üncü Maddenin işletilmesini talep edebilir. -Bu Maddenin işletilmesi kararlaştırıldığında, konu tartışılır ve İttifak adına müşterek bir karar veya eyleme geçilebilir. -NATO Anlaşmasının 4'üncü Maddesi, 5'inci Maddenin ilanına bir "ön hazırlık" niteliği taşımakla birlikte, bir ön koşul değildir.	- 5'inci Maddenin ilanı ile her Müttefik hangi şartlarda hangi desteği sağlayacağına karar verir. - Bu destek askeri olmak zorunda değildir ve her ülkenin imkân kabiliyetine bağlıdır. Bu nedenle, desteğin niteliği her ülkenin kendi değerlendirmesine bırakılmıştır.
4'üncü Maddenin İşletilmesi (5 Kez) -19 Şubat 2003: Irak'taki gelişmeler kapsamında Türkiye'ye destek -26 Haziran 2012: F-4 Türk Uçağının Suriye tarafından düşürülmesi 03 Ekim 2012: Suriye'den Türkiye'ye yapılan havan atışı 04 Mart 2014: Ukrayna'daki gelişmeler kapsamında 28 Temmuz 2015: Türkiye'deki DEAŞ ve PKK saldırıları kapsamında	**5'inci Maddenin İşletilmesi (1 Kez)** 12 Eylül 2001: İttifaf ABD talebi üzerine, 5'inci Maddenin işletilmesine karar vermiştir. (saldırının ABD dışından yapıldığı şartıyla) 02 Ekim 2001: NATO Konseyi, 11 Eylül saldırılarının ülke dışından yönetildiğine karar vermiştir. 04 Ekim 2001: NATO, ABD'ye destek kapsamında sekiz tedbiri belirlemiş ve uygulamaya koymuştur.

Tablo 4.2: NATO Antlaşması 4. ve 5. Madde Karşılaştırması

Klasik savaş tanımlarının yetersiz kaldığı yeni siber terör faaliyetlerinden önce Beril DEDEOĞLU'nun savaş ifadesinin nitelikleri incelenirse;

- Diğer yöntemler ile çözümlenemeyen bir durumun var olduğu,
- Radikal bir çözüm yolu olarak şiddet uygulanması kararının alınması,
- Silahların organize kullanılması,
- Siyasal bir eylem ve araç olması,
- Bir geçmişi ve geleceği olması,
- Başarının sadece askeri ve operasyonel başarılara indirgenemeyeceği,

- Yüksek maliyetli olduğu,
- Egemenler tarafından belirli ideallerle şekillendirilmiş katılımı yüksek bir eylem olduğu,
- Hasmın iradesini engelleme ve ona kendi iradesini kabul ettirmeyi içerdiği,
- Güç kullanma tekeli devlette olmakla birlikte her türlü siyasal otoritenin şiddet uygulaması,
- Genel mantığı olarak ekonomik kaynakları ve stratejik olanakları ele geçirerek genişlemeyi hedeflediği,
- Savaşan tarafların kendilerine müttefik aramaları,
- Ulusal ya da uluslararası değişimleri hızlandırması[146]

şeklinde sıralandığı görülebilir. Ancak siber savaş ifade edildiğinde bu özelliklerin neredeyse hiçbiri ile kesişmediği görülmektedir. Bu kesişme yoksunluğu herhangi bir saldırı durumunda karşılığında uygulanması gereken kaidelerin ne olacağı belirsizliği nedeniyle tartışmaları körüklemektedir.

Konvansiyonel savaşın niteliklerine göre şekillenen Silahlı Çatışma Hukuku ve uluslararası hukukun söz konusu saldırılar karşısında yetersiz kalması ulus-devletleri önce güvenlikleri konusunda ne yapmaları daha sonra saldırıya karşı nasıl bir cevap vermeleri hususunda meşruiyet tartışmalarının içine sokmaktadır. Çünkü siber saldırıların boyutları, kaynağı, devlet desteği ile mi yoksa ayrı çalışan aktörler tarafından mı gerçekleştirildiği gibi hususlarının tespitinin zor ve genelde imkânsız olması kısır döngüyü devam ettirmektedir.

Siber saldırıların hangi hukuk esaslarına göre değerlendirileceğinin belirsiz olması ve bu konudaki uluslararası hukukun gelişmemiş olmasının ittifak üyelerinin siber savunmasını zayıflattığına her tartışmada vurgu yapılmaktadır. Ayrıca bu durumun aynı Soğuk Savaş dönemindeki gibi bir süreci de beraberinde getireceği ifade edilmektedir. Çünkü teknoloji çok hızlı ilerleyen yapısı nedeniyle tehdit-savunma boyutunda yeni bir "dehşet dengesini" beraberinde getirmektedir. Asıl sorun NATO'nun sahip olduğu yapısı ve özelliklerinde her ne kadar değişiklik yapılsa da buna ayak uydurup uyduramayacağıdır. "NATO'nun hedefi artık "en kötüyü" önlemek değil, Avrupa-Atlantik bölgesi için yeni bir güvenlik mimarisinin sağlanması suretiyle, "en iyiyi gerçekleştirmek" olarak ifade edilmeye başlanmıştır.

[146] Beril DEDEOĞLU, "Savaş", **Uluslararası İlişkiler Giriş Kavram ve Teoriler,**(ed. Haydar ÇAKMAK), Ankara, Platin Basın Yayın Dağıtım, 2006, s.25-30

NATO Antlaşması 5. Madde kapsamını daha geniş bir çerçevede ele alarak doğrudan bir NATO üyesine saldırı gerçekleşmediği durumlarda da krizlere müdahale edebileceğini kabul etmiştir. Yani hem ittifak toprakları dışında hem de 5. Madde kapsamı dışındaki operasyonlarda bulunabileceğini ifade etmiştir. Bu anlayış silahlı bir saldırı sonucu BM Yasasının 51. Maddesi kapsamındaki bireysel ya da toplu öz savunma hakkına dayandırılmaktadır. 11 Eylül saldırıları sonucunda "tek bir üye ülkeye yapılan saldırı bütün NATO ülkelerine yapılmış sayılır" anlamına gelen 5.madde ilk defa uygulanmıştır.

Soğuk Savaş'ın sona ermesi ile somut tehdidi ortadan kalkan NATO'nun sona erdirilmesi gereken bir oluşum olduğu tartışılmaktayken örgüt kendini yeniden tanımlama ve varlık nedenini yenileme çabası içine girmiştir. Konjonktüre göre yenilenme ve yeni strateji oluşturma amacıyla NATO'nun üyelerinin güvenliğini sağlamak için risk oluşturabilecek muhtemel gelişmelere ve müttefiklerin ortak endişe alanlarına yönelik gerekli koordinasyonu sağlayacak Atlantik ötesi bir forum kazanması gerekliliği kabul edilmiştir. Ayrıca onlara yönelik "herhangi bir" saldırı tehdidine karşı ortak savunma ve caydırıcılık sağlanması kararları alınmıştır. Etnik çatışmalar, bölgesel sorunlar vb. dışında çağın getirdiği teknolojik tehditler de ittifakın gündemine girmeye başlamıştır. Bununla beraber NATO, yeni kurumlar oluşturarak ve var olan kurumlarını da bu yönde değiştirmeye başlayarak sürece ayak uydurmuştur.

Özellikle bilginin yeterince hızlı ve güvenle paylaşılmadığı takdirde üye ülkelerin muhtemel NATO harekâtlarına katılımının mümkün olmayacağı düşüncesi üzerine bu oluşumlar meydana getirilmiştir. Örgütün kurumları içinde bu değişimler ve yeni oluşumlar gün geçtikçe daha gözle görülür hale gelmektedir. Bunlar gerçekleşirken yeni tartışmalar gündeme gelmeye başlamıştır. 5.maddenin, yani kolektif güvenlik tanımlamasının hangi durumlarda devreye gireceği sorunu belirmiştir. Silahlı bir saldırıya karşı devreye sokulacak olan bu maddenin, siber saldırıların, hayati zararlar verebilecek tehlikeli maddelerin kullanılması ve enerji kaynaklarının kesilmesi gibi tehditler karşısında nasıl kullanılacağı belirsizlik olarak değerlendirilmeye başlanmıştır. 2009 Starsbourgh- Kehl Zirvesi bunun özellikle tartışıldığı zirvelerden biri olmuştur. Hem üyelerin beklentileri hem örgütün tanımları ile üyeler için en önemli dayanak olan 5. maddenin yani güvenlik alanının, tanksız, topsuz, gürültüsüz, kaynağı belirsiz saldırı karşısında nasıl şekilleneceği açıklanmaya çalışılmıştır.

İttifak tarafından atılan ilk adım olarak kabul edilen Siber Savunma Yönetimi'nin kabul edilmesi, ikinci adım olarak da 2010 yılında kabul edilen "Stratejik Kavram" görülebilir. Söz konusu Kavram "sürekliliği artan, daha organize hale gelen ve devlet organizasyonlarına, ekonomiye, özel sektöre kadar geniş bir yelpazede zararı hissedilen siber saldırıların Avrupa-Atlantik güvenliğini, istikrarını tehdit eden bir seviyeye ulaştığını" dile getirmektedir. Bu çalışmaları 2011 yılında güncellenen Siber Savunma Yönetimi ve Siber Savunma Eylem Planı izlemiştir. Aynı yıl Ağustos ayında ise, Talin, NATO Kolektif Siber Savunma Mükemmeliyet Merkezi siber savunmanın ana karargâhı olmuştur.

NATO'nun ve uluslararası ortamın değişen tehdit algısı ve bu kapsamda alınan kararlar ve uygulamaların önemi, Soğuk Savaş'ın bölgesel örgütlerinden biri olan NATO'nun 29 üye devlet, 20 Barış için Ortaklık (BİO) devleti, 7 Akdeniz Diyaloğu devleti, 4 İstanbul İşbirliği Girişimi ile beraber 60 devleti kapsayan bir yapı haline gelmiş olması olarak görülebilir.[147] Farklı coğrafyalardaki ülkelerin de çeşitli işbirliği ilişkileri kapsamında NATO ile ilişkilerini geliştirmesi örgütün günümüz şartlarında bölgesellikten evrenselliğe taşınıyor olduğu görüşlerini artırmaktadır. "Örgütleri Düşmanları ayakta tutar. İttifaklar, algılanan tehdide karşı kurulur."[148]

Soğuk Savaş sonrası değişen konjonktür kapsamında uluslararası tehditlerin başında yer alan terörizm ve onunla mücadele özellikle 11 Eylül 2001 ve sonrasında yapılan Zirvelerin ana teması haline gelmiştir. 2002 yılında Prag Zirvesi'nde müttefikler arasında terörizme karşı Ortak Eylem Planı benimsenmiştir. 2004 yılında İstanbul Zirvesi'nde de terörizmin her türlüsüne uluslararası hukuk hükümlerinde karşı gelineceği ifade edilmiştir.[149] Terörizmle mücadelenin önemi üzerinde durulmuş, NATO askeri güçlerinin caydırma, engelleme, savunma faaliyetlerini sürdüreceği belirtilmiştir.

19 Kasım 2010 Lizbon Zirvesinde ittifak yeni stratejisini oluşturmuştur. 1999 yılında kabul edilen stratejik kavramın yerini almıştır. 60. yılında altıncı strateji "Yeni Stratejik Kavram" olarak kabul edilmiştir. "Yeni Stratejik Kavram" dokümanı ile ittifakın geleceğe yönelik amaçları, rolü ve kabiliyetleri ifade edilmiştir. İttifakın gelecekte karşılaşabileceği durumlara göre kendini yenilediği bu belge de sayılan potansiyel

[147] Enver BOZKURT, NATO'nun Geleceği
[148] Kenneth WALTZ, "**Uluslararası Politikanın Değişen Yapısı**", Uluslararası İlişkiler, Cilt 5, Sayı 17 (Bahar 2008), s.19
[149] Enver BOZKURT, NATO'nun Geleceği

tehditlerden biri de hükümetlere, ekonomik sistemlere ve kritik kabul edilebilecek diğer yapılara karşı olabilecek siber saldırılardır.[150]

2010 yılındaki "Stratejik Kavram" ile NATO; siber tehdite karşı önleme, saptama, savunma ve kurtarma konusunda yeteneklerini geliştirme ve buna yönelik çalışmalarını merkezileştirme kararı almış, üyelerinin de farkındalığını artırmayı hedeflemiştir. Müteakiben 2011 yılında da kapsamlı Siber Savunma Planı oluşturmuştur.[151]

NATO temel olarak üç şeyi savunmaktadır. İttifak üyelerinin topraklarını, vatandaşlarını ve üyelerinin çıkarlarını... Bu anlayış temelinde değerlendirildiğinde NATO'nun çok geniş bir savunma alanından sorumlu olduğu anlaşılmaktadır. Bu nedenle de birçok güvenliği tehdit eden riske maruz kalabileceği kabul edilmektedir. Siber tehditler de bunlara dâhildir. Fakat Siber güvenlik noktasında direkt bir silahlı saldırı söz konusu olmadığı için NATO taahhüt ettiği savunmayı gerçekleştirmekte zorluk yaşayacaktır. Böyle bir saldırıya maruz kalan müttefikine saldırı ile başa çıkabilmesi için öncesi ve sonrasında destekleyici rol oynayacağını ifade etmektedir. Bunu da İttifakın 4. maddesi kapsamında gerçekleştirecektir.[152] Bu açıdan değerlendirildiğinde varolan işbirliği ve destek ile müşterek güvenlik sisteminin kendi güvenliklerini yeterince gözettiğini gören devletler, uluslararası ilişkilerde güç kullanmaktan imtina edeceklerdir.[153]

Soğuk Savaş'ın sona ermesi ile daha önce farklı bloklara ait ülkelerin arasındaki sınırlar; ekonomik, iletişim vb. araçlar ile önemini eskiden olduğu kadar koruyamamaktadır. Bu nedenle de küreselleşme ile ortaya çıkan gelişmelerin belli siyasi müdahalelerle denetlenmemesi/yönlendirilmemesi veya düzenlenmemesi halinde, küresel sorunların çözülemeyeceği ileri sürülebilir.[154]

Soğuk Savaş esnasında tehdit ve muhtemel saldırıya karşı 5. Madde uygulaması sorun çıkarmıyorken, günümüzde NATO'nun yeni tehdit ve görev sahaları belirlemesi 5. Madde kapsamının da sorgulanmasına neden olmuştur. Söz konusu

---

[150] Claire TAYLOR, NATO Summit 2010,Aralık 2010, SN/IA/5788
[151] Sally McNAMARA, **"NATO Summit 2010: Time to Turn Words Into Action"** Heritage Foundation, No.2498, 2010, s.7
[152] Karl-Heinz KAMP, **" NATO's Strategy After The Lisbon Summit"**
[153] Berdal ARAL, **Soğuk Savaş Sonrasında "Siyasallaşan" Uluslararası Hukuk ve Başlıca Mağdurları**
[154] Hakkı BÜYÜKBAŞ, Kenan ÖREN, Küreselleşme, **Birleşmiş Milletler ve Uluslararası Sosyal Düzen Anlayışı,**

tehditler, NATO'nun en temel amacı olan üyeleri için savunma şemsiyesinin yeni potansiyel tehditler çerçevesinde kullanım alanı ve şeklini belirsizleştirmiştir.[155] Tehditlerin ve risklerin çeşitlenmesi 5.maddenin ne zaman, hangi durumda devreye gireceğini ve nasıl uygulanacağının sorgulanmasına neden olmuştur. Bu da ad hoc kararların devreye girebileceği görüşlerinin ortaya atılmasına neden olmaktadır. Çünkü yeni tehditlere karşı uygulanacak yaptırımlar konusunda ortaklaşa belirlenmiş ölçütler söz konusu değildir. Örgüt bu boşluğu farkında olarak 5. Maddenin işletilemediği durumlarda Washington anlaşmasının 4. Maddesine dayanarak danışma faaliyetleri kapsamında üyelerine savunma konusunda alabileceği tedbirlerde destek olmaktadır. Bu farklılıklar dönemin özellikleri çerçevesinde varlığını devam ettiren başlangıçta teritoryal savunma örgütü olan NATO'nun adaptasyon sürecindeki tanımlama ve uygulama belirsizliklerinden kaynaklanmaktadır.

Hala belirleyici önemini koruyan ulus-devletler, siyasi belirleyici aktörler olarak, uluslararası antlaşma ve düzenlemelerin meşruiyet araçları olma özelliklerini sürdürmektedir.[156] Bu nedenle de zaman zaman anarşik hale gelebilen dünya düzeninde devletlerarası ilişkilere yönelik belli düzenlemeler gerekli hale gelmektedir.

İttifakın desteği ile Estonya'da 2008 yılında kurulmuş ve akredite olmuş olan Siber Savunma Mükemmeliyet Merkezi'ne (Cyber Defence Centre of Excellence (CCD COE) Almanya, İtalya, Litvanya, Letonya, Slovakya ve İspanya sponsor olan ülkelerin başlıcalarıdır.[157] Mükemmeliyet merkezine ek olarak Örgütün konu kapsamında kurumsallaşmasının göstergelerinden biri olarak kabul edilebilecek Bilgi Güvenliği Teknik Merkezi de oluşturulmuştur.[158]

Siber olaylara müdahale süreçlerinin tanımlanması ve bu süreçlerin ilgili kurum ve kuruluşlarla koordineli biçimde işletilmesi siber güvenlik için öncelikli amaç olmaktadır. NATO tarafından bu gereklilik tatbikatlar ile üye ülkelerin siber saldırılara karşı savunma tekniklerini ve ülkeler/kurumlar arası koordinasyon yeteneklerini geliştirmeye çalışılarak sağlanmaktadır. Mükemmeliyet Merkezi tarafından tesis

---

[155] Ali L. KARAOSMANOĞLU, **"NATO'nun Dönüşümü",** Ed. Mustafa AYDIN, İstanbul Bilgi Üniversitesi Yayınları, 2012,s.31-34

[156] Hakkı BÜYÜKBAŞ, Kenan ÖREN, **Birleşmiş Milletler ve Uluslararası Sosyal Düzen Anlayışı,** http://dergisosyalbil.selcuk.edu.tr/susbed/article/view/672, (Erişim: 18.03.2015)

[157] Lorents, P., Ottis, R., Rikk, R.(2009) "Cyber Society and Cooperative Cyber Defence. In Internationalization, Design and Global Development. **"Cyber Society and Cooperative Cyber Defence"** Lecture Notes in Computer Science, Vol.5623.s.185

[158] Michael HOROWITZ, "Acommon Future? NATO and Protection of the Commons", The Chicago Council on Global Affairs, Transatlantic Paper Series No.3,2010,s.9

edilen tatbikatlara yerel tatbikat merkezleri iştirak etmektedir. Bunlardan NATO Kilitli Kalkan Tatbikatı (NATO Locked Shields) NATO Siber Savunma Mükemmeliyet Merkezi koordinatörlüğünde her yıl bir ülke ev sahipliğinde icra edilmektedir. Böylece değişen tehditlere karşı üyeler arası koordinasyon ve işbirliği yol ve yöntemlerinin güncellenmesi hedeflenmektedir. Tatbikat kapsamında katılımcıların eğitiminde kullanılacak olan teknik içeriğin sağlanması maksadıyla sanal bir ağ şeklinde Estonya'ya ait siber tatbikat ortamı kullanılmaktadır.

Tatbikat Eğitimin Hedefi	Hedef Kitle
Mevcut bilgi ve kaynakların kullanımıyla olay müdahale süreçlerini optimize etmek ve benzer olayların tekrarlanmasını engellemek	NATO Bilgisayar Olayları Müdahale Yeteneği Teknik Merkezi (NCIRCTC), NATO Muhabere ve Bilgi Sistemler Grubu Siber Savunma Birimi (NCISGCD) NATO Muhabere ve Bilgi Sistem Ajansı Hukuk Danışmanı, Ulusal Teknik Merkez, Ulusal Hukuk Danışmanı
Bir siber olay süresince NATO varlıklarına etkilerinin, durumsal farkındalığın ve analiz sonuçlarının ortaya konulmasını sağlamak	
NATO'nun sabit ve görev ağlarını ilgilendiren siber olayları desteklemek açısından uluslararası hukukun uygulanmasını sağlamak	
Siber olaylara tepki süresinde ulusal ve/veya uluslararası hukukun uygulanmasını denemek	
Ülkelerin siber savunma birimlerinin ve NCIRC'ın NATO ağları, NATO üye ülke ağları veya NATO ile işbirliği yapan ülkelerin ağlarında teknik seviyede siber savunma işlemlerini planlama	

Tablo 4.3: Siber Savunma Tatbikatları Kapsamı

NATO sürekli kendini geliştirmeye devam ederken 09 Ocak 2017 tarihinde yayımlanan Çok Büyük Birleşik Harekât Kavrami (Major Joint Operation Plus-MJOT); günümüzde veya öngörülebilir gelecekte (10-15 yıl) en üst seviyede icra edilebilecek bir konvansiyonel harekâtın NATO düşünce yapısı ve NATO savunma Planlama yönetimine (NDPP) göre nasıl olabileceğini öngören bir doküman olmuştur. Kavram dokümanında MJOT'un detaylı tanımı ile birlikte, konuya ilişkin terminolojik tanımlar da yer almaktadır. İlk bölüme tüm alanlarda (kara, hava, deniz, siber) icra edilecek Kapsamlı Harekât (Comprehensive All-Domain Operations-CADO) şeklinde bir isim verilmiştir. CADO Kavrami ile siber ve uzay alanlarına vurgu yapılmakta, öngörülen hedeflerin gerçekleşebilmesi için ülkelerin ilave eğitim, tatbikat ve kuvvet tahsis etmelerinin gerekeceği belirtilmektedir. Bu yeni anlayış ile NATO için ek sorumluluklar ve kaynak ihtiyaçlarının (personel, bütçe, hukuki ve fiziksel alt yapı) ortaya çıkabileceği ve üye ülke silahlı kuvvetlerinin dönüşümü ihtiyacını da beraberinde getireceği değerlendirilmektedir.

Sınırlı da olsa uluslararası örgütlerin belli bir düzenleme ve devlet davranışlarını yönlendirme işlevi olduğunu ileri sürmek mümkündür. Uluslararası sistemdeki anarşik yapı dolayısıyla merkezi bir düzenlemenin olamaması durumu söz konusu düzenlemelerin oluşması için ulus-devlet hükümetlerinin işbirliği içine girmesi gerekliliğini ortaya çıkarmaktadır.[159]

1965 yılında kabul edilen "Devletlerin İçişlerine Karışmanın Kabul Edilemezliği ve Özgürlüklerinin ve Egemenliklerinin Korunması Hakkında Bildiri" ile sadece "silahlı müdahale" değil bir devletin varlığına veya kişiliğine yönelmiş her türlü tehdit girişimi veya müdahale kınanmıştır.[160] Terörist tehdidinin değişen yapısı ve uluslararası toplum tarafından terörizm olarak algısının değişmesi beraberinde kuvvet kullanma yasaklarının yeniden değerlendirilmesi ihtiyacını da gündeme getirmektedir.[161] Bu kapsamda da örgütün çekici yanını oluşturan 5. Madde üye devletlerarasında farklı algılanmaya ve yeni görev alanı tartışmalarını oluşturmaya başlamıştır. Örneğin, Lizbon Zirvesi bu farklılığın görüldüğü Zirve'dir denilebilir. Söz konusu Zirve'de Avrupa

[159] Hakkı BÜYÜKBAŞ, Kenan ÖREN, Küreselleşme, **Birleşmiş Milletler ve Uluslararası Sosyal Düzen Anlayışı,**
[160] Fatih TOSUN, **Uluslararası Hukuk'ta " Kuvvet Kullanma ve Karışma" Kavramlarının Değişen Anlamı,** s.110
[161] Fatih TOSUN, Uluslararası Hukuk'ta " Kuvvet Kullanma ve Karışma" Kavramlarının Değişen Anlamı, s.113

ülkeleri 5. Madde kapsamında gerçekleştirilecek operasyonların Avrupa coğrafyasını konvansiyonel tehlikelere karşı korumak amaçlı olmasını savunurken, Birleşik Devletler ve İngiltere seferberlik anlayışının genişletilmesi gerektiği şeklinde bir duruş sergilemiş, asimetrik tehditlerin söz konusu olduğunu dile getirmiştir.[162]

Siber Saldırının neticesinde 5. Madde kapsamında harekete geçilip geçilmemesi tartışmalarında seçeneklerden biri kolektif savunma olarak görülmektedir. Her ne kadar Galler Zirvesinde müttefikler tarafından 5. Maddenin devreye sokulabileceği ifade edilse de bu karar hep siyasi bir karar olarak kalmaya devam edecektir. Çünkü kriter olarak ifade edilen "silahlı saldırı etkilerine sahip olma" standart bir tanımlamadan ziyade olaydan olaya değişkenlik gösterecek ve müttefiklerin farklı algıları ile değerlendirilerek alınabilecek bir karar olma özelliği taşımaktadır. Bunun yanında olumlu olarak değerlendirilebilecek husus ise söz konusu tehdit karşısında belirli bir harekât tarzı ve planlamaya sahip olunarak siber saldırıya karşı hazırlıklı bir yapı oluşturulması ve riskleri önleyici çalışmalar yapılması olarak ifade edilebilir. Buna karşı bu şekilde yapılan bir belirleme, çizilen sınırların dışında gerçekleşen bir saldırının savunma kapsamına dâhil edilmemesine neden olacaktır. Ayrıca net bir standardın getirilmesi üye devletleri gereksiz, istenmeyen ve standartları karşıladığı için ispatlanmamış, doğrulanmamış savaşın içine sokabilir.[163]

[162] Sally McNAMARA, **NATO Summit 2010: Time to Turn Words Into Action"**, heritage Foundation, 2010,s.3

[163] Michael HOROWITZ, **"Acommon Future? NATO and Protection of the Commons"**, The Chicago Council on Global Affairs, Transatlantic Paper Series No.3,2010,s.7

SONUÇ

Yeni güvenlik ortamında barış ve savaş dönemleri arasındaki sınırlar ortadan kalkmış, ortaya çıkan kriz durumu, topyekûn harbe dönüşmeyen ancak çatışmayı da içerebilen ara durumlar şeklinde yaşanır hale gelmiştir. Geçişteki belirsizlikler, değişen durumlara hızla uyum sağlama yeteneğinin geliştirilmesini ve her an harbe hazır olacak yapı ve yeteneklerin kazanılması ile etkili bir askeri stratejinin uygulanmasını gerekli kılmaktadır.

Günümüz güvenlik ortamında tehdit yelpazesi genişlemiş, güvenliğe yönelik risk ve tehditler, tek boyutlu devletten devlete ve simetrik yapıdan çok boyutlu ve çok kaynaklı asimetrik ve çok bilinmeyenli hale dönüşmüştür. Bu kapsamda yeni güvenlik ortamı tahmin edilebilir olma özelliğini büyük ölçüde kaybetmiş, öngörülmesi zor ve istikrarsız bir hale gelmiştir. Risk ve tehditler uluslar ötesi ve çok yönlü bir yapıyla ortaya çıkmaya başlamıştır. Bu kapsamda yeni güvenlik ortamının en önemli özelliklerini "değişim, belirsizlik ve karmaşıklık" oluşturmaktadır. Sürdürülebilir güvenlik, belirsiz risk ve tehditlerle mücadele etme ile geleceğin öngörülemeyen risk ve tehditleri için hazır olmayı gerektirmektedir. Bu doğrultuda devletler ve çok uluslu güvenlik kuruluşları da askeri ve sivil yeteneklerin birlikte kullanılmasını öngören kapsamlı yaklaşım arayışına yönelmektedir.

Fiziken korunamayan küresel ortak alanlar (deniz, hava, uzay, siber) yeni güvenlik ortamında risk ve tehdit kaynaklarının kullanıldığı öncelikli alan haline gelmiştir. Özellikle siber güvenlik, milli güvenliğe yönelik en büyük mücadele alanlarından biri haline gelmiş siber uzay yeni bir muharebe sahası olarak ortaya çıkmıştır. Siber saldırılar tüm ülkelerin refahını, güvenliğini ve istikrarını tehdit eder hale gelmiş, toplum üzerinde psikolojik etki ve bazı ülkeler tarafından dış politikada bir ikna ve cezalandırma aracı olarak kullanılmaya başlanmıştır.

Söz konusu değişen güvenlik ortamı, Soğuk Savaş sonrası kendini yenileyen varoluşuna meşru tehditler yaratan NATO'nun hem doğuya hem de güneye yönelik olarak kolektif savunma temel görevinin, savunma ve caydırıcılık yapısının güçlendirilmesinin önemini artırmaktadır. Bu kapsamda NATO'da zamana ayak uydurmak için sürekli dönüşmektedir. Çünkü Soğuk Savaş'ın bitmesi NATO için 2.Dünya Savaşı sonrası oluşan düzenin sona ermesi anlamına gelmektedir. 1945-1989 dönemi dünyanın iki başlı düzende iki farklı bloğa ayrıldığı, devletlerin de bu iki blok çevresinde örgütlendiği dönem olmuştur. Bu iki blok için yaşanan sürecin ana

dinamiğini, ruhunu silahlanma yarışı oluşturmuş, iki taraf da birbirini tehdit olarak algılayıp güvenlik amacıyla caydırıcılık sağlamayı hedeflemiştir. Karşılıklı olarak meydana getirdikleri savunma örgütleri aracılığıyla caydırıcılığa ulaşılmaya çalışıldığı görülmüştür. Bu yapılanma içinde Batı Blokunun askeri örgütlenmesini NATO oluşturmuştur. Soğuk savaş her iki taraf için de silahlanma yarışı, karşı tarafı caydırma ve dehşet dengesi kavramlarının yanında yumuşama, nükleer silahlarda indirim yapma gibi kavramları da içeren bir süreç olmuştur.

NATO için Soğuk Savaş sonrası tehdit, SSCB'nin konvansiyonel ve nükleer kuvvetlerinin tehdidinden farklı olduğu için bugünün konvansiyonel olmayan asimetrik tehditlerine karşı da NATO'nun hazır hale gelmesi gereği doğmuştur. Yapılan düzenleme ve dönüşümler ile bugünün güçleri inisiyatif kullanabilecek nitelikte cepheleri belirgin olmayan bir savaş meydanında manevra kabiliyetine sahip olmak zorundadır. 21.yüzyılda sürecek olan bu yeni yapılanma ile istenen acil ve tehlike içeren durumlarda en kısa sürede ve en etkili biçimde askeri kuvvetlerin o alana yerleştirilmesini sağlayacak bir askeri güç oluşturmaktır. Ancak bu standardı yakalamak üyeler arasındaki farklılıklar nedeniyle çok sağlanamamaktadır.

NATO içinde müttefikler bulundukları coğrafya, tarihi geçmişleri vb. nedenlerle tehdit ve riskleri bu sahip oldukları özellikler gereği farklı algılamaktadır. Dolayısıyla bağlı oldukları Savunma Örgütü'nün en etkin silahı olan 5.madde kapsamında beklentileri de kendi tehdit algıları çerçevesinde şekillenmektedir. Bu nedenle farklı perspektifler Soğuk Savaş dönemine kıyasla kapsamlı bir askeri doktrin ve uygulama alanlarının belirlenmesinin gecikmesinde en büyük etkenlerden biri haline gelmektedir. Mutabakat eksikliği ve tehditlerin farklı algılanışı ortak bir uygulama geliştirilmesini engellemektedir.

NATO içinde Estonya örneği bu kapsamda önemlidir. Estonya'nın bilgi ve iletişim teknolojilerini toplumsal her alanda kullanan bir ülke olması, bir ülkenin bilgi ve iletişim teknolojilerine ne kadar bağlı olursa, siber saldırılara karşı da o kadar da savunmasız olacağını dünyaya göstermiştir. Bu duruma verilebilecek reaksiyon kapsamında devlet ve uluslararası örgüt ikilemini de gündeme taşımıştır.

Şiddet kullanma meşruiyeti hala devlette ve devletlerin oluşturduğu uluslararası örgütlerdedir. Bu durum, kaynağı devlet olmayan tehditlere karşı yaptırımda devletlerin etkili olduğu sonucunu beraberinde getirmektedir. Uluslararası

güvenliği tehdit kapsamında artık devlet dışından kaynaklı tehditler söz konusuyken güvenlik tarafı ulus-devlet açısından değerlendirilmeye devam etmektedir.[164]

Siber savunma kavramı konvansiyonel savaş taktiklerine göre şekillendirilmiş ordular için yeni bir alandır ve farklı yaklaşımları gerektirmektedir. Siber savunma stratejisine geçişin önündeki en büyük yanılgı, NATO merkez karargâhlarının biçimlendirdiği bir stratejinin ittifakın bütün üyeleri tarafından hemen kabul edildiği yanılgısıdır. Üye ülkeler kendi özelliklerine göre farklı biçimlerde dirençler göstermektedir. Dirençlere neden olarak her ülkenin aynı hızla bu teknolojiyi kucaklamadığı örnek olarak verilebilir. Öte yandan, NATO'nun stratejik kararlarının politik olarak kabul edilmesinin, uygulamanın hızla gerçekleşeceği garantisini veremediği de unutulmamalıdır.

NATO'nun merkezindeki gelişimin hızıyla ittifak üyelerindeki değişimin hızı da birbirinden farklıdır. Bu ikili yapının tamamını kapsayacak bir değişim, düşünülenden daha uzun bir zamana yayılabilir. Konuya siber güvenlik açısından bakıldığında, NATO'nun üyeleri arasında dijital bir bölünmüşlük olduğu açıkça görülmektedir. Bir yanda gelişmiş sinyal izleme sistemleri kullanan siber ordulara sahip ABD ve İngiltere gibi ülkeler yer alırken diğer tarafta dijital yarışta çok geride bulunan Romanya, Bulgaristan, Litvanya ve Çek Cumhuriyeti gibi ülkeler bulunmaktadır.[165]

NATO'nun siber savunma konusunda hızla ilerlemesinin önündeki engellerden bir diğeri de tehdidin özelliği olarak ifade edilebilir. Tehdidin stabil olmama özelliği ona karşı alınacak önlemlerin de dinamik olmasını gerektirmektedir. Bu durum, siber tehdidi diğer tehditlerden farklılaştırarak sürekli takip ve izlemeyi gerektirmektedir. Bu türde bir faaliyetin gerektirdiği enerjinin miktarı ve devamlılık gereği maliyetleri de artırmaktadır. Siber tehdidin nispeten görünmez oluşu, kaynağının tespitinin zor hatta çoğu zaman imkânsız olması da tehdidin algılanmasında bir takım yanılgıların doğmasına yol açmaktadır.

Yaşanan siber saldırılardan alınan ders; internetin insanları bilgiye ulaştırma ve dünyanın her noktası ile iletişim içinde olmasını sağlama konusunda güçlendirirken fiziksel olarak nerede bulunursa bulunsun internet ile bağlantı kurduğu andan itibaren

[164] Beril DEDEOĞLU;"Uluslararası Güvenlik ve Strateji",Yeni yüzyıl yayınları,2008,s.59
[165] Jan A.G.M. van Dijk, "One Europe, Digitally Divided", Andrew Chadwick ve Philip N. Howard (Der.), Routledge Handbook of International Politics, Oxon, 2009, s.288–304.

açık hedef haline getirmesidir.[166] Buna örnek olarak 2010'dan itibaren ortaya çıkan Stuxnet, Duqu, Flame, Mehdi ve Gauss virüsleri verilebilir. Örneğin Stuxnet önceden belirlenmiş bilgisayar ve sistemlere zarar verme amaçlıyken, Duqu, Stuxnet için hedef seçmektedir. Flame ve Mehdi ise bilgi sızdırmaya yöneliktir.[167]

Yaşanan siber saldırılarda edinilen tecrübeler göstermektedir ki saldırılar NATO üyelerinin hazırlıksız oldukları alanları hedeflemektedir. Bu yüzden ittifak üyelerinin kendi içlerinde de işbirliği ve koordinasyonu sağlaması savunma açısından ilk adımı oluşturmaktadır Bütün bu yapılanmalara ve gelişmelere rağmen tehdidin varlığını sürdürmesinin nedeni ise asimetrik oluşudur. Saldırı yapıldıktan sonra saldırganların hızla izlerini silebiliyor olması en önemli engel olmaktadır.

Siber alandaki en tehlikeli oyuncular hala ulus devletler şeklinde ifade edilebilir. Örneğin saldırı yetenekleri giderek artan organize suç ağları gelecekte teröristler gibi devlet dışı oyuncular tarafından kullanılabilirler. Ancak siber etki alanında hayli gelişmiş casusluk ve sabotaj için hala bir ulus devletin yetenek, kararlılık ve maliyet-yarar rasyoneline ihtiyacı vardır. Daha henüz fiziksel zarar ve gerçek kinetik siber terörizm gerçekleşmedi. Ancak siber saldırılarda kullanılan teknoloji artık sadece can sıkıcı bir sorun olmaktan çıkıp bilgi güvenliğine ve hatta kritik ulusal alt yapıya yönelik ciddi bir tehdit haline gelmektedir. Bu tehdidin yer aldığı siber uzay ise devlet-üstü bir yapı olduğundan herhangi bir devletin kontrolünden bahsedilememektedir.

Hiç şüphe yok ki bazı uluslar daha şimdiden askeri amaçla kullanılabilecek siber yeteneklere büyük yatırımlar yapmaktalar. İlk bakışta dijital silah yarışı açık ve kaçınılmaz bir mantığa dayanıyor gibi görünüyor zira siber savaşın çeşitli avantajları var, bu savaş asimetrik, çok cazip gelecek kadar ucuz ve ayrıca en başta avantaj saldıran tarafta. Bunlara ek olarak siber savaşa karşı etkili bir caydırıcı da hala bulunmamakta çünkü saldırganı belirlemek son derece zor ve uluslararası hukuka bağlı kalmak neredeyse imkânsız. Bu şartlar altında her hangi bir askeri misilleme hem yasal hem de siyasi açıdan son derece sorunlu gözükmektedir.

Günümüzün yapılanmasıyla hem NATO hem de üye ülkeler seviyesinde siber saldırılara ve suçlularına hızla cevap vermek mümkün gözükmemektedir. Bu nedenle

---

[166] Lorents, P., Ottis, R., Rikk, R.(2009) "Cyber Society and Cooperative Cyber Defence. In Internationalization, Design and Global Development. Lecture Notes in Computer Science, Vol.5623.s.184

[167] Börteçin EGE,**" Siber Savaşlar Bilişimin Karanlık Yüzü"**,s. 19

konuyla ilgili 5. Madde kapsamında Örgüt tarafından nasıl bir reaksiyon verilebileceği hala netliğe kavuşmuş değildir. Tehditin doğası gereği saldırının kaynağının belirsizliği ve aktör tanımlarının dışında yer alması NATO'nun güvenlik anlayışında siber boyut kapsamında 5. Maddenin devreye sokulması olasılığını çok düşürmekte hatta imkânsızlaştırmaktadır. Bu nedenle İttifak eğitim, tatbikat ve siber alan konusunda yetişmiş personel eksikliğini gidermeye çalışmaktadır.

Sonuç olarak; NATO tarafından görülen bu tehdit unsuru/yeni savaş alanı kapsamında yapılan ve yapılmaya çalışılanlara rağmen hala eksiklikler içermektedir. İttifakın üyelerine kavramlerinde dile getirdiği taahhütleri yerine getirebilmesi ve herhangi bir saldırı esnasında kolektif savunma yapılabilmesi için;

- Öncelikli olarak silahlı saldırı gibi siber saldırı tanımını da netleştirmesi,
- Karşılığında nasıl "orantılı" bir karşılık verileceğini açık şekilde dokümanlarında ortaya koyması,
- Siber savaş doktrinleri oluşturması, geliştirilmesi, söz konusu savunma ve karşılık kapsamındaki değerlendirmelerinde ittifakın sivil sektöre olan bağları düzenlemelerde dikkate alması,
- İttifak üyeleri arasındaki koordinasyonun artırılması faaliyetlerine devam edilmesi,
- Ortak operasyon yapabilme kapasitesinin ilerletilmesi gerekmektedir.

Hala üyeler arasında siber yetenekler açısından aynı düşünülerek yatırım yapılmadığına yönelik çekinceler vardır. Bu nedenle yatırım yapanlar tarafından sahip olduğu yetenekleri açma konusunda çekinceler mevcuttur. Var olan bu durum da bilgi, teknoloji paylaşımını engellemektedir. Kritik teknoloji ve bilgi paylaşımı önündeki bu engeller, ittifakın siber saldırıları önleme kapasitesini düşürmektedir. 5.maddenin devreye girmesi ihtimalini düşürmektedir.

KAYNAKÇA

ADA, Mehmet, Hüseyin ÇAKIR — **Kuzey Atlantik Antlaşma Örgütü'nün (NATO) Siber Güvenlik Stratejisinin İncelenmesi**, Düzce Üniversitesi Bilim ve Teknoloji Dergisi, 2017,

AĞAOĞULLARI, Mehmet Ali, Filiz ZABCI, Reyda ERGÜN — **Kral Devletten Ulus Devlete**, 2. Baskı, Ankara, İmge Kitabevi, 2009

AĞAOĞULLARI, Mehmet Ali, Levent KÖKER — **Kral-Devlet ya da Ölümlü Tanrı**, 4. Baskı, Ankara, İmge Kitabevi, 2009

AKAD, Mehmet Tanju — **Savaş Tarihinin Dönüm Noktaları**, İstanbul, Kastaş Yayınevi,2005

AKKUŞ, Bülent — **Özgürlük ve Güven(sizlik) İkileminde Siber Uzay-Yeni Dünya İçin Toplum Sözleşmesi Denemesi,** Milenyum Yayınları, 2016

ARAL, Berdal — **Soğuk Savaş Sonrasında "Siyasallaşan" Uluslararası Hukuk ve Başlıca Mağdurları**, (Çevrimiçi) http://dergiler.ankara.edu.tr/dergiler/42/479/5528.pdf, 11.08.2012

ARMAOĞLU, Fahir — **20. Yüzyıl Siyasi Tarihi**, İstanbul: Alkım Yayınları,2005

AYTAÇ, Gizem BİLGİN — **"ÜÇÜNCÜ DÜNYA GÜVENLİĞİ VE İNSANİ MÜDAHALE İnsan Güvenliğinden Irak Müdahalesine Eleştirel Güvenlik Yaklaşımları**" Dezanj Yayınları, İstanbul, 2014

BAUMAN, Zygmunt — **Küreselleşme Toplumsal Sonuçları,** (Çev. Abdullah YILMAZ), Ayrıntı Yayınları, İstanbul,1999

BAYRAM, Duygu Çağla — **"İnsan Güvenliği ve Terörizm" Yüksek Lisan Tezi**, Karadeniz Teknik Üniversitesi Sosyal Bilimler

Enstitüsü Anabilim Dalı Yüksek Lisans Programı, Trabzon

BIÇAKCI, Salih **Yeni Savaş ve Siber Güvenlik Arasında NATO'nun Yeniden Doğuşu, Uluslararası İlişkiler**, Cilt 9, Sayı 34 (Yaz 2012)

BIRDSOLL, Andrea **"The International Politics of Judicial Intervention: Crating a More Just Order"** London:Routledge,2009

BOZKURT, Bozkurt **Uluslararası Hukukta Kuvvet Kullanma**, Asil Yayınları, Ankara, 2007

BOZKURT, Bozkurt **NATO'nun Geleceği**, (Çevrimiçi) http://www.usakgundem.com/yazarlar.php?id=614&type=22, 18, 17.05.2012

BLAKE, D., IMBURGIA, J.S. **Bloodless Weapons? The Need To Conduct Legal Reviews Of Certain Capabilities And The Implications Of Defining Them As "Weapons", The Air Force Law Review Articles**, Vol.66,2010

BOYRAZ, Hacı Mehmet **"İnfografya: NATO'nun Siber Güvenlik Politikasında Kırılma Noktaları"** http://biltekhaber.net/infografya-natonun-siber-politikasında-kırılma-noktaları/ (Erişim: 02.12.2015)

BRAUCH, Hans Günter **Güvenliğin Yeniden Kavramsallaştırılması: Barış Güvenlik, Kalkınma ve Çevre Kavramsal Dörtlüsü"** (Çev.Zeynep ARKAN), Uluslararası İlişkiler, Cilt 5, Sayı 18, 2008

BUZAN, Barry **"From International to World Society?: English School Theory and the Social Structure of Globalization"** Cambridge University Press, Cambridge,2004

BÜYÜKAKINCI, Erhan **Küreselleşme Üzerine Kuramsal Tartışmalar: Merkezi Devlet ve Yeni Aktörler**,(Der.:Cem KARADELİ),Küreselleşme ve Alternatif Küreselleşme, Ankara, Phoenix Yayınevi, 2005

BÜYÜKBAŞ, Hakkı, Kenan ÖREN	**Birleşmiş Milletler ve Uluslararası Sosyal Düzen Anlayışı,** http://dergisosyalbil.selcuk.edu.tr/susbed/article/view/672, (Erişim: 18.03.2015)
CASTELLS, Manuel	**The Rise of the Network Society**, West Sussex, Wiley- Blackwell, 2010
CEYLAN, Musa	**Yeni NATO Soğuk Savaş'tan Sıcak Savaşa**, Ülke Kitapları, Kasım 1999
CLARKE, Richard, Robet K. KNAKE	**Siber Savaş Ulusal Güvenliğe Yönelik Yeni Tehdit**, Çev. Murat ERDURAN, İstanbul Kültür Üniversitesi, İstanbul,2011
CZOSSECK, Christian Günter, Karlis PODINS	**"An Evaluation of State- Level Strategies Against Botnets in the Context of Cyber Conflicts",A Vulnerability-Based Model Of Cyber Weapons And Its Implications For Cyber Conflict Estonian Business School,Doctoral Thesis in Management**, No.14, Talinn 2012
ÇELİK, Şener	**Stuxnet Saldırısı ve ABD'nin Siber Savaş Stratejisi: Uluslararası Hukukta Kuvvet Kullanmaktan Kaçınma İlkesi Çerçevesinde Bir Değerlendirme**, Dokuz Eylül Üniversitesi Hukuk Fakültesi Dergisi, Cilt:15, Sayı:1
ÇİFTÇİ, Hasan	**Her Yönüyle Siber Savaş,** TÜBİTAK Popüler Bilim Kitapları, 2013
DEDEMAN, Fatih	**Geleceğin Güvenlik Ortamının Şekillenmesinde Hibrit Savaş Modelinin Değerlendirilmesi,** Güvenlik Bilimleri Dergisi 5, 2016
DEDEOĞLU, Beril	**Uluslararası Güvenlik ve Strateji**, İstanbul, Derin Yayınları, 2003

DEDEOĞLU, Beril — **"Savaş", Uluslararası İlişkiler Giriş Kavram ve Teoriler**,(ed. Haydar ÇAKMAK), Ankara, Platin Basın Yayın Dağıtım, 2006

DENNING, Peter J. Dorothy E. DENNING — **"The Profession of IT Discussing Cyber Attack"**, Viewpoints,September 2010 Vol.53 No.9 http://calhoun.nps.edu/bitstream/handle/10945/35515/cacmSep10.pdf?sequence=1

DERIAN, James Der — **Virtuous War/Virtual Theory, International Affairs**, Cilt 76, No.4, Ekim 2000

EGE, Börteçin — **"Siber Savaşlar Bilişimin Karanlık Yüzü"**, (Çevrimiçi) http://bortecin.com/2012_11_Bilisimin_Karanl%C4%B1k_Yuzu_Siber_Savaslar.pdf, 01.09.2013

FOUCAULT, Michel — **Hapishanenin Doğuşu**, (Çev. Mehmet Ali KILIÇBAY), İmge Kitabevi, 2006

GEERS, Kenneth — **Strategic Cyber Security: Evaluating Nation-State Cyber Attack Mitigation Strategies with DEMATEL**,Tallinn University Of Technology Faculty of Information Technology Department of Informatics PhD Thesis, 2010

GEMALMAZ, Haydar Burak — **Sanal Dünyalarda Özgürlük ve İktidar**, İstanbul, Beta Yayıncılık, 2011

GERVAİS, Michael — **Cyber Attacks and the Laws of War**, Berkeley Journal of International Law, Vol.30, Issue 2 (2012)

GIBSON, William — **Neuromancer**, (Çev.Melike ALTINTAŞ), İstanbul, Gündüz Yayınları, 1984

GÜVEN, Sevgi KESİM — **Gözetim Toplumu ve Toplumsal Meşruiyet**, Mimar Sinan Güzel Sanatlar Üniversitesi Sosyal Bilimler Enstitüsü Sosyoloji Anabilim Dalı Genel Sosyoloji ve Metodoloji Programı Doktora Tezi, 2007

HASGÜLER, Mehmet, Mehmet B. ULUDAĞ — **NATO, Devletlerarası ve Hükümetler-dışı Uluslararası Örgütler**, Nobey Yayın, Ankara, 2005

HERZOG, Stephen — **Revisiting the Estonian Cyber Attacks: Digital Threats and Multinational Responses**, Journel of Strategic Security, Volume 4, Number 2 Summer 2011: Strategic Security in the Cyber Age

HOBBES, Thomas — **Yurttaşlık Felsefesinin Temelleri**, (Çev.Deniz ZARAKOLU), İstanbul, Belge Yayınları, 2007

HOROWITZ, Michael — **"Acommon Future? NATO and Protection of the Commons"**, The Chicago Council on Global Affairs, Transatlantic Paper Series No.3,2010

HİSAROĞLU, Fulya GÖKCAN — **(Ed. Mustafa AYDIN), Güvenlik Çalışmaları Serisi 1-10**,Kitap İncelemesi İstanbul Bilgi Üniversitesi Yayınları, İstanbul, 2012

HUGHES, Rex B. — **NATO Cyber Defence, Nisan 2009**, (Çevrimiçi) https://www.atlcom.nl/site/english/nieuws/wp-content/Hughes.pdf , 12.07.2014

JACOBSEN, Trudy — **"The End of Westphalia? Re-envisioning"** Hampshire,Ashgate Publishing,2008

KAMP, Karl-Heinz — **" NATO's Strategy After The Lisbon Summit"** (Çevrimiçi) https://www.atlcom.nl/ap_archive/pdf/AP%202010%20nr.%208/Kamp.pdf, 23.07.2012

KALDOR, Mary — **New and Old Wars: Organized Violence in a Global Era**, 3rd ed. 2012,Cambridge: Polity Press,

KALDOR, Mary — **In Defence of New Wars, Stability**, 2013, 2(1):4, (Çevrimiçi) http://dx.doi.org/10.5334/sta.at 17.11.2016

KARADELİ, Cem — **Küreselleşme ve Alternatif Küreselleşme**, Ankara, Phoenix Yayınevi, 2005

KARAOSMANLIOĞLU, L. Ali **"NATO'nun Dönüşümü"**, Ed. Mustafa AYDIN, İstanbul Bilgi Üniversitesi Yayınları, 2012

KEÇECİ, Orçun **Siber Suçlar ve Siber Terörizm**, s.12, (Çevrimiçi) http://www.academia.edu/2333087/Siber_Su%C3%A7lar_ve_Ter%C3%B6rizm 25 Ocak 2016

KESKİN, Funda **Uluslararası Hukukta Kuvvet Kullanma: Savaş, Karışma ve Birleşmiş Milletler**, Ankara, Mülkiyeliler Birliği Vakfı Yayınları, 1998

KESKİN, Funda **"BM ve Kuvvet Kullanma"**, Avrasya Dosyası, BM Özel, Cilt: 8,Sayı: 1, İlkbahar–2002

KORYBKO, Andrew **Hybrid Wars The Indirect Adaptive Approach to Regime Change**, Moscow Peoples' University of Russia, 2015

KÖKNAR, Ali Murat **Sanal Ortamda Terörizm, TC Dışişleri Bakanlığı Bilişim ve İnternet Teknolojilerinin Ceza Hukuku Açısından Doğurduğu Yeni Sorunlar Semineri Bildirisi**, Bursa 24 Mart 2011

LAQUEUR, Walter **"Post Modern Terorism"**, Foreign Affairs, C.75, No:5, Eylül-Ekim, 1996

LORENTS, P., OTTIS, R., RIKK, R. **"Cyber Society and Cooperative Cyber Defence. In Internationalization, Design and Global Development. "Cyber Society and Cooperative Cyber Defence" Lecture Notes in Computer Science**, Vol.5623.2009

LYOTARD, Jean-François **Post Modern Durum-Postmodernizm**, (Çev. Ahmet ÇİĞDEM), Ara Yayıncılık, İstanbul,1990

MATHIESEN, Thomas **The Viewer Society: Michel Foucault's "Panopticon' revisited**, Theoretical Criminology, 1997, 1: 215 London: Sage,

McNAMARA, Sally **"NATO Summit 2010: Time to Turn Words Into Action" Heritage Foundation**, No.2498, 2010

MİŞ, N. **”Güvenlikleştirme Teorisi ve Siyasal Alanın Güvenlikleştirilmesi” Akademik İncelemeler Dergisi**, 6 (2), 2011

MUMCU, Özgür **Jus ad Bellum ve Jus in Bello Açısından Siber Saldırı Kavramı, Geleceğin Savaşları ve Silahları**, Uğur Mumcu Araştırma Gazetecilik Vakfı Yayınları, Ankara, 2014

NATO **The Prague Summit and NATO’s Tranformation,** North Atlantic Treaty Organisation, s.1-50

NATO **Bucharest Summit Declaration**, http://www.nato.int/cps/en/natolive/official_texts_8443.htm (20 Nisan 2012

NATO **“NATO Rapid Reaction Team to fight cyber attack”,** http://www.nato.int/cps/en/SID-163341AC-07A0EF3D/natolive/news_85161.htm, (Erişim: 10 Mayıs 2013)

NATO **“Strasbourg/Kehl Summit Declaration**, 04 Nisan 2009”, http://www.nato.int/cps/en/natolive/ news_52837.htm?mode=pressrelease (Erişim Tarihi 19 Aralık 2011)

NATO **Lisbon Summit Declaration,** http://www.nato.int/nato_static/assets/pdf_2010_11/2010_11_11DE1DB9B73CF9BBFB52B2C94722EAC_PR_CP_2010_0155_ENG-Summit_LISBON.pdf (12 Ocak 2014)

NATO **The Allience Strategic Consept for Defence and Security of the Member of the North Atlantic Treaty Organisation by the Heads of State and Government in Lisbon: Active Engagement, Modern Defence,** http://www.nato.int/lisbon2010/strategic_concept_eng.pdf (30 Haziran 2014)

NATO COE DAT	**Critical Infrastructure Protection Against Terrorist Attacks,** Course Report, NATO COE DAT, Ankara,2014
NATO CIS Cervices Agency	**NATO Cyber Defence Management**, 2011
NETANEL, NEİL WEİNSTOCK,	**Cyberspace Self-Governance: A Skeptical View From Liberal Democratic Theory**, 88 Cal. L. Rev. 395 (2000). http://scholarship.law.berkeley.edu/californialawreview/vol88/iss2/8 (08 Ocak 2017)
OTTIS, Rain	**"Theoretical Model for Creating a Nation-State Level Offensive Cyber Capability",** In Proceedings of the 8th European Conference on Information Warfare and Security, ECIW 2009, 6-7 July, Lisbon, Portugal. Reading: Academic Publishing Limited
OTTIS, Rain	**A Systematic Approach to Offensive Volunteer Cyber Militia"** Faculty of Information Technology PhD Thesis, 2011, TUT Press
ÖZCAN, Mehmet	**"Siber Terörizm ve Ulusal Güvenliğe Tehdit Oluşturma Boyutu"** (Çevrimiçi) http://www2.cbu.edu.tr/kalac/dokumanlar/siber.pdf 13.11.2015
ÖZCAN, Mehmet	**Siber Terörizm ve Ulusal Güvenlik: İnternet ve Hukuk",** İstanbul Bilgi Üniversitesi Yay.2002
ÖZKAN, Tezcan	**"Siber Terörizm Bağlamında Türkiye'ye Yönelik Faaliyet Yürüten Terör Örgütlerinin İnternet Sitelerine Yönelik Bir İçerik Analizi",** Yüksek Lisans Tezi, Anadolu Üniversitesi Sosyal Bilimler Enstitüsü, Ağustos 2006
PASTORSATORRAS, Romualdo, Alessandro VESPIGNANI	**Evolution and Structure of the Internet: A Statistical Physics Approach,**Cambridge University Press, Cambridge, 2004
PAZARCI, Hüseyin	**Uluslararası Hukuk,** Ankara, Turhan Kitabevi, 2007

PEKSARI, Derya Gonca — **"NATO'nun Değişen Kavramı",** Edt: Enver BOZKURT,Asil Yay,2007

PERNIK, Piret — **Improving Cyber Security NATO and EU, International Centre for Defence Studies**, Tallinn, 2014

PULAT, Mustafa — **" Avrupa Güvenlik ve Savunma Politikası",** Gazi Üniversitesi Sosyal Bilimler Enstitüsü Uluslararası İlişkiler Anabilim Dalı, Ankara: Yayınlanmış Yüksek Lisans Tezi,2002

ROSENOU, James N. — **"The Complexities and Contradictions of Globalization"** Current History, Vol.96 No.613,1997

ROUSSEAU, Jean-Jacques — **Toplum Sözleşmesi,** (Çev.Vedat GÜNYOL), Türkiye İş Bankası Kültür Yayınları, İstanbul, 2010

SCHMITT, Michael N. — **Tallinn Manual on the International Law Applicable to Cyber Warfare**, International Group of Experts Invited by the NATO Cooperative Cyber Defence of Excellence, 2012

SHINDER, Debra L. — **Scene of the Cybercrime:Computer Forensics Handbook**, USA, Syngress Publication, 2002

SINGER, J.D — **The Level of Analysis Problem in International Relatons**, (der. K. Knorr, S. Verba), The International System:Therotical Essays, Princeton University Press, 1961

SINGER, P.W., Allan FRIEDMAN — **Siber Güvenlik ve Siber Savaş**, Çev: Ali ATAV, Buzdağı Yayınevi,2015

SOLOMON, Michaek G., Mike CHAPPLE — **Information Security Illuminated**, Jones and Barlett Publishers, USA, 2005

SUR, Melda — **Uluslararası Hukukun Esasları**, Beta Yayınları, İstanbul, 2006

TANNENBAUM, Donald G., David G. SHULZ — **Siyasi Düşünce Tarihi ve Fikirleri,** (Çev. Fatih DEMİRCİ), Ankara, Adres Yayınları, 2011

TANRISEVER, Oktay F.	**Devlet, (der. Atila ERALP), Devlet ve Ötesi Uluslararası İlişkilerde Temel Kavramlar**, İletişim Yayınları, İstanbul, 2006
TAYLOR, Claire	**NATO Summit 2010**,Aralık 2010, SN/IA/5788
TIKK, Ennenen TIKK, Kadir KASKA, Liis VIHUL	**International Cyber Incident- Legal Considerations**, Cooperative Cyber Defence Centre of Excellence, Talinn, 2010
TOPAL, Ahmet Hamdi	**Uluslararası Terörizm ve Terörist Eylemlere Karsı Kuvvet Kullanımı**, Beta Yayınları, İstanbul, 2005
TOSUN, Fatih	**Uluslararası Hukuk'ta " Kuvvet Kullanma ve Karışma" Kavramlarının Değişen Anlamı**, (Çevrimiçi) http://www.msu.edu.tr/GuvenlikStratejileriDergisi/dokuman/GSD_9/GSD_9_Art_3_062009.pdf 12.08.2013
United States General Accounting Office	**Critical Infrastructure Protection, Challenges and Efforts to Secure Control Systems**, March 2004
UŞAKLI, Ali Bülent	**Savaşın Dönüşümü ve Teknoloji,** Lalezar Kitabevi, Ankara, 2008
Ünver, M., C. CANBAY, A.G.MİRZAOĞLU	**Siber Güvenliğin Sağlanması: Türkiye'deki Mevcut Durum ve Alınması Gereken Tedbirler",** Bilgi Teknolojileri ve Koordinasyon Dairesi Başkanlığı, 2009
VAN DIJK, A.G.M.JAN	**"One Europe, Digitally Divided",** Andrew Chadwick ve Philip N. Howard (Der.), Routledge Handbook of International Politics, Oxon, 2009
VEYSAL, Çetin	**Savaşın Felsefesi**, İstanbul, Etik Yayınları,2006
WALTZ, Kenneth	**"Uluslararası Politikanın Değişen Yapısı",** Uluslararası İlişkiler, Cilt 5, Sayı 17 (Bahar 2008),
WILLIAMS, Howard, Moorhead WRIGHT, Tony EVANS	**Hobbes, Uluslararası İlişkiler ve Siyaset Teorisi Üzerine Bir Derleme**, Siyasal Yayınevi, Ankara, 2007
WHITTAKER, Jason	**The Cyberspace Handbook,**Oxon, Routledge, 2004

YALVAÇ, Faruk — **Devlet, (der. Atila ERALP), Devlet ve Ötesi Uluslararası İlişkilerde Temel Kavramlar**, İletişim Yayınları, İstanbul, 2006

YURDUSEV, Nuri — **'Uluslararası İlişkiler' Öncesi, Devlet(2003,Sistem ve Kimlik**, İletişim Yayınları, İstanbul,2006

Cooperative Cyber Defence Centre of Excellence, Cyber Attacks Against Georgia: Legal Lessons Identified",2008

Summaries of EU Legislation," European Programme for Critical Infrastructure Potection", (Çevrimiçi) http://europaeu/legislation_summaries/justice_freedom_security/fight_against_terrorism/133260_en.htm, 17 Temmuz 2013

"Convention on Cyberspace", Council of European Treaties Series, No.185, http://conventins,coe,int/Treaty/Commun/QueVulezVous.asp?NT=185&CL=ENG,04.06. 2014

BM Sözleşmesi madde 2 (4), Charter of the United Nations, " Chapter I: PURPOSES AND PRINCIPLES", http://www.un.org/en/documents/charter/chapter1.shtml, (Erişim: 27 Haziran 2012)

Siber Savaşa Uygulanacak Hukuk Hakkında Tallinn El Kitabı, http://www.mgk.gov.tr/index.php/siber-savasa-uygulanacak-hukuk-hakk-nda-tallinn-el-kitab-uluslararas-siber-guevenlik-hukuku#, (Erişim: 15 Mart 2015

The Alliance's Strategic Concept, 24 Nisan 1999", 23. madde, http://www.nato.int/cps/en/natolive/official_texts_27433.htm (Erişim Tarihi 12 Aralık 2011).

“An Alliance for the 21st Century’ Washington Summit Communiqué issued by the Heads of State and Government participating in the meeting of the North Atlantic Council in Washington, D.C. on 24th April 1999” http://www.nato.int/cps/en/natolive/official_texts_27440.htm (Erişim Tarihi 13 Aralık 2011

The Prague Summit and NATO’s Transformation, 2003 http://www.nato.int/docu/rdr-gde-prg/ rdr-gde-prg-eng.pdf (Erişim Tarihi 14 Aralık 2011)

173 DSCFC 09 E bis - NATO and Cyber Defence, 2009, http://www.nato-pa.int/default. Asp?SHORTCUT=1782 (Erişim Tarihi 13 Aralık 2011).